EM&M

EMotional intelligence & cybersecurity environMents in youth education

PODRĘCZNIK

DLA OSÓB PRACUJĄCYCH Z MŁODZIEŻĄ I INTERESARIUSZY

Numer referencyjny projektu: 2024-2-RO01-KA220-YOU-000293190

Dofinansowane przez Unię Europejską

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Narodowej Agencji Programów Wspólnotowych w Dziedzinie Edukacji i Kształcenia Zawodowego (ANPCDEFP). Unia Europejska ani ANPCDEFP nie ponoszą za nie odpowiedzialności.

Spis treści

Dofinansowane przez Unię Europejską

Dofinansowane przez Unię Europejską

Dofinansowane przez Unię Europejską

Wprowadzenie

Podręcznik EM&M – Emotional Intelligence and Cybersecurity Environments in Youth Education został opracowany w ramach projektu Erasmus+ EM&M (Emotional Intelligence and Cybersecurity Environments in Youth Education). Projekt stanowi odpowiedź na rosnące wyzwania, przed którymi stają młodzi ludzie i pracujący z nimi specjaliści w coraz bardziej cyfrowym świecie. W dzisiejszym świecie postęp technologiczny niesie ze sobą zarówno ogromne możliwości, jak i zagrożenia związane z bezpieczeństwem w Internecie, dobrym samopoczuciem emocjonalnym i odpowiedzialnym zachowaniem w sieci.

Technologia całkowicie zmieniła sposób, w jaki komunikujemy się, uczymy się i wchodzimy w interakcje społeczne. Narzędzia cyfrowe są świetne dla innowacji i łączności, ale narażają również młodych ludzi na zagrożenia internetowe, dezinformację i stres emocjonalny. Badania i praktyczne doświadczenia pokazują, że istnieje pilna potrzeba zwrócenia większej uwagi na inteligencję emocjonalną młodych ludzi i cyberbezpieczeństwo. Umożliwi im to podejmowanie świadomych, przemyślanych i zdecydowanych decyzji w mediach społecznościowych.

Projekt EM&M odpowiada na tę potrzebę poprzez kompleksowe podejście edukacyjne, które łączy rozwój umiejętności emocjonalnych z edukacją w zakresie cyberbezpieczeństwa. Projekt ma na celu pokazanie, jak technologie cyfrowe wpływają na zachowania emocjonalne i społeczne. Jednocześnie ma on na celu zapewnienie pracownikom młodzieżowym i edukatorom praktycznych narzędzi pozwalających uniknąć zagrożeń internetowych, takich jak phishing, nadużywanie danych, nękanie w sieci i uzależnienie od technologii cyfrowych.

Niniejszy podręcznik został opracowany, jako praktyczne źródło informacji dla pracowników młodzieżowych, takich jak pracownicy młodzieżowi, edukatorzy, trenerzy i inne zainteresowane strony. Zawiera jasne instrukcje, sposoby działania, ćwiczenia i materiały edukacyjne, które wspierają edukację nieformalną i poza formalną. Treść podręcznika pokazuje, że projekt poświęcony jest integracji, umiejętnościom cyfrowym i nowym pomysłom w pracy z młodzieżą. Jest to zgodne z celami programu Erasmus+, którymi są gotowość cyfrowa, integracja wszystkich osób i zapewnienie młodzieży dobrej edukacji.

W połączeniu z narzędziami do opowiadania historii EM&M oraz środowiskiem mikronauki niniejszy podręcznik pomaga stworzyć zrównoważony ekosystem edukacyjny, który umożliwia młodym profesjonalistom promowanie bezpiecznego, świadomego emocjonalnie i odpowiedzialnego uczestnictwa w życiu cyfrowym. EM&M pomaga młodym ludziom lepiej zrozumieć przestrzenie

cyfrowe. Odbywa się to poprzez poprawę ich świadomości technicznej i umiejętności emocjonalnych. Pomaga im to poruszać się w przestrzeni cyfrowej z pewnością siebie, empatią i umiejętnościami krytycznego myślenia.

Moduł 1 – Podstawy cyberbezpieczeństwa i inteligencji emocjonalnej w edukacji młodzieży

Przegląd modułu

Moduł ten przygotowuje edukatorów młodzieżowych do przedstawienia podstawowych pojęć związanych z cyberbezpieczeństwem i inteligencją emocjonalną w sposób angażujący, dostosowany do wieku i istotny dla codziennego życia cyfrowego młodych ludzi. Wyjaśnia, w jaki sposób zachowania w cyberprzestrzeni wpływają na samopoczucie i ryzyko, dlaczego stany emocjonalne wpływają na podejmowanie decyzji w Internecie oraz w jaki sposób wychowawcy mogą wspierać proaktywne i odporne reakcje na zagrożenia cyfrowe. Nacisk kładziony jest na jasność pojęć, wspólne słownictwo i gotowość wychowawców do prowadzenia refleksyjnych dyskusji przed przejściem do praktycznych ćwiczeń w kolejnych modułach. Proste ćwiczenia oparte na dyskusji i lekkie materiały informacyjne wspierają nauczanie mieszane i konteksty o niskiej przepustowości.

Dzięki ustanowieniu solidnych podstaw młodzież zyskuje wspólny język do rozmów na temat bezpieczeństwa w Internecie – od phishingu i fałszywych zaproszeń do grona znajomych po cyberprzemoc, internetowych przestępców i przypadkowe pobieranie złośliwego oprogramowania – oraz zrozumienie, w jaki sposób ich uczucia (takie jak ciekawość lub strach przed przegapieniem czegoś) mogą sprawić, że będą bardziej lub mniej narażeni na niebezpieczeństwo. Edukatorzy będą przygotowani do jasnego wyjaśniania podstawowych pojęć, zachęcania do refleksji i tworzenia prostych procedur, które uczniowie będą mogli faktycznie stosować w codziennym życiu.

Treść modułu

Dlaczego podstawy mają znaczenie

Młodzi ludzie żyją w nieustannie aktywnym środowisku cyfrowym, gdzie nawyki internetowe kształtują tożsamość, relacje i możliwości. Podstawowa wiedza na temat cyberbezpieczeństwa i inteligencji emocjonalnej daje młodzieży wspólny język zrozumienia zagrożeń i praktyczną ścieżkę do bezpieczniejszych, spokojniejszych wyborów w Internecie. Bez tych podstaw nastolatek może nie rozpoznać sytuacji ryzykownej – czy to przyjaznego gestu cyberprzestępcy, czy oferty oszusta – lub może zareagować impulsywnie w sposób, który narazi go na niebezpieczeństwo (na przykład udostępniając prywatne zdjęcie pod presją lub klikając podejrzany link ze strachu). Moduł ten wyposaża edukatorów w umiejętności jasnego wyjaśniania podstawowych pojęć, zachęcania do osobistej refleksji i tworzenia prostych procedur, które uczniowie będą mogli faktycznie stosować w codziennym życiu. Wspólne

słownictwo i pojęcia zmniejszają zamieszanie i ułatwiają poszukiwanie pomocy:, gdy wszyscy rozumieją terminy takie jak phishing, prywatność lub samoświadomość, młodzież łatwiej jest poprosić o pomoc lub zastosować odpowiednie strategie w danej sytuacji.

Podstawowe pojęcia z zakresu cyberbezpieczeństwa w języku przyjaznym dla młodzieży

Przedstawienie kluczowych pojęć związanych z cyberbezpieczeństwem używając definicji przyjaznym młodzieżą i przykładów z życia codziennego:

- **Aktywa**– coś, co ma dla ciebie znaczenie w Internecie (np. twoja tożsamość, zdjęcia, dane osobowe, dostęp do kont). Aktywa jest tym, co chcesz chronić.
- **Zagrożenie** – coś, co może spowodować szkody dla twoich aktywów. Przykładowe zagrożenia to wiadomości phishingowe, cyberprzemoc, infekcje złośliwym oprogramowaniem lub osoby wykorzystujące Internet do pozyskiwania danych osobowych.
- **Podatność** – słaby punkt, który może zostać wykorzystany przez zagrożenie. Przykładami podatności są: używanie słabego hasła, nadmierne udostępnianie informacji prywatnych, pochopne udzielanie odpowiedzi lub zbytnia ufność. Tworzą one luki, które mogą zostać wykorzystane przez zagrożenia (takie jak hakerzy lub osoby podszywające się pod inne osoby).
- **Ryzyko**– prawdopodobieństwo, że zagrożenie wykorzysta lukę w zabezpieczeniach, aby wyrządzić szkodę. Ryzyko wzrasta, gdy zagrożenia i luki w zabezpieczeniach są ze sobą powiązane (na przykład zagrożenie phishingiem + luka w zabezpieczeniach wynikająca z ciekawości = wysokie ryzyko kliknięcia). Ryzyko maleje, gdy zmienisz zachowanie lub wzmocnisz ochronę (na przykład włączenie uwierzytelniania dwuskładnikowego lub zatrzymanie się, aby pomyśleć, zmniejsza ryzyko przejęcia konta).
- **Higiena** – drobne codzienne nawyki, które składają się na bezpieczeństwo. Są to rutynowe zachowania ochronne, takie jak instalowanie aktualizacji, stosowanie uwierzytelniania dwuskładnikowego (2FA), sprawdzanie ustawień prywatności lub zatrzymywanie się, aby zweryfikować wiadomości przed podjęciem działania. Tak jak higiena osobista pozwala zachować zdrowie, tak higiena cyfrowa zapewnia bezpieczeństwo w sieci.

Definicje powinny być proste i zrozumiałe. Aby zilustrować każdą koncepcję, należy posługiwać się konkretnymi przykładami zaczerpniętymi ze świata uczniów. Można na przykład omówić przejmowanie kont w aplikacjach

społecznościowych, fałszywe oferty nagród, fałszywe zaproszenia do grona znajomych lub podszywanie się pod inne osoby, cyberprzestępców próbujących nawiązać rozmowę, wirusowe plotki lub fałszywe wiadomości oraz presję, aby udostępniać treści lub hasła. Należy pokazać, w jaki sposób każdy z przykładów wiąże się z zasobami, zagrożeniami, podatnością na zagrożenia i ryzykiem:

Przykład: wiadomość na Instagramie twierdzi, że wygrałeś nowy telefon, jeżeli klikniesz w link. Zagrożone aktywa: dostęp do konta i dane. Zagrożenie: oszustwo phishingowe. Podatność: podekscytowanie i strach przed przegapieniem okazji (FOMO) mogą skłonić Cię do kliknięcia bez sprawdzenia. Ryzyko: wysokie, jeśli nie zachowasz ostrożności. Higiena: bezpieczniejszym nawykiem jest nie klikać losowych linków z nagrodami – zamiast tego sprawdź je na oficjalnej stronie.

Inteligencja emocjonalna i zachowanie w sieci

Inteligencję emocjonalną można nauczyć w postaci czterech praktycznych umiejętności, które mają ogromny wpływ na zachowanie i bezpieczeństwo w Internecie:

- **Świadomość siebie** – zauważanie tego, co czujesz, zanim zaczniesz działać. Na przykład, rozpoznanie „Jestem zły z powodu tej uwagi" lub „Jestem podekscytowany tą wiadomością" to pierwszy krok.
- **Samokontrola**– stosowanie krótkich technik regulujących stres i impulsy. Może to oznaczać wzięcie głębokiego oddechu, policzenie do 10 lub zastosowanie cyklu oddechowego 4-4-6 (wdech 4 sekundy, trzymanie 4, wydech 6), aby uspokoić się, gdy pojawi się wiadomość wywołująca emocje.
- **Świadomość społeczna** – zrozumienie perspektyw innych osób i dynamiki relacji online. Obejmuje to empatię (rozpoznawanie, kiedy przyjaciel może czuć się zdenerwowany lub kiedy wiadomość ma na celu wywołanie paniki) oraz dostrzeganie sygnałów społecznych (np. świadomość, że wiadomość z żądaniem „nie mów nikomu" jest podejrzana).
- **Umiejętności interpersonalne** – jasna i asertywna komunikacja, szukanie pomocy w razie potrzeby oraz ustalanie granic w sieci. Na przykład umiejętność grzecznego powiedzenia „Nie, nie mogę udostępnić tej informacji" lub zwrócenia się do zaufanej osoby dorosłej, jeśli podejrzewasz, że ktoś jest fałszywym przyjacielem lub przestępcą.

Naucz uczniów, że emocje wpływają na wybory dokonywane w Internecie i postrzeganie ryzyka. Podekscytowanie, złość lub strach mogą zaburzać zdolność oceny sytuacji. Przedstaw prosty, powtarzalny cykl EI zapewniający

bezpieczniejsze działanie w sieci: Świadomość → Refleksja → Regulacja → Reakcja. W praktyce oznacza to:

- **Świadomość**: zatrzymaj się i zwróć uwagę na swój stan emocjonalny (np. „Czuję niepokój z powodu tej pilnej wiadomości e-mail").
- **Refleksja**: pomyśl o tym, dlaczego tak się czujesz i jaka jest sytuacja (np. „Ta wiadomość stara się mnie przestraszyć. Jest prawdziwa?").
- **Regulacja**: podejmij działania, aby się uspokoić (np. ćwiczenia oddechowe lub liczenie do 5).
- **Reakcja**: wybierz bezpieczną, rozsądną reakcję (np. nie klikaj linku; sprawdź w oficjalnej aplikacji lub poproś kogoś o radę).

Ucz tego cyklu, jako powtarzalnej rutyny. Uczniowie mogą przypomnieć sobie te kroki pod presją. Podkreśl, że uczucia to normlany sygnał – czucie niepewności czy zainteresowania w sieci nie jest „złe", jest ludzkie. Najważniejsze to zauważyć te uczucia i użyć ich bardziej, jako sygnał do zwolnienia i pomyślenia niż do natychmiastowej reakcji.

Typowe wzorce zagrożeń dla młodzieży i taktyki perswazji

Wiele zagrożeń internetowych skierowanych do młodzieży opiera się bardziej na perswazji emocjonalnej niż na hakowaniu technicznym. Pomóż uczniom rozpoznać typowe schematy, w których emocje są wykorzystywane, jako czynniki wyzwalające:

- **Pilność i strach:** wiadomości typu „Działaj teraz, bo inaczej..." (Np., „Jeśli nie potwierdzisz teraz, Twoje konto zostanie zawieszone za 30 minut!"). Wyzwalaczem jest panika lub strach przed stratą. Oszuści i cyberprzestępcy wykorzystują pilność, aby skłonić Cię do działania bez zastanowienia.
- **Autorytet:** ktoś podaje się za osobę sprawującą władzę (wsparcie techniczne, nauczyciel, znany influencer), aby wywrzeć na Tobie presję (np. „Tu wsparcie techniczne, musisz przesłać swoje hasło, aby rozwiązać problem"). Wywołaną emocją jest często niepokój lub posłuszeństwo wobec autorytetu.
- **Empatia i wzajemność:** apel, który porusza serce (np. „Proszę, pomóż mi, utknąłem i potrzebuję, abyś szybko przesłał mi kod swojego konta!"). Wywołuje to współczucie, poczucie winy lub chęć pomocy przyjacielowi, – co może być wykorzystywane przez oszustów, a nawet cyberprzestępców nawiązujących przyjaźnie.
- **Ciekawość i status społeczny:** zapowiedzi wykorzystujące FOMO lub niepewność (np. „Zobacz, co o Tobie napisali! Wszyscy o tym mówią – kliknij tutaj, aby zobaczyć"). Wyzwalaczem jest ciekawość lub strach przed przegapieniem czegoś ważnego społecznie. Podobnie

sensacyjne fałszywe wiadomości lub plotki mogą wywołać silną ciekawość lub oburzenie, skłaniając do impulsywnego udostępniania.

- **Nagroda (zbyt piękna by była prawdziwa):** „Gratulacje, wygrałeś nagrodę!" lub „Zdobądź darmowych obserwujących, klikając tutaj". Wywołuje to podekscytowanie, chciwość lub strach przed przegapieniem okazji (FOMO). Oszuści często wykorzystują ograniczone czasowo oferty lub ekskluzywne nagrody, aby zamazać osąd.
- **Dowód społeczny lub presja otoczenia:** (związane z FOMO) sugestie, że „wszyscy to robią" lub wyzwanie, które „wszyscy Twoi znajomi już podjęli". Wywołuje to strach przed przegapieniem okazji lub chęć dostosowania się, co może prowadzić do ryzykownych zachowań, takich jak udział w wirusowych wyzwaniach lub klikanie niezweryfikowanych linków.

Dla każdego wyzwalacza omów emocjonalny haczyk i połącz go ze strategią spokojnej reakcji. Na przykład:

- **Wyzwalacz pilności → spokojna reakcja:** rozpoznaj pośpiech, weź głęboki oddech i zweryfikuj informację za pośrednictwem innego kanału. („Zaloguję się przez oficjalną aplikację zamiast klikać w ten link").
- **Wyzwalacz empatii → spokojna reakcja:** zwolnij tempo i zweryfikuj informację. („Chcę pomóc, ale zadzwonię bezpośrednio do mojego przyjaciela, aby sprawdzić, czy to prawda").
- **Wyzwalacz ciekawości → spokojna reakcja:** uznaj pokusę, a następnie zatrzymaj się i sprawdź. („To może być podstęp. Zamiast klikać, zapytam innego przyjaciela, czy słyszał o tym").

Nazywając emocję wywołującą reakcję (np. „Ta wiadomość ma mnie przestraszyć" lub „To naprawdę mnie intryguje") i mając wcześniej zaplanowane działanie, młodzież może zapobiec manipulacji. Podkreśl, że wiele zagrożeń internetowych – od oszustw phishingowych, przez clickbait, po cyberprzemoc – opiera się na wywołaniu reakcji emocjonalnej, a nie na przechytrzeniu Cię pod względem technicznym. Rozpoznanie tych taktyk jest jak dostrzeżenie sznurków marionetki:, kiedy już zobaczysz sztuczkę, łatwiej jest nie dać się wciągnąć.

Włączające ułatwienie i postawa zapewniająca bezpieczeństwo

Podczas nauczania tych podstawowych zasad ważne jest stworzenie integracyjnego środowiska sprzyjającego nauce:

- **Używaj prostego języka:** unikaj żargonu, chyba, że od razu go wyjaśnisz. Na przykład nie zakładaj, że wszyscy wiedzą, co to jest „phishing” – zdefiniuj to proste słowami („fałszywa wiadomość, która nakłania cię do podania informacji”) i być może odnieś to do czegoś, co uczniowie widzieli.
- **Traktuj emocje, jako sygnały, nie problemy:** wyjaśnij, że strach przed ostrzeżeniem lub podekscytowanie nagrodą są naturalne. Nie ma nic złego w reagowaniu; celem jest zauważenie tego i poradzenie sobie z tym. Zmniejsza to piętno i zachęca do szczerej dyskusji. Na przykład powiedz, że nawet dorośli odczuwają „panikę”, gdy otrzymują oficjalnie brzmiącą wiadomość e-mail z groźbą – ważne jest to, jak radzimy sobie z paniką.
- **Anonimowy udział w dyskusjach na tematy wrażliwe:** zapewnij uczniom kanały umożliwiające anonimowe dzielenie się opiniami (np. skrzynka sugestii lub ankieta internetowa) podczas omawiania wrażliwych doświadczeń. Młodzież może być bardziej skłonna przyznać się do tego, że „kiedyś podała swoje hasło fałszywemu znajomemu” lub „opublikowała coś, czego teraz żałuje”, jeśli może to zrobić prywatnie. Anonimowe pytania mogą ujawnić powszechne problemy, takie jak publikowanie prywatnych informacji, których później żałujesz, lub napotykanie agresywnych zachowań, bez narażania żadnego ucznia na kompromitację.
- **Ustal podstawowe zasady:** na początku stwórz bezpieczną przestrzeń. Sugerowane podstawowe zasady: poufność (to, co zostało powiedziane w klasie, pozostaje w klasie), brak zawstydzania lub wyśmiewania doświadczeń innych osób oraz możliwość rezygnacji dla każdego, kto czuje się niekomfortowo. Jest to kluczowe, jeśli dyskusje mogą dotyczyć osobistych przypadków cyberprzemocy, molestowania lub kontaktów z nieznajomymi.
- **Bądź gotowy do zapewnienia bezpieczeństwa:** poznaj procedury eskalacji, jeśli uczeń ujawni poważną krzywdę (np. jest uwodzony przez internetowego przestępcę lub poważnie prześladowany). Zapewnij zasoby lub kontakty umożliwiające uzyskanie profesjonalnej pomocy. Młodzież powinna wiedzieć, że traktujesz takie kwestie poważnie i pomożesz jej uzyskać odpowiednie wsparcie. Częścią podstawowych zasad bezpieczeństwa cybernetycznego w edukacji młodzieży jest zapewnienie im zaufanych dorosłych i zasobów, do których mogą się zwrócić, gdy coś pójdzie nie tak.

Nauczanie rutyn, które się przenoszą

Skoncentruj się na niewielkim zestawie łatwych do zapamiętania rutynowych czynności lub mikro umiejętności, które uczniowie mogą ćwiczyć w klasie i wykorzystywać w prawdziwym życiu. Lepiej jest mieć kilka silnych nawyków niż długą listę wskazówek, o których szybko zapomną. Niektóre podstawowe rutynowe czynności obejmują:

- **"Zatrzymaj się – oddychaj – sprawdź" rutynowa przerwa**:, kiedy w sieci dzieje się coś pilnego lub emocjonującego, po prostu się zatrzymaj (odsuń ręce od klawiatury/telefonu na 3 sekundy), weź głęboki oddech (lub wykonaj cykl 4-4-6), a potem sprawdź, co się dzieje z Tobą i sytuacją. Zadaj sobie pytania:, „Co czuję? O co naprawdę prosi mnie ta wiadomość? Czy stanowi to zagrożenie dla moich aktywów? Jak mogę to bezpiecznie zweryfikować?". Ta 10–20-sekundowa procedura może zapobiec niezliczonym błędom (takim jak kliknięcie złośliwego linku lub wysłanie pochopnej odpowiedzi).
- **4-4-6 oddychanie na zmniejszenie stresu:** naucz prostego wzorca oddychania: wdech przez 4 sekundy, wstrzymanie oddechu przez 4 sekundy, wydech przez 6 sekund (koncentrując się na dłuższym wydechu). Wykonanie tego ćwiczenia kilka razy może fizjologicznie obniżyć tętno i uspokoić układ nerwowy. Pomaga to zwłaszcza wtedy, gdy wiadomość wywołuje strach lub złość, umożliwiając jaśniejsze myślenie przed udzieleniem odpowiedzi.
- **Podwójna kontrola przez znajomych:** zachęcaj do konsultowania się z przyjacielem lub zaufaną osobą przed podjęciem działań w przypadku podejrzanych lub budzących emocje sytuacji. Na przykład:, „Jeśli otrzymasz dziwną wiadomość prywatną lub prośbę, która wydaje się podejrzana, zrób zrzut ekranu i wyślij go znajomemu z pytaniem: „Czy to wygląda podejrzanie?". Często osoba postronna może dostrzec sygnały ostrzegawcze, które umknęły Twojej uwadze. Wzmacnia to również kulturę wzajemnej troski w sieci.
- **Dwuetapowa weryfikacja (nie ufaj linkom):** Wprowadź zasadę, aby nigdy nie klikać linków ani nie wykonywać poleceń zawartych w niechcianych wiadomościach. Zamiast tego przeprowadź dwuetapową weryfikację: wejdź samodzielnie na oficjalną stronę lub w aplikację albo skontaktuj się z daną osobą za pośrednictwem innego kanału. Na przykład, jeśli w wiadomości e-mail znajduje się informacja „Twoje konto bankowe zostało zablokowane, kliknij tutaj", nie należy klikać – należy otworzyć osobno aplikację bankową lub zadzwonić do banku. Jeśli konto znajomego prosi o podanie kodu, należy zadzwonić do tej osoby, aby potwierdzić. Ten nawyk pozwala uniknąć większości oszustw

phishingowych i podszywających się pod inne osoby, w tym fałszywych ofert nagród i oszustw typu „przyjaciel w potrzebie".

Wykorzystaj krótkie modelowanie i ćwiczenia dla każdej procedury. Na przykład, zademonstruj „Zatrzymaj się – Oddychaj – Sprawdź" za pomocą przykładowej wiadomości na ekranie, opisując swoje myśli. Następnie poproś grupę o wykonanie szybkiej serii ćwiczeń z innym przykładem. Podaj wskazówkę lub skojarzenie, które pomoże im zapamiętać to później – może to być ikona wizualna lub hasło. Celem jest utrwalenie tych reakcji, tak, aby w rzeczywistej sytuacji stresowej (np. otrzymanie przerażającej wiadomości od drapieżnika lub komentarza o znęcaniu się) młodzież automatycznie przechodziła do bezpieczniejszej procedury.

7. Ocena oświetlenia dla zrozumienia

Po nauczeniu podstawowych informacji należy przeprowadzić szybką, nieobciążającą ocenę, aby sprawdzić poziom zrozumienia i skorygować błędne przekonania:

Podpowiedzi na zakończenie: pod koniec sesji poproś każdego ucznia, aby napisał jedno zdanie na temat tego, co zmieniło się w jego rozumieniu dzisiejszej lekcji. Na przykład: „Kiedyś uważałem, że pośpiech jest w porządku, ale teraz postrzegam go, jako słabość" lub „Dowiedziałem się, co oznacza phishing". Pomaga to utrwalić kluczowe wnioski i pozwala zobaczyć, co zapadło w pamięć.

Głośne myślenie: poproś kilku uczniów, aby opowiedzieli, jak zareagowaliby na daną wiadomość lub sytuację. Na przykład przedstaw hipotetyczną wiadomość („Twój znajomy wysłał Ci link z informacją, że zostałeś opublikowany na koncie cringe") i poproś ucznia, aby opisał swoją reakcję: „Czułbym się zawstydzony i zaciekawiony... ale zatrzymałbym się i wziął głęboki oddech, pamiętałbym, żeby nie klikać w linki, może sprawdziłbym bezpośrednio konto lub zapytałbym znajomego, czy naprawdę wysłał tę wiadomość". Słuchanie tych głośnych myśli pokazuje, czy uczniowie potrafią zastosować pojęcia takie jak zagrożenia, czynniki wyzwalające i rutyny w kontekście. Buduje to również pewność siebie w używaniu nowego słownictwa.

Sprawdzanie słownictwa: podaj uczniom kluczowe terminy z modułu (zagrożenie, podatność, ryzyko itp.) i poproś ich, aby zdefiniowali je własnymi słowami lub podali przykład. Możesz zrobić z tego szybką grę (np. bingo ze słownikiem lub dopasowywanie terminów do definicji). Upewnij się, że uczniowie rozumieją każdy termin na tyle dobrze, aby mogli wyjaśnić go kolegom. Na przykład uczeń może powiedzieć: „Podatność jest jak słabość – dla mnie nadmierne dzielenie się informacjami jest podatnością, ponieważ mam tendencję do publikowania postów bez zastanowienia, a to może być ryzykowne".

Pytania scenariuszowe: przedstaw bardzo krótki scenariusz i zadaj kilka pytań wielokrotnego wyboru lub pytań typu „tak/nie”, aby sprawdzić zrozumienie. Na przykład:, „Jeśli otrzymasz wiadomość prywatną od nieznajomej osoby oferującej nagrodę za zarejestrowanie się na stronie internetowej, jakie zagrożenie się z tym wiąże? Jaką lukę w zabezpieczeniach może to wykorzystać? Jaka jest bezpieczna reakcja?”. Można to zrobić poprzez szybkie podniesienie rąk lub ankietę online.

Celem oceny nie jest tutaj „ocenianie” kogokolwiek, ale zapewnienie jasności. Pomaga to również wcześnie wykryć wszelkie nieporozumienia, aby można było się nimi zająć (np., jeśli ktoś nadal uważa, że „jeśli pochodzi od znajomego, to musi być bezpieczne”, można to skorygować). Zachowaj pozytywny i zachęcający ton – chwal poprawne koncepcje i delikatnie poprawiaj błędy, udzielając jasnych, przyjaznych dla młodzieży wyjaśnień.

Zwiększony słownik

- **Aktywa:**, co cenisz i co chcesz chronić w sieci (konta, dane, reputacja).
- **Zagrożenie:** wszystko, co może zaszkodzić tym zasobom (phishing, hakerzy, prześladowcy, przestępcy, złośliwe oprogramowanie).
- **Podatność:** słabość lub luka, która zwiększa prawdopodobieństwo powodzenia zagrożenia (słabe hasło, szybkie zaufanie, silne emocje, takie jak panika, nadmierne udostępnianie danych osobowych).
- **Ryzyko:** prawdopodobieństwo wykorzystania luki w zabezpieczeniach w celu wyrządzenia szkody (może być wysokie lub niskie, podejmujemy działania mające na celu jego zmniejszenie).
- **Higiena:** codzienne nawyki bezpieczeństwa, które cię chronią (aktualizacje, 2FA, linki weryfikacyjne, przemyślenie przed opublikowaniem).
- **Świadomość siebie:** świadomość swoich uczuć w danej chwili (szczególnie w Internecie).
- **Samokontrola:** Strategie radzenia sobie z emocjami i impulsami (ćwiczenia oddechowe, przerwy).
- **Świadomość społeczna:** rozumienie emocji innych i intencji w sieci (empatia, czytanie treści, rozpoznanie manipulacji).
- **Umiejętności interpersonalne:** zdrowe sposoby interakcji w sieci (asertywna komunikacja, ustalanie granic, szukanie pomocy).
- **Wyzwalacz perswazji:** element wiadomości, który ma na celu wywołanie emocji (poczucie pilności, strach, ciekawość itp.) i wpłynięcie na Twoje zachowanie.
- **Krok weryfikacyjny:** działanie mające na celu sprawdzenie, czy coś jest prawdziwe, zanim zareagujesz (np. skontaktowanie się z przyjacielem za pośrednictwem innej aplikacji lub sprawdzenie oficjalnego źródła).

Poprzez przyswojenie tych terminów uczniowie zyskują możliwość bardziej przejrzystego omawiania i rozwiązywania problemów związanych z cyberprzestrzenią. Na przykład uczeń może później powiedzieć: „Zauważyłem, że wiadomość wykorzystywała poczucie pilności, jako bodziec, więc uznałem to za sygnał ostrzegawczy – moja samoświadomość zadziałała i podjąłem kroki weryfikacyjne, dzwoniąc na infolinię firmy”. Taki poziom wyrazistości jest oznaką prawdziwego przyswojenia wiedzy i stanowi podstawę do bardziej praktycznych ćwiczeń w kolejnych modułach.

Moduł 2 – Ramy szkoleniowe

Przegląd modułu

Moduł ten zapewnia pracownikom młodzieżowym i edukatorom ustrukturyzowane i praktyczne ramy szkoleniowe, które integrują inteligencję emocjonalną (EI) i świadomość w zakresie cyberbezpieczeństwa z edukacją młodzieży. Opierając się na wynikach badania porównawczego EM&M i zgodnie z metodologią nauczania mieszanego stosowaną w projekcie, moduł 2 określa, jakie treści należy przekazywać młodym ludziom, aby wzmocnić ich odporność emocjonalną, umiejętności cyfrowe i profilaktyczne zachowania w Internecie.

Moduł podkreśla, w jaki sposób umiejętności EI – takie jak samokontrola, świadomość emocjonalna, radzenie sobie ze stresem, empatia i krytyczna refleksja – bezpośrednio wpływają na podatność młodych ludzi na zagrożenia w Internecie. Zawiera wskazówki dla pracowników młodzieżowych dotyczące włączenia tych umiejętności do edukacji w zakresie cyberbezpieczeństwa, jednocześnie odnosząc się do najczęstszych zagrożeń dotykających dzisiejszą młodzież, w tym:

- Cyberprzestępcy i uwodzenie dzieci w sieci
- Fałszywe zaproszenia do znajomych i próby podszywania się pod inne osoby
- Publikowanie prywatnych informacji lub treści, których później można żałować
- Taktyki phishingowe
- Oszustwa związane z nagrodami, wynagrodzeniami lub wywoływaniem strachu przed przegapieniem okazji (FOMO)
- Cyberprzemoc i wroga komunikacja cyfrowa
- Dezinformacja oraz brakujące lub zmanipulowane informacje
- Przypadkowe pobieranie złośliwego oprogramowania.

Opierając się na dowodach zebranych w sześciu krajach partnerskich, moduł kładzie nacisk na nauczanie mieszane, jako najbardziej integracyjne i skuteczne podejście do edukacji młodzieży. Wspiera on nauczycieli w dostosowaniu ram EM&M do różnych lokalnych realiów (miejskich/wiejskich, społeczno-ekonomicznych, kulturowych), równoważąc zajęcia stacjonarne z narzędziami internetowymi i cyfrowymi dostosowanymi do indywidualnego tempa nauki, takimi jak Teams, Moodle, Zoom, YouTube, Canva i Kahoot.

Ostatecznie moduł ten stanowi koncepcyjne i strukturalne podstawy dla modułu 3, który rozszerza ramy o konkretne metody integracyjnego nauczania

mieszanego. Moduły 2 i 3 tworzą spójną ścieżkę od tego, *czego* pracownicy młodzieżowi muszą nauczyć, do tego, *jak* mogą skutecznie i bezpiecznie emocjonalnie wdrożyć te treści.

Ramy szkoleniowe EM&M

Integracja inteligencji emocjonalnej, cyberbezpieczeństwa i uczenia mieszanego

Od dowodów → przez praktykę → do odporności młodzieży

Dlaczego te ramy? Aby pomóc pracownikom młodzieżowym budować u młodych ludzi odporność emocjonalną i bezpieczeństwo cyfrowe poprzez uczenie mieszane.

Infrastruktura i dostęp

- *Urządzenia i łączność*
- *Opcje niskiego zużycia danych*

Innowacje pedagogiczne

- *Grywalizacja*
- *Mikro-uczenie*
- *Metody interaktywne*

Wsparcie emocjonalne i społeczne

- *Inteligencja emocjonalna i wsparcie rówieśnicze*
- *Bezpieczne przestrzenie*

Kluczowe elementy ram

Uczenie mieszane

- *Zajęcia stacjonarne . Online . Nauka we własnym tempie*
- *Opcje niskiego zużycia danych*

Inteligencja emocjonalna

- *Samoświadomość Samoregulacja*
- *Empatia*

Redukcja barier

- *Łączność Motywacja*
- *Obciążenie pracą*

Prewencyjne cyberbezpieczeństwo

- *Unikanie zagrożeń zanim wyrządzą szkody*

Zagrożenia cyfrowe a inteligencja emocjonalna – rozpoznaj i reaguj

Zagrożenie cybernetyczne	Wyzwalacz emocjonalny	Kluczowa kompetencja EI	EI w działaniu	Bezpieczne działanie cyfrowe
Phishing	Pilność, strach	Zarządzanie stresem	Zatrzymaj się i reguluj emocje przed reakcją	Sprawdź nadawcę i link przed kliknięciem
Fałszywe profile	Ciekawość, zaufanie	Samoświadomość	Kwestionuj intencje i stawiaj granice	Potwierdź tożsamość przed akceptacją
Cyberprzemoc	Złość, wstyd	Regulacja emocji i empatia	Uspokój się i wybierz konstruktywną reakcję	Zablokuj, zgłoś lub poszukaj wsparcia
Dezinformacja	Strach, oburzenie	Krytyczne myślenie	Zyskaj dystans emocjonalny i przeanalizuj	Sprawdź źródła przed udostępnieniem

Dwutorowe uczenie mieszane

Edukatorzy

- *Ustrukturyzowane sesje*
- *Teams, Moodle, Zoom*

Młodzież

- *Elastyczne uczenie się*
- *YouTube, Canva, Kahoot!*

Inteligencja emocjonalna nie jest dodatkiem. Jest kompetencją cyberbezpieczeństwa.

Dofinansowane przez Unię Europejską

Cele nauczania

Po ukończeniu tego modułu pracownicy młodzieżowi i edukatorzy będą potrafili:

- Rozumieć i stosować ramy szkoleniowe EM&M w swojej pracy z młodymi ludźmi.
- Włączać umiejętności związane z inteligencją emocjonalną (radzenie sobie ze stresem, empatia, zdolność adaptacji, świadomość emocjonalna) do szkoleń z zakresu cyberbezpieczeństwa.
- Nauczać strategii zapobiegawczych związanych z głównymi zagrożeniami internetowymi zidentyfikowanymi w projekcie (cyberprzestępcy, podszywanie się pod inne osoby, phishing, oszustwa, cyberprzemoc, dezinformacja, ryzykowne pliki do pobrania i nadmierne udostępnianie informacji).
- Dostosować ramy do lokalnych warunków, zapewniając jednocześnie integrację i dostępność dla różnych grup młodzieży.
- Wykorzystać podejście oparte na nauczaniu mieszanym, łączące bezpośrednią pracę z uczestnikami, synchroniczne i asynchroniczne interakcje online oraz opcje mobilne.
- Zajmować się barierami utrudniającymi zaangażowanie, takimi jak spadek motywacji, problemy z łącznością i nierówności cyfrowe.
- Wspierać odporność psychiczną i krytyczną świadomość młodzieży poprzez strategie uczenia się oparte na inteligencji emocjonalnej i gamifikacji.

Treść modułu

Wprowadzenie do ram szkoleniowych

Dlaczego ramy szkoleniowe dotyczące inteligencji emocjonalnej i cyberbezpieczeństwa?

W dzisiejszych czasach młodzi ludzie żyją w cyfrowym świecie, gdzie emocje i technologia stale wzrasta. Na ich wybory w sieci często mają wpływ:

- Presja otoczenia,
- Impulsywne reakcje,
- Stres lub strach,

- Pragnienie nawiązania kontaktu,
- Poszukiwanie aprobaty lub potwierdzenia.

Ta dynamika emocjonalna może zwiększać podatność na zagrożenia internetowe, taki jak:

- Cyberprzestępcy
- Podszywanie się pod inne osoby
- Phisihng
- Oszustwa
- Cyberprzemoc
- Dezinformacja
- Złośliwe oprogramowanie
- Nadmierne udostępnianie informacji

Pracownicy młodzieżowi potrzebują, zatem jasnej, praktycznej struktury, która pomoże im uczyć zarówno bezpieczeństwa cyfrowego, jak i inteligencji emocjonalnej (EI), jako wzajemnie powiązanych umiejętności.

Właśnie to zapewnia program szkoleniowy EM&M.

Ramy zbudowane na prawdziwych potrzebach

Badanie porównawcze EM&M, przeprowadzone w sześciu krajach z udziałem 329 uczestników, wykazało, że:

Młodzież często boryka się z:

- Rozpoznaniem zagrożeń cybernetycznych,
- Regulowaniem emocji podczas konfliktów w Internecie,
- Odpornością na manipulacje (np. oszustwa, fałszywe profile, wyzwalacze FOMO),
- Krytyczną oceną informacji.

Pracownicy młodzieżowi potrzebują:

- Łatwych do aplikowania struktur szkoleniowych,
- Narzędzia do nauczania mieszanego, odpowiednie do różnych kontekstów,
- Metod, które łączą *uczucia* z *podejmowaniem decyzji w Internecie*,
- Podejście integracyjne dla osób o różnym pochodzeniu i poziomie dostępu do technologii cyfrowych.

Ramy odpowiadają oferując:

- Ustrukturyzowany plan działania,
- Elastyczne cele nauczania,
- Profilaktyczne podejście oparte na emocjach,
- Wskazówki dotyczące nauczania mieszanego,
- Narzędzia i aktywności gotowe do użytku.

Dlaczego inteligencja emocjonalna jest ważna w cyberbezpieczeństwie

Zagrożenia w sieci rzadko są „tylko techniczne". Odnoszą sukces, ponieważ wyzwalają emocje.

Zagrożenia w sieci	Wyzwalacz emocjonalny	Wynik
Phishing	Pilność, panika	Szybkie ryzykowne kliknięcie
Oszustwa	Podekscytowanie, szukanie nagród, FOMO	Irracjonalne wybory
Cyberprzestępcy	Zaufanie, samotność	Podatność
Cyberprzemoc	Złość, wstyd	Impulsywne reakcje
Fałszywe wiadomości	Strach, zakłopotanie	Rozpowszechnianie fałszywych informacji

EI pomaga młodzieży zwolnić, jasno myśleć i podejmować bezpieczniejsze wybory.

- Z mocnymi umiejętnościami EI możesz:
- Rozpoznać manipulacje emocjonalną
- Regulować stres i impulsywność
- Komunikować się asertywnie
- Stawiać granice
- Prosić o pomoc, gdy jest potrzebna
- Stosować krytyczne myślenie przed podjęciem działania

W ten sposób EI staje się narzędziem bezpieczeństwa cyfrowego, a nie tylko umiejętnością rozwoju osobistego.

Co zapewniają ramy szkoleniowe EM&M

Ramy te stanowią dla pracowników młodzieżowych praktyczny, szczegółowy przewodnik dotyczący wdrażania EI i cyberbezpieczeństwa w każdym środowisku młodzieżowym. Wspierają one:

Różnorodne grupy młodzieżowe

- Miejskie/wiejskie
- Niski/wysoki dostęp cyfrowy
- Różnorodność społeczno-ekonomiczna
- Zróżnicowane konteksty kulturowe
- Różne potrzeby nauczania

Elastyczne nauczanie mieszane

- Zajęcia bezpośrednie
- Synchronizowane warsztaty online
- Asynchroniczne mikro nauczanie
- Narzędzia dostosowane do urządzeń mobilnych (YouTube, Canva, Padlet, Kahoot)

Zapobieganie przez wzmacnianie pozycji

Zamiast reagować na problemy po ich wystąpieniu, program pomaga młodzieży:

- Przewidywać ryzyko,
- Zarządzać wyzwalaczami wpływającymi na emocje,
- Rozpoznawać manipulację,
- Rozwijać bezpieczne nawyki,
- Budować odporność psychiczną.

Powiązanie z modułem 3

Aby podręcznik był spójny:

- Moduł, 2 = CZEGO *uczą pracownicy młodzieżowi*: EI + cyberbezpieczeństwo + ramy prewencyjne + cele nauczania.
- Moduł 3 = *JAK uczą tego pracownicy młodzieżowi*: konkretne modele, narzędzia, metody, scenariusze i praktyki integracyjne w zakresie nauczania mieszanego.

Razem tworzą konkretną ścieżkę szkoleniową: od zrozumienia → poprzez projektowanie → do wdrażania wysokiej, jakości sesji z młodzieżą.

Najważniejsze wnioski dla pracowników młodzieżowych

- Świat cyfrowy jest emocjonalny; bezpieczeństwo w Internecie wymaga inteligencji emocjonalnej.
- Młodzież potrzebuje umiejętności w zakresie cyberbezpieczeństwa opartych na zapobieganiu i emocjach.
- Niniejsze ramy zapewniają jasną, przystępną strukturę, która pomoże Ci w praktyce.
- Nauczanie mieszane zwiększa zaangażowanie i elastyczność.
- Moduł 3 pomoże Ci zamienić te ramy w rzeczywiste sesje i zadania.

Podstawy ram szkoleniowych EM&M

Ramy szkoleniowe EM&M opierają się na trzech podstawowych filarach, które określają, w jaki sposób pracownicy młodzieżowi mogą skutecznie włączać integrację emocjonalną (EI) i świadomość cyberbezpieczeństwa do środowisk edukacyjnych młodzieży. Filary te gwarantują, że doświadczenie edukacyjne jest integracyjne, praktyczne, elastyczne i zapewnia wsparcie emocjonalne, niezależnie od kontekstu.

Fundament 1: Infrastruktura i dostęp

Zapewnienie sprawiedliwości, dostępności i równych szans dla wszystkich młodych ludzi.

Zanim pracownicy młodzieżowi będę mogli przekazać treści związane z cyberbezpieczeństwem lub EI muszą zająć się rzeczywistymi warunkami nauki, z jakimi borykają się młodzi ludzie. Badanie porównawcze uwypukliło różnice w następujących obszarach:

- Dostęp do Internetu (szczególnie na obszarach wiejskich lub o niskich dochodach)
- Dostępność sprzętu (wspólne telefony, przestarzałe urządzenia)
- Narzędzia cyfrowe i platformy wykorzystywane w różnych krajach i organizacjach

Dlaczego jest to istotne

Młodzi ludzie, którzy nie mają stabilnego dostępu do Internetu lub odpowiednich urządzeń, często tracą zainteresowanie, pozostają w tyle lub całkowicie rezygnują z udziału w zajęciach. Ma to bezpośredni wpływ na wyniki nauczania w zakresie świadomości cyberbezpieczeństwa i odporności emocjonalnej.

Co powinni zrobić pracownicy młodzieżowi

- Zapewnić alternatywne rozwiązania wymagające niewielkiej przepustowości (arkusze robocze do pracy offline, materiały drukowane).
- Wybrać narzędzia dostosowane do urządzeń mobilnych, ponieważ większość młodych ludzi korzysta ze smartfonów.
- Upewnić się, że wszystkie działania mają format zapasowy (np. wersja oparta na dyskusji w przypadku zadań online).
- Priorytetowe traktowanie platform znanych młodzieży:

  Zoom • Teams • Moodle (do zorganizowanego uczenia się) ·YouTube • Canva • mikro filmy w stylu TikTok • Padlet • Kahoot (do zaangażowania)

Cel: Żadna młoda osoba nie jest wykluczona z procesu uczenia się z powodu barier technicznych.

Fundament 2: Innowacja pedagogiczna

Utrzymanie zaangażowania, motywacji i aktywności młodzieży.

Pracownicy młodzieżowi wielokrotnie zgłaszały, że zmęczenie motywacyjne, zmęczenie ekranem oraz nudne lub powtarzalne formaty zmniejszają skuteczność uczenia się – zwłaszcza w Internecie. Zauważyły również, że młodzież preferuje:

- Krótkie dynamiczne momenty nauki
- Treści wizualne
- Praktyczne rozwiązywanie problemów
- Doświadczenie oparte na grach
- Możliwości wykazania się kreatywnością

Dlaczego jest to istotne

Szkolenia z zakresu cyberbezpieczeństwa często stają się zbyt techniczne lub abstrakcyjne. Bez innowacji młodzież szybko traci zainteresowanie, co sprawia, że staje się bardziej podatna na zagrożenia internetowe.

Co powinni uwzględnić pracownicy młodzieżowi

- Grywalizacja (quizy, wyzwania, pokoje zagadek, odznaki)
- Filmy edukacyjne (3–7 minut)
- Ćwiczenia oparte na scenariuszach (wyzwania związane z phishingiem, odgrywanie ról z wykorzystaniem fałszywych profili)
- Interaktywne ankiety i reakcje na żywo
- Techniki dramatyczne, improwizacja lub opowiadanie historii w przypadku tematów budzących emocje
- Chwile refleksji łączące emocje z zachowaniem

Cel: Spraw, aby nauka była znacząca, istotna i angażująca emocjonalnie.

Fundament 3: Wsparcie emocjonalne i społeczne

Budowanie odporności emocjonalnej, jako podstawowej umiejętności w zakresie cyberbezpieczeństwa.

Fundacja ta odzwierciedla kluczową obserwację EM&M: emocje mają silny wpływ na decyzje podejmowane w Internecie.

Młodzież często pada ofiarą oszustw, klika niebezpieczne linki, udostępnia zbyt wiele informacji lub angażuje się w cyberprzemoc z powodu bodźców emocjonalnych, takich jak:

- Niepokój
- Podekscytowanie
- Frustracja
- Samotność
- Ciekawość
- Chęć dopasowania się.

W ramach tych wytycznych podkreśla się, że EI nie jest opcjonalna — jest niezbędna do bezpiecznego zachowania w Internecie.

Dlaczego jest to istotne

Kiedy młodzież rozumie i reguluje swoje emocje, potrafi:

- Zastanowić się przed kliknięciem,
- Szybciej rozpoznać manipulację,
- Rozważnie reagować na cyberprzemoc,
- Bardziej krytycznie weryfikować informacje,
- Unikać impulsywnego udostępniania treści,
- Komunikować się z większym szacunkiem w sieci.

Co powinni wdrożyć pracownicy młodzieżowi

- Sprawdzanie stanu emocjonalnego na początku sesji
- Ćwiczenia z zakresu radzenia sobie ze stresem przed wyzwaniami związanymi z cyberbezpieczeństwem
- Dyskusja na temat czynników wywołujących emocje (strach, FOMO, wstyd, podekscytowanie)
- Pytania do refleksji nad inteligencją emocjonalną („Jak się czułeś, kiedy…?")
- Kręgi wsparcia rówieśniczego sprzyjające bezpiecznej komunikacji
- Trening empatii w zakresie rozwiązywania konfliktów i scenariuszy cyberprzemocy

Cel: Wyposażenie młodzieży w umiejętności pozwalające zachować spokój, refleksyjność i bezpieczeństwo w przestrzeni cyfrowej.

Jak współgrają trzy fundamenty

Fundacje te wspierają pracowników młodzieżowych w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa, które są:

Fundament	Co to wnosi	Dlaczego jest to istotne

Dofinansowane przez Unię Europejską

Numer referencyjny projektu: 2024-2-RO01-KA220-YOU-000293190

Infrastruktura i dostęp	Równe szanse uczestnictwa	Żadna młodzież nie zostaje pominięta
Innowacja pedagogiczna	Angażujące, motywujące działania	Młodzież pozostaje w kontakcie i pogłębia swoją wiedzę
Wsparcie emocjonalne i społeczne	Odporność psychiczna, empatia, bezpieczne podejmowanie decyzji	Zmniejsza podatność na zagrożenia internetowe

W połączeniu tworzą one holistyczne, integracyjne i transformacyjne środowisko edukacyjne.

Najważniejsze wnioski dla pracowników młodzieżowych (szybkie streszczenie)

- Przed rozpoczęciem nauczania treści dotyczących cyberbezpieczeństwa należy zapewnić dostępne warunki nauki.
- Wykorzystaj innowacyjne i przyjazne dla młodzieży metody, aby utrzymać zaangażowanie.
- Niech EI stanie się podstawowym elementem każdej lekcji poświęconej cyberbezpieczeństwu, a nie tylko dodatkiem.
- Skup się na rzeczywistych czynnikach wywołujących emocje, które leżą u podstaw ryzykownych zachowań w Internecie.
- Pamiętaj: Stworzona przez Ciebie podstawa decyduje o tym, jak skutecznie młodzież będzie się uczyć, stosować i zachowywać umiejętności w zakresie cyberbezpieczeństwa.

Najważniejsze elementy schematów szkoleniowych EM&M

Element 1: Podejście do nauczania mieszanego

Elastyczne połączenie nauki stacjonarnej, online i samodzielnej.

Nauczanie mieszane nie polega po prostu na dodaniu elementów online do tradycyjnych warsztatów — chodzi o zaprojektowanie celowych, powiązanych ze sobą doświadczeń edukacyjnych, które odpowiadają preferencjom młodzieży w zakresie zaangażowania.

Dofinansowane przez Unię Europejską

Co wykazało badanie porównawcze

- Pracownicy młodzieżowi preferują sesje o ustalonej strukturze (bezpośrednie lub synchroniczne online).
- Młodzi ludzie preferują działania asynchroniczne, elastyczne i dostosowane do urządzeń mobilnych.
- Zaangażowanie wzrasta, gdy sesje łączą krótkie wyjaśnienia, zadania praktyczne i interaktywne elementy cyfrowe.

Ramy polecają:

- Połączenie sesji warsztatowej z narzędziami cyfrowymi (np. Kahoot, Canva, Padlet).
- Wykorzystanie mikro nauczania (krótkie filmy, wyzwania, mini-quizy) do przekazania kluczowych pojęć z zakresu cyberbezpieczeństwa.
- Zapewnienie zarówno formalnej ścieżki edukacyjnej (Teams/Moodle/Zoom), jak i platformy kreatywnej (YouTube, Discord, Canva).
- Stworzenie „ścieżki hybrydowej", która pozwoli młodzieży pracować online, gdy jest zmotywowana, a offline, gdy łączność jest ograniczona.

Cel: Tworzenie dynamicznej, dostępnej i dostosowanej do uwarunkowań kulturowych edukacji, niezależnie od lokalnego kontekstu.

Element 2: Inteligencja emocjonalna w cyberbezpieczeństwie

Umiejętności EI, jako podstawa bezpieczeństwa w Internecie.

EI stanowi sedno każdego aspektu ram EM&M. Młodzież jest bardziej podatna na cyberzagrożenia, gdy doświadcza:

- Stresu,
- Presji czasu,
- Samotności,
- Złości,
- Ciekawości,
- Pragnienia akceptacji społecznej.

To sprawia, że zarządzanie emocjami jest równie ważne jak rozpoznawanie ryzyka technicznego.

Kluczowe elementy EI zintegrowane z lekcjami dotyczącymi cyberbezpieczeństwa:

Dofinansowane przez Unię Europejską

- Świadomość siebie → dostrzeganie czynników wywołujących emocji przed podjęciem reakcji
- Samokontrola → zatrzymanie się przed kliknięciem, udostępnieniem, odpowiedzią
- Empatia i zrozumienie społeczne → konstruktywna reakcja na cyberprzemoc
- Zdolność adaptacji → zachowanie spokoju podczas zakłóceń lub konfliktów
- Umiejętności komunikacyjne → asertywne wyznaczanie granic w kontaktach z nieznajomymi lub podejrzanymi osobami

Praktyczne przykłady:

- Nauczanie rozpoznawania phishingu wraz z technikami oddychania pomagającymi radzić sobie ze stresem.
- Omawianie cyberprzemocy z empatią i ćwiczeniami refleksji emocjonalnej.
- Badanie oszustw, skupiając się na emocjach, poszukiwaniu nagród i czynnikach wywołujących FOMO.

Cel: Pomoc młodzieży w podejmowaniu bezpieczniejszych i bardziej uzasadnionych emocjonalnie decyzji w Internecie.

Element 3: Pokonywanie barier w wyzwań

Usuwanie przeszkód, które uniemożliwiają młodzieży pełne uczestnictwo.

Pracownicy młodzieżowi wielokrotnie napotykają wyzwania, które osłabiają zaangażowanie i skuteczność uczenia się. Ramy te bezpośrednio wspierają nauczycieli w pokonywaniu tych barier.

Najczęstsze zidentyfikowane wyzwania:

- Słabe połączenie internetowe
- Brak urządzeń lub wspólne korzystanie z urządzeń
- Niska pewność siebie w technologii cyfrowej
- Zmęczenie motywacyjne (zwłaszcza w Internecie)
- Przeciążenie ekranem
- Ograniczony czas lub zasoby na przygotowanie się

Ramy zapewniają następujące rozwiązania:

- Wersje wszystkich ćwiczeń dostosowane do niskiej przepustowości łącza

Dofinansowane przez Unię Europejską

- Alternatywne rozwiązania offline dla sesji cyfrowych
- Moduły mikronauki, które zmniejszają zmęczenie
- Zadania oparte na mechanizmach grywalizacji, które zwiększają motywację
- Mentoring prowadzony przez rówieśników, który wzmacnia zaangażowanie
- Dostępny projekt minimalizujący przeciążenie poznawcze

Praktyczne strategie dla pracowników młodzieżowych:

- Użycie arkusza roboczego do identyfikacji phishingu lub oszustw, które można wydrukować.
- Zapewnienie elastycznych terminów uczestnictwa w zadaniach asynchronicznych.
- Uproszczenie narzędzi cyfrowych i unikanie przeciążenia platformy.
- W długich przerwach uwzględnienie przerwy na ruch lub refleksję.

Cel: Sprawienie, aby edukacja w zakresie cyberbezpieczeństwa i inteligencji emocjonalnej była dostępna, wykonalna i skuteczna dla wszystkich młodych ludzi, niezależnie od ograniczeń.

Element 4: Profilaktyka w zakresie cyberbezpieczeństwa

Uczenie młodzieży do unikania ryzyka—nie tylko do reagowania na nie.

Młodzi ludzie często spotykają się z zagrożeniami w Internecie, zanim zdobędą odpowiednią wiedzę lub dojrzałość emocjonalną, aby sobie z nimi poradzić. Dlatego też ramy EM&M kładą nacisk na profilaktykę, a nie na reagowanie.

Podstawowe umiejętności prewencyjne, na które kładzie się nacisk:

- Rozpoznanie wzorców phishingu i oszustw
- Weryfikacja tożsamości w Internecie
- Stosowanie bezpiecznych ustawień prywatności
- Sprawdzanie źródeł w celu zwalczania dezinformacji
- Zastanowienie się przed publikacją lub udostępnieniem
- Unikanie ryzykownych pobrań
- Zgłaszanie cyberprzemocy i cyberprzestępców
- Utrzymywanie nawyków związanych z cyberhigieną

Prewencja + EI = silna ochrona

Przykład 1:

Dofinansowane przez Unię Europejską

Wiadomość phishingowa wywołuje poczucie pilności→ EI „zatrzymaj się i oddychaj” → krytyczna ocena → bezpieczna decyzja.

Przykład 2:

Cyberprzemoc wywołuje ból→ EI samoregulacja→ asertywna komunikacja → wspierająca reakcja rówieśników.

Narzędzia wykorzystane w ramach zawierają:

- Scenariusze
- Symulacje
- Gamifikowane pokoje zagadek
- Karty do odgrywania ról
- Mapowanie emocji
- Dzienniki refleksyjne
- Programy ambasadorów rówieśniczych.

Cel: Wyposażenie młodzieży w codzienne nawyki i siłę emocjonalną, które zmniejszają ich narażenie na cyberzagrożenia.

Dofinansowane przez Unię Europejską

Szybkie podsumowanie:, co osiągają razem te cztery elementy

Element	Co daje pracownikom młodzieżowym	Korzyść dla młodzieży
Nauczanie mieszane	Elastyczne opcje nauczania	Angażująca, przystępna nauka
Integracja EI	Stabilność emocjonalna i bezpieczniejsze podejmowanie decyzji	Większa odporność w sieci
Pokonywanie barier	Praktyczne narzędzia dla różnorodnych grup	Włączające uczestnictwo
Prewencyjne cyberbezpieczeństwo	Proaktywne unikanie ryzyka	Mniejsza podatność na zagrożenia

Wszystkie te elementy sprawiają, że szkolenie z zakresu cyberbezpieczeństwa przestaje być tylko tematem technicznym, a staje się całościowym procesem wzmacniania pozycji młodzieży.

Powiązanie inteligencji emocjonalnej, nauczanie mieszane i głównych zagrożeń internetowych

Zagrożenia dla cyberbezpieczeństwa mają nie tylko charakter techniczny, ale także emocjonalny i behawioralny. Młodzi ludzie często padają ofiarą zagrożeń internetowych nie, dlatego, że brakuje im wiedzy, ale dlatego, że emocje przeważają nad racjonalnym podejmowaniem decyzji. Nauczanie mieszane oferuje elastyczne sposoby nauczania EI i cyberbezpieczeństwa, pomagając młodzieży praktykować bezpieczniejsze nawyki cyfrowe poprzez realistyczne, angażujące i oparte na emocjach działania.

Ten rozdział przedstawia jasne, praktyczne powiązania pomiędzy:

- Umiejętnościami EI, które potrzebuje młodzież,
- Typowymi zagrożeniami, z jakimi się spotykają oraz
- Metodami nauczania mieszanego, które mogą stosować pracownicy młodzieżowi.

Dlaczego EI jest umiejętnością związaną z cyberbezpieczeństwem

Zagrożenia internetowe odnoszą sukces, ponieważ wykorzystują emocje, takie jak strach, ciekawość, podekscytowanie, samotność lub poczucie

Dofinansowane przez Unię Europejską

przynależności. Kiedy młodzież wzmacnia umiejętności EI, staje się mniej podatna na manipulację i bardziej zdolna do podejmowania bezpiecznych wyborów.

Kluczowe umiejętności EI istotne dla cyberbezpieczeństwa:

- Samoświadomość: dostrzeganie reakcji emocjonalnych
- Samokontrola: zatrzymanie się przed podjęciem działania
- Zarządzanie stresem: zachowanie spokoju w sytuacjach stresowych
- Empatia: konstruktywne reagowanie na innych
- Krytyczna refleksja: kwestionowanie informacji i intencji

Nauczanie mieszane pozwala rozwinąć te umiejętności poprzez interaktywne warsztaty, symulacje cyfrowe, zadania dostosowane do urządzeń mobilnych oraz przestrzenie online sprzyjające refleksji.

Podstawowa mapa ramowa

Wizualny przegląd sposobu, w jaki EI + nauczanie mieszane radzą sobie z każdym zagrożeniem

Zagrożenie cybernetyczne	**Emocje, które zwiększają podatność na zagrożenie**	**Potrzebne umiejętności EI**	**Przykłady nauczania mieszanego**
Cyberprzestępcy	Samotność, pragnienie uznania	Wyznaczanie granic, samoświadomość	Odgrywanie ról (offline), mikro filmy weryfikujące tożsamość, anonimowe pytania i odpowiedzi online
Fałszywe zaproszenia do znajomych / podszywanie się pod inne osoby	Ciekawość, presja społeczna	Zatrzymaj się-zastanów-podejmij decyzję, krytyczne myślenie	Cyfrowe wyzwanie „Znajdź fałszywy profil”, dyskusje w małych grupach
Nadmierne udostępnianie informacji /	Impulsywność, podekscytowani	Kontrola impulsów,	Ćwiczenie refleksyjne „Zastanów się,

Dofinansowane przez Unię Europejską

posty, których później można żałować	e, potrzeba akceptacji	świadomość emocjonalna	zanim opublikujesz", audyt mediów społecznościowych
Phishing	Pilność, dezorientacja, strach	Stres, powolne myślenie	Gra symulacyjna dotycząca phishingu, quiz mikro uczenia
Oszustwa / pułapki FOMO	Podekscytowanie, poszukiwanie nagrody, strach przed przegapieniem czegoś	Regulacja emocji sceptycyzm	Pokój zagadek online, wyzwanie związane z drzewem decyzyjnym
Cyberprzemoc	Złość, wstyd, frustracja	Komunikacja, empatia samoregulacja	Odtworzenie scen z dramatu, rekonstrukcja czatu cyfrowego, prywatny dziennik
Dezinformacja / fałszywe wiadomości	Strach, oburzenie, rezonans emocjonalny	Krytyczne myślenie, dystans emocjonalny	Wyścigi związane z weryfikacją faktów, ankiety online, porównanie nagłówków
Pobieranie złośliwego oprogramowania	Ciekawość, niecierpliwość	Ostrożność ocena konsekwencji	Quiz dotyczący bezpiecznego i ryzykownego pobierania plików, lista kontrolna ryzyka dostosowana do urządzeń mobilnych

Najważniejsze wnioski dla pracowników młodzieżowych

Dofinansowane przez Unię Europejską

- Każde zagrożenie cybernetyczne wiąże się z konkretnymi czynnikami wywołującymi emocje.
- Umiejętności związane z inteligencją emocjonalną sprawiają, że młodzież jest mniej podatna na zagrożenia i bardziej świadoma.
- Nauczanie mieszane pozwala na interaktywne prowadzenie zajęć, niezależnie od warunków technologicznych.
- Nie musisz być ekspertem w dziedzinie cyberbezpieczeństwa — wystarczy, że połączysz emocje, zachowania i przykłady.

Praktyczne wytyczne dla pracowników młodzieżowych

W niniejszym rozdziale przedstawiono jasne, praktyczne wskazówki dotyczące tego, w jaki sposób pracownicy młodzieżowi mogą włączyć inteligencję emocjonalną (EI) i cyberbezpieczeństwo do swojej codziennej praktyki, korzystając z ram szkoleniowych EM&M. Wytyczne te pomagają nauczycielom w tworzeniu bezpiecznych, integracyjnych, motywujących i zróżnicowanych środowisk edukacyjnych, które wzmacniają odporność cyfrową młodych ludzi.

Wytyczna 1: Przed rozpoczęciem oceń potrzeby młodzieży

Zacznij od tego, gdzie faktycznie znajdują się młodzi ludzie, a nie od tego, gdzie według Ciebie powinni się znajdować.

Co należy ocenić:

- Dostęp do technologii cyfrowych: urządzenia? Internet? Wspólne konta?
- Poziom umiejętności cyfrowych: pewność siebie czy niepewność?
- Potrzeby emocjonalne: stres, niska pewność siebie, konflikty, izolacja?
- Dotychczasowe doświadczenia w Internecie: cyberprzemoc, oszustwa, naruszenia prywatności.
- Preferencje dotyczące nauki: wizualne? Praktyczne? Grywalizowane? Oparte na dyskusji?

Narzędzia, które możesz używać:

- Krótkie anonimowe ankiety (online lub papierowe)
- Dyskusje przełamujące bariery: „Moim największym strachem w sieci jest…”
- Szybkie ankiety (Mentimeter, reakcje Zoom, WhatsApp)

Cel: Dostosowanie szkolenia do rzeczywistych potrzeb i uniknięcie przytłoczenia lub znudzenia uczestników.

Dofinansowane przez Unię Europejską

Wytyczna 2: Stwórz bezpieczne emocjonalnie środowisko nauki

Młodzi ludzie lepiej się uczą, gdy czują się szanowani, wspierani i wysłuchani.

Stwórz emocjonalne bezpieczeństwo przez:

- Otwarte rozmowy: „Jak się dzisiaj czujesz?”
- Umowy grupowe: szacunek, poufność, brak osądzania.
- Opcje rezygnacji: pozwól na opuszczenie zajęć podczas omawiania delikatnych tematów.
- Anonimowe narzędzia do dzielenia się opiniami: Padlet, Mentimeter, Slido.
- Sygnały wsparcia: kolorowe karty lub emotikony do wyrażania poziomu komfortu.

Przykład:

„Jeśli w dowolnym momencie dyskusja stanie się dla Ciebie niekomfortowa, możesz mi o tym powiedzieć lub zrobić przerwę. Twoje samopoczucie emocjonalne jest ważne”.

Cel: Połączenie inteligencji emocjonalnej z cyberbezpieczeństwem w sposób pełen szacunku i uwzględniający traumę.

Wytyczna 3: Włącz momenty EI do każdej czynności związanej z cyberbezpieczeństwem

Nawet 2-minutowa refleksja wzmacnia odporność emocjonalną. Proste techniki integracji EI:

- Zatrzymaj się i oddychaj: przed odpowiedzią na wiadomości lub kliknięciem linków.
- Nazywanie emocji:, „Co teraz czuję?”
- Mapowanie wyzwalaczy: zidentyfikuj emocje, które prowadzą do ryzykownych decyzji.
- Przyjmowanie perspektywy: „Jak czułaby się inna osoba w tej sytuacji?”
- Ponowna ocena: Przeformułowanie negatywnych myśli w stresujących sytuacjach cyfrowych.

Przykładowe pytania dotyczące inteligencji emocjonalnej:

- „Jakie uczucia wywołała w Tobie ta wiadomość?”
- „Jakie emocje mogą skłonić kogoś do padnięcia ofiarą tego oszustwa?”

Dofinansowane przez Unię Europejską

- „Co pomogłoby Ci zauważyć spokój w tej sytuacji?”

Cel: Automatyczne stosowanie umiejętności związanych z inteligencją emocjonalną w codziennym zachowaniu online.

Wytyczna 4: Wykorzystaj nauczanie mieszane, aby utrzymać zaangażowanie młodzieży

Łącz różne formaty, aby utrzymać energię i uwagę.

Zrównoważ swoje metody:

Bezpośrednie:

- Odgrywanie ról
- Dyskusje
- Mapowanie emocjonalne
- Warsztaty dotyczące cyberhigieny

Online/Synchroniczne:

- Symulacja phishingu
- Cyfrowe pokoje zagadek
- Tablice współpracy (Padlet, Miro)

Asynchroniczne:

- Filmy o mikronauce
- Krótkie quizy
- Dzienniki refleksyjne

Zadania związane z opowiadaniem historii w Canva

Wskazówka: Zawsze zapewnij wersję dostosowaną do urządzeń mobilnych — wielu młodych ludzi korzysta głównie ze smartfonów.

Cel: Utrzymanie motywacji i udostępnienie koncepcji poprzez wiele kanałów nauczania.

Wytyczna 5: Wykorzystaj realistyczne scenariusze oparte na doświadczeniach młodzieży

Autentyczność zwiększa skuteczność.

Stwórz scenariusze, z którymi młodzież może się utożsamić, obejmujące:

Dofinansowane przez Unię Europejską

- Fałszywych obserwujących
- Oszustwa związane z kampaniami FOMO
- Profile „przyjaciół przyjaciół”
- Cyberprzemoc w czatach grupowych
- Posty wywołujące emocje
- Dezinformację rozpowszechnianych w grupach klasowych
- „Oferty” bezpłatnego streamowania/pobierania

Wykorzystaj metodę scenariusza 3-etapowego:

1. Przedstaw krótką sytuację (wiadomość, film, zrzut ekranu).
2. Określ emocje, ryzyko, intencje, konsekwencje.
3. Omów bezpieczniejsze alternatywy, korzystając z narzędzi EI.

Cel: Połączenie teorii z rzeczywistym cyfrowym światem młodzieży.

Wytyczna 6: Wybierz narzędzia, które wspierają integrację

Narzędzia powinny dostosowywać się do młodzieży-nie odwrotnie.

Wybierz narzędzia na podstawie:

- Dostępności (napisy, zamiana tekstu na mowę, łatwa nawigacja)
- Niskiej przepustowości
- Intuicyjnego projektu
- Funkcji bezpieczeństwa i prywatności

Rekomendowane narzędzia:

- Do refleksji: Padlet, Google Forms, Mentimeter
- Do gywalizacji: Kahoot, Quizizz, Genially
- Do kreatywności: Canva, Storyboarder
- Do współpracy: Miro, Jamboard, Teams Channels

Unikaj:

- Zbyt wielu platform jednocześnie
- Narzędzi wymagających utworzenia kont, których młodzież nie chce zakładać
- Filmów o dużej zawartości merytorycznej, dłuższych niż 7 minut

Cel: Zmniejszenie barier i wsparcie różnorodnych potrzeb edukacyjnych.

Dofinansowane przez Unię Europejską

Wytyczna 7: Zachęcaj do wzajemnego wsparcia i przywództwa młodzieży

Młodzi ludzie najlepiej uczą się od siebie nawzajem.

Wdrażaj podejście oparte na rówieśnikach:

- Role ambasadorów cyberbezpieczeństwa
- Kręgi mentorskie rówieśników
- Projekty grupowe dotyczące dezinformacji, oszustw, audytów prywatności
- Wspólne wyzwania związane z weryfikacją faktów

Korzyści:

- Normalizuje zachowania pomocy związane z poszukiwaniem
- Zwiększa motywacje
- Wzmacnia zaangażowanie
- Umożliwia młodzieży rozwijanie ról przywódczych

Cel: Sprawić, by cyberbezpieczeństwo stało się wspólną odpowiedzialnością, a nie indywidualnym zadaniem.

Wytyczna 8: Ciągła ocena, refleksja i dostosowywanie

Poprawa jest częścią procesu.

Ocena poprzez:

- Kwestionariusze przed/po
- Szybkie sprawdzanie emoji („Jak bardzo czujesz się teraz pewny siebie?")
- Cotygodniowe pytania do dziennika refleksji
- Obserwacje interakcji w grupie
- Informacje zwrotne na temat działań i narzędzi

Zapytaj młodzież:

- „Co ułatwiło Ci dzisiaj naukę?"
- „Jakie ćwiczenie pomogło Ci zrozumieć swoje emocje w sieci?"
- „Które zagrożenia w sieci są nadal niejasne?"

Dostosuj na podstawie:

- Poziomu motywacji młodzieży
- Wyzwań związanych z łącznością
- Reakcji emocjonalnych na określone tematy

Dofinansowane przez Unię Europejską

- Niuansów kulturowych lub językowych

Cel: Utrzymanie środowiska nauki responsywnego, bezpiecznego i skutecznego.

Krótkie podsumowanie dla pracowników młodzieżowych

Oceń potrzeby młodzieży

Zadbaj o bezpieczeństwo emocjonalne

Włącz elementy EI do każdej aktywności

Korzystaj z różnych form nauczania

Nauczaj poprzez rzeczywiste scenariusze

Wybieraj narzędzia sprzyjające integracji

Zachęcaj do wzajemnego uczenia się

Oceniaj i dostosowuj na bieżąco

Zastosowanie ram szkoleniowych EM&M w praktyce pracy z młodzieżą

Moduł 2 dostarczył pracownikom młodzieżowym kompleksowe ramy łączące inteligencję emocjonalną (EI), świadomość cyberbezpieczeństwa i strategie nauczania mieszanego. Niniejszy rozdział łączy wszystkie elementy i zawiera praktyczne wskazówki dotyczące skutecznego stosowania tych ram w rzeczywistych warunkach pracy z młodzieżą, zapewniając płynne przejście do modułu 3.

Co możesz teraz zrobić, jako pracownik młodzieżowy

Po ukończeniu tego modułu pracownicy młodzieżowi będą potrafili:

- Zrozumieć, jak inteligencja emocjonalna wpływa na decyzje podejmowane w sieci: młodzież będzie potrafiła lepiej rozpoznawać próby phishingu, oszustwa, cyberprzemoc i dezinformację, gdy najpierw zrozumie swoje emocjonalne wyzwalacze.
- Nauczać cyberbezpieczeństwa poprzez scenariusze, z którymi młodzież może się utożsamić i które są oparte na emocjach: ramy programowe zapewniają sposoby na włączenie opowiadania historii, odgrywania ról, studiów przypadków i refleksji prowadzonej przez młodzież.

Dofinansowane przez Unię Europejską

- Wykorzystywać nauczanie mieszane, aby utrzymać zaangażowanie młodych ludzi: przechodzenie między dyskusjami offline, wyzwaniami online, filmami z mikro-nauczaniem i aktywnościami mobilnymi sprawia, że sesje są dynamiczne i przystępne.
- Zajmij się pełnym spektrum typowych zagrożeń cybernetycznych: w tym: cyberprzestępcami, fałszywymi zaproszeniami do grona znajomych, nadmiernym udostępnianiem informacji, phishingiem, oszustwami, cyberprzemocą, dezinformacją i złośliwym oprogramowaniem.
- Stwórz integracyjne i bezpieczne emocjonalnie środowisko: sprzyja to pełnemu szacunku dialogowi, pomaga młodym ludziom dzielić się trudnymi doświadczeniami i kształtuje umiejętności emocjonalne potrzebne do bezpiecznego zachowania w sieci.

Przed wdrożeniem: lista kontrolna gotowości pracownika młodzieżowego

Praktyczna lista kontrolna zapewniająca dobre przygotowanie sesji i zgodność z ramami EM&M.

A. Przygotowanie emocjonalne

- Zaplanowałem sprawdzenie stanu emocjonalnego lub ćwiczenie uziemiające.
- Jestem przygotowany do omówienia delikatnych tematów w sposób bezpieczny i pełen szacunku.
- Potrafię rozpoznać, kiedy młoda osoba jest zestresowana, przytłoczona lub wywołana.

B. Przygotowanie merytoryczne

- Wybrałem 1–3 kluczowe zagrożenia cybernetyczne, na których należy się skupić.
- Włączyłem elementy EI (przerwa, refleksja, nazwanie emocji, zmiana perspektywy).
- Sprawdziłem, czy moje przykłady są lokalne, istotne i odpowiednie dla wieku uczestników.

C. Przygotowanie techniczne

- Mam zarówno wersję online, jak i offline ćwiczenia.
- Wiem, z jakich urządzeń będą korzystać młodzi ludzie (telefon, tablet, komputer).
- Wybrałem narzędzia, które są dostępne, bezpieczne i łatwe w obsłudze.

Dofinansowane przez Unię Europejską

D. Integracja i dostępność

- Sprawdziłem, czy wszystkie materiały są zrozumiałe dla osób o różnym poziomie umiejętności czytania i pisania.
- Mam przykłady neutralne pod względem płci i wrażliwe kulturowo.
- Wziąłem pod uwagę uczestników o niskim poziomie umiejętności cyfrowych.

E. Ocena i informacje zwrotne

- Przygotowałem szybką ocenę (quiz, ankieta, pytanie do refleksji).
- Zbieram informacje zwrotne na koniec sesji.
- Mam plan dostosowania kolejnej sesji w oparciu o odpowiedzi młodzieży.

Jak zacząć wdrażać te zasady kro po kroku

Prosta i elastyczna ścieżka dla pracowników młodzieżowych.

Krok 1: Wybierz jeden temat związany z cyberbezpieczeństwem

Przykłady: phishing, cyberprzemoc, podszywanie się pod inne osoby, dezinformacja.

- Zacznij od czegoś małego. Nie próbuj uczyć wszystkiego naraz.

Krok 2: Dodaj umiejętności EI psujące do zagrożenia

Przykłady:

- Phishing – zarządzanie stresem + krytyczne myślenie
- Oszustwa – kontrola impulsów + sceptycyzm
- Cyberprzemoc - empatia + regulacja emocji
- Fałszywe profile - samoświadomość + ustalanie granic

Krok 3: Wybierz metodę mieszaną

Wybierz, co najmniej jedną metodę online i jedną offline:

- Online: quiz, pokój zagadek, mikrofilm, refleksja na czacie grupowym
- Offline: karty scenariuszowe, mapowanie emocji, odgrywanie ról

Dzięki temu sesja będzie interaktywna i integracyjna.

Krok 4: Stwórz moment refleksji nad EI

Nawet 1–2 minuty refleksji wzmacniają odporność emocjonalną:

Dofinansowane przez Unię Europejską

Przykłady:

- „Jak czułbyś się w tej sytuacji?”
- „Jakie emocje mogłyby zaciemnić twój osąd?”
- „Co powiedziałbyś przyjacielowi, który doświadcza tego?”

Krok 5: Zakończ praktycznym nawykiem

Przykłady:

- „Zanim zareagujesz, zatrzymaj się na chwilę”
- „Zanim zaufasz, sprawdź”
- „Zastanów się, zanim opublikujesz”
- „Sprawdź źródło”
- „Poproś o pomoc, jeśli coś wydaję się nieprawidłowe”

W ten sposób wiedza przekształca się w codzienne nawyki związane z higieną cyfrową.

Przygotowanie pracowników młodzieżowych do modułu 3

Moduł 3 wykorzysta wszystko, czego nauczyłeś się w module 2, i przekształci to w gotowe do użycia praktyki nauczania.

Moduł, 2 = CZEGO *uczyć*

- Związek między EI a cyberbezpieczeństwem
- Osiem głównych zagrożeń w online
- Filary i elementy ram
- Jak nauczanie mieszane wspiera zaangażowanie
- Praktyczne wytyczne dotyczące wdrażania

Moduł 3 = *JAK tego uczyć*

Będzie zawierał:

- Modele nauczania mieszanego sprzyjające integracji
- Szczegółowe szablony sesji
- Scenariusze zajęć (krok po kroku)
- Zestawy narzędzi do realizacji zajęć online/offline

Dofinansowane przez Unię Europejską

- Strategie Uniwersalnego Projektowania w Edukacji (UDL)
- Wytyczne dotyczące dostępności i adaptacji kulturowej

Moduł 3 to praktyczny podręcznik, który pozwala wykorzystać w praktyce wszystko, czego nauczyłeś się tutaj.

Końcowa motywacja dla pracowników młodzieżowych

Praca z młodymi ludźmi w środowisku cyfrowym może stanowić wyzwanie, ale ramy EM&M zostały opracowane, aby zapewnić wsparcie, a nie przytłoczyć.

Pamiętaj:

- Nie musisz być ekspertem w dziedzinie cyberbezpieczeństwa.
- Wystarczy, że połączysz emocje z zachowaniem w sieci.
- Spójność jest ważniejsza niż złożoność.
- Każda najmniejsza umiejętność, której nauczysz, zmniejsza podatność młodych ludzi na zagrożenia.
- Twoja rola jest kluczowa — młodzież ufa Ci bardziej niż jakimkolwiek narzędziom lub platformom internetowym.

Stosując ramy EM&M pomagasz młodym ludziom stać się:

- Bezpieczniejszymi,
- Bardziej odpornymi,
- Świadomymi emocjonalnie,
- Krytycznymi myślicielami,
- I odpowiedzialnymi obywatelami cyfrowymi.

Kształtujesz pokolenie, które potrafi poruszać się po cyfrowym świecie z pewnością siebie, empatią i inteligencją.

Dofinansowane przez Unię Europejską

Moduł 3 – Łączone metody nauczania i uczenia się mieszanego

Przegląd modułu

W czasach, gdy zaangażowanie młodzieży w świat cyfrowy, jej dobre samopoczucie emocjonalne i bezpieczeństwo w sieci coraz bardziej się ze sobą łączą, pracownicy młodzieżowi i trenerzy muszą szybko zacząć stosować podejście pedagogiczne, które łączy inteligencję emocjonalną (EI), świadomość cyberbezpieczeństwa i umiejętności cyfrowe. Ten moduł odpowiada na tę potrzebę, oferując oparte na teorii i praktyce ramy dla nauczania mieszanego, specjalnie dostosowane do pracy z młodzieżą.

W tym miejscu skupiamy się na ośmiu kluczowych obszarach ryzyka w Internecie:

1. Cyberprzestępcy
2. Fałszywe zaproszenia do grona znajomych i podszywanie się pod inne osoby
3. Publikowanie prywatnych informacji i wpisów, których później żałujemy
4. Phishing
5. Oszustwa (nagrody/wynagrodzenia/oparte na FOMO)
6. Cyberprzemoc
7. Brakujące informacje i fałszywe wiadomości
8. Przypadkowe pobieranie złośliwego oprogramowania

Moduł pokazuje, jak wykorzystać integracyjne, dostępne i oparte na inteligencji emocjonalnej nauczanie mieszane, aby pomóc młodym ludziom z różnych środowisk ekonomicznych, kulturowych, społeczno-cyfrowych i o różnych umiejętnościach w rozwijaniu odporności emocjonalnej, umiejętności cyfrowych i bezpieczniejszych zachowań w Internecie. Dzięki połączeniu technik opartych na inteligencji emocjonalnej (empatia, samoregulacja, refleksja emocjonalna) z praktycznymi narzędziami cyfrowymi, pracownicy młodzieżowi mogą projektować, realizować i oceniać sesje, które umożliwiają młodym ludziom rozpoznawanie zagrożeń w Internecie, reagowanie na nie i zapobieganie im.

Czym jest nauczanie mieszane w tym kontekście?

W tym przypadku nauczanie mieszane wykracza poza proste połączenie metod bezpośrednich i internetowych. Odnosi się ono do tworzenia wzajemnie powiązanych ekosystemów edukacyjnych, w których kompetencje emocjonalne, cyfrowe i obywatelskie wzajemnie się wzmacniają. Kluczowym

Dofinansowane przez Unię Europejską

elementem tego podejścia jest silne zaangażowanie na rzecz integracji, zapewniające wszystkim młodym ludziom – niezależnie od ich pochodzenia – możliwość znaczącego uczestnictwa i rozwijania umiejętności potrzebnych do odnoszenia sukcesów w środowisku cyfrowym.

Cel modułu 3

Moduł 3 zawiera praktyczne metody, narzędzia i strategie przekazywania tych treści w sposób, który jest:

- Integracyjny: dostosowany do różnych profili uczniów (np. młodzież wiejska, uczniowie z zaburzeniami neurologicznymi, uczniowie o niskiej umiejętności korzystania z technologii cyfrowych).
- Emocjonalnie inteligentne: oparte na zasadach inteligencji emocjonalnej (np. samoświadomość, empatia, samoregulacja).
- Mieszane: łączące podejście online i offline w celu zapewnienia maksymalnego zaangażowania i dostępności.
- Praktyczne: wyposażające pracowników młodzieżowych w gotowe do użycia ćwiczenia, szablony i narzędzia oceny.

Po ukończeniu tego modułu edukatorzy młodzieży zdobędą:

1. Solidne podstawy koncepcyjne

- Dogłębne zrozumienie integracyjnej pedagogiki mieszanej i jej roli w rozwijaniu odporności emocjonalnej, umiejętności cyfrowych i świadomości w zakresie cyberbezpieczeństwa.
- Wiedzy na temat związku między inteligencją emocjonalną (EI) a bezpieczeństwem w Internecie oraz znaczenia tego związku dla rozwoju młodzieży.
- Znajomość zasad Uniwersalnego Projektowania w Edukacji (UDL) oraz sposobu, w jaki zapewniają one dostępność i równość w środowiskach nauczania mieszanego.

2. Praktyczny zestaw narzędzi

- Metody i strategie projektowania angażujących emocjonalnie i cyfrowo sesji mieszanych.

Dofinansowane przez Unię Europejską

- Narzędzia cyfrowe (np. Moodle, Kahoot, Padlet, Canva) i alternatywne rozwiązania offline do tworzenia interaktywnych, integracyjnych i bezpiecznych doświadczeń edukacyjnych.
- Mikronaukowe działania, które można łatwo włączyć do istniejących programów dla młodzieży, zapewniając elastyczność i możliwość dostosowania.

3. Umiejętność projektowania, realizacja i oceny

- Umiejętności projektowania sesji mieszanych, które sprzyjają odporności emocjonalnej, bezpieczeństwu w Internecie, zaangażowaniu i poczuciu przynależności.
- Techniki przekazywania treści w sposób emocjonalnie inteligentny, integracyjny i dostosowany do różnych profili młodzieży.
- Narzędzia do oceny skuteczności sesji, w tym jakościowe i ilościowe miary integracyjności, dostępności i wpływu emocjonalnego.

Ramy koncepcyjne

Pedagogika mieszana w zakresie bezpieczeństwa w Internecie

W tym module nauczanie mieszane łączy **bogactwo społeczne interakcji osobistych z elastycznością przekazywania treści cyfrowych**, tworząc **holistyczny ekosystem nauczania**, który zajmuje się **ośmioma kluczowymi obszarami ryzyka w Internecie**. Według Garrison & Vaughan (2008) skuteczny projekt mieszany celowo integruje **doświadczenia online i bezpośrednie** w celu wzmocnienia **obecności społecznej, poznawczej i dydaktycznej**. W pracy z młodzieżą integracja ta pozwala na **ciągłą więź emocjonalną** – uczestnicy mogą kontynuować dyskusje na temat **cyberprzemocy, phishingu lub podszywania się** z sesji offline na **forach cyfrowych**, podtrzymując refleksję i zaangażowanie między spotkaniami.

Inteligencja emocjonalna (EI) i zagrożenia w Internecie

EI—zdolność do **rozpoznawania, rozumienia i zarządzania własnymi emocjami oraz emocjami innych osób** (Salovey & Mayer, 1990) – ma kluczowe znaczenie w tych ramach. Włączenie EI do nauczania mieszanego pomaga pracownikom młodzieżowym i uczniom **radzić sobie z frustracją, konfliktami i empatią** w interakcjach online.

Na przykład:

Dofinansowane przez Unię Europejską

- **Dyskusja oparta na EI** na temat **cyfrowej empatii** może przekształcić **przypadki cyberprzemocy** w okazje do rozwoju.
- **Techniki samoregulacji** mogą pomóc młodzieży **oprzeć się impulsywnym reakcjom** na **oszustwa, phishing lub czynniki wywołujące FOMO.**
- **Ćwiczenia empatii** mogą zmniejszyć prawdopodobieństwo **opublikowania treści, których można później żałować**, lub narażenia się na **próby podszywania się.**

Uniwersalny Projekt w Edukacji (UDL) w bezpieczeństwie cyfrowym

CAST (2018) definiuje UDL, jako projektowanie środowisk edukacyjnych, które **przewidują zmienność** poprzez zapewnienie **wielu sposobów zaangażowania, reprezentacji i wyrażania się**. W tym module UDL gwarantuje, że wszystkie materiały i działania są **dostępne i dostosowane** do różnych profili młodzieży, w tym osób z **ograniczonym dostępem do technologii cyfrowych, niepełnosprawnościami lub barierami językowymi**.

Przykłady obejmują:

- **Napisy i transkrypcje** filmów dotyczących **zapobiegania phishingowi lub złośliwemu oprogramowaniu**.
- **Arkusze robocze do wydrukowania** do zajęć offline dotyczących **zagrożeń dla prywatności lub fałszywych wiadomości**.
- **Alternatywne rozwiązania niskotechnologiczne** dla młodzieży **z obszarów wiejskich lub o niskich dochodach,** umożliwiające udział w dyskusjach na temat **cyberprzestępców lub oszustw**.

Włączenie społeczne i równość cyfrowa w edukacji dotyczącej bezpieczeństwa w Internecie

Integracyjne nauczanie mieszane rozwiązuje problem **przepaści cyfrowej**, oferując **zarówno opcje zaawansowane technologicznie, jak i proste**, zapewniając **równy udział** wszystkim młodym ludziom.

W tym module kładzie się nacisk na:

- **Przykłady istotne z kulturowego punktu widzenia** do dyskusji na temat **cyberprzemocy lub podszywania się pod inne osoby**.

Dofinansowane przez Unię Europejską

- **Język zrównoważony pod względem płci i neutralny** w ćwiczeniach dotyczących **zagrożeń dla prywatności lub nieodwracalnych wpisów**.
- **Elastyczne narzędzia** (np. Padlet, Kahoot, Moodle) dostosowane do **różnych poziomów umiejętności cyfrowych** podczas nauczania o **dezinformacji lub złośliwym oprogramowaniu**.

Słowa klucze: Nauczanie mieszane, inteligencja emocjonalna, projektowanie uniwersalne, równość cyfrowa, cyberprzemoc, phishing, oszustwa, podszywanie się, zagrożenia dla prywatności, fałszywe wiadomości, złośliwe oprogramowanie, integracja.

Model pedagogiczny

Model ten zapewnia **cykliczne, angażujące emocjonalnie i integracyjne** podejście do nauczania o **ośmiu obszarach zagrożeń internetowych**. Każda faza ma na celu **budowanie wiedzy, umiejętności i odporności emocjonalnej** u młodych ludzi.

Faza	Cel	Przykłady ćwiczeń	EI / skupienie cyfrowe
Połącz	Budowanie integracji, zaufania i bezpieczeństwa emocjonalnego	Przełamanie barier: „Podziel się sytuacją, w której czułeś się niebezpiecznie w Internecie – czy było to spowodowane **cyberprzemocą, oszustwem lub podszywaniem się**?”. Cyfrowa ściana imion dotycząca **zagrożeń dla prywatności** lub **fałszywych zaproszeń do grona znajomych**.	Empatia, samoświadomość i budowanie zaufania
Odkrywaj	Wprowadzenie pojęć i zagrożeń związanych z **ośmioma obszarami ryzyka w Internecie**	Krótki film o **działaniu phishingu** + ankieta na żywo:, „Jakie emocje mogą skłonić kogoś do kliknięcia podejrzanego linku?”. Dyskusja na temat **oszustw FOMO** lub **taktyk dezinformacyjnych.**	Ciekawość, świadomość i krytyczne myślenie

Dofinansowane przez Unię Europejską

Ćwicz	Wykorzystanie zdobytej wiedzy poprzez wspólne, praktyczne działania	Odgrywanie ról: Reagowanie na **cyberprzestępcę** lub **fałszywe zaproszenie do grona znajomych**. Symulacja:, „Co byś zrobił, gdybyś przypadkowo pobrał **złośliwe oprogramowanie**?”	Samoregulacja, podejmowanie decyzji i wsparcie rówieśników
Zastanów się	Analiza emocji, zachowań i wyników	Dzienniki: „Jak się czułeś podczas **symulacji phishingu**?” Mapowanie emocji związanych z **postami, których żałujesz** lub **incydentami cyberprzemocy**. Tablice Padlet:, „Co byś zrobił inaczej, gdybyś spotkał się z **oszustwem** lub **próbą podszywania się**?”	Umiejętność dostosowania się, krytyczna refleksja i odporność emocjonalna
Podziel się	Wspieranie wzajemnego uczenia się, przywództwa i zaangażowania społeczności	Prezentacje młodzieży: „Jak rozpoznać **fałszywe wiadomości** lub **wiadomości phishingowe**”. Prezentacje online: „Moja strategia **ochrony prywatności** i **bezpiecznego pobierania plików**”.	Umiejętności społeczne, sprawczość i mentoring rówieśniczy

Słowa klucze: Nauka przez doświadczenie, interakcja z rówieśnikami, budowanie zaufania, samokontrola, obywatelstwo cyfrowe, bezpieczeństwo w Internecie.

Łączenie: Budowanie zaufania i bezpieczeństwa emocjonalnego

Cel

Faza **Łączenie** koncentruje się na **budowaniu relacji, zaufania i bezpieczeństwa emocjonalnego** — podstawy skutecznego uczenia się. Młodzież musi czuć się **dostrzegana, wysłuchana i doceniana**, zanim zaangażuje się głęboko w treść, zwłaszcza, gdy porusza się delikatne tematy, takie jak **cyberprzemoc lub zagrożenia dla prywatności**.

Dofinansowane przez Unię Europejską

Kluczowe działania

- **Przełamanie barier i sprawdzanie:** Wykorzystaj ćwiczenia, które zachęcają młodzież do **dzielenia się emocjami, doświadczeniami i oczekiwaniami.** Przykład: „Dwie prawdy i jedno kłamstwo” (wersja cyfrowa: „Dwa fakty i jedna bajka” dotyczące doświadczeń online).
- **Umowy grupowe:** Wspólnie stwórzcie **zasady komunikacji opartej na szacunku** (np. „Słuchamy bez osądzania”, „Zachowujemy poufność osobistych historii”).
- **Różnorodna reprezentacja:** Upewnijcie się, że wszyscy młodzi ludzie widzą siebie w wykorzystywanych **treściach i przykładach** (np. studia przypadków przedstawiające różne kultury, umiejętności i płcie).

Rozwijanie umiejętności EI

- **Świadomość siebie:** Młodzież rozpoznaje swoje **emocje i uprzedzenia,** wchodząc w przestrzeń edukacyjną.
- **Empatia:** Młodzież ćwiczy **słuchanie i akceptowanie** doświadczeń rówieśników.
- **Przynależność:** Młodzież czuje się **związana z grupą**, co zmniejsza niepokój związany z uczestnictwem.

Przykład nauczania mieszanego

- **Online:** Wykorzystaj **ścianę Padlet**, na której młodzież umieszcza emoji i krótkie frazy przedstawiające ich uczucia dotyczące dzisiejszego tematu (np. cyberprzemoc).
- **Offline:** Następnie przeprowadź **dyskusję w kręgu**, podczas której młodzież omówi swoje posty.

Odkrywaj: Przedstawienie pojęć z ciekawością i krytycznym myśleniem

Cel

Faza **Odkrywaj** polega na **rozbudzaniu ciekawości** i **przedstawianiu kluczowych pojęć** w sposób, który zachęca do **krytycznego myślenia i**

Dofinansowane przez Unię Europejską

zaangażowania emocjonalnego. Młodzież jest zachęcana do **zadawania pytań, kwestionowania założeń i łączenia** nowych idei z własnym życiem.

Kluczowe działania

- **Prowokacyjne pytania:** Zacznij od pytań otwartych, takich, jak: „Co *sprawia, że ktoś jest podatny na oszustwa phishingowe?”* lub *„Jak Twoim zdaniem emocje wpływają na udostępnianie danych osobowych w Internecie?"*
- **Treści multimedialne:** Wykorzystaj **filmy, infografiki lub podcasty** do przedstawienie informacji w interesujący sposób. Przykład: krótki film na temat **„Jak oszuści manipulują emocjami”**, po którym następuje dyskusja.
- **Scenariusze z życia wzięte:** Przedstaw **studia przypadków lub wiadomości** dotyczące cyberzagrożeń (np. nastolatek, który dał się nabrać na fałszywe zaproszenie do grona znajomych).

Rozwijanie umiejętności EI

- **Ciekawość:** Młodzież staje się **wewnętrznie zmotywowana** do pogłębiania wiedzy.
- **Krytyczne myślenie:** Młodzież **analizuje i kwestionuje** informacje, zamiast przyjmować je bezkrytycznie.
- **Świadomość emocjonalna:** Młodzież dostrzega, jak **emocje wpływają na decyzje** (np. strach prowadzący do impulsywnych kliknięć).

Przykład nauczania mieszanego

- **Online:** Młodzież ogląda **film TED-Ed** na temat dezinformacji i zamieszcza **jedno** pytanie, które nasunęło im się podczas oglądania, we wspólnym dokumencie.
- **Offline:** młodzież w małych grupach **omawia swoje pytania** i zastanawia się nad sposobami weryfikacji informacji znalezionych w Internecie.

Praktyka: Stosowanie umiejętności w bezpieczny u wspierający sposób

Cel

W **fazie praktycznej** młodzież **wykorzystuje zdobytą wiedzę** w niskim ryzyku, sprzyjającym środowisku. Faza ta koncentruje się na **rozwoju umiejętności poprzez działania oparte na doświadczeniu i współpracy**, pomagając

Dofinansowane przez Unię Europejską

młodzieży **wewnętrznie przyswoić** strategie związane z inteligencją emocjonalną i bezpieczeństwem cyfrowym.

Kluczowe działania

- **Odgrywanie ról:** Symuluj **rzeczywiste dylematy związane z cyfrowym światem** (np. reagowanie na cyberprzemoc, wykrywanie wiadomości phishingowych). Przykład: *„Otrzymujesz wiadomość z informacją: „Kliknij ten link, bo inaczej Twoje konto zostanie usunięte". Co robisz?"*
- **Grywalizacja:** Wykorzystaj **quizy, pokoje zagadek lub symulacje**, aby utrwalić wiedzę. Przykład: **Gra Kahoot**, w której młodzież identyfikuje sygnały ostrzegawcze w fałszywych profilach w mediach społecznościowych.
- **Nauczanie rówieśnicze:** Młodzież **uczy się nawzajem** (np. jedna grupa wyjaśnia, jak skonfigurować ustawienia prywatności, a inna pokazuje, jak zgłaszać przypadki nękania).

Rozwijanie umiejętności EI

- **Samokontrola:** Młodzież ćwiczy **zatrzymywanie się i zastanawianie** przed podjęciem działania w Internecie.
- **Rozwiązywanie problemów:** Młodzież **opracowuje strategie** radzenia sobie z wyzwaniami cyfrowymi.
- **Współpraca:** Młodzież **współpracuje w celu rozwiązywania problemów**, rozwijając umiejętności społeczne.

Przykład nauczania mieszanego

- **Online:** Młodzież uczestniczy w **cyfrowym pokoju zagadek**, gdzie rozwiązuje zagadki związane z prywatnością w Internecie.
- **Offline:** Podsumowanie w formie **dyskusji grupowej** na temat tego, czego się nauczyli i jak wykorzystają tę wiedzę w praktyce.

Refleksja: Pogłębienie zrozumienia poprzez samoświadomość

Cel

Faza refleksji zachęca młodzież do **spojrzenia w głąb siebie i powiązania nauki z osobistymi doświadczeniami**. Refleksja pomaga młodzieży **wewnętrznie**

Dofinansowane przez Unię Europejską

przyswoić sobie lekcje, dostrzec postępy i zidentyfikować obszary wymagające dalszego rozwoju.

Kluczowe działania

- **Prowadzenie dziennika:** Młodzież zapisuje lub nagrywa **refleksje** na temat pytań takich jak:, „W jaki *sposób dzisiejsze zajęcia zmieniły Twoje podejście do dzielenia się informacjami w Internecie?”*
- **Wymiana doświadczeń w grupie:** Młodzież **dobrowolnie dzieli się spostrzeżeniami** w kręgu lub małej grupie.
- **Kreatywna ekspresja:** Młodzież tworzy **dzieła sztuki, wiersze lub memy**, aby przedstawić to, czego się nauczyła.

Rozwijanie umiejętności EI

- **Samorefleksja:** Młodzież **analizuje swoje zachowania i emocje**.
- **Nastawienie na rozwój:** Młodzież postrzega **błędy, jako okazje do nauki**.
- **Empatia:** Młodzież **bierze pod uwagę perspektywy** i doświadczenia innych osób.

Przykład nauczania mieszanego

- **Online:** Młodzież przesyła **krótką notatkę głosową lub pisemną refleksję** na platformę taką jak Flipgrid.
- **Offline:** Młodzież dzieli się swoimi przemyśleniami w parach **lub małych grupach**, pogłębiając dyskusję.

Udostępnij: Wzmacnianie procesu uczenia się przez społeczność

Cel

Faza Udostępnij koncentruje się na **wzmocnieniu głosu młodzieży** i **rozszerzeniu nauki poza grupę**. Młodzież **uczy innych, tworzy projekty publiczne lub promuje** bezpieczeństwo cyfrowe w swoich społecznościach, pogłębiając własną wiedzę i budując pewność siebie.

Kluczowe działania

- **Warsztaty prowadzone przez młodzież:** Młodzież **projektuje i prowadzi** mini-warsztaty dla rówieśników lub młodszych uczestników.
- **Kampanie cyfrowe:** Młodzież tworzy **reklamy społeczne, blogi lub posty na media społecznościowe** na temat bezpieczeństwa w sieci.

Dofinansowane przez Unię Europejską

- **Projekty społeczne:** Młodzież **współpracuje z miejscowymi organizacjami** (np. biblioteki, szkoły) w celu promowania umiejętności cyfrowych.

Rozwijanie umiejętności EI

- **Przywództwo:** Młodzież **bierze odpowiedzialność** za swoją naukę i pełni rolę mentorów dla innych.
- **Rzecznictwo:** Młodzież **wykorzystuje swój głos** do promowania bezpiecznych i odpowiedzialnych zachowań w sieci.
- **Pewność siebie:** Młodzież **czuje dumę** ze swojej zdolności do wprowadzania zmian.

Przykład nauczania mieszanego

- **Online:** Młodzież tworzy **filmik na TikTok lub post na Instagramie**, podsumowujący najważniejsze wnioski z modułu.
- **Offline:** Młodzież prezentuje swoje projekty podczas **wydarzenia społecznego lub apelu szkolnego**.

Cykliczność modelu

Pięć faz – **nawiązywanie kontaktów, odkrywanie, praktyka, refleksja, dzielenie się** – **nie ma charakteru liniowego**, lecz **cyklicznego**. Po dzieleniu się doświadczeniami młodzież często **powraca do fazy nawiązywania kontaktów** z większym zaufaniem i nowymi pytaniami, tworząc **ciągłą pętlę uczenia się i rozwoju**. Model ten gwarantuje, że młodzież **stopniowo rozwija umiejętności**, a **EI i kompetencje cyfrowe** wzajemnie się wzmacniają na każdym etapie.

Praktyczne wskazówki dla pracowników młodzieżowych

1. **Zacznij od małych kroków:** Rozpocznij od **jednej lub dwóch faz** i stopniowo wdrażaj pełny cykl.
2. **Bądź elastyczny:** Dostosuj model do **potrzeb swojej grupy** — niektórzy młodzi ludzie mogą potrzebować więcej czasu, aby nawiązać kontakt lub zastanowić się nad czymś.
3. **Daj przykład EI:** Pokaż młodym ludziom, jak **regulujesz swoje emocje, myślisz krytycznie i zastanawiasz się** — będą podążać za Twoim przykładem.

Dofinansowane przez Unię Europejską

4. **Celowo wykorzystuj technologię:** Wybierz narzędzia cyfrowe, które **zwiększają zaangażowanie**, nie przytłaczając młodzieży (np. Padlet do refleksji, Kahoot do ćwiczeń).
5. **Świętuj rozwój:** doceniaj **małe sukcesy** i postępy, a nie tylko ostateczne wyniki.

Wytyczne dotyczące wdrożenia

Wprowadzenie

W niniejszym rozdziale przedstawiono **praktyczne, szczegółowe wytyczne** dla pracowników młodzieżowych dotyczące **projektowania, prowadzenia i oceny** integracyjnych sesji nauczania mieszanego. Niezależnie od tego, czy uczysz **cyberbezpieczeństwa, inteligencji emocjonalnej (EI) czy umiejętności cyfrowych**, niniejsze wytyczne pomogą Ci stworzyć **angażujące, dostępne i skuteczne** doświadczenia edukacyjne dla różnorodnych grup młodzieży.

Projektowanie z myślą o integracji i dostępności

Aby zapewnić wszystkim młodym ludziom — niezależnie od pochodzenia, umiejętności lub dostępu do technologii cyfrowych — możliwość zapoznania się z **ośmioma obszarami ryzyka w Internecie**, należy wykonać następujące czynności:

- **Określenie potrzeb uczniów:** Ocena **poziomu dostępu uczestników do technologii cyfrowych, ich biegłości w posługiwaniu się technologią oraz potencjalnych barier** (np. język, niepełnosprawność lub status społeczno-ekonomiczny).
    - Przykład: dla młodzieży z **ograniczonym dostępem do technologii cyfrowych** należy zapewnić **materiały drukowane dotyczące phishingu, oszustw lub zagrożeń dla prywatności** wraz z zasobami cyfrowymi.
- **Zapewnij wiele sposobów zaangażowania:** wykorzystaj **Uniwersalne Projektowanie w Edukacji (UDL),** aby stworzyć **elastyczne, integracyjne zajęcia** dla każdego obszaru ryzyka:
    - **Cyberprzemoc:** zaproponuj **scenariusze odgrywania ról** (w przypadku sesji stacjonarnych) i **interaktywne fora** (w przypadku dyskusji online).

Dofinansowane przez Unię Europejską

- **Fałszywe wiadomości:** wykorzystaj **infografiki** (dla osób uczących się wzrokowo) i **podcasty audio** (dla osób uczących się słuchowo), aby wyjaśnić **taktyki dezinformacji**.
- **Podszywanie się:** uwzględnij **studia przypadku z życia wzięte** i **anonimowe symulacje czatów**, aby zbadać reakcje emocjonalne.

- **Treści dostosowane do kontekstu kulturowego i zrównoważone pod względem płci:** Upewnij się, że przykłady i scenariusze odzwierciedlają **różnorodne konteksty kulturowe i tożsamości płciowe,** aby dyskusje na temat **cyberprzestępców, oszustw lub żałosnych, których można żałować** były zrozumiałe i integracyjne.

Twórz przestrzenie bezpieczne emocjonalnie

Bezpieczeństwo emocjonalne ma kluczowe znaczenie podczas zajmowania się **wrażliwymi zagrożeniami internetowymi**, takimi jak **cyberprzemoc, podszywanie się pod inne osoby lub złośliwe oprogramowanie**. Skorzystaj z poniższych strategii:

- **Sprawdzanie stanu emocjonalnego:** Rozpocznij każdą sesję od **ćwiczenia sprawdzającego**, skupiającego się na omawianym **obszarze ryzyka**.
  - Przykład: „Jak się czujesz, udostępniając dane osobowe w Internecie?" (W przypadku **zagrożeń związanych z prywatnością**) lub „Czy kiedykolwiek czułeś się pod presją **oszustwa FOMO**?
- **Ustaw normy cyfrowego obywatelstwa:** Wspólnie stwórzcie **grupowe porozumienia** dotyczące szacunku, zgody i poufności
  - Przykład: „Zgadzamy się nie udostępniać bez zgody innych osób ich osobistych historii dotyczących **cyberprzemocy** lub **postów, których żałują**".
- **Możliwość rezygnacji i wsparcie następcze:** Zaproponuj **alternatywne zajęcia** dla uczestników, którzy nie czują się komfortowo z niektórymi tematami (np. **cyberprzestępcami** lub **złośliwym oprogramowaniem**).
  - Przykład: Zapewnij **prywatny dziennik refleksji** dla osób, które nie chcą rozmawiać o **oszustwach lub podszywaniu się** w grupie.

Dofinansowane przez Unię Europejską

Zintegruj mikronaukę z zagrożeniem w Internecie

Mikronauka dzieli złożone tematy na **krótkie, angażujące ćwiczenia** (5–10 minut), które skupiają się na **jednym obszarze ryzyka naraz**:

- **Phishing:**
  - **Ćwiczenie:** „Wykryj sygnały ostrzegawcze” – **10-minutowy quiz** polegający na identyfikowaniu podejrzanych elementów w wiadomościach e-mail lub innych wiadomościach.
  - **Narzędzie:** Kahoot lub Quizizz.
- **Oszustwa (oparte na FOMO):**
  - **Ćwiczenie:** „Test presji” – **krótki film** pokazujący, w jaki sposób oszuści wykorzystują poczucie pilności, a następnie **pytanie do dyskusji**:, „Jakie emocje wywołało to w Tobie?”
- **Fałszywe wiadomości:**
  - **Ćwiczenie:** „Fakt czy fikcja?” – **5-Minutowe wyzwanie** polegające na sprawdzeniu prawdziwości popularnego postu za pomocą **wyszukiwania obrazów** lub **wiarygodnych źródeł**.
- **Cyberprzemoc:**
  - **Ćwiczenie:** „Empatia w działanie” – **scenariusz odgrywania ról**, w którym uczestnicy ćwiczą reagowanie na wrogie wiadomości z empatią.
- **Narzędzia do mikronauki:**
  - **Moodle** (do quizów dotyczących **prywatności lub złośliwego oprogramowania**).
  - **Canva Docs** (do tworzenia **infografik dotyczących podszywania się lub oszustw**).
  - **Padlet** (do dzielenia się **osobistymi strategiami unikania żałowanych postów**).

Wybierz etyczne i dostępne narzędzia cyfrowe

Wybierz platformy zgodne z **normami dotyczącymi prywatności, dostępności i etyki**, aby uczyć o **ośmiu obszarach ryzyka**:

Dofinansowane przez Unię Europejską

Obszar ryzyka	Polecane narzędzia	Cel
Cyberprzemoc	Padlet, Jamboard, Miro	Wspólne dyskusje, anonimowe dzielenie się informacjami i mapowanie emocji.
Phishing/oszustwa	Kahoot, Quizizz, Moodle	Quizy w formie gry, żeby sprawdzić wiedzę o **czerwonych flagach** i **emocjonalnych wyzwalaczach**.
Fałszywe wiadomości/dezinformacja	Canva Docs, Google Slides	Tworzenie **przewodników weryfikujących fakty** lub **infografik** w celu obalenia mitów.
Ryzyko związane z prywatnością	Mentimeter, Google Forms	Ankiety refleksyjne:, „Jakich danych osobowych nigdy nie udostępniłbyś w Internecie?”
Podszywanie się	Zoom (z napisami), Flipgrid	Filmy z odgrywaniem ról lub dyskusje na temat **weryfikacji tożsamości** i **reakcji emocjonalnych**
Złośliwe oprogramowanie	Interaktywne symulacje (np. laboratoria cyberbezpieczeństwa)	Praktyczne ćwiczenia w zakresie **rozpoznawania złośliwych linków lub plików do pobrania**.
Wpisy, których żałują	Padlet, Reflection Journals	Dzielenie się **wyciągniętymi wnioskami** i **alternatywnymi działaniami** w przyjaznej atmosferze.
Cyberprzestępcy	Bezpieczne, moderowane fora (np. Teams)	Dyskusja na temat **bezpiecznych interakcji w Internecie** i **mechanizmów zgłaszania**.

Dofinansowane przez Unię Europejską

Ułatwienie zaangażowania hybrydowego

Połącz **warsztaty na żywo** z **asynchroniczną refleksją**, aby umożliwić młodzieży **przetworzenie emocji w prywatności** przed publiczną dyskusją:

- **Przykład dotyczący cyberprzemocy:**
  - **Warsztaty na żywo:** Odgrywanie ról w odpowiedzi na **wrogie wiadomości**.
  - **Asynchroniczna refleksja:** Pytanie do prywatnego dziennika: „Jak się czułeś podczas odgrywania ról? Co zrobiłbyś inaczej?”
- **Przykład dotyczący Phishingu/oszustw:**
  - **Warsztaty na żywo:** Analiza grupowa **podejrzanej wiadomości e-mail**.
  - **Asynchroniczna refleksja:** Wpis na Padlet:, „Jakich wskazówek nie zauważyłeś? Jak możesz to zastosować w prawdziwym życiu?”
- **Przykład dotyczący fałszywych wiadomości:**
  - **Warsztaty na żywo:** Debata na temat **wpływu dezinformacji**.
  - **Asynchroniczna refleksja:** Znajdź i udostępnij **artykuł zweryfikowany pod kątem faktów** na ten temat.

Kwestie etyczne związane z ochroną danych

- **Animizacja wrażliwych treści:** Usuń dane osobowe z **studium przypadków** dotyczących **cyberprzemocy lub niefortunnych wpisów**.
- **Bezpieczne platformy:** Korzystaj z **narzędzi zgodnych z RODO** (np. Moodle, Teams) do dyskusji na temat **zagrożeń dla prywatności lub podszywania się pod inne osoby**.
- **Zgoda i poufność:** Upewnij się, że uczestnicy rozumieją, **w jaki sposób ich dane** (np. wpisy do dziennika) będą wykorzystywane i chronione.

Najważniejsze wnioski dla pracowników młodzieżowych

1. **Planuj z celem:** Dostosuj każde działanie do **jasnych celów** i **umiejętności EI**.
2. **Projektuj dla wszystkich:** Korzystaj z UDL, aby zapewnić **dostępność i zaangażowanie.**

Dofinansowane przez Unię Europejską

3. **Mądrze wybieraj narzędzia:** Wybieraj **narzędzia cyfrowe i offline**, które usprawniają naukę, nie przytłaczając młodzieży.
4. **Facylitacja za pomocą EI:** Modeluj **świadomość emocjonalną** i stwórz **bezpieczne, wspierające środowisko**.
5. **Oceniaj i dostosowuj:** Wykorzystaj **informacje zwrotne i obserwacje**, aby udoskonalić swoje podejście.

Słowa klucze: Projektowanie inkluzywne, bezpieczeństwo emocjonalne, mikronauka, dostępność, narzędzia cyfrowe, zaangażowanie hybrydowe, UDL, prywatność, kwestie etyczne.

Ocena i refleksja

Inkluzywne nauczanie mieszane wymaga wielopoziomowej oceny wiedzy, umiejętności, postaw i odporności emocjonalnej związanych z ośmioma obszarami ryzyka online. Aby zmierzyć wpływ i udoskonalić praktykę, należy stosować następujące metody:

Ocena wiedzy i umiejętności

Oceń zrozumienie przez uczestników **ryzyka związanego z Internetem** oraz ich umiejętność stosowania **strategii EI i bezpieczeństwa cyfrowego**:

- **Testy przed i po szkoleniu:**
  - **Cyberprzemoc:** Quiz dotyczący **rozpoznawania wrogiej komunikacji** i **empatycznych reakcji**.
  - **Phishing/oszustwa:** Test umiejętności **rozpoznawania sygnałów ostrzegawczych** w wiadomościach e-mail lub innych wiadomościach.
  - **Fałszywe wiadomości:** Ćwiczenie polegające na sprawdzaniu faktów w celu **wykrycia dezinformacji**.
  - **Ryzyko związane z prywatnością:** Pytania oparte na scenariuszach dotyczące **bezpiecznego udostępniania danych osobowych**.
  - **Złośliwe oprogramowanie:** Rozpoznawanie **podejrzanych linków lub plików do pobrania**.
- **Demonstracja umiejętności:**

Dofinansowane przez Unię Europejską

- Odgrywanie ról w celu **reagowania na cyberprzestępców, podszywanie się pod inne osoby lub oszustwa FOMO**.
- Symulacje **zgłaszania cyberprzemocy lub nieodpowiednich postów**.

Dofinansowane przez Unię Europejską

Obserwacja zmian zachowań

Śledź **zmiany w zachowaniu i reakcjach emocjonalnych** podczas działań skupionych na **ośmiu obszarach ryzyka**:

Obszar ryzyka	Obserwacja	Narzędzia/metody
Cyberprzemoc	Empatia, łagodzenie napięć i wzajemne wsparcie podczas dyskusji.	Zajęcia grupowe, wzajemna ocena.
Phishing/oszustwa	Krytyczne myślenie i **samokontrola** w obliczu podejrzanych treści.	Ankiety na żywo, analiza scenariusza.
Fałszywe wiadomości	Umiejętność **kwestionowania źródeł** i unikania udostępniania niezweryfikowanych informacji.	Debaty, zadania związane z weryfikacją faktów.
Podszywanie się	Ostrożność i **świadomość emocjonalna** podczas weryfikacji tożsamości w Internecie.	Odgrywanie ról, dzienniki refleksji.
Ryzyko związane z prywatnością	**Podejmowanie decyzji** dotyczących udostępniania danych osobowych.	Studia przypadków, grupowe dyskusje.
Wpisy, których żałują	**Samorefleksja** na temat poprzednich postów i przyszłych zamiarów.	Wskazówki dotyczące dzienników, udostępnienie Padlet.
Złośliwe oprogramowanie	**Czujność** w identyfikowaniu i unikaniu złośliwych treści.	Interaktywne symulacje, quizy.
Cyberprzestępcy	**Asertywność** w wyznaczaniu granic i szukaniu pomocy.	Odgrywanie ról, analiza scenariusza.

Dofinansowane przez Unię Europejską

Analiza zaangażowania

Wykorzystaj **dane z platform cyfrowych**, aby ocenić udział i zaangażowanie w **treści dotyczące zagrożeń internetowych**:

- **Padlet/Kahoot:** Śledź odpowiedzi na **quizy dotyczące phishingu** lub **dyskusje na temat cyberprzemocy**.
- **Moodle/Teams:** Monitoruj ukończenie **modułów mikronauki** dotyczących **oszustw, fałszywych wiadomości lub prywatności**.
- **Mentimeter/Google Forms:** Analizuj **odpowiedzi dotyczące** emocji związane z **podszywaniem się lub złośliwym oprogramowaniem**.

Notatki refleksji i dzienniki

Zachęcaj do **cotygodniowych refleksji**, aby połączyć **emocje, działania i naukę** w **ośmiu obszarach ryzyka**:

- **Przykłady pytań:**
  - **Cyberprzemoc:** „Opisz sytuację, w której byłeś świadkiem lub doświadczyłeś cyberprzemocy. Jak się czułeś? Co byś teraz zrobił?”
  - **Phishing:**, „Jakie emocje mogą sprawić, że ktoś da się nabrać na oszustwo? Jak możesz wykorzystać samokontrolę, aby zachować bezpieczeństwo?”
  - **Fałszywe wiadomości:**, „W jaki sposób zweryfikowałeś informacje w tym tygodniu? Jakie wyzwania napotkałeś?”
  - **Ryzyko związane z prywatnością:**, „Jakich danych osobowych nie chciałbyś udostępniać? Dlaczego?”
  - **Złośliwe oprogramowanie:**, „Jakie kroki podejmujesz, aby uniknąć przypadkowego pobrania złośliwego oprogramowania? Jak się czujesz, gdy nie masz pewności, co do linku?”
- **Informacja zwrotna dla moderatora:** Przejrzyj dzienniki, aby **zidentyfikować powtarzające się czynniki wywołujące emocje** (np. strach, ciekawość) i odpowiednio **dostosować działania**.

Audyt integracji

Dofinansowane przez Unię Europejską

Skorzystaj z **listy kontrolnej**, aby ocenić **dostępność i integracyjność** działań dla wszystkich młodych ludzi:

Kryteria	Przykłady
Zgodność z UDL	Czy materiały dotyczące **phishingu lub oszustw** są dostępne w **różnych formatach** (tekstowym, audio, wizualnym)?
Znaczenie kulturowe	Czy przykłady odzwierciedlają **różnorodne doświadczenia** związane z **cyberprzemocą lub podszywaniem się**?
Dostępność cyfrowa	Czy w przypadku działań związanych z **złośliwym oprogramowaniem lub prywatnością** zapewniono **alternatywne rozwiązania o niskim stopniu zaawansowania technologicznego**?
Bezpieczeństwo emocjonalne	Czy w przypadku wrażliwych tematów, takich jak **cyberprzestępcy**, zaoferowano **możliwość rezygnacji**?
Przejrzystość języka	Czy język używany w dyskusjach na temat **nieodpowiednich postów lub fałszywych wiadomości** jest **neutralny i zrozumiały**?

Najważniejsze wnioski

1. **Ocena jest procesem ciągłym:** Wykorzystaj **ocenę formatywną i sumatywną**, aby kierować procesem uczenia się i mierzyć jego efekty.
2. **Refleksja pogłębia proces uczenia się:** Zachęcaj młodzież do **łączenia lekcji z własnym życiem** poprzez prowadzenie dziennika, dyskusje lub kreatywną ekspresję.
3. **Integracja ma znaczenie:** Regularnie sprawdzaj swoje sesje, aby upewnić się, że **wszyscy młodzi ludzie czują się integrowani i wspierani.**
4. **Dostosowuj się i ulepszaj:** Wykorzystaj informacje zwrotne, aby **udoskonalić swoje praktyki** i lepiej zaspokajać potrzeby młodzieży.

Pracownicy młodzieżowi powinni dawać przykład refleksji, prowadząc własny dziennik facylitacji – dokumentując nastrój emocjonalny, dynamikę grupy i ulepszenia na przyszłość. Dane z oceny są bezpośrednio wykorzystywane w ramach projektu EM&M w celu ciągłego doskonalenia.

Dofinansowane przez Unię Europejską

Słowa klucze: ocena formatywna, wskaźniki behawioralne, dzienniki refleksji, kontrola integracji, ciągłe doskonalenie.

Dofinansowane przez Unię Europejską

Moduł 4 – Ocena podatności online i ćwiczenia z rozpoznawania zagrożeń

Przegląd modułu

Moduł 4 wyposaża pracowników młodzieżowych i edukatorów w praktyczne narzędzia, oceny i ćwiczenia, które pomagają młodym ludziom identyfikować zagrożenia internetowe, rozumieć je i reagować na nie w sposób emocjonalnie inteligentny. Opiera się on na podstawach z modułu 1, przechodząc do praktycznych ćwiczeń, które łączą świadomość techniczną z umiejętnościami inteligencji emocjonalnej (EI). Nacisk kładziony jest na wzmacnianie odporności młodzieży, krytycznego myślenia i spokojnego podejmowania decyzji w obliczu zagrożeń cybernetycznych. Moduł ten zawiera ćwiczenia krok po kroku, gotowe do użycia narzędzia oceny oraz scenariuszowe doświadczenia edukacyjne, które łączą wrażliwość behawioralną i emocjonalną z konkretnymi strategiami zapobiegawczymi.

Kluczowym aspektem modułu 4 jest elastyczność: został on zaprojektowany z myślą o mieszanym przekazie w różnych kontekstach i infrastrukturach. Niezależnie od tego, czy pracownik młodzieżowy dysponuje zaawansowanym technologicznie laboratorium, czy tylko jednym smartfonem w centrum społecznościowym, ćwiczenia można dostosować (wiele z nich ma opcje mobilne lub opcje dla niskiej przepustowości). Wykorzystujemy również elementy grywalizacji i popularne platformy (takie jak Kahoot, Padlet lub Discord), aby dotrzeć do młodzieży tam, gdzie się znajduje, i sprawić, by nauka była angażująca. Moduł ten jest zgodny ze wspólną strukturą podręcznika i mieszanym podejściem dydaktycznym programu oraz zawiera wnioski z badania porównawczego dotyczącego zachowań młodzieży w cyberprzestrzeni.

Zasadniczo moduł 4 wykorzystuje informacje zawarte w module 1 (i innych wcześniejszych modułach) dotyczące, „czego" i „dlaczego" i przekształca je w „jak" – jak oceniać podatność na zagrożenia, jak szybko rozpoznawać zagrożenia i jak stosować reakcje oparte na inteligencji emocjonalnej. Ostatecznym celem jest promowanie profilaktycznych zachowań cyfrowych i struktur wsparcia rówieśniczego, które mogą zapewnić bezpieczne praktyki online w dłuższej perspektywie, nawet po zakończeniu formalnego szkolenia.

Cele nauczania

Po ukończeniu tego modułu pracownicy młodzieżowi i edukatorzy będą potrafili:

Dofinansowane przez Unię Europejską

- **Rozpoznawać** typowe zagrożenia internetowe dla młodzieży w wielu wymiarach: technicznym (np. przestarzałe oprogramowanie), behawioralnym (np. nadmierne udostępnianie informacji, impulsywne klikanie), emocjonalnym (np. reakcje na stres) i społecznym (np. presja rówieśników, ufność wobec nieznajomych).
- **Wdrażać** krótkie, przystępne samooceny w celu oceny narażenia młodych ludzi na ryzyko i poziomu ich świadomości. (Na przykład za pomocą listy kontrolnej lub quizu, aby sprawdzić, czy dana osoba ma skłonność do ufania nieznajomym w Internecie lub pomijania ustawień prywatności).
- **Ułatwić** ćwiczenia rozpoznawania zagrożeń, które łączą wykrywanie wskazówek technicznych (takich jak fałszywy adres URL lub podejrzany profil) z refleksją emocjonalną (zwracanie uwagi na to, jak czuli się podczas próby oszustwa) i regulacją (z wykorzystaniem technik EI w celu zachowania spokoju).
- **Zintegrować** strategie EI – takie jak zarządzanie stresem, zdolność adaptacji, empatia i spokojna komunikacja – z działaniami szkoleniowymi w zakresie cyberbezpieczeństwa. Zamiast uczyć świadomości cyberbezpieczeństwa i umiejętności emocjonalnych oddzielnie, należy je połączyć (np. nauczanie technik oddychania w trakcie symulacji phishingu).
- **Przeprowadzać** zróżnicowane, integracyjne i oparte na grach sesje, korzystając z narzędzi powszechnie preferowanych przez grupę docelową. Będziesz również w stanie dostosować te ćwiczenia do warunków słabej łączności. Na przykład, wiedząc, jak przeprowadzić „quiz" offline przy użyciu papieru i długopisu, jeśli Kahoot nie jest dostępny, lub jak dostosować odgrywanie ról dla małej nieformalnej grupy w porównaniu z klasą.
- **Promować** zachowania zapobiegawcze i wzajemne wsparcie w społecznościach młodzieżowych. Oznacza to zachęcanie do nawyków, takich jak regularne sprawdzanie prywatności, krytyczne myślenie przed udostępnieniem informacji, pomaganie znajomym w rozpoznawaniu oszustw oraz tworzenie kultury, w której młodzież przypomina sobie nawzajem o zachowaniu bezpieczeństwa (stając się razem „ludzką zaporą ogniową").

Dofinansowane przez Unię Europejską

Treść modułu

Zrozumienie podatności w sieci

W cyberbezpieczeństwie podatność to po prostu słaby punkt lub luka, którą może wykorzystać zagrożenie. Ten moduł rozszerza tę koncepcję, uwzględniając nie tylko słabe punkty techniczne, ale także czynniki ludzkie i emocjonalne. Przyglądamy się kategoriom podatności, takim jak:

- **Słabe punkty związane z technologią:** Słabe punkty sprzętu lub oprogramowania. Na przykład używanie przestarzałego oprogramowania, brak instalacji aktualizacji zabezpieczeń, słabe hasła, brak programu antywirusowego lub korzystanie z ustawień domyślnych. Są one jak „otwarte okna" w cyfrowym domu. Mogą one prowadzić do problemów, takich jak przypadkowe pobranie złośliwego oprogramowania, (jeśli system nie jest zaktualizowany) lub włamanie, ponieważ hasło jest łatwe do odgadnięcia.
- **Słabe punkty związane z zachowaniem:** Niebezpieczne nawyki lub zachowania w Internecie. Na przykład nadmierne udostępnianie danych osobowych (publiczne publikowanie numeru telefonu lub adresu lub udostępnianie intymnych zdjęć), impulsywne klikanie bez zastanowienia, akceptowanie zaproszeń do grona znajomych od nieznajomych lub używanie tego samego hasła wszędzie. Takie zachowania zwiększają ryzyko. Publikowanie prywatnych informacji, których później można żałować, jest klasyczną podatnością behawioralną, – gdy coś trafi do sieci, trudno to cofnąć i może zostać wykorzystane przeciwko Tobie (np. cyberprzemoc lub przestępcy seksualni zapisujący te informacje).
- **Słabe punkty związane z emocjami:** Sposoby, w jakie nasze uczucia mogą zmniejszyć nasze bezpieczeństwo w Internecie. Emocje wpływają na postrzeganie ryzyka; na przykład, jeśli ktoś czuje się samotny lub pragnie uznania, może być bardziej ufny wobec nieznajomego w Internecie (osoby o złych zamiarach często to wykorzystują, podając się za przyjaciela lub osobę zainteresowaną romantyczną relacją). Jeśli ktoś jest zły lub zdenerwowany, może zareagować, publikując coś agresywnego lub klikając złośliwy link złośliwie (nie myśląc jasno). Nawet pozytywne emocje, takie jak podekscytowanie, mogą stanowić słabość (nadmierne podekscytowanie „nagrodą" i nie zauważenie oszustwa).
- **Słabe punkty związane z relacjami społecznymi:** Pokrywają się one z zachowaniem i emocjami, ale dotyczą środowiska społecznego. Należą do nich presja rówieśników, zachowania stadne i zaufanie do

Dofinansowane przez Unię Europejską

społeczności internetowych. Na przykład, jeśli „wszyscy biorą udział w nowym, modnym wyzwaniu", nastolatek może zignorować ryzyko (złośliwe oprogramowanie lub kwestie prywatności) z powodu presji społecznej. Lub zaufać rekomendacji tylko, dlatego, że podzielił się nią przyjaciel, bez sprawdzania jej wiarygodności (w ten sposób rozprzestrzeniają się fałszywe informacje). Fałszywe zaproszenia do grona znajomych lub podszywanie się pod inne osoby to kolejny obszar podatności społecznej – młodzież może zaakceptować zaproszenie, ponieważ ma wspólnych znajomych, nie zdając sobie sprawy, że jest to fałszywy profil (prawdopodobnie cyberprzestępcy lub oszusta).

(Uwaga: W module 1 przedstawiliśmy pojęcie „podatności" w uproszczonej formie. Tutaj rozszerzamy je. Niektóre modele łączą podatność społeczną z behawioralną lub emocjonalną, ale uważamy, że warto omówić czynniki społeczne w sposób wyraźny, stąd osobne omówienie).

Jak emocje wpływają na ryzyko: Czysto techniczna kwestia może ulec pogorszeniu przez czynniki ludzkie – np. przestarzała aplikacja (techniczna) staje się problemem tylko wtedy, gdy ktoś kliknie złośliwy link (behawioralny), co zrobił z ciekawości lub strachu (emocjonalny).

Przykład: Nastolatka padła ofiarą uwodzenia w Internecie (przypadek przestępcy seksualnego). Analiza: Jej słabością społeczną było to, że zaufała osobie, która schlebiała jej na czacie w grze; słabością emocjonalną była jej niska samoocena (pragnęła komplementów); przestępca wykorzystał to, aby uzyskać jej prywatne zdjęcia (słabość behawioralna: udostępniła prywatne informacje). Nie było potrzeby stosowania zaawansowanych technik hakerskich – wystarczyła manipulacja emocjonalna.

Inny przykład: grupa uczniów rozpowszechniła fałszywy artykuł dotyczący zagrożenia zdrowia. Nie zweryfikowali go (podatność behawioralna: brak sprawdzenia źródeł), ponieważ wywołał on u nich niepokój i był popularny (czynniki emocjonalne + społeczne: strach i zachowanie stadne). Doprowadziło to do paniki, a niektórzy nawet kliknęli link w fałszywej wiadomości, który wykradł ich dane (w artykule znajdował się link phishingowy).

Jeszcze jedno: laptop studenta został zainfekowany wirusem po pobraniu darmowego pirackiego oprogramowania muzycznego (podatność techniczna: brak programu antywirusowego i pobieranie z niezaufanego źródła;

Dofinansowane przez Unię Europejską

behawioralna: chęć uzyskania darmowych rzeczy przeważyła nad ostrożnością; emocjonalna: być może podekscytowanie lub wpływ rówieśników, ponieważ przyjaciele również otrzymywali darmowe rzeczy).

Kluczowa kwestia: zrozumienie własnych słabości daje siłę, a nie powoduje wstyd. Każdy ma słabe punkty; identyfikując je, możemy podjąć działania (np. wzmocnić słaby punkt). I chociaż nie możemy wyeliminować wszystkich słabości (jesteśmy ludźmi, mamy emocje i popełniamy błędy), możemy budować świadomość, aby zmniejszyć stopień, w jakim nas one narażają.

Rozpoznawanie zagrożeń: od świadomości do działań

W tym miejscu łączymy typowe zagrożenia, na jakie narażona jest młodzież, z reakcjami psychologicznymi, które często wywołują te zagrożenia, oraz sposobami szkolenia młodzieży, aby przechodziła od początkowej świadomości zagrożenia do podjęcia odpowiednich działań.

Typowe zagrożenia dotyczące młodzieży:

- **Phishing:** Nieuczciwe próby kradzieży informacji (za pośrednictwem poczty elektronicznej, SMS-ów, prywatnych wiadomości). Obejmuje to takie rzeczy, jak fałszywe strony logowania, oszustwa związane z „resetowaniem hasła" lub fałszywe linki do nagród. Phishing jest bardzo powszechny i często dostosowany do zainteresowań młodzieży (np. darmowe skórki do gier, bilety na imprezy lub weryfikacje kont w mediach społecznościowych).
- **Fałszywe profile i podszywanie się:** Konta, które nie są tym, za co się podają. Może to być nieznajomy podszywający się pod rówieśnika, aby zdobyć zaufanie (czasami w celu wyłudzenia), osoba podszywająca się pod znaną osobę (np. fałszywe konto celebryty proszące o pieniądze na cele charytatywne) lub haker, który przejął konto prawdziwego przyjaciela. Prowadzi to do oszustw lub uwodzenia.
- **Cyberprzestępcy i uwodzenie:** Dorośli (lub czasami inni młodzi ludzie), którzy zaprzyjaźniają się z nieletnimi w Internecie, aby ich wykorzystać lub znęcać się nad nimi. Często używają fałszywych profili i manipulacji emocjonalnej (pochlebstwa, prezenty, empatia), aby z czasem zdobyć zaufanie ofiary. Jest to poważne zagrożenie mające wpływ na bezpieczeństwo emocjonalne i fizyczne.
- **Kradzież tożsamości i przejmowanie kont:** Kradzież danych osobowych lub przejmowanie kont. Młodzież może myśleć, że „nie ma tożsamości, którą można by ukraść", ale kradzież konta w grze lub konta społecznościowego również jest kradzieżą tożsamości. Ponadto, jeśli

Dofinansowane przez Unię Europejską

ponownie używają haseł, a jedno z nich zostanie ujawnione, atakujący mogą przejąć konta, a następnie oszukać ich znajomych lub zrujnować ich reputację.

- **Dezinformacja/fałszywa informacja:** Rozpowszechnianie fałszywych informacji, które mogą skłonić młodzież do podjęcia niebezpiecznych działań lub po prostu wywołać u nich niepokój lub złość. Na przykład fałszywe wiadomości o możliwości uzyskania stypendium, które w rzeczywistości są linkiem do oszustwa, lub plotki podżegające do znęcania się („Taki a taki zrobił coś strasznego...", podczas gdy nie jest to prawdą). Nauczanie młodzieży rozpoznawania brakującego kontekstu lub podejrzanych twierdzeń oraz weryfikowania wiadomości jest częścią rozpoznawania zagrożeń.
- **Cyberprzemoc i nękanie:**, Chociaż nie są to „zagrożenia techniczne", stanowią one powszechne niebezpieczeństwo dla młodzieży w Internecie. Nieprzyjemne wiadomości, publiczne poniżające posty, rozpowszechnianie plotek – zagrażają one emocjonalnemu dobrostanowi młodych ludzi i mogą prowadzić do niebezpiecznych wyborów (takich jak spotkanie się z agresorem w celu konfrontacji lub zemsty, co może spowodować jeszcze większe kłopoty.
- **Złośliwe oprogramowanie i „przypadkowe" pobieranie plików:** Sztuczki, które prowadzą młodzież do nieświadomego pobierania wirusów lub złośliwych aplikacji. Na przykład wyskakujące okienko z komunikatem „Twoje urządzenie jest zainfekowane, kliknij, aby je wyczyścić" (ironiczna sztuczka, która w rzeczywistości instaluje złośliwe oprogramowanie) lub bezpłatne pobieranie kodu do gry, który w rzeczywistości jest złośliwym oprogramowaniem. Młodzi ludzie nie zawsze potrafią rozpoznać oznaki fałszywej strony pobierania lub złośliwej aplikacji.
- **Oszustwa i nadużycia:** Oprócz phishingu, oszustwa związane z zakupami online (płatność za produkt, który nigdy nie dotarł), programy „szybkiego wzbogacenia się" skierowane do nastolatków (na przykład poprzez reklamy w mediach społecznościowych) lub oszustwa matrymonialne (starsze nastolatki mogą być celem ataków w aplikacjach lub na platformach randkowych, nie zdając sobie sprawy, że dana osoba jest fałszywa i chce wyłudzić pieniądze).

W przypadku każdego rodzaju zagrożenia należy wspomnieć o typowej reakcji emocjonalnej lub psychologicznej, którą próbuje ono wywołać:

- **Phishing** często wykorzystuje strach (problem z kontem) lub podekscytowanie (wygrałeś coś).

Dofinansowane przez Unię Europejską

- **Podszywanie się** wykorzystuje zaufanie i dezorientację (myślisz, że to twój przyjaciel lub ktoś wiarygodny).
- **Przestępcy** wykorzystują empatię, miłość i tajemnicę (sprawiają, że młodzież czuje się zrozumiana, wyjątkowa i mogą wzbudzać strach przed powiedzeniem o tym innym).
- **Dezinformacja** wykorzystuje silne emocje, takie jak gniew lub poczucie pilności (oburzenie czymś lub plotki oparte na strachu).
- **Cyberprzemoc** wywołuje ból, gniew lub wstyd.
- **Złośliwe oprogramowanie** może wywoływać strach (scareware „jesteś zainfekowany!") lub ciekawość („kliknij tutaj, aby zobaczyć niespodziankę"
- **Oszustwa** wykorzystują chciwość, podekscytowanie, a czasem współczucie (jak w przypadku fałszywych oszustw charytatywnych).

Reakcje psychologiczne na bodźce zagrażające: Ważne jest, aby omówić, w jaki sposób nasz mózg reaguje na te bodźce. Często jest to walka, ucieczka lub zamrożenie – lub, w kategoriach poznawczych, panika, zaprzeczenie lub impulsywność. Na przykład:

- **Strach/panika:** Alert phishingowy może wywołać panikę, a osoba pospiesznie postępuje zgodnie z instrukcjami (walczy z impulsem, aby szybko rozwiązać problem).
- **Zaprzeczenie/ignorowanie:** Niektórzy mogą dostrzec zagrożenie (np. wiadomość o epidemii wirusa) i zaprzeczyć jego istnieniu („to nie może być prawda"), co również może być niebezpieczne, jeśli zignorują uzasadnione ostrzeżenia. Albo uczeń może zignorować oznaki obecności drapieżnika, ponieważ nie chce, aby to była prawda.
- **Impulsywność:** Podekscytowanie lub złość mogą sprawić, że ktoś zacznie działać bez zastanowienia (kliknie link, wyśle złośliwą odpowiedź itp.) niemal automatycznie.
- **Przytłoczenie/paraliż**: Czasami zbyt wiele ostrzeżeń lub zagrożeń prowadzi do odrętwienia – młody człowiek może widzieć tak wiele „alarmów bezpieczeństwa", że po prostu je ignoruje, (co niektórzy oszuści wykorzystują, wysyłając wiele e-maili, aby osoba ta się poddała i kliknęła jeden z nich).

Celem jest spokojne przejście od świadomości do działania. Jak więc nauczyć młodzież, aby przechodziła od „wyczuwam zagrożenie" (lub jeszcze lepiej, dostrzegała oznaki zagrożenia, zanim w pełni się ono pojawi) do „będę działać (lub nie działać) w bezpieczny sposób"? Stosujemy profilaktykę opartą na inteligencji emocjonalnej: świadomość – refleksja – regulacja – reakcja (ten sam cykl z modułu 1, teraz w działaniu).

Dofinansowane przez Unię Europejską

W związku z tym, ucząc rozpoznawania zagrożeń:

1. Zacznij od uświadamiania sobie sygnałów ostrzegawczych: np. zauważenia, że adres URL jest dziwny, lub że „ta osoba jest zbyt miła zbyt szybko" lub „ta wiadomość zawiera wiele literówek". Ponadto, uświadom sobie swoje emocje: „Czuję, że denerwuję się tym komentarzem".
2. Następnie refleksja: przeanalizuj, dlaczego jest to zagrożenie lub dlaczego tak się czujesz. „To wydaje się podejrzane, bo dlaczego konkurs miałby wymagać wpłacenia pieniędzy? Serce mi wali, może, dlatego, że mnie to przeraża – może właśnie tego chcą".
3. Następnie regulacja: opanuj emocje (weź głęboki oddech, nie reaguj od razu, porozmawiaj z kimś). Zapobiega to popełnianiu pochopnych błędów.
4. Na koniec reakcja: podejmij działanie – może to być nieodpowiadanie na prowokację, a raczej zgłoszenie użytkownika, zweryfikowanie informacji w innym miejscu, użycie narzędzia technicznego (np. uruchomienie skanowania antywirusowego, zmiana hasła itp.) lub po prostu zablokowanie danej osoby.

Naucz młodzież pewnego rodzaju listy kontrolnej służącej rozpoznawaniu zagrożeń:

1. Zauważ – Czy coś jest nie tak lub próbuje wywołać u mnie emocje? (Jeśli tak, zatrzymaj się).
2. Pomyśl, – Jakiego rodzaju zagrożenie to może być? (Phishing, oszustwo, znęcanie się itp.) Czego ode mnie chcą?
3. Poczuj – Co czuję? Nazwij to (boję się/jestem podekscytowany/itp.), aby móc to kontrolować.
4. Oddychaj/uspokój się – poświęć chwilę, aby nie pozwolić, aby to uczucie przejęło kontrolę.
5. Zweryfikuj – jeśli to możliwe, sprawdź to inną metodą (nie ufaj ślepo treści wiadomości).
6. Działaj bezpiecznie – zdecyduj się zignorować, zablokować, poprosić o pomoc lub odpowiedzieć ostrożnie, jeśli to konieczne.

Dzięki powtarzającym się ćwiczeniom (takim jak te zawarte w zadaniach tego modułu) młodzież w idealnym przypadku wyrobi sobie nawyk, że gdy w Internecie wydarzy się coś dziwnego, domyślną reakcją będzie zatrzymanie się i analiza sytuacji, a nie ślepa reakcja. Analogia: podobnie jak w przypadku nauki defensywnej jazdy – uczy się kierowców rozpoznawania potencjalnych zagrożeń (dziecko na chodniku może wybiegnąć na jezdnię, samochód przed nami gwałtownie skręca) i reagowania na nie spokojnie (hamowanie, płynne

Dofinansowane przez Unię Europejską

skręcanie kierownicą) zamiast nie zwracania na nie uwagi lub reagowania zbyt gwałtownie.

Narzędzia do oceny podatności

W tej sekcji omówiono sposoby oceny aktualnej świadomości i nawyków młodzieży w zakresie bezpieczeństwa w Internecie – zasadniczo szybkie samooceny i diagnostykę – oraz sposoby wykorzystania tych wyników do pobudzenia refleksji i poprawy.

Projektowanie krótkich, przystępnych samoocen: Dostarczamy lub sugerujemy kwestionariusze, listy kontrolne lub quizy, które młodzież może wypełnić, aby dowiedzieć się, na jakim etapie znajduje się pod względem zachowań związanych z bezpieczeństwem w Internecie i gotowości emocjonalnej. Kluczowe cechy tych narzędzi:

- **Krótkie:** 5–10 pytań, aby nie stracić uwagi. Można je wypełnić w 5 minut.
- **Język przyjazny młodzieży:** brak żargonu w pytaniach. Na przykład zamiast „Czy codziennie stosujesz dobre praktyki w zakresie cyberhigieny?" zapytaj „Czy aktualizujesz swoje aplikacje i telefon, gdy pojawia się taka prośba?"
- **Obejmują aspekty techniczne, behawioralne i emocjonalne:** Na przykład pytania mogą obejmować: „Używam różnych haseł do różnych kont" (nawyk techniczny), „Często publikuję osobiste informacje w Internecie bez zastanowienia" (nawyk behawioralny), „Kiedy coś mnie denerwuje w Internecie, reaguję natychmiast" (nawyk emocjonalny), „Jeśli znajomy wysyła mi dziwny link, klikam go, ponieważ mu ufam" (nawyk społeczny/behawioralny).
- **Skala Likert lub format wielokrotnego wyboru:** Łatwiejszy dla młodzieży sposób udzielania odpowiedzi. Np. Prawie zawsze / Czasami / Rzadko / Nigdy – jak pokazano w Handout_M4 (załącznik 1). Jest to mniej onieśmielające niż pytania otwarte i zapewnia pewną miarę ilościową.
- **Korzystanie z narzędzi cyfrowych do anonimowych odpowiedzi:** Wielu młodych ludzi jest bardziej otwartych, gdy odpowiedzi są anonimowe. Proponujemy korzystanie z narzędzi takich jak Google Forms, Kahoot (tryb ankiety), Mentimeter, a nawet prostej ankiety na Discordzie/Telegramie, jeśli pracujesz z grupą online. Pozwalają one również na natychmiastowe agregowanie wyników. Jeśli nie masz dostępu do technologii, to samo można zrobić za pomocą karteczek papierowych zebranych w pudełku, aby zapewnić prywatność.

Dofinansowane przez Unię Europejską

- **Refleksja grupowa na temat wzorców:** Po samoocenie ważne jest, aby omówić ogólne wyniki (bez wytykania nikogo). Można na przykład powiedzieć: „Wygląda na to, że tylko 2 z 20 osób zawsze robią przerwę przed odpowiedzią na nieoczekiwane wiadomości – to coś, nad czym możemy popracować" lub „Wielu z was stwierdziło, że rzadko aktualizujecie swoje aplikacje; aktualizacje mogą usuwać luki w zabezpieczeniach, więc porozmawiajmy o tym, dlaczego aktualizacje są ważne".

Chodzi o to, aby znaleźć wzorce zachowań i emocji:

- Czy wielu młodych ludzi przyznaje się do działania pod wpływem emocji? W takim przypadku należy położyć nacisk na zarządzanie stresem.
- Czy niewielu młodych ludzi korzysta z ustawień prywatności lub 2FA? W takim przypadku można wdrożyć szybkie rozwiązania techniczne.
- Czy czują się komfortowo, prosząc o pomoc (czy zaznaczyli, że często proszą o pomoc, czy nie)? Jeśli nie, być może istnieje problem z zaufaniem lub brakiem wiedzy na temat tego, gdzie można uzyskać pomoc, – więc zajmujemy się tym.

Można stworzyć prosty wykres lub zestawienie odpowiedzi, aby to zwizualizować. Na przykład pytanie „Rozpoznaję, kiedy emocje są wykorzystywane, aby skłonić mnie do szybkiego działania", – jeśli większość odpowiedzi brzmi „Rzadko" lub „Nigdy", to najwyraźniej dana osoba potrzebuje praktyki w rozpoznawaniu manipulacji emocjonalnej.

Narzędzia te nie służą do oceniania ani zawstydzania kogokolwiek, ale do zapewnienia punktu odniesienia i spersonalizowanego wglądu. Podkreśl: „To nie jest test. Nie ma ocen. Ma to na celu skłonienie cię do zastanowienia się nad tym, co robisz teraz, abyś mógł zdecydować, czy chcesz coś zmienić w przyszłości". Zamienia to abstrakcyjne porady w coś bardziej konkretnego: „Och, odpowiedziałem „nigdy" na pytanie o aktualizowanie telefonu – to ryzyko, którego nie zdawałem sobie sprawy".

Często samo wypełnienie quizu skłania do autorefleksji: „O rany, odpowiedziałem, że często klikam bez zastanowienia – może powinienem to zmienić". Jako nauczyciel możesz to wykorzystać, zachęcając uczniów do wyznaczenia sobie mikro celu.

Zachęć uczniów do podzielenia się wynikami w parach lub małych grupach, (jeśli czują się z tym komfortowo): „Czy coś w waszych odpowiedziach was

Dofinansowane przez Unię Europejską

zaskoczyło?" lub „Jaka jest jedna rzecz, którą według was robicie dobrze, a jaka jest jedna rzecz, którą moglibyście poprawić?". Ta dyskusja między rówieśnikami uświadamia wszystkim, że każdy ma kilka odpowiedzi „rzadko" – nikt nie jest idealny, – ale każdy może wybrać coś, w czym chce się poprawić.

Grywalizacja i nauka oparta na scenariuszach

W tej sekcji wyjaśniono, dlaczego używamy gier i scenariuszy oraz jak połączyć je z elementami nauki emocjonalnej.

Dlaczego grywalizacja zwiększa retencję wiedzy: Grywalizacja oznacza wykorzystanie elementów gry (punkty, rywalizacja, wyzwania, nagrody) w celu uczynienia nauki zabawną i angażującą. W przypadku cyberbezpieczeństwa, dziedziny, która może być nudna lub przerażająca, gry sprawiają, że staje się ona przystępna. Młodzież jest przyzwyczajona do grania w gry, więc gdy dobrze się bawi, wzrasta jej uwaga i retencja wiedzy. Quiz z tabelą wyników (np. Kahoot) może sprawić, że będą chcieli poznać prawidłowe odpowiedzi dotyczące phishingu. Wyzwanie „znajdź flagę" może zmotywować ich do nauczenia się sztuczki bezpieczeństwa, aby wygrać. Badania wykazały, że dobrze zaprojektowane gry dotyczące cyberbezpieczeństwa poprawiają wyniki nauczania, ponieważ uczestnicy są zanurzeni w doświadczeniach, a nie tylko w wykładach.

Ważne: gamifikacja nie powinna przesłaniać celów edukacyjnych. Jest to środek do osiągnięcia celu. Wykorzystujemy ją, aby wzbudzić zainteresowanie i zachęcić do udziału, zwłaszcza w przypadku tematów takich jak bezpieczne zachowanie w Internecie, które w innym przypadku mogą brzmieć moralizatorsko.

Nauka emocjonalna poprzez odgrywanie ról i rozwiązywanie problemów: Nauka oparta na scenariuszach (np. odgrywanie ról, studia przypadków, symulacje) jest skuteczna, ponieważ stawia młodzież w sytuacji, w której może zastosować swoje umiejętności. Jest to nauka poprzez działanie. Dodanie odgrywania ról pozwala im w szczególności poczuć niektóre emocje w kontrolowanym środowisku. Na przykład odgrywanie roli rówieśnika naciskającego na innego, aby podzielił się hasłem, może wywołać uczucie dyskomfortu i pokazać im, jak trudne może to być, ale także pozwolić im przećwiczyć odmowę. Buduje to odporność emocjonalną na rzeczywiste sytuacje.

Włączamy inteligencje emocjonalną poprzez:

Dofinansowane przez Unię Europejską

- Omówienie nie tylko „tego, co się wydarzyło” w scenariuszu, ale także, „jakie to było uczucie?” I „jak sobie z tym uczuciem poradziłeś?”
- Zachęcanie do empatii w grach: np. w scenariuszu dotyczącym cyberprzemocy, gdy ktoś wciela się w rolę ofiary, a ktoś inny w rolę sprawcy, można zwiększyć empatię podczas późniejszej dyskusji.
- Zachęcanie do rozwiązywania problemów zespołowych w grach: np. grupowa łamigłówka polegająca na znalezieniu wszystkich sygnałów ostrzegawczych w fałszywym profilu skłania uczestników do rozmowy i wspólnego radzenia sobie z niewielkim stresem lub presją czasu, co pozwala rozwijać umiejętności społeczno-emocjonalne, takie jak komunikacja i praca zespołowa.

Integracja z platformami:

- **Genially lub Canva:** Można je wykorzystać do tworzenia interaktywnych treści lub cyfrowych łamigłówek związanych z cyberbezpieczeństwem (np. serii wskazówek i zamków, które można otworzyć za pomocą wiedzy z zakresu cyberbezpieczeństwa).
- **Padlet:** Doskonałe narzędzie do wspólnego burzy mózgów lub publikowania odpowiedzi w formie gry (np. cyfrowa galeria pomysłów).
- **Moodle:**, Jeśli dostępne jest formalne środowisko edukacyjne, istnieją formaty lekcji oparte na grach lub moduły quizów.
- **Discord:** Wielu młodych ludzi korzysta z Discorda; można na nim organizować quizy (za pomocą botów) lub po prostu prowadzić dyskusje na temat scenariuszy, a nawet „symulacje” w czasie rzeczywistym (np. symulować atak phishingowy za pomocą wiadomości Discord, aby w bezpieczny sposób zobaczyć reakcje).
- **Kahoot/Mentimeter/Quizizz:** Do quizów, ankiet, interaktywnych pytań z elementami rywalizacji.
- **Canva/Genially do gier fabularnych:** Można stworzyć historię typu „wybierz własną przygodę”, w której wybory prowadzą do różnych rezultatów (dobrze, jeśli pozwala na to technologia).
- **Creately lub Miro:** Do gier polegających na tworzeniu map myśli lub mapowania podatności.

Warto również zwrócić uwagę na adaptacje wykorzystujące proste technologie:, jeśli nie dysponujesz żadnymi urządzeniami, nadal możesz zastosować gamifikację, używając drukowanych kart, organizując konkursy na najszybsze sortowanie kart lub przekształcając scenariusze w gry planszowe itp. (Zostało to szczegółowo opisane w następnej sekcji, ale warto o tym wspomnieć już tutaj).

Dofinansowane przez Unię Europejską

Łączenie wyzwań związanych z cyberbezpieczeństwem z czynnikami wyzwalającymi inteligencję emocjonalną: Projektując scenariusze gier, celowo uwzględnij elementy emocjonalne:

- Quiz z limitem czasowym wywołuje presję (jak sobie z tym radzą? Omów to).
- Odgrywanie ról może wymagać od kogoś okazywania gniewu lub błagania (wywołuje empatię lub niepokój).
- Gra zespołowa może wiązać się z rywalizacją (wywołuje podekscytowanie lub stres).

Po każdym z nich lub w trakcie ich trwania zatrzymaj się, aby zastanowić się:, Jakie wywołało to w Tobie uczucia? Czy ktoś czuł się pospieszany lub sfrustrowany? To podobna sytuacja do tej w prawdziwym życiu – jak sobie z nią radzimy? Na przykład podczas symulacji „cyberincydentu pod presją" możesz zauważyć, że zespoły są zdezorientowane – później zwróć uwagę: „Zauważcie, jak odliczanie wywołało u Was niepokój – właśnie tego oczekują atakujący. Jakie strategie pomogły zachować spokój?".

W ten sposób zapewniasz, że emocjonalna strona nie zostanie zagubiona w emocjach. Młodzież uczy się nie tylko umiejętności technicznych (rozpoznawanie fałszywych adresów URL), ale także umiejętności emocjonalnych (zachowanie spokoju, nawet, jeśli zegar tyka lub ktoś krzyczy).

Wytyczne dotyczące realizacji programu w formie mieszanej

W tej części przedstawiono praktyczne porady dotyczące realizacji powyższej treści w różnych warunkach, zapewniające integrację i zaangażowanie niezależnie od dostępnych zasobów.

Równowaga między elementami online i offline: Idealna kombinacja może się różnić, ale podejście mieszane może obejmować, powiedzmy, 50% dyskusji/ćwiczeń w formie bezpośredniej i 50% narzędzi online. Elementy online (takie jak quiz Kahoot lub cyfrowe poszukiwanie skarbów) świetnie nadają się do angażowania wizualnego i skalowalności; elementy offline (takie jak dyskusja w kręgu lub fizyczna gra fabularna) świetnie nadają się do nawiązywania osobistych relacji i w środowiskach o niskim poziomie zaawansowania technologicznego.

Przykładowy stosunek może wyglądać następująco: zacznij od przełamania barier offline, następnie quiz online, następnie odgrywanie ról offline, a na koniec wspólna refleksja online na Padlet.

Dofinansowane przez Unię Europejską

Jeśli łączność stanowi problem, zaplanuj rezerwowe rozwiązanie low-tech dla każdego działania online. Na przykład, jeśli Kahoot nie działa, wydrukuj quiz lub po prostu przeczytaj pytania na głos i poproś zespoły o podniesienie rąk lub udzielenie pisemnych odpowiedzi. Jeśli nie ma dostępu do formularza online, zadaj pytania ustnie lub na papierze.

Z drugiej strony, jeśli mamy do czynienia z sytuacją lockdownu lub pracy zdalnej, upewnij się, że każdy pomysł offline ma swój odpowiednik online: np. odgrywanie ról można przeprowadzić za pomocą Zoom breakouts, a mapy podatności można narysować na wspólnej tablicy Miro.

Zarządzanie zaangażowaniem w środowiskach o słabej łączności:

Kilka wskazówek:

- Jeśli nie można polegać na łączności internetowej, należy wcześniej pobrać lub wydrukować materiały (zrzuty ekranu z przykładami phishingu itp..
- Jeśli nie ma dostępu do Internetu, ale są telefony, należy skorzystać z rozwiązań opartych na wiadomościach SMS lub czacie (na przykład quiz można przeprowadzić za pomocą ankiety SMS-owej lub po prostu wysyłając odpowiedzi SMS-em do moderatora).
- Wykorzystaj bardziej opowiadanie historii i wyobraźnię, gdy nie możesz pokazać filmów lub efektownych treści. Dobrze opowiedziana historia z sytuacją, z którą można się utożsamić, może przyciągnąć uwagę odbiorców bez użycia technologii.
- Zachęcaj do odgrywania ról i dyskusji, które nie wymagają żadnej technologii, ale są bardzo angażujące i interaktywne
- Ogranicz wykorzystanie technologii do minimum (np. offline PowerPoint lub jeden telefon z danymi, który może załadować kilka stron, które następnie opisujesz innym).

Wspieranie integracji w grupach mieszanych: Możesz mieć do czynienia z młodzieżą o różnym pochodzeniu (mieszkańcy miast vs mieszkańcy wsi, różne płcie, różne poziomy umiejętności):

- Unikaj założeń. Nie zakładaj, że wszyscy znają określone aplikacje lub mają takie same doświadczenia. W razie potrzeby wyjaśnij i zdefiniuj terminy. Na przykład niektórzy mogą nie korzystać z Instagrama, ale używać TikToka – staraj się używać przykładów z wielu platform.
- Kwestie związane z płcią: pamiętaj, że w niektórych kontekstach dziewczęta mogą doświadczać pewnych zagrożeń (takich jak

Dofinansowane przez Unię Europejską

przestępcy seksualni lub molestowanie) inaczej niż chłopcy lub odwrotnie (chłopcy mogą nie zgłaszać przypadków znęcania się ze względu na piętno społeczne itp.). Upewnij się, że przykłady obejmują różne perspektywy (np. wspomnij, że każdy może paść ofiarą oszustwa lub przestępcy seksualnego; nie przedstawiaj tego, jako zagrożenia dotyczącego tylko jednej płci).

- Zachęcaj wszystkich do dzielenia się, ale szanuj też tych, którzy są cisi. Wykorzystaj dyskusje w małych grupach, aby każdy mógł zabrać głos. Czasami osoby z mniej uprzywilejowanych środowisk mogą się wahać; mniejsze grupy sprawiają, że czują się bezpieczniej.
- Jeśli istnieje duża różnica w umiejętnościach (niektórzy są bardzo obeznani z technologią, inni w ogóle), rozważ połączenie ich w zespoły o zróżnicowanych umiejętnościach, aby mogli uczyć się od siebie nawzajem. Osoby bardziej biegłe mogą wykazać się w wykrywaniu problemów technicznych, podczas gdy osoby mniej biegłe mogą zaoferować świeże spojrzenie lub zadawać pytania, które prowadzą do ważnych wyjaśnień.
- Zapewnij alternatywne sposoby uczestnictwa: pisanie, rysowanie, mówienie – nie tylko jeden. Na przykład w ćwiczeniu „wykryj ryzyko" osoba, która nie czuje się komfortowo wypowiadając się, może zakreślić pewne elementy na wydruku.

Dostosowanie ćwiczeń do kontekstu:, Jeśli jesteś w szkole, a nie w ośrodku pomocy społecznej lub bibliotece, weź pod uwagę:

- Ograniczenia czasowe: w szkole lekcje mogą być krótkie, więc wybierz lub podziel ćwiczenia odpowiednio do tego. Podczas warsztatów możesz mieć więcej czasu, więc możesz połączyć kilka ćwiczeń lub pogłębić temat.
- Formalne vs nieformalne: W formalnych salach lekcyjnych może być konieczne dostosowanie się do programu nauczania lub uzyskanie określonych zgód. W nieformalnych warunkach można być bardziej elastycznym lub kreatywnym.
- Kontekst kulturowy: Niektóre tematy (takie jak dyskusja na temat przestępców seksualnych lub niektórych przykładów oszustw) mogą być drażliwe w niektórych kulturach. Dostosuj scenariusze, aby były odpowiednie i adekwatne do danej kultury. Na przykład, można położyć nacisk na oszustwa związane z popularnymi lokalnymi aplikacjami lub przykładami w lokalnym języku.
- Przestrzeń fizyczna:, Jeśli dysponujesz dużą salą, możesz przeprowadzić gry ruchowe (np. umieścić w rogach sali tabliczki z

Dofinansowane przez Unię Europejską

napisami „Prawda” i „Fałsz” i poprosić młodzież, aby do nich podeszła). Jeśli przestrzeń jest ograniczona, przeprowadź zajęcia w pozycji siedzącej lub w małych grupach przy stołach.

Ostatecznie, niezależnie od sposobu realizacji, najważniejsze jest zaangażowanie młodzieży, pobudzenie jej do myślenia, odczuwania i działania. Treść jest skuteczna tylko wtedy, gdy młodzież aktywnie uczestniczy w zajęciach, a nie biernie ich słucha.

Dofinansowane przez
Unię Europejską

Moduł 5 – Moja rola, jako ambasadora młodzieży ds. kultury bezpieczeństwa

Przegląd modułu

Moduł ten zawiera informacje na temat tego, w jaki sposób pracownicy młodzieżowi mogą pełnić rolę ambasadorów kultury bezpieczeństwa, edukując i wspierając młodych ludzi w rozwijaniu świadomych, emocjonalnie inteligentnych i odpowiedzialnych zachowań w sieci. Pełniąc rolę ambasadorów, pracownicy młodzieżowi są wiarygodnymi posłańcami, którzy budują zaufanie, kierują młodych ludzi ku bezpiecznym praktykom w sieci i zabiegają o to, by ich głos był słyszalny w sprawach dotyczących ich aktywności w siec.

Kultura bezpieczeństwa wykracza poza ochronę techniczną lub zapobieganie ryzyku. Polega ona na kultywowaniu wspólnych wartości, codziennych nawyków i norm społecznych, które promują zaufanie, szacunek, empatię i zbiorową odpowiedzialność w przestrzeni cyfrowej. Pracownicy młodzieżowi odgrywają kluczową rolę w przekładaniu tych wartości na praktykę, pomagając młodym ludziom rozpoznawać zagrożenia, zarządzać emocjami i podejmować świadome decyzje podczas interakcji w Internecie.

Po odpowiednim przeszkoleniu i wsparciu pracownicy młodzieżowi pełniący rolę ambasadorów są w stanie:

Wzorcowo prezentować bezpieczne i etyczne nawyki cyfrowe, które młodzi ludzie mogą wykorzystywać w codziennych interakcjach.

Opracowywać i realizować mikro kampanie, warsztaty i sesje wzajemnego uczenia się, które zwiększają świadomość na temat zagrożeń internetowych i dobrego samopoczucia emocjonalnego.

Zapewniać dokładne zasoby, aby pomóc młodym ludziom uzyskać dostęp do profesjonalnego lub społecznego wsparcia w przypadku pojawienia się trudności.

Pośredniczyć w konfliktach internetowych, wykorzystując umiejętności z zakresu inteligencji emocjonalnej, takie jak samokontrola, empatia i asertywna komunikacja.

Oprócz roli edukacyjnej, pracownicy młodzieżowi pełnią funkcję rzeczników i budowniczych mostów między młodymi ludźmi a szerszą społecznością. Reprezentują oni perspektywę młodzieży w dialogu z instytucjami, organizacjami pozarządowymi i decydentami w różnych kwestiach, w tym w

Dofinansowane przez Unię Europejską

zakresie integracji cyfrowej, zdrowia psychicznego, zrównoważonego rozwoju i zaangażowania obywatelskiego.

Moduł oferuje praktyczne metody, przykłady i narzędzia, które umożliwiają pracownikom młodzieżowym włączenie tego ambasadorskiego podejścia do swojej codziennej pracy. Wspiera je w projektowaniu działań partycypacyjnych, mentorowaniu młodych liderów oraz promowaniu kultury bezpieczeństwa, empatii i wspólnej odpowiedzialności w przestrzeni online i offline.

Cele nauczania

Po ukończeniu tego modułu pracownicy młodzieżowi będą potrafili:

1. Rozumieć i stosować zasady kultury bezpieczeństwa, promując wśród młodych ludzi bezpieczne, odpowiedzialne i empatyczne zachowania w sieci.
2. Przyjąć rolę ambasadorów, służąc, jako wzór do naśladowania, demonstrując bezpieczne nawyki cyfrowe i inteligencję emocjonalną w interakcjach online.
3. Edukować i wspierać młodych ludzi w podejmowaniu świadomych decyzji dotyczących korzystania z technologii cyfrowych, rozpoznawaniu zagrożeń i konstruktywnym reagowaniu na wyzwania związane z Internetem.
4. Opracowywać i wdrażać inicjatywy podnoszące świadomość, takie jak warsztaty, kampanie i sesje wzajemnego uczenia się, które promują wspólną kulturę bezpieczeństwa w Internecie.
5. Zapewniać wskazówki i mediację w konfliktach, gdy młodzi ludzie stają przed dylematami cyfrowymi, wykorzystując empatię, samoregulację i asertywne komunikowanie się.
6. Pełnić rolę rzeczników i budowniczych mostów, wzmacniając głos młodzieży i łącząc ją z instytucjami i interesariuszami w celu wzmocnienia integracyjnych, zrównoważonych i odpornych społeczności cyfrowych.

Treść modułu

Zrozumienie kultury bezpieczeństwa

W ramach EM&M kultura bezpieczeństwa wykracza poza cyberbezpieczeństwo lub ochronę danych. Jest to wspólny zestaw wartości,

Dofinansowane przez Unię Europejską

postaw i zachowań, które promują bezpieczeństwo emocjonalne, odpowiedzialność etyczną i zbiorowe zaufanie w środowiskach cyfrowych. Łączy w sobie świadomość techniczną (wiedza o tym, jak zachować bezpieczeństwo w Internecie) z inteligencją emocjonalną i społeczną (wiedza o tym, jak reagować, nawiązywać kontakty i świadomie wspierać innych).

Pracownik młodzieżowy promujący kulturę bezpieczeństwa wspiera młodych ludzi w:

- Rozpoznawaniu zagrożeń cyfrowych i czynników wywołujących emocje.
- Budowaniu odporności na manipulację, dezinformację i wrogość w Internecie.
- Wykorzystywaniu empatii i samoświadomości do kierowania swoimi działaniami w Internecie.
- Zrozumieniu, że bezpieczeństwo emocjonalne jest częścią bezpieczeństwa cyfrowego.

Kultura bezpieczeństwa reprezentuje, zatem sposób myślenia społeczności: ochronę siebie i innych poprzez szacunek, odpowiedzialność i aktywną troskę w świecie cyfrowym.

Wskazówka: Zaproś młodych ludzi do wspólnego zaprojektowania krótkiego „plakatu cyfrowej życzliwości" zawierającego pięć zasad bezpiecznego i pełnego szacunku zachowania w sieci. Wyeksponuj go w swojej przestrzeni młodzieżowej lub w mediach społecznościowych, aby promować zbiorową odpowiedzialność.

Rola pracownika młodzieżowego, jako ambasadora

Pracownicy młodzieżowi to nie tylko wychowawcy; są oni mentorami, liderami i rzecznikami, którzy wpływają na to, jak młodzi ludzie postrzegają świat cyfrowy i angażują się w niego. Pełniąc rolę ambasadorów, stają się wiarygodnymi posłańcami, cieszącymi się zaufaniem młodzieży i uznaniem społeczności za swoje zaangażowanie na rzecz cyfrowego dobrostanu.

- Dawanie przykładu

Pracownicy młodzieżowi wykazują się uczciwością i samoświadomością w interakcjach cyfrowych. Ich zachowanie, zarówno w sieci, jak i poza nią, stanowi wzór odpowiedzialnego postępowania, które starają się zaszczepić. Pokazują, że bezpieczne korzystanie z Internetu to nie tylko unikanie zagrożeń, ale także życie zgodnie z wartościami cyfrowymi: autentycznością, szacunkiem, integracją i empatią.

Dofinansowane przez Unię Europejską

Przykład: Pracownik młodzieżowy, który w sposób przejrzysty omawia swoje osobiste doświadczenia związane z cyberprzemocą i sposób, w jaki poradził sobie z nią dzięki regulacji emocji, zapewnia młodym ludziom zarówno wskazówki, jak i poczucie bezpieczeństwa.

Wskazówka: Od czasu do czasu pokaż swojej grupie, w jaki sposób weryfikujesz wiadomości przed ich udostępnieniem lub jak z szacunkiem radzisz sobie z nieporozumieniami w komentarzach. Prawdziwe przykłady sprawiają, że wzorce do naśladowania stają się widoczne i łatwiejsze do zrozumienia.

- Pełnienie roli mentora

Jako mentorzy ambasadorzy towarzyszą młodym ludziom w refleksji nad ich tożsamością cyfrową, wyborami dokonywanymi w Internecie i reakcjami emocjonalnymi:

- *Jakie uczucia wywołała w Tobie ta interakcja w Internecie?*
- *Co możesz zrobić inaczej następnym razem?*
- *Do kogo możesz się zwrócić, jeśli coś wydaje Ci się nie w porządku?*

Mentoring polega na wzmacnianiu samoświadomości i zdolności do działania, a nie na kontroli.

W tym kierunku, poprzez wspierający i refleksyjny dialog, rola ambasadorów polega na pomaganiu młodzieży w odkrywaniu:

- Jak przemyślane zachowanie przed opublikowaniem postu może uchronić ich przed niepożądaną uwagą lub krzywdą w przyszłości.
- Jak dostosowanie ustawień prywatności pozwala im wybrać, kto może przeglądać ich treści, wysyłać im wiadomości lub komentować ich posty.
- Jak zgłaszanie lub ograniczanie szkodliwych interakcji może pomóc im odzyskać kontrolę nad swoim środowiskiem online.
- Jak narzędzia takie jak blokowanie, wyciszanie lub ograniczanie komentarzy mogą zmniejszyć narażenie na negatywne lub niepokojące zachowania, często bez wiedzy drugiej osoby.
- Jak przeglądanie lub edytowanie poprzednich postów może wspierać cyfrową tożsamość, z którą czują się komfortowo.

Można to osiągnąć, zadając pytania, takie jak:

- Zanim opublikujesz to, jak byś się czuł, gdyby ktoś później wykorzystał to poza kontekstem?

Dofinansowane przez Unię Europejską

- Jakie informacje o sobie możesz bezpiecznie udostępnić? Co wydaje Ci się zbyt osobiste?
- Kto może teraz zobaczyć Twoje treści i kto według Ciebie powinien je zobaczyć?

Wskazówka: Zorganizuj „cyfrowe kręgi refleksji", podczas których młodzież będzie dzielić się cotygodniowymi doświadczeniami online i omawiać emocje lub wyzwania, z którymi się spotkała. Wykorzystaj te sesje, aby znormalizować refleksję emocjonalną w kontekście cyfrowym.

- Rzecznicy i osoby budujące mosty

Ambasadorzy łączą młodzież z interesariuszami, takimi jak szkoły, organizacje pozarządowe, gminy i inicjatywy dotyczące bezpieczeństwa w Internecie, zapewniając, że głosy młodych ludzi mają wpływ na kształt polityki w zakresie integracji cyfrowej i dobrostanu. Pełnią również rolę mediatorów międzypokoleniowych, pomagając dorosłym zrozumieć cyfrową rzeczywistość młodzieży, a młodzieży – komunikować swoje potrzeby w sposób pewny siebie i pełen szacunku.

Wskazówka: Ułatw międzypokoleniową dyskusję między rodzicami a młodymi ludźmi na temat „zaufania w Internecie". Niech każda ze stron wyrazi swoje obawy i oczekiwania, a następnie wspólnie opracujcie „umowę cyfrową".

Przywództwo i komunikacja na rzecz kultury bezpieczeństwa

Rozwijanie kultury bezpieczeństwa wśród młodych ludzi wymaga przywództwa opartego na empatii i inteligencji emocjonalnej.

- Przywództwo, jako służba

Młodzi ambasadorzy przewodzą nie poprzez autorytet, ale poprzez dawanie przykładu. Pełnią rolę katalizatorów wzmacniania pozycji, zachęcając innych do przyjmowania bezpiecznych, świadomych i integracyjnych zachowań w sieci.

Przywództwo tu oznacza:

- Słuchanie przed działaniem
- Budowanie relacji opartych na zaufaniu
- Wspieranie uczestnictwa i wspólnej odpowiedzialności

Wskazówka: Zachęć swoją grupę do przejęcia inicjatywy w projektowaniu własnych działań uświadamiających, takich jak tworzenie cyfrowych plakatów,

Dofinansowane przez Unię Europejską

krótkich filmów lub hashtagów promujących empatię w sieci lub weryfikację faktów.

- Promocja i widoczność

Ambasadorzy wzmacniają głos młodych ludzi. Wspierając inicjatywy, kampanie lub mentoring rówieśniczy prowadzone przez młodzież, zwiększają widoczność pozytywnych praktyk cyfrowych.

Wskazówka: Wspieraj młodzież prowadzącą kampanię w mediach społecznościowych (np. „#ThinkBeforeYouType" lub „#EmotionCheck") i pomóż jej zmierzyć jej zasięg i zaangażowanie.

- Studium przypadku: „Kindly" UNICEF-u

Praktycznym przykładem empatii w cyberprzestrzeni jest inicjatywa Kindly UNICEF-u, platforma oparta na sztucznej inteligencji, której celem jest pomaganie młodym ludziom w zastanowieniu się nad emocjonalnym wydźwiękiem swoich wiadomości przed ich opublikowaniem. Kindly nie karze ani nie zawstydza, ale zachęca młodych ludzi do zastanowienia się przez chwilę nad tym, jak ich słowa mogą wpłynąć na innych, i do poszukiwania alternatywnych, bardziej życzliwych wiadomości. To refleksyjne, wspierające podejście pokazuje, jak można wykazać się inteligencją emocjonalną w przestrzeni cyfrowej bez użycia autorytetu lub przymusu. Zarówno młodzież, jak i dorośli korzystają z Kindly, aby przeanalizować swoją komunikację online, ucząc się przekładać inteligencję emocjonalną na codzienne zachowania cyfrowe.

Dla ambasadorów Kindly stanowi praktyczny przykład tego, jak tworzyć środowiska, które pomagają młodzieży bezpiecznie angażować się, krytycznie myśleć i regulować swoje reakcje emocjonalne. Pokazuje również siłę rzecznictwa i widoczności, ponieważ UNICEF wzmacnia głos młodzieży, zachęcając ją do współtworzenia treści, testowania funkcji i dzielenia się doświadczeniami. Wielu młodych użytkowników zainicjowało mikro kampanie inspirowane Kindly, dzieląc się wiadomościami „przed i po", tworząc wyzwania związane z życzliwością lub produkując krótkie filmy o tym, jak chwila empatii może zmienić całą interakcję online. Te działania prowadzone przez młodzież wzmacniają pozytywne normy cyfrowe i pokazują, jak delikatne interwencje mogą zmienić kulturę grupy w kierunku empatii, zaufania i świadomej komunikacji.

Przypadek ten ilustruje rolę ambasadora: wspieranie inicjatyw prowadzonych przez młodzież, modelowanie komunikacji opartej na inteligencji emocjonalnej i uwidacznianie życzliwości w Internecie. Dzięki prostym, przystępnym

Dofinansowane przez Unię Europejską

narzędziom, takim jak Kindly, młodzi ludzie doświadczają kultury bezpieczeństwa nie, jako zbioru zasad, ale jako wspólnego zobowiązania do traktowania się nawzajem z godnością w przestrzeni cyfrowej.

Wspieranie młodych ludzi w radzeniu sobie z wyzwaniami emocjonalnymi i cyfrowymi

Aby stać się zaufanymi osobami kontaktowymi, pracownicy młodzieżowi muszą rozpoznawać bariery, które powstrzymują młodzież przed szukaniem pomocy, i nauczyć się praktycznych sposobów ich pokonywania.

- Zrozumienie barier i dyskretne działanie

- Strach przed osądem lub wstydem: młodzi ludzie mogą ukrywać błędy popełnione w Internecie.
- Nieufność wobec dorosłych: mogą obawiać się kary zamiast wsparcia.
- Różnice kulturowe lub pokoleniowe: różne postrzeganie tego, co jest „poważnym" zachowaniem w sieci.
- Przeciążenie emocjonalne: młodzież może mieć trudności z wyrażeniem, jak doświadczenia cyfrowe na nią wpływają.
- Uznanie wrażliwości: należy przypomnieć młodzieży, że każdy może stać się ofiarą w sieci, a ich wahanie przed zgłoszeniem incydentu jest oznaką napięcia emocjonalnego, a nie słabości.

Ambasadorzy muszą przeciwdziałać tym barierom poprzez empatię, cierpliwość i poufność. Powinni skupić się nie na instruowaniu młodych ludzi, aby zgłaszali incydenty, ale na usuwaniu barier emocjonalnych i relacyjnych, które uniemożliwiają im bezpieczne szukanie pomocy. Dzięki spokojnej obecności, empatii i zapewnianiu wsparcia pracownicy młodzieżowi budują zaufanie potrzebne młodym ludziom, aby się otworzyli, rozważyli dostępne opcje i podjęli kroki, które chronią zarówno ich samych, jak i ich rówieśników.

Wskazówka: Korzystaj z anonimowych „skrzynek na pytania" (fizycznych lub cyfrowych), aby młodzież mogła zadawać pytania dotyczące bezpieczeństwa w Internecie lub kwestii emocjonalnych, których mogłaby się wstydzić zadać bezpośrednio.

- Stawanie się zaufaną osobą wspierającą

Pracownicy młodzieżowi mogą budować swoją wiarygodność poprzez:

- Okazywanie szczerego zainteresowania życiem młodzieży w Internecie.
- Bycie konsekwentnym i przystępnym.

Dofinansowane przez Unię Europejską

- Dotrzymywanie obietnic i szanowanie prywatności.
- Unikanie nadmiernych reakcji: najpierw słuchaj potem doradzaj.

Wskazówka: Podziel się krótkimi studiami przypadków, „co zrobiłem, gdy…" aby zilustrować rzeczywiste rozwiązywanie problemów (np. radzenie sobie z komentarzami pełnymi nienawiści). Historie pokazują, że szukanie pomocy jest bezpieczne i normalne.

- Rozpoznawanie zagrożeń cyfrowych i odpowiadanie na nie

Ambasadorzy powinni być przygotowani do rozpoznawania wczesnych oznak:

- Cyberprzemoc lub wykluczenia
- Nękanie w Internecie lub mowy nienawiści
- Dezinformacji lub kontaktu z radykalnymi treściami

Cierpienia emocjonalnego związanego z aktywnością cyfrową

Wskazówka: Zawsze najpierw skup się na reakcji emocjonalnej („Jak się z tym czujesz?"), a dopiero potem na rozwiązaniu technicznym, („Co możemy zgłosić lub zablokować?").

Wskazówka: Nawiąż współpracę z lokalnym psychologiem, organizacją pozarządową lub jednostką ds. cyberbezpieczeństwa, aby zorganizować wspólne sesje, podczas których młodzież nauczy się zarówno emocjonalnych, jak i technicznych reakcji związanych z bezpieczeństwem.

Inteligencja emocjonalna w mediacji cyfrowej

Kultura bezpieczeństwa opiera się na świadomości emocjonalnej. Konflikty, dezinformacja lub stres cyfrowy mogą być skutecznie rozwiązywane tylko wtedy, gdy obecna jest inteligencja emocjonalna (EI).

- T4 obszary EI w praktyce

Umiejętności EI	Zastosowane kultury bezpieczeństwa
Samoświadomość	Rozpoznawaj emocje wywołane interakcjami cyfrowymi.
Samoregulacja	Unikaj impulsywnych reakcji w Internecie.

Dofinansowane przez Unię Europejską

Empatia	Zanim zaczniesz oceniać lub odpowiadać, spróbuj zrozumieć uczucia innych.
Umiejętności społeczne	Komunikuj się asertywnie i buduj relacje oparte na wsparciu.

Wskazówka: Po zakończeniu każdego projektu grupowego online zorganizuj krótką sesję „sprawdzania emocji", podczas której młodzież opisuje jedną emocję, której doświadczyła, oraz jedną rzecz, której dowiedziała się o sobie.

- Techniki medytacyjne dla pracowników młodzieżowych

- Stosuj zasadę „zatrzymaj się i nazwij": pomóż młodzieży zatrzymać się przed udzieleniem odpowiedzi online i nazwać swoje emocje.
- Zachęcaj do przyjmowania perspektywy drugiej osoby:, „Co może czuć druga osoba?"
- Naucz asertywnej komunikacji: wyrażaj uczucia i granice bez agresji.
- Zamień konflikty w okazje do nauki, analizując przyczyny i związane z nimi emocje.

Mikroaktywność: Pokaż zrzut ekranu z kłótnią online i omów, jak przeformułować emocjonalne reakcje, używając empatii i spokojnego rozumowania.

Wskazówka: Wprowadź w swojej grupie „zasadę ochłonięcia" – przed udzieleniem odpowiedzi na wiadomość dotyczącą konfliktu wszyscy czekają 10 minut i zastanawiają się nad swoim stanem emocjonalnym.

Praktyczne umiejętności, potrzebne, aby zostać ambasadorem

Pracownicy młodzieżowi mogą rozpocząć swoją przygodę z ambasadorstwem od małych, wykonalnych działań, które stopniowo budują przywództwo i wiarygodność.

Ścieżka	**Przykłady działań**	**Oczekiwane wyniki**
Budowanie świadomości	Organizuj krótkie sesje informacyjne na temat bezpieczeństwa emocjonalnego w Internecie.	Młodzież staje się bardziej świadoma zagrożeń emocjonalnych.

Dofinansowane przez Unię Europejską

Mentoring i coaching	Oferuj indywidualne doradztwo dla młodzieży borykającej się z wyzwaniami w Internecie.	Budowanie zaufania i pozycjonowanie pracownika młodzieżowego, jako bezpiecznego kontaktu.
Działania prowadzone przez rówieśników	Wspieraj młodych ludzi w prowadzeniu warsztatów lub kampanii.	Wzmacnia przywództwo i zaangażowanie.
Rzecznictwo i sieci	Reprezentuj poglądy młodzieży w dialogach z interesariuszami.	Promuje systemową zmianę na rzecz włączenia młodzieży w kulturę bezpieczeństwa
Refleksja i ocena	Regularnie oceniaj wpływ działań na podstawie opinii młodzieży.	Zapewnia ciągłe doskonalenie i dostosowanie się.

Wskazówka: Dokumentuj i świętuj działania podejmowane przez młodzież (zdjęcia, opinie lub mini studia przypadków). Publiczne uznanie wzmacnia motywację i promuje pozytywne zachowania w sieci.

Dofinansowane przez Unię Europejską

Moduł 6 – Repozytorium dodatkowych informacji i zasobów

Kategoria zasobu	Nazwa zasobu	Typ	Opis	Link/informacje dotyczące dostępu
Cyberbezpieczeństwo	Better internet for kids (BIK)	Strona internetowa	Europejska agenda cyfrowa ma na celu zapewnienie wszystkim Europejczykom dostępu do technologii cyfrowych. Dzieci mają szczególne potrzeby i są szczególnie narażone na zagrożenia w Internecie, jednak internet stanowi również dla nich źródło możliwości dostępu do wiedzy, komunikacji, rozwoju umiejętności oraz poprawy perspektyw zawodowych i szans na zatrudnienie	https://better-internet-for-kids.europa.eu/en
Cyberbezpieczeństwo	Agencja Unii Europejskiej ds. Cyberbepieczeństwa (ENISA) – publikacje	Strona internetowa	Oficjalny zasób UE zawierający praktyczne materiały, kampanie i wytyczne dotyczące świadomości w zakresie cyberbezpieczeństwa. Przydatny podczas warsztatów dla młodzieży, ćwiczeń z rozpoznawania zagrożeń oraz edukacji profilaktycznej zgodnej	https://www.enisa.europa.eu/publications

Dofinansowane przez Unię Europejską

			z normami europejskimi.	
Inteligencja emocjonalna	Six seconds emotional intelligence network	Strona internetowa	Six Seconds to organizacja non-profit, której misją jest zwiększanie inteligencji emocjonalnej na świecie. Six Seconds prowadzi badania i zajmuje się nauczaniem inteligencji emocjonalnej. Tworzymy oparte na dowodach narzędzia i metody wspierające transformacyjne zmiany w jednostkach i organizacjach.	https://www.6seconds.org/
Inteligencja emocjonalna	CASEL – Ramy nauczania społeczno-emocjonalnego	Strona internetowa	Zapewnia szeroko stosowaną strukturę dla nauki społeczno-emocjonalnej, obejmującą samoświadomość, samokontrolę, empatię i odpowiedzialne podejmowanie decyzji. Istotne dla włączenia inteligencji emocjonalnej do edukacji w zakresie bezpieczeństwa cyfrowego.	https://casel.org
Cyfrowe obywatelstwo i integracja	Digcomp	Ramy UE	Europejskie ramy kompetencji cyfrowych (DigComp) opisują, co jest potrzebne, aby być	https://joint-research-centre.ec.europa.eu/projects-

Dofinansowane przez Unię Europejską

			kompetentnym cyfrowo w dzisiejszym społeczeństwie, i wspierają rozwój kompetencji cyfrowych wśród osób w każdym wieku. Obejmują one szeroki zakres poziomów umiejętności, od podstawowych do bardzo zaawansowanych, i stanowią stabilny punkt odniesienia w szybko zmieniającym się świecie technologii cyfrowych.	and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp_en
Narzędzia wsparcia dla młodzieży	Youthpass	Narzędzie walidacyjne	Youthpass to europejski instrument uznawania służący do identyfikacji i dokumentowania efektów uczenia się osiągniętych w ramach projektów realizowanych w ramach programów Erasmus+ Młodzież i Europejski Korpus Solidarności. Youthpass promuje indywidualną refleksję i świadomość dotyczącą uczenia się oraz pomaga uwidocznić efekty uczenia się zarówno dla samych uczących	https://www.youthpass.eu/en/

Dofinansowane przez Unię Europejską

			się, jak i dla innych osób.	
Narzędzia wsparcia dla młodzieży	SALTO youth	Strona internetowa	SALTO-YOUTH to skrót od Support, Advanced Learning and Training Opportunities for Youth (wsparcie, zaawansowana nauka i możliwości szkoleniowe dla młodzieży). Działa w ramach programów Erasmus+ Młodzież i Europejski Korpus Solidarności.	https://www.salto-youth.net/
Cyberbezpieczeństwo	EU vs Disinfo	Strona internetowa	Inicjatywa UE wyjaśniająca typowe techniki dezinformacji i strategie manipulacji. Wspiera krytyczne myślenie, umiejętność korzystania z mediów oraz działania związane z dezinformacją w edukacji młodzieży.	https://euvsdisinfo.eu
Cyberbezpieczeństwo	Stay Safe Online – Globalny Sojusz Cyberbezpieczeństwa	Strona internetowa	Zawiera jasne i przystępne wskazówki dotyczące cyberhigieny i bezpiecznych nawyków w Internecie. Można je dostosować do potrzeb młodzieży, tworząc listy kontrolne i kampanie profilaktyczne.	https://staysafeonline.org

Dofinansowane przez Unię Europejską

Cyberbezpieczeństwo	DigComp 3.0: European Digital Competence Framework	Strona internetowa	Europejskie ramy określające kluczowe kompetencje cyfrowe, w tym bezpieczeństwo i umiejętność korzystania z informacji. Przydatne, jako punkt odniesienia dla dostosowania celów szkoleniowych do polityki UE w zakresie edukacji cyfrowej.	https://joint-research-centre.ec.europa.eu/digcomp_en
Inteligencja emocjonalna	CASEL – Ramy nauczania społeczno-emocjonalnego	Strona internetowa	Zapewnia szeroko stosowane ramy dla nauki społeczno-emocjonalnej, obejmujące samoświadomość, samokontrolę, empatię i odpowiedzialne podejmowanie decyzji. Istotne dla włączenia inteligencji emocjonalnej do edukacji w zakresie bezpieczeństwa cyfrowego.	https://casel.org
Inteligencja emocjonalna	Salovey, P., & Mayer, J. D. (1990). Emotional Intelligence	Artykuł	Podstawowy artykuł naukowy wprowadzający pojęcie inteligencji emocjonalnej. Stanowi teoretyczne uzasadnienie podejść opartych na IE stosowanych w całym podręczniku EM&M.	https://doi.org/10.2190/DUGG-P24E-52WK-6CDG

Dofinansowane przez Unię Europejską

Narzędzia wsparcia dla młodzieży	Council of Europe – Digital Citizenship Education	Strona internetowa	Zapewnia oparte na wartościach zasoby służące promowaniu etycznego, bezpiecznego i partycypacyjnego zaangażowania cyfrowego wśród młodych ludzi.	https://www.coe.int/en/web/education/dce-for-educators
Cyberbezpieczeństwo	Livingstone, S., & Third, A. (2017). *Children and young people's rights in the digital age. An emerging agenda.* New Media & Society, 19(5), 657–670.	Artykuł	Silna podstawa dla udziału młodzieży, jej głosu i rzecznictwa w kontekście cyfrowym.	https://doi.org/10.1177/1461444816686318
Cyberbezpieczeństwo	UNICEF- Cyberprzemoc:, czym jest i jak ją powstrzymać	Strona internetowa	Informacje na temat cyberprzemocy i sposobów radzenia sobie z nią.	https://www.unicef.org/stories/how-to-stop-cyberbullying?utm
Narzędzia wsparcia dla młodzieży	Komisja Europejska: Plan działania w dziedzinie edukacji cyfrowej	Publikacja	Zawiera jasne i przystępne wskazówki dotyczące cyberhigieny i bezpiecznych nawyków w Internecie. Można je dostosować do potrzeb młodzieży, tworząc listy kontrolne i kampanie profilaktyczne.	https://education.ec.europa.eu/focus-topics/digital-education/plan

Dofinansowane przez Unię Europejską

Inteligencja emocjonalna	Goleman, D. (1995). *Emotional Intelligence: Why It Can Matter More Than IQ*. New York: Wydawnictwo Bantam.	Książka	Podstawowa teoria leżąca u podstaw samoświadomości, samoregulacji, empatii i umiejętności społecznych wykorzystywanych w całym module.	https://books.google.gr/books?id=OgXxhmGiRB0C&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false https://www.youtube.com/watch?v=erfgEHHfFkU
Narzędzia wsparcia dla młodzieży	Komisja Europejska: Developing digital youth work. Policy recommendations, training needs and good practice examples. For youth workers and decision-makers.	Publikacja	Przedstawia przykłady innowacyjnych praktyk w zakresie realizacji cyfrowych działań na rzecz młodzieży oraz podnoszenia kompetencji cyfrowych pracowników młodzieżowych; zalecenia dotyczące polityki w zakresie rozwoju cyfrowych działań na rzecz młodzieży; identyfikację potrzeb szkoleniowych pracowników młodzieżowych, istotnych dla cyfrowych działań na rzecz młodzieży.	https://op.europa.eu/en/publication-detail/-/publication/fbc18822-07cb-11e8-b8f5-01aa75ed71a1
Narzędzia wsparcia dla młodzieży	UNICEF: Kindly	Strona internetowa	Inicjatywa UNICEF-u mająca na celu	https://www.unicef.org/innovation/kindly

Dofinansowane przez Unię Europejską

			położenie kresu cyberprzemocy.	
Edukacja o cyberbezpieczeństwie	Better Internet for Kids (BIK)	Platforma UE	Okołounijna inicjatywa oferująca zasoby dotyczące bezpieczeństwa w Internecie, obywatelstwa cyfrowego i odpowiedzialnego korzystania z Internetu przez dzieci i młodzież. Przydatna dla pracowników młodzieżowych, które opracowują sesje uświadamiające i działania angażujące rodziców/młodzież.	https://www.betterinternetforkids.eu
Inteligencja emocjonalna	CASEL – Ramy nauczania społeczno-emocjonalnego (SEL)	Ramy/artykuły	Międzynarodowo uznane ramy rozwoju inteligencji emocjonalnej, samokontroli, empatii i umiejętności społecznych. Pracownicy młodzieżowi mogą dostosować zasady SEL, aby wzmocnić odporność emocjonalną w kontekście cyfrowym.	https://casel.org
Inteligencja emocjonalna	MindTools – Emotional Intelligence Resources	Artykuły /narzędzia	Praktyczne artykuły i narzędzia służące zrozumieniu i zastosowaniu umiejętności związanych z	https://www.mindtools.com

Dofinansowane przez Unię Europejską

			inteligencją emocjonalną, takich jak radzenie sobie ze stresem, zdolność adaptacji i komunikacja. Odpowiednie do samodzielnego szkolenia nauczycieli i uproszczonych zajęć dla młodzieży.	
Zdrowie psychiczne młodzieży i EI	UNICEF – Mental Health & Psychosocial Support Resources	Raporty / Zestawy narzędzi	Oparte na dowodach naukowych wytyczne dotyczące zdrowia psychicznego młodzieży, dobrego samopoczucia emocjonalnego i wsparcia psychospołecznego. Pomoc dla pracowników młodzieżowych w radzeniu sobie z emocjonalnymi reakcjami na zagrożenia związane z Internetem i stresem cyfrowym.	https://www.unicef.org/mental-health
Umiejętności cyfrowe i media	Europejskie Obserwatorium Mediów Cyfrowych (EDMO)	Sieć UE / Zasoby	Zapewnia narzędzia i badania dotyczące dezinformacji, weryfikacji faktów i umiejętności korzystania z mediów. Przydatne do szkolenia młodzieży w zakresie krytycznej oceny informacji w Internecie i radzenia sobie z	https://edmo.eu

Dofinansowane przez Unię Europejską

			emocjonalnymi reakcjami na fałszywe treści.	
Nauczanie mieszane	European Schoolnet Academy	Kursy online	Oferuje bezpłatne kursy doskonalenia zawodowego z zakresu pedagogiki cyfrowej, nauczania mieszanego i innowacyjnych metod nauczania. Pracownicy młodzieżowi mogą korzystać z kursów w celu samodoskonalenia i czerpania inspiracji metodologicznej.	https://www.europeanschoolnetacademy.eu
Narzędzia nauczania mieszanego	Kahoot!	Narzędzia cyfrowe	Platforma edukacyjna z elementami grywalizacji, odpowiednia do quizów, sprawdzianów wiedzy i interaktywnych ćwiczeń dotyczących cyberbezpieczeństwa i sztucznej inteligencji. Wspiera zaangażowanie i motywację w środowiskach nauczania mieszanego.	https://kahoot.com
Narzędzia nauczania mieszanego	Canva dla edukacji	Narzędzia cyfrowe	Platforma do projektowania wizualnego służąca do tworzenia plakatów, infografik, tablic refleksyjnych i ćwiczeń związanych z	https://www.canva.com/education

Dofinansowane przez Unię Europejską

			opowiadaniem historii. Wspiera kreatywną refleksję nad inteligencją emocjonalną i ćwiczenia związane ze świadomością cyberbezpieczeństwa.	
Udział młodzieży i integracja społeczna	SALTO Youth – Participation & Inclusion Resources	Centrum zasobów UE	Zapewnia narzędzia, metody i publikacje wspierające uczestnictwo młodzieży, integrację i edukację poza formalną. Przydatne do dostosowania działań EM&M do różnych kontekstów społeczno-ekonomicznych i kulturowych.	https://www.salto-youth.net
Kontekst rumuński – cyberbezpieczeństwo	Romanian National Cyber Security Directorate (DNSC)	Strona internetowa instytucji	Krajowy organ odpowiedzialny za ostrzeżenia dotyczące cyberbezpieczeństwa, kampanie uświadamiające i wytyczne dostosowane do warunków rumuńskich. Może być wykorzystywany do podawania lokalnych przykładów i przekazywania komunikatów profilaktycznych..	https://www.dnsc.ro
Kontekst rumuński –	ANPCDEFP – Erasmus+ Youth Resources	Strona internetowa	Zasoby agencji krajowej dotyczące programu Erasmus+ w	https://www.anpcdefp.ro

Dofinansowane przez Unię Europejską

młodzież i edukacja		instytucji	zakresie edukacji młodzieży, kształcenia poza formalnego i dobrych praktyk. Przydatne do dostosowania działań EM&M do krajowych standardów i projektów dotyczących pracy z młodzieżą.	

Dofinansowane przez Unię Europejską

Ćwiczenia

Ćwiczenia modułu 1

Poniżej znajduje się kilka ćwiczeń do modułu 1. Zostały one opracowane w celu utrwalenia podstawowych zagadnień w interaktywny sposób. Zachęcają one do dyskusji, refleksji i wykorzystania strategii inteligencji emocjonalnej w zrozumieniu podstaw cyberbezpieczeństwa. Każde ćwiczenie można dostosować do wieku i kontekstu grupy, a każde z nich kładzie nacisk na różne aspekty treści modułu (od słownictwa po praktyczne czynności). Uwaga: Można dowolnie dostosowywać scenariusze, aby uwzględnić różne zagrożenia, takie jak fałszywe profile, próby phishingu, dylematy związane z nadmiernym udostępnianiem informacji lub przypadki cyberprzemocy, upewniając się, że wszystkie kluczowe obszary tematyczne (osoby wykorzystujące inne osoby, oszustwa, prywatność itp.) są poruszane w ramach wszystkich ćwiczeń.

Ćwiczenie 1

Seminarium poświęcone podstawom – budowanie wspólnego słownictwa i powiązań

Cele edukacyjne ćwiczeń

- Rozumieć i stosować podstawowe terminy związane z cyberbezpieczeństwem i inteligencją emocjonalną.
- Rozpoznawać, w jaki sposób emocje wpływają na wybory dokonywane w Internecie i podejmowanie ryzyka.
- Rozpoznawać typowe sytuacje cyfrowe, w których świadomość emocjonalna sprzyja bezpieczniejszym zachowaniem.

Przegląd ćwiczeń:

Działanie rozpoczyna się od zwięzłego wykładu interaktywnego, podczas którego przedstawiane są kluczowe pojęcia, a następnie odbywa się ćwiczenie polegające na tworzeniu mapy pojęć. Nauczyciele wyjaśniają, w jaki sposób pojęcia związane z cyberbezpieczeństwem (takie jak zagrożenia i podatności) łączą się z elementami inteligencji emocjonalnej (takimi jak świadomość i regulacje) w rzeczywistych sytuacjach cyfrowych. Pomaga to w stworzeniu mentalnego modelu powiązań między uczuciami a zagrożeniami. Ujawnia również wcześniejsze przekonania lub błędne wyobrażenia uczestników na temat bezpieczeństwa w Internecie.

Dofinansowane przez Unię Europejską

1. **Instrukcje:** Miniwykład **(5–7 minut):** Rozpocznij od krótkiej prezentacji lub wykładu. Wyraźnie zdefiniuj następujące pojęcia: zagrożenie, podatność, ryzyko, higiena (pojęcia związane z cyberbezpieczeństwem) oraz samoświadomość, samokontrola, świadomość społeczna, umiejętności interpersonalne (pojęcia związane z inteligencją emocjonalną). Użyj prostych przykładów podanych w treści modułu. Na przykład narysuj szybki szkic lub użyj analogii (np. „podatność jest jak pozostawienie otwartych drzwi wejściowych – nie oznacza to, że złoczyńca jest w Twoim domu, ale ułatwia mu to wejście"). Niech zajęcia będą angażujące – zapytaj grupę, czy słyszeli te słowa lub doświadczyli podobnych sytuacji.
2. **Lisa codziennych cyfrowych momentów:** Poproś uczestników, aby wymienili pięć codziennych cyfrowych momentów, które często wywołują emocje u młodych ludzi. Mogą je wykrzykiwać lub zapisywać na karteczkach samoprzylepnych. Przykłady: wyskakujące powiadomienie o pilnej sprawie, publiczny komentarz do ich zdjęcia (może to być pochwała lub złośliwość – obie reakcje mogą wywołać emocje), zaproszenie do grona znajomych od nieznajomej osoby, szokujący nagłówek wiadomości w mediach społecznościowych, wiadomość „wygrałeś nagrodę". Postaraj się uwzględnić różnorodne sytuacje: takie, które mogą wywołać niepokój (np. wiadomość o „problemie z kontem"), takie, które wywołują podekscytowanie (nagroda lub ważna wiadomość), takie, które wywołują ciekawość lub zazdrość (popularny post lub plotka), takie, które wywołują strach lub złość (np. złośliwy komentarz lub cyberprzemoc). Zapisz je na tablicy.
3. **Ćwiczenie z mapą koncepcyjną:** Rozdaj uczestnikom arkusz roboczy z mapą koncepcyjną (załącznik A). Poproś ich, aby wybrali jedno z cyfrowych wydarzeń z listy (to, które najbardziej do nich przemawia lub losowo) i zapisali je w środkowej części mapy koncepcyjnej. Następnie, indywidualnie lub w parach, niech wypełnią otaczające węzły: określą prawdopodobne zagrożenie w tym scenariuszu, podatność, która może mieć znaczenie, zachowanie typowe dla młodzieży, emocje, które odczuwają, bezpieczniejszą reakcję, którą powinni wykazać, oraz krok weryfikacyjny, aby dokładnie sprawdzić. Powinni również narysować strzałki i dodać krótkie notatki wyjaśniające powiązania (np. „Odczuwanie niepokoju (emocja) może być słabym punktem, ponieważ może skłonić mnie do kliknięcia linku (zachowanie) bez sprawdzenia").
4. **Podziel się i omów:** Zbierz 2–3 przykładowe mapy (poproś ochotników lub wybierz losowo) i poproś uczestników o wyjaśnienie ich scenariusza i powiązań. Omów podobieństwa i wspólne motywy. Na przykład możesz zauważyć, że „pośpiech" pojawia się, jako słaby punkt na wielu

Dofinansowane przez Unię Europejską

mapach lub że „zapytanie znajomego" często pojawia się, jako bezpieczna reakcja. Wspólnie stwórzcie na tablicy krótki, wspólny słownik na podstawie tego, co się pojawiło – np. napiszcie „Ryzyko = szansa na szkodę (wielu wspomniało, że wzrasta, gdy jesteśmy pod wpływem emocji) „ lub „Higiena = codzienny bezpieczny nawyk (jak napisało kilku z was „aktualizuj telefon")". Upewnijcie się, że formalne definicje z miniwykładu są zgodne ze słowami uczestników.

5. **Podsumuj powiązanie cyfrowe EI: Zakończ** podsumowaniem, które połączy wszystkie elementy. Podkreśl, w jaki sposób świadomość emocjonalna prowadzi do bezpieczniejszych działań. Na przykład: „Na tych mapach widzieliśmy, że kiedy ktoś czuł złość lub strach, był bardziej skłonny do podjęcia ryzykownego działania, takiego jak reagowanie bez zastanowienia. Ale jeśli wykorzystał samoświadomość, aby zauważyć to uczucie, a następnie samokontrolę, aby zatrzymać się i odetchnąć, mógł wybrać bezpieczniejszą reakcję, taką jak sprawdzenie informacji. Oto cykl: świadomość → refleksja → regulacja → bezpieczniejsze działanie". Zachęcaj do zadawania pytań w celu wyjaśnienia wszelkich terminów lub powiązań, które uczestnicy nadal uważają za niejasne.

Refleksja i dyskusja: Zapytaj:, „Które pojęcie lub powiązanie było dzisiaj najbardziej zrozumiałe?" oraz „Gdzie Twoim zdaniem uczniowie (młodzież) najbardziej potrzebują jaśniejszego języka lub pojęć?". Pozwoli to nauczycielom wskazać, na jakich ideach chcą się skupić podczas nauczania. Na przykład ktoś może powiedzieć: „Zdałem sobie sprawę, że nigdy nie rozmawialiśmy z naszymi uczniami o tym, czym jest „wrażliwość", więc kiedy coś idzie nie tak, obwiniają siebie. Chcę używać tego słowa, aby pokazać im, że jest to po prostu coś, co można naprawić, a nie osobista porażka". Ktoś inny może powiedzieć: „Zrozumienie, że emocje nie są złe, a są tylko sygnałami – to było dla mnie nowe i myślę, że moje nastolatki też powinny to usłyszeć".

Najważniejsze wnioski:

- Wspólny język dotyczący cyberbezpieczeństwa i emocji eliminuje niejasności i piętno. Kiedy młodzież zna odpowiednie słowa, może otwarcie rozmawiać i prosić o pomoc („Myślę, że padłem ofiarą phishingu" lub „Czułem presję, żeby udostępnić swoje zdjęcie i żałuję tego").

Emocje są sygnałami, a nie dyrektywami. Odczuwanie czegoś nie oznacza, że musisz natychmiast podjąć działanie. Zauważenie i nazwanie emocji może faktycznie pomóc w podjęciu bezpieczniejszej decyzji w świecie cyfrowym (np. „Czuję się sprowokowany tym komentarzem, co jest znakiem, że nie powinienem teraz odpowiadać").

Dofinansowane przez Unię Europejską

Ćwiczenie 2

Przykłady przypadków i dialogi – emocje kryjące się za zagrożeniami

Cele edukacyjne ćwiczeń

- Rozpoznawanie typowych zagrożeń internetowych i taktyk manipulacji emocjonalnej.
- Rozpoznawanie czynników wywołujących emocje w wiadomościach i postach internetowych.
- Ćwiczenie używania spokojnego, jasnego języka, aby bezpiecznie reagować w sytuacjach stresowych.

Opis ćwiczenia:

W tym ćwiczeniu uczestnicy pracują z krótkimi, anonimowymi kartami scenariuszy (przykładami), które ilustrują typowe zagrożenia internetowe skierowane do młodzieży. Każda sytuacja jest krótką wiadomością lub postem z minimalnym kontekstem. Nauczyciele analizują te scenariusze w parach, identyfikując sygnały ostrzegawcze i emocjonalne wyzwalacze, a następnie zastanawiają się nad bezpiecznymi sposobami reagowania. Następnie odbywa się dyskusja grupowa, której celem jest normalizacja rozpoznawania manipulacji i dzielenie się skutecznymi sposobami reagowania. Nacisk kładziony jest tutaj na czytanie między wierszami wiadomości, – jakie emocje próbuje wywołać dana wiadomość i jak można na nią odpowiedzieć, wykorzystując inteligencję emocjonalną (zachowując spokój i wyznaczając granice)?

Instrukcje:

1. **Rozdaj arkusze z opisem przypadków:** Każdej parze uczestników daj jeden arkusz z opisem przypadku. Każdy arkusz zawiera krótki scenariusz i pytania. Na przykład:
    a. „Kontakt z pomocą techniczną: „Naruszyłeś zasady społeczności. Kliknij tutaj, aby potwierdzić swoją tożsamość, w przeciwnym razie Twoje konto zostanie dzisiaj zawieszone”. (To prawdopodobnie wywoła poczucie pilności/strachu).
    b. „Przyjaciel w pośpiechu: „Cześć, to ja. Zmieniłem numer. Czy możesz mi przesłać swój kod logowania, abym mógł się zalogować?” (Wywołuje empatię/presję, aby pomóc – może to być scenariusz z oszustem lub zhakowanym przyjacielem).
    c. „Nagroda: „Gratulacje! Jesteś szczęśliwym zwycięzcą nowego telefonu. Zapłać 2 euro za wysyłkę tutaj, aby odebrać nagrodę w

Dofinansowane przez Unię Europejską

ciągu najbliższej godziny". (Wywołuje podekscytowanie/chciwość/FOMO związane z nagrodą).(Opcjonalnie można stworzyć dodatkowe scenki obejmujące inne tematy, takie jak przykład cyberprzemocy: np. „Ktoś opublikował Twoje krępujące zdjęcie, skomentuj tutaj, aby odpowiedzieć", co wywołuje złość lub wstyd; lub przykład drapieżcy: „Cześć, podoba mi się Twój profil, wyglądasz na dojrzałą jak na 14 lat – porozmawiajmy prywatnie", co wywołuje pochlebstwo lub ciekawość. Jednak trzy podane przykłady obejmują wiele podstawowych czynników wyzwalających).

2. **Analiza w parach:** Poproś pary, aby przeczytały przydzieloną im scenę. Na kartce powinny podkreślić lub zanotować wszelkie sygnały ostrzegawcze (podejrzane elementy) oraz zakreślić słowa lub frazy, które wywołują emocjonalną reakcję. Następnie omówią, jakie uczucia mogą się pojawić (np. strach, pilna potrzeba, współczucie, podekscytowanie). Następnie poproś ich, aby napisali spokojną, dwuzdaniową odpowiedź, na jaką zasługuje wiadomość, tak jakby byli młodymi osobami odpowiadającymi na nią. Odpowiedź ta powinna być uprzejma, ale stanowcza i nie powinna ujawniać żadnych danych osobowych ani zawierać żadnych linków. Na przykład w przypadku scenariusza „Kontakt z pomocą techniczną" spokojną odpowiedzią może być: „Nie kliknę tego linku. Sprawdzę swoje konto za pomocą oficjalnej aplikacji". Na koniec muszą zaproponować jeden krok weryfikacyjny wykraczający poza treść wiadomości – np. „otworzyć bezpośrednio oficjalną stronę", „zadzwonić do znajomego w celu potwierdzenia" lub „zignorować i zgłosić tę wiadomość".
3. **Podziel się przykładowymi odpowiedziami:** Poproś każdą parę, aby krótko opisała swój scenariusz, co było bodźcem i jaką bezpieczną odpowiedź zaproponowała. Po każdym opisie udziel informacji zwrotnej, a następnie podaj przykładową odpowiedź dla danego scenariusza, (jeśli coś przeoczyli). Na przykład w przypadku „przyjaciela w pośpiechu" po opisie możesz podkreślić: „Czerwona flaga to prośba o podanie kodu logowania – to informacja prywatna. Czynnikiem wyzwalającym emocje jest poczucie, że musisz szybko pomóc przyjacielowi. Doskonałą odpowiedzią jest: „Nie udostępniam kodów. Zadzwonię do ciebie, żeby to wyjaśnić". Weryfikacją jest faktyczne zadzwonienie do tego przyjaciela (na jego stary numer lub inny kanał) w celu sprawdzenia, czy naprawdę potrzebuje pomocy". Zapisz szczególnie dobre zwroty, które wymyślili uczestnicy, lub podaj kilka przydatnych „neutralnych odpowiedzi" (podanych na arkuszu z opisem sytuacji i poniżej).

Dofinansowane przez Unię Europejską

4. **Zbierz typowe czynniki wyzwalające:** Na tablicy flipchart lub białej tablicy sporządź krótką listę czynników wyzwalających, które pojawiły się w różnych scenariuszach. Prawdopodobnie zobaczysz te z treści: pilność/strach, autorytet, empatia, nagroda, ciekawość itp. Obok każdego z nich poproś grupę o zaproponowanie odpowiedniej neutralnej lub asertywnej odpowiedzi. Na przykład:
    a. Pilność/strach → Odpowiedź: „Nie ma pośpiechu – sprawdzę to w oficjalnym źródle".
    b. Empatia/pomoc→ Odpowiedź: „Chciałbym pomóc, ale najpierw muszę to sprawdzić w inny sposób".
    c. Nagroda podekscytowanie → Odpowiedź: „Brzmi świetnie, ale nie klikam w linki. Sprawdzę to na oficjalnej stronie internetowej".
    d. Autorytet → Odpowiedź: „Nie udzielam takich informacji. Sam skontaktuję się bezpośrednio z pomocą techniczną".
    e. Ciekawość → Odpowiedź: „Zapytałem o to kogoś innego. Nie otwieram nieznanych linków".

    Stają się one zbiorem „domyślnych bezpiecznych odpowiedzi", których nauczyciele mogą później nauczyć swoich uczniów.
5. **Wzmocnienie EI → Bezpieczniejsze działania:** Podsumuj ponownie, w jaki sposób zastosowaliśmy właśnie powiązanie EI–cyberprzestrzeń: **świadomość → refleksja → regulacja → reakcja**. Na przykład powiedz: „W każdym przypadku najpierw zauważyliśmy nasze uczucia (świadomość), następnie zastanowiliśmy się, dlaczego (ta wiadomość próbuje wywołać we mnie uczucie X), zregulowaliśmy nasze reakcje, nie reagując od razu (być może biorąc głęboki oddech, przemyślając to w parach), a następnie wybraliśmy spokojną i bezpieczną odpowiedź. Właśnie tego chcemy nauczyć młodzież – czytania wiadomości z uwzględnieniem ich umysłów i uczuć"

Refleksja i dyskusja: Zadaj pytanie:, „Jakie sformułowanie najlepiej równoważy uprzejmość i bezpieczeństwo, gdy trzeba zwolnić tempo lub odmówić w Internecie?". To skłania uczestników do zastanowienia się nad tonem wypowiedzi – jak być asertywnym bez eskalacji konfliktu. Nauczyciele mogą podzielić się swoimi ulubionymi zwrotami, takimi jak „Nie klikam w linki; sprawdzę aplikację" lub „Nie czuję się komfortowo z tą prośbą". Omów, dlaczego uprzejmy, ale stanowczy język jest skuteczny (rozładowuje potencjalną konfrontację, ale nadal chroni Ciebie). Zapytaj również:, „Jakie wrażenie wywarło na was tworzenie tych odpowiedzi i jak może się czuć nastolatek, używając ich?". Może to prowadzić do ciekawych spostrzeżeń, na przykład ktoś może powiedzieć: „Trochę niezręcznie było pisać tak formalnie do przyjaciela – nastolatek może po prostu zignorować wiadomość zamiast

Dofinansowane przez Unię Europejską

odpowiadać, i to też jest w porządku. Najważniejsze, żeby nie zgodził się na to". Podkreśl, że ignorowanie lub brak odpowiedzi jest w wielu przypadkach również uzasadnioną i bezpieczną reakcją.

Najważniejsze wnioski:

- Wiele zagrożeń internetowych opiera się raczej na emocjonalnej presji lub manipulacji niż na sztuczkach technicznych. Już samo uświadomienie sobie, że „ta wiadomość ma na celu wywołanie u mnie paniki/podekscytowania", daje Ci siłę, by się jej oprzeć.
- Przygotowanie kilku neutralnych zwrotów lub działań może pomóc w sytuacjach stresowych. W sytuacji stresowej nasz umysł może się wyłączyć; jeśli młodzież przećwiczyła odpowiedzi typu „Sprawdzę to i dam ci znać" lub nawet po prostu wyjście z aplikacji, aby pomyśleć, jest bardziej prawdopodobne, że w sytuacji stresowej zachowa spokój.
- Ćwiczenie z wyprzedzeniem (poprzez scenariusze takie jak te) buduje pewność siebie. To jak ćwiczenia przeciwpożarowe w przypadku zagrożeń internetowych, – kiedy naprawdę do nich dojdzie, nie będziesz sparaliżowany; przypomnisz sobie, że radziłeś sobie już z czymś podobnym.

Ćwiczenie 3

Modelowanie głośnego myślenia – spowolnienie emocjonalnych komunikatów

Cele edukacyjne ćwiczeń

- Obserwowanie i zrozumienie, jak zatrzymać się i bezpiecznie reagować na emocjonalne komunikaty online.
- Nauka słów i działań, które pomagają zmniejszyć stres i uniknąć ryzykownych wyborów.
- Ćwiczenie własnej reakcji krok po kroku przy użyciu metody głośnego myślenia.

Przegląd ćwiczenia:

To ćwiczenie pokazuje, w jaki sposób nauczyciel może modelować pożądany proces podejmowania decyzji dla uczniów, myśląc na głos. Uczestnicy będą obserwować, jak prowadzący przechodzi przez dwa przykładowe komunikaty, omawiając każdy krok (nazywanie uczucia, zatrzymanie się, weryfikacja, reagowanie). Następnie uczestnicy opracują i przećwiczą własną 60-sekundową metodę głośnego myślenia dla wybranego przez siebie scenariusza. Dzięki temu nauczyciele nauczą się jasno przekazywać uczniom

Dofinansowane przez Unię Europejską

kolejne etapy procesu myślowego, a nie tylko wyniki, co ma kluczowe znaczenie dla nauki samodzielnego podejmowania decyzji przez młodzież. Zasadniczo pokazujesz uczniom, „co dzieje się w mojej głowie", gdy mam do czynienia z trudną wiadomością, dzięki czemu mogą oni uczyć się na przykładzie

Instrukcje:

1. **Przedstaw dwa podstawowe komunikaty:** Przygotuj dwa krótkie scenariusze komunikatów, które ilustrują różne czynniki wywołujące emocje. Na przykład:
    a. Komunikat A (pilność): „PILNE: Twoje konto zostanie zablokowane za 5 minut! Zweryfikuj teraz: [link] „ – wykorzystanie pilności/strachu.
    b. Komunikat B (empatia/oszustwo): „Cześć, jestem administratorem grupy szkolnej. Widziałem, że ktoś opublikował o Tobie nieprzyjemne rzeczy. Mogę pomóc w ich usunięciu, potrzebuję tylko Twoich danych logowania". – wykorzystanie połączenia autorytetu (administrator) i empatii (oferta pomocy) lub zastosowanie czegoś w rodzaju sztuczki opartej na empatii: „Naprawdę martwię się o Ciebie, kliknij teraz ten formularz bezpieczeństwa, abyśmy wiedzieli, że wszystko jest w porządku". (Możesz dostosować te przykłady, aby uwzględnić inne czynniki wyzwalające, takie jak scenariusz z przestępcą: „Hej, ślicznotko, zauważyłem, że masz tylko 15 lat, a ja mam 17, powinniśmy porozmawiać prywatnie" – czynnik wyzwalający pochlebstwo; ale upewnij się, że jest to odpowiednie dla odbiorców. Do modelowania zazwyczaj stosujemy typowe przykłady, takie jak phishing i podszywanie się pod inne osoby).
2. **Demonstracja głośnego myślenia przez facylitatora:** Dla każdej wiadomości „wykonaj" głośne myślenie przed grupą. Ponieważ jest to demonstracja, wyolbrzymiaj jasność poszczególnych kroków. Na przykład weź wiadomość A i powiedz na głos, jakbyś opisywał swój wewnętrzny dialog:
    a. „OK, właśnie otrzymałem tę wiadomość i serce mi zamarło – czuję, że jestem naprawdę zaniepokojony i podekscytowany. To dla mnie sygnał, że muszę zwolnić". (Określiłeś uczucie i czynnik wywołujący – pilność).
    b. „Ta wiadomość wykorzystuje pilność, aby mnie przestraszyć. Chcą, żebym spanikował. Najpierw, więc wezmę głęboki oddech". (Zatrzymujesz się i opanowujesz emocje – może faktycznie wykonaj szybki wdech i wydech w widoczny sposób).

Dofinansowane przez Unię Europejską

c. „O co oni proszą? Chcą, żebym kliknął link i podał informacje. To poważny sygnał ostrzegawczy – prawdopodobnie zagrożenie phishingiem. Zamiast klikać, przeprowadzę weryfikację: otworzę swoje konto w oficjalnej aplikacji, aby sprawdzić, czy naprawdę jest jakiś problem". (Zidentyfikowałeś potrzebną reakcję).
d. „Nie klikam tego. Gdyby to była prawdziwa wiadomość, zobaczyłbym powiadomienie w aplikacji lub mógłbym zapytać naszego nauczyciela informatyki. Poinformuję również moich znajomych, że ta wiadomość krąży w sieci – lepiej ostrzec innych". (Podsumowujesz odpowiedź, być może wspominając również o umiejętnościach interpersonalnych, takich jak dzielenie się wiedzą lub proszenie o pomoc).
e. „Cieszę się, że się zatrzymałem. Pamiętaj: zatrzymanie się pomaga mi zachować bezpieczeństwo". (Na zakończenie dodajesz kilka słów wzmacniających pewność siebie).

Zrób podobną analizę na głos do wiadomości B, pokazując, jak rozpoznajesz potencjalną próbę wzbudzenia współczucia, ale też zauważasz coś dziwnego (np. administrator proszący o dane logowania – nadużycie władzy). Mów spokojnym, pewnym głosem, a może nawet pokaż, jak spokojnie można odpowiedzieć (np. „Nie podałbym swoich danych; powiedziałbym:, „Dzięki, ale nie udostępniam haseł. Porozmawiam z nauczycielem o tych postach"). Dzięki dwóm nieco różniącym się przykładom uczestnicy dostrzegają wszechstronność tej metody.

3. **Dostarcz szablon „myśl na głos":** Rozdaj wszystkim szablon skryptu „Myśl na głos". Szablon ten zawiera podpowiedzi do wypełnienia: etykieta uczucia, zauważony czynnik wyzwalający, pauza, pytanie dotyczące ryzyka, krok weryfikacyjny, zdanie odpowiedzi, decyzja, monolog wewnętrzny. Przejrzyj szybko szablon, aby upewnić się, że uczestnicy rozumieją każdą część. Podkreśl, że cały skrypt powinien trwać około 60 sekund, więc kluczowe znaczenie ma zwięzłe sformułowanie.
4. **Uczestnicy piszą własny skrypt:** Teraz poproś każdego uczestnika, aby pomyślał o scenariuszu wiadomości, z którym może się spotkać lub który może go niepokoić (lub wybrał jeden z podanych, najlepiej taki, który nie został użyty w kroku 1 lub inny odpowiedni, np. fałszywa wiadomość udostępniona przez grupę rodzinną, która go zdenerwowała, lub komentarz dotyczący cyberprzemocy skierowany do niego). Powinni napisać krótki opis scenariusza na górze („Rodzaj wiadomości: np. podejrzany link na Discordzie" lub „Rodzaj wiadomości: złośliwy komentarz do mojego posta"), a następnie wypełnić szablon dla

Dofinansowane przez Unię Europejską

tego scenariusza. Zachęć ich, aby faktycznie wyobrazili sobie emocje: „Gdybyś otrzymał ten komentarz, jak byś się czuł? Nazwij to... Jaka jest sztuczka lub czynnik wyzwalający? Uświadom sobie to... Co zrobisz, aby zatrzymać się? Zanotuj to... Jak to zweryfikujesz lub z kim się skonsultujesz?...” i tak dalej.

5. **Ćwiczenie w parach:** Po przygotowaniu scenariuszy uczestnicy dzielą się na pary i ćwiczą głośne myślenie. Jedna osoba wykonuje około 60-sekundowe ćwiczenie głośnego myślenia, a druga słucha. Słuchacz może pokazać kciuk w górę za dobrze wykonane zadania i zasugerować jedną poprawkę, jeśli coś było niejasne lub można było poprawić płynność wypowiedzi. Następnie role się zamieniają.
6. **Wymiana doświadczeń w grupie(opcjonalnie):** Poproś 1–2 ochotników, (jeśli czas na to pozwala i ludzie są chętni), aby przedstawili swoje myśli na głos przed całą grupą. Po każdym wystąpieniu podkreśl skuteczne sformułowania lub kroki, które zastosowali. Na przykład, jeśli jeden z ochotników powiedział: „Zauważyłem, że czuję ciekawość, co oznacza, że muszę być ostrożny” – możesz zwrócić uwagę: „Świetnie, dostrzegła czynnik wywołujący ciekawość i potraktowała go, jako sygnał do zachowania ostrożności, a nie, jako powód do kliknięcia”. W razie potrzeby delikatnie popraw lub doprecyzuj wszystko (upewnij się, że odpowiedź była rzeczywiście bezpieczna itp., chociaż zazwyczaj na tym etapie powinny one być trafne). Zapisz szczególnie zapadające w pamięć zwroty lub techniki na tablicy flipchart, aby je utrwalić (np. „Prawdziwe wsparcie nigdy nie wymaga podania hasła” lub „Najpierw oddychaj, a potem zajmij się sprawą”).

Refleksja i dyskusja: Zapytaj grupę:, „Które zwroty lub podejście najlepiej spowolniły sytuację, nie eskalując jej i nie wprawiając nikogo w zakłopotanie?”. Zasadniczo, jakie sformułowania pozwoliły zachować spokój? Uczestnicy mogą na przykład wspomnieć: „Podoba mi się zwrot z jednego scenariusza: „Sprawdzę to oficjalnymi kanałami” – jest neutralny i nie wywołuje konfrontacji”. Ktoś inny może powiedzieć: „Pomocne wydawało się użycie krótkiego monologu wewnętrznego, np. „Dam radę, zachowaj spokój”. Omów znaczenie tonu głosu: spokojny, pewny siebie ton może rozbroić oszusta lub prześladowcę, podczas gdy gniewny lub przerażony ton może ich zachęcić lub jeszcze bardziej zdenerwować młodzież. Omów również, w jaki sposób opisanie procesu (uczniom) zapewnia im schemat, który mogą zapamiętać. Na przykład: „Słyszenie, jak ktoś mówi: „OK, czuję X, więc zrobię Y” ma ogromną moc – pokazuje krok po kroku. Dzieci często widzą tylko wynik (np. nieklikniecie), ale nie proces myślenia. To sprawia, że niewidzialny proces myślenia staje się widoczny.”

Dofinansowane przez
Unię Europejską

Najważniejsze wnioski:

- Głośne modelowanie jest potężnym narzędziem dydaktycznym. Kiedy nauczyciele pokazują dokładnie, jak radzić sobie w trudnych sytuacjach w Internecie, uwzględniając również aspekty emocjonalne, uczniowie uczą się nie tylko tego, co należy zrobić, ale także tego, jak dojść do takiej decyzji.
- Spokojny ton i konkretne kroki są dla młodzieży bardziej zapadające w pamięć niż abstrakcyjne ostrzeżenia. Zamiast po prostu mówić „Nie klikaj dziwnych linków" (łatwo powiedzieć, trudno zrobić, gdy emocje biorą górę), modelowanie pokazuje, jak faktycznie oprzeć się pokusie: poprzez dostrzeganie uczuć i rozmowę z samym sobą.
- Narracja tworzy mentalny scenariusz dla uczniów. Później uczeń może dosłownie przypomnieć sobie głos nauczyciela mówiącego: „Czuję strach, ale zamierzam oddychać i nie klikać" i naśladować to zachowanie. To tak, jakby dać im wewnętrznego trenera, który poprowadzi ich w decydującym momencie.

Ćwiczenie 4

Wyzwanie związane z błędnymi przekonaniami – prawda, fałsz czy zależy?

Cele edukacyjne ćwiczeń

- Odkrywanie i korygowanie popularnych mitów dotyczących cyberbezpieczeństwa i emocji.
- Ćwiczenie udzielania i przyjmowania prostych wyjaśnień w celu lepszego zrozumienia zagrożeń.
- Budowanie pewności siebie w zakresie wiedzy i bezpiecznych zachowań w Internecie.

Przegląd ćwiczenia:

Błędne przekonania mogą utrudniać naukę – na przykład nastolatek może wierzyć, że „tylko osoby starsze padają ofiarą oszustw" lub „jeśli używam silnego hasła, jestem w 100% bezpieczny". To ćwiczenie to dyskusja w formie gry, w której uczestnicy dostają zestaw krótkich stwierdzeń na temat cyberbezpieczeństwa i inteligencji emocjonalnej. Muszą sklasyfikować każde z nich, jako prawda, fałsz lub zależy (kontekstowo), a potem dodać jednozdaniowe sprostowanie lub wyjaśnienie. Pracując w grupach, będą dyskutować nad tymi punktami, a potem podzielą się najlepszymi wyjaśnieniami i dopracują je. Najważniejsze jest, aby robić to w sposób uprzejmy, bez osądzania, odpowiedni dla młodzieży. Oznacza to unikanie

Dofinansowane przez Unię Europejską

stwierdzeń typu „To nieprawda” i zamiast tego delikatne kierowanie rozmowy w stronę prawdy (np. „W rzeczywistości oszuści często atakują młodych ludzi, oferując im darmowe rzeczy…”). Na koniec grupa będzie miała zbiór „stwierdzeń korygujących”, które będzie mogła wykorzystać w nauczaniu.

Instrukcje:

1. **Karty z błędnymi przekonaniami:** Przygotuj zestaw około 10 stwierdzeń odzwierciedlających popularne mity lub nieporozumienia (przykłady znajdują się w załączniku E). Rozdaj listę, jako materiał informacyjny lub pokaż ją pojedynczo. Przykładowe stwierdzenia:
    a. „Jeśli moje hasło jest silne, nie potrzebuję uwierzytelniania dwuskładnikowego”.
    b. „Jeśli wiadomość pochodzi z konta znajomego, jest bezpieczna”.
    c. „Tylko osoby starsze padają ofiarą oszustw”.
    d. „Jeśli czuję niepokój, powinienem zignorować swoje odczucia i po prostu działać szybko”.
    e. „Oficjalna pomoc techniczna może poprosić mnie o podanie hasła, aby mi pomóc”.
    f. „Jeśli sprawa jest pilna, powinienem najpierw kliknąć, a potem pomyśleć”.
    g. „Korzystanie z publicznej sieci Wi-Fi jest zawsze bezpieczne, jeśli strona jest zabezpieczona protokołem HTTPS”.
    h. „Ustawienia prywatności nie mają znaczenia, jeśli nie jestem sławny”.
    i. „Jeśli nagroda wiąże się z niewielką „opłatą za wysyłkę”, prawdopodobnie jest prawdziwa”
    j. „Emocje osłabiają Cię w Internecie”.
2. **Upewnij się, że wśród nich znajdują się pozycje obejmujące tematy, które nas interesują:** hasło/2FA (techniczne), bezpieczeństwo konta znajomego (ryzyko oszustwa), wiek i oszustwa (każdy może stać się ofiarą), ignorowanie uczuć (niewłaściwe podejście do inteligencji emocjonalnej), prośba o informacje ze strony pomocy technicznej (oszustwo), pilność (czerwona flaga), publiczna sieć Wi-Fi (częściowa prawda), prywatność (każdy jej potrzebuje), oszustwo związane z niewielką opłatą (częsta taktyka oszustów), emocje (w rzeczywistości mogą być atutem, jeśli się nimi odpowiednio zarządza). Możesz dostosować sformułowania do swoich odbiorców.
3. **Klasyfikacja grupowa:** Podziel uczestników na małe grupy (3-5 osób w każdej). Ich zadanie: dla każdego stwierdzenia zdecydować, czy jest ono prawdziwe, fałszywe, czy „zależy”, (co oznacza, że ma niuanse). Następnie, – co najważniejsze – niech sformułują jednozdaniowe

Dofinansowane przez Unię Europejską

wyjaśnienie, które przekazaliby młodym ludziom, aby wyjaśnić im rzeczywistość. Wyjaśnienie powinno być uprzejme i konstruktywne. Na przykład w przypadku stwierdzenia „Tylko osoby starsze padają ofiarą oszustw" zaznaczyliby Fałsz i mogliby napisać: „Oszustwa są skierowane do wszystkich – oszuści często tworzą specjalne sztuczki również dla młodych ludzi". W przypadku stwierdzenia „Korzystanie z publicznej sieci Wi-Fi jest zawsze bezpieczne, jeśli jest to HTTPS" mogą zaznaczyć „Zależy" i wyjaśnić: „HTTPS jest dobre, ale publiczna sieć Wi-Fi nadal może być ryzykowna; unikaj wrażliwych transakcji w sieciach publicznych". Zachęć ich do używania analogii lub prostych terminów (np. „drugi zamek" dla 2FA). Daj im około 10–15 minut na omówienie wszystkich punktów.

4. **Dziel się i porównuj:** Przejrzyjcie wszystkie stwierdzenia po kolei w całej grupie. Zapytaj jedną grupę, jaką podjęła decyzję i jakie jest jej uzasadnienie/wyjaśnienie. Następnie zapytaj, czy inne grupy dokonały innej klasyfikacji lub sformułowały swoje wyjaśnienia w inny sposób. W przypadku rozbieżności między grupami (np. niektóre stwierdziły „zależy" vs „nieprawda") omówcie niuanse – jest to doskonała okazja do nauki. Postaraj się osiągnąć konsensus w sprawie każdego stwierdzenia, podając prawidłową odpowiedź i dopracowane, przyjazne dla młodzieży wyjaśnienie. Jako moderator, wnieś swój wkład i potwierdź dokładność informacji. Na przykład:
    a. „Jeśli moje hasło jest silne, nie potrzebuję 2FA". – Większość powinna odpowiedzieć „Fałsz". Wyjaśnienie: „Silne hasła są pomocne, ale 2FA dodaje drugą warstwę zabezpieczeń, która znacznie zwiększa bezpieczeństwo".
    b. „Jeśli wiadomość pochodzi z konta znajomego, jest bezpieczna". – Fałsz. Wyjaśnienie: „Konta mogą zostać zhakowane lub podszywane; jeśli coś wydaje się dziwne, sprawdź to za pomocą innego kanału".
    c. „Tylko osoby starsze padają ofiarą oszustw". – Fałsz. Wyjaśnienie: „Oszustwa są skierowane do wszystkich; istnieją oszustwa specjalnie zaprojektowane dla młodych ludzi (np. oszustwa związane z grami lub nagrodami)". Być może warto dodać statystyki lub anegdoty, jeśli takie posiadasz, (aby obalić mit „Jestem zbyt mądry/młody, aby dać się oszukać").
    d. „Jeśli czuję niepokój, powinienem zignorować swoje uczucia i po prostu działać". – Nieprawda. Wyjaśnienie: „Uczucia to sygnały. Jeśli czujesz niepokój, właśnie wtedy powinieneś zwolnić tempo i się zastanowić – a nie ignorować to uczucie".

Dofinansowane przez Unię Europejską

e. „Oficjalna pomoc techniczna może poprosić mnie o podanie hasła, aby mi pomóc”. – Nieprawda. Wyjaśnienie: „Prawdziwi pracownicy pomocy technicznej nigdy nie proszą o podanie hasła ani prywatnych kodów”.
f. „Jeśli sprawa jest pilna, powinienem najpierw kliknąć, a potem pomyśleć”. – Nieprawda. (Być może ktoś powie „To zależy” dla żartu, ale należy jasno powiedzieć, że jest to niebezpieczny mit). Wyjaśnienie: „Pilne wiadomości są często sygnałem ostrzegawczym oszustwa; zawsze należy poświęcić chwilę na przemyślenie i sprawdzenie – nie ma sprawy tak pilnej, aby nie można było poświęcić na to 10 sekund”.
g. „Korzystanie z publicznej sieci Wi-Fi jest zawsze bezpieczne, jeśli strona ma protokół HTTPS”. – Prawdopodobnie zależy. Wyjaśnienie: „HTTPS to dobre szyfrowanie, ale w publicznej sieci Wi-Fi nadal możesz być narażony na zagrożenia (np. połączenie z fałszywym hotspotem); lepiej unikać logowania się do serwisów wymagających podania poufnych danych w publicznej sieci Wi-Fi lub korzystać z VPN”. Wyjaśnienie powinno być proste i niezbyt techniczne.
h. „Ustawienia prywatności nie mają znaczenia, jeśli nie jestem sławny.” – Nieprawda. Wyjaśnienie: „Ustawienia prywatności są przydatne dla każdego. Ograniczają one krąg osób, które mają wgląd w Twoje dane – dzięki temu można zapobiec sytuacji, w której nieznajomi, a nawet przyszłe szkoły czy pracodawcy, zobaczą informacje, których nie chcesz upubliczniać”.
i. „Jeśli nagroda wiąże się z niewielką „opłatą za wysyłkę”, prawdopodobnie jest prawdziwa”. – Nieprawda. Wyjaśnienie: „Opłaty i liczniki czasu to klasyczne taktyki oszustów; prawdziwa nagroda nie wymaga płacenia z góry”.
j. „Emocje osłabiają Cię w Internecie”. – Fałsz. (Można by powiedzieć „zależy”, jeśli ktoś zinterpretuje to w dziwny sposób, ale należy skłaniać się ku fałszowi). Wyjaśnienie: „Emocje mogą Cię wzmocnić w Internecie, jeśli jesteś ich świadomy. Inteligencja emocjonalna – świadomość tego, kiedy jesteś zdenerwowany lub podekscytowany – pomaga kontrolować swoje działania. To nie jest słabość, to mądrość”. W miarę omawiania każdego z nich zapisz prawidłowy werdykt (P/F/Zależy) i dopracowane wyjaśnienie na tablicy lub w wspólnym dokumencie. Na koniec otrzymasz ładną listę obalających mity.

5. **Twórz poprawne zadania:** Zwróć uwagę na wzorce w wyjaśnieniach. Wiele z nich ma podobną strukturę: uznaj sedno prawdy lub problem, a

Dofinansowane przez Unię Europejską

następnie popraw go. Na przykład: „Silne hasła pomagają, ale 2FA dodaje drugą blokadę" lub „Oszustwa dotyczą wszystkich; taktyki są dostosowane również do młodzieży". Ta struktura („tak..., ale..." lub zwięzłe stwierdzenie prawdy) to świetny sposób na poprawę bez zawstydzania. Podkreśl kilka przydatnych zwrotów, które uczestnicy mogą ponownie wykorzystać:

a. „X pomaga, ale potrzebne jest również Y..." (w przypadku błędnych przekonań dotyczących wielopoziomowego bezpieczeństwa).
b. „Prawdziwa [instytucja] nigdy nie [podejmuje podejrzanych działań]..." (w przypadku oszustw – np. prawdziwe banki nigdy nie proszą o przesłanie hasła).
c. „Może się wydawać, że... ale w rzeczywistości..." (ogólny format obalenia).
d. „Wszyscy są narażeni na ryzyko, ponieważ..."
e. „Uczucie X jest sygnałem do wykonania Y, a nie powodem do paniki".
f. „Jeśli coś brzmi zbyt dobrze, aby mogło być prawdziwe, prawdopodobnie tak jest". Te zwroty mogą stać się częścią słownictwa nauczycieli.

Refleksja i dyskusja:, Które z błędnych przekonań zaskoczyło Cię najbardziej lub które Twoim zdaniem najczęściej pojawia się w Twoim otoczeniu? Jakie krótkie wyjaśnienie Twoim zdaniem najlepiej sprawdzi się w przypadku Twoich uczniów, aby skorygować to błędne przekonanie? Nauczyciele mogą zastanowić się, czy sami wierzyli wcześniej w któryś z mitów („Kiedyś uważałem, że wystarczające są silne hasła, ale teraz rozumiem, jak ważne jest uwierzytelnianie dwuskładnikowe – na pewno będę to podkreślał") lub zidentyfikować mity, które często powtarzają ich uczniowie („Moje nastolatki zawsze uważają, że tylko głupi ludzie padają ofiarą oszustw. Następnym razem, gdy to usłyszę, użyję zdania „oszustwa dotyczą wszystkich"""). Omów, w jaki sposób przedstawianie poprawek w sposób nieoceniający ma kluczowe znaczenie dla utrzymania zaufania – nigdy nie chcemy, aby uczeń czuł się źle z powodu posiadania błędnego przekonania; chcemy, aby czuł się silniejszy dzięki posiadaniu prawidłowej wiedzy.

Najważniejsze wnioski:

- Jasność i życzliwość zmniejszają opór. Kiedy korygujesz błędne przekonania, robienie tego z empatią i prostą logiką (a nie tylko „Nie, to nieprawda") sprawia, że młodzi ludzie są bardziej otwarci na zmianę swojego myślenia.

Dofinansowane przez Unię Europejską

- Posiadanie zapasu krótkich, korygujących wyjaśnień lub analogii ułatwia nauczanie. Można szybko obalać mity na bieżąco. (Np. „Pomyśl o 2FA jak o drugim zamku w drzwiach – jeden zamek można otworzyć, dwa zamki są znacznie trudniejsze do sforsowania").

Ćwiczenie to często ujawnia, że nawet nauczyciele mogą mieć przestarzałe lub błędne przekonania. Ciągłe uczenie się jest częścią cyberbezpieczeństwa – sytuacja się zmienia i ważne jest, aby być na bieżąco (np. znać nowe taktyki oszustów lub funkcje platform).

Ćwiczenia modułu 2

Ćwiczenie 1: Mapa cyberemocji

Zagrożenia, którym poświęcono uwagę: phishing, cyberprzemoc, dezinformacja, podszywanie się pod inne osoby

Cel: Pomoc młodzieży w rozpoznaniu, w jaki sposób zagrożenia internetowe wywołują emocje i wpływają na podejmowanie decyzji.

Format: Mieszany (dyskusja + tablica internetowa)

Kroki:

1. Przedstaw krótkie studia przypadków dotyczące różnych zagrożeń internetowych.
2. Młodzież identyfikuje emocje wywołane przez te zagrożenia.
3. Wspólne stworzenie „mapy emocji w cyberprzestrzeni".
4. Omówienie strategii radzenia sobie opartych na inteligencji emocjonalnej.

Ćwiczenie 2: Cyfrowy pokój zagadek – edycja cyberzagrożeń

Zagrożenia, którym poświęcono uwagę: oszustwa, phishing, fałszywe profile, złośliwe oprogramowanie

Cel: Nauczyć młodzież rozpoznawania zagrożeń internetowych pod presją czasu.

Format: Online lub hybrydowy

Kroki:

1. Zespoły rozwiązują zadania związane z cyberbezpieczeństwem.
2. Uwzględnij pytania dotyczące presji i stresu.

Dofinansowane przez Unię Europejską

3. Zastanów się nad emocjami i decyzjami.

Ćwiczenie 3: Odgrywanie ról związanych z EI i cyberbezpieczeństwem

Poruszane zagrożenia: cyberprzemoc, podszywanie się pod inne osoby, przestępcy seksualni, dezinformacja

Cel: Wzmocnienie empatii i komunikacji w sytuacjach konfliktowych w Internecie.

Format: Zajęcia stacjonarne z opcjonalną kontynuacją online

Ćwiczenie 4: wyzwanie związane z listą kontrolną dotyczącą cyberhigieny

Zagrożenia, którym poświęcone jest ćwiczenie: złośliwe oprogramowanie, phishing, nadmierne udostępnianie informacji

Cel: Promowanie codziennych zachowań zapobiegających zagrożeniom cyfrowym.

Format: online + offline

Ćwiczenie 5: Stres pod ekranem – warsztaty radzenia sobie ze stresem

Zagrożenia: impulsywne reakcje na phishing, oszustwa, cyberprzemoc

Cel: nauczyć technik zarządzania stresem opartych na inteligencji emocjonalnej.

Format: offline lub hybrydowy

Ćwiczenie 6: Krąg rówieśniczy ambasadorów cyberbezpieczeństwa

Zagrożenia: wszystkie osiem kluczowych zagrożeń internetowych

Cel: budowanie systemów wzajemnego wsparcia rówieśniczego.

Format: mieszany

Ćwiczenie 7: Opowiadanie historii z wykorzystaniem emocji i bezpieczeństwa

Zagrożenia, którym dotyczy: nadmierne dzielenie się informacjami, cyberprzemoc, oszustwa, dezinformacja

Cel: Połączenie osobistych historii cyfrowych z lekcjami dotyczącymi inteligencji emocjonalnej i cyberbezpieczeństwa.

Format: mieszany

Dofinansowane przez Unię Europejską

Ćwiczenie 8: Szybki quiz i refleksja

Zagrożenia, którym dotyczy: wszystkie kluczowe zagrożenia

Cel: Wzmocnienie wiedzy poprzez gamifikację.

Format: Quiz online

Dofinansowane przez
Unię Europejską

Ćwiczenia Modułu 3

Ćwiczenie 1: Cyfrowe lustro empatii

Temat: Cyberprzemoc i wroga komunikacja cyfrowa

Opis: To ćwiczenie ma na celu pomóc uczestnikom **rozwinąć inteligencję emocjonalną (EI)** poprzez uświadomienie im, że **komunikacja cyfrowa pozbawiona jest sygnałów niewerbalnych**, co może prowadzić do **nieporozumień, konfliktów i cyberprzemocy**. Porównując **interakcje online i bezpośrednie**, uczestnicy odkrywają, w jaki sposób **empatia, samoświadomość i regulacja emocjonalna** mogą zmniejszyć ryzyko **wrogich lub wykluczających zachowań cyfrowych**.

Cele nauczania:

- **Rozpoznawanie sygnałów emocjonalnych** (lub ich braku) w **komunikacji cyfrowej** (np. ton, dobór słów, emotikony).
- **Zrozumienie emocjonalnego wpływu nieporozumień komunikacyjnych** w środowisku internetowym, szczególnie w przypadku **cyberprzemocy lub wrogich wymian zdań**.
- **Ćwiczenie empatii, jako umiejętności ochronnej** w celu **łagodzenia konfliktów cyfrowych** i **budowania pełnych szacunku społeczności internetowych**.
- **Stosowanie samoświadomości w osobistej komunikacji cyfrowej,** zapewniając, że wiadomości są **jasne, uprzejme i celowe**.

Czas trwania: 50 minut (25 min online, 25 min osobiście)

Wielkość grupy: 8–20 uczestników

Materiały/narzędzia:

- **Anonimowe transkrypcje czatów** (3–4 przykłady **cyberprzemocy, języka wykluczającego lub nieporozumień**).
- **Tablica Padlet** do wspólnej refleksji.
- **Karty emocji** (np. złość, smutek, dezorientacja, strach, podekscytowanie).
- **Projektor lub wspólny ekran** do dyskusji grupowych.
- **Wydrukowane arkusze robocze** (do wykładów stacjonarnych).

Instrukcje:

Dofinansowane przez Unię Europejską

1. **Połącz się (online):**
    - ***Wprowadzenie:*** *Zacznij od* ***krótkiego filmu (3–5 min)*** *wyjaśniającego, w jaki sposób* ***brak tonu i mowy ciała w komunikacji cyfrowej*** *może prowadzić do* ***nieporozumień i cyberprzemocy****.*
    - ***Pytanie do dyskusji:*** *„Czy kiedykolwiek wysłałeś lub otrzymałeś wiadomość, która została źle zrozumiana? Jak się wtedy czułeś?”*
    - *Podziel się* ***3–4 anonimowymi przykładami czatów*** *(np.* ***wroga rozmowa grupowa, język wykluczający lub sarkastyczna uwaga potraktowana poważnie****).*
    - *Zapytaj:, „Jakie emocje mogą odczuwać nadawca i odbiorca? Jakich wskazówek brakuje w tej cyfrowej wymianie?”*
2. **Zbadaj (osobiście):**
    - ***Praca w parach:*** *W parach uczestnicy* ***analizują jeden przykład*** *czatu i omawiają*
        - *„Jakie emocje są obecne w tej wymianie zdań?”*
        - *„Jak ta rozmowa mogłaby przebiegać inaczej w sytuacji bezpośredniego kontaktu?”*
    - ***Odgrywanie ról:*** *Pary* ***odgrywają czat osobiście****, zwracając uwagę na* ***ton, mimikę twarzy i język ciała****.*
    - ***Dyskusja grupowa:*** *„Jak zmieniło się znaczenie, gdy zobaczyliście i usłyszeliście tę osobę? Jakich niewerbalnych wskazówek brakowało w oryginalnym czacie?”*
3. **Ćwiczenie (mieszane):**
    - ***Przepisywanie czatu:*** *Grupy* ***przepisują czat****, aby uczynić go* ***bardziej empatycznym i zrozumiałym****.*
        - *Przykład:, Jeśli oryginalna rozmowa była* ***wroga****, jak można ją przeformułować, aby* ***okazać zrozumienie i szacunek****?*
    - ***Refleksja cyfrowa:*** *Opublikuj przepisany czat na Padlet z adnotacją: „Jak empatia zmieniła interakcję? Jakie emocje wzięliście pod uwagę?”*
    - ***Opcja low-tech:*** *Uczestnicy z ograniczonym dostępem do technologii cyfrowych mogą* ***zapisać swoje odpowiedzi na***

Dofinansowane przez Unię Europejską

arkuszach roboczych *i podzielić się nimi podczas następnej sesji stacjonarnej.*

4. **Refleksja (online):**
    - ***Pytanie do dziennika:****, „Jakich sygnałów często brakuje w komunikacji online? W jaki sposób empatia może zapobiegać nieporozumieniom lub cyberprzemocy?”*
    - ***Ankieta Mentimeter:*** *„W skali od 1 do 5, jak bardzo czujesz się pewnie w rozpoznawaniu cyberprzemocy i reagowaniu na nią po tym ćwiczeniu?”*
5. **Podziel się (osobiście):**
    - ***Prezentacje grupowe:*** *Każda grupa przedstawia swoją* ***przepisana rozmowę*** *i wyjaśnia swoje* ***emocjonalne i językowe wybory****.*
    - ***Dyskusja podsumowująca****: „Jaka jest jedna zmienna, którą wprowadzisz w swojej komunikacji cyfrowej, aby zapewnić jej empatię i jasność?”*

Pytania do refleksji:

- Jakie **sygnały emocjonalne** najtrudniej jest przekazać w komunikacji cyfrowej?
- W jaki sposób **empatia** może pomóc w rozwiązywaniu **konfliktów online**?
- Jaka jest jedna zmiana, którą wprowadzisz w swojej **komunikacji cyfrowej** po tym ćwiczeniu?

Najważniejsze wnioski: Empatia i **aktywna interpretacja emocji** są kluczem do **budowania bezpieczniejszych i bardziej szanujących się społeczności cyfrowych**.

Ćwiczenie 2: Laboratorium scenariuszy cyberprzestępczości

Temat: Phishing, **oszustwa** i **podszywanie się**

Opis: Uczestnicy współpracują, aby **przeanalizować i odegrać scenariusze cyberzagrożeń** (np. wiadomości phishingowe, próby podszywania się, oszustwa FOMO). **Mapują emocje** wszystkich zaangażowanych osób i **wspólnie tworzą strategie zapobiegania** przy użyciu **technik EI**.

Cele nauczania:

Dofinansowane przez Unię Europejską

- Rozpoznawanie **czynników wywołujących emocje** w **phishingu i oszustwach**.
- Ćwiczenie **samokontroli** w celu uniknięcia impulsywnych reakcji.
- Opracowywanie **strategii wzajemnego wsparcia** w reagowaniu na **podszywanie się pod inne osoby lub oszustwa**.

Czas trwania: 90 minut (60 min osobiście, uzupełniające 30 min online)

Wielkość grupy: 10–25 uczestników

Materiały/narzędzia:

- **Karty przypadków** (scenariusze: wiadomość phishingowa, fałszywe zaproszenie do grona znajomych, oszustwo FOMO).
- **Flipchart lub cyfrowa tablica** (Miro/Jamboard).
- **Canva** do tworzenia **scenariuszy lub plakatów profilaktycznych**.
- **Forum Moodle/Teams** do refleksji uzupełniających.

Instrukcje:

1. **Połącz się (osobiście):**
    - Podziel uczestników na zespoły składające się z 4–5 osób. Przydziel każdemu zespołowi **scenariusz zagrożenia cybernetycznego** (np. phishing, podszywanie się, oszustwo).
    - Zapytaj:, „Jakie *emocje mogą odczuwać ofiara, obserwator i sprawca w tej sytuacji?”*
2. **Zbadaj (osobiście):**
    - Zespoły mapują emocje każdej osoby w scenariuszu.
    - Omów:, „Co *sprawia, że ta sytuacja jest ryzykowna? W jaki sposób inteligencja emocjonalna może pomóc?”*
3. **Ćwiczenie (osobiście):**
    - Zespoły tworzą **3-minutową scenkę lub scenariusz** przedstawiający **problem i strategię zapobiegania**.
    - Skoncentruj się na **technikach EI**: samoregulacji, przyjmowaniu perspektywy, wsparciu rówieśników.
4. **Refleksja (online):**

Dofinansowane przez Unię Europejską

- Opublikuj na **Moodle/Teams**:, „Jakie emocje wpłynęły na zachowanie w Twoim scenariuszu? W jaki sposób inteligencja emocjonalna może zapobiec szkodom?”

5. **Podziel się (osobiście + online):**
    - Zespoły przedstawiają swoje **skecze/scenariusze**.
    - Dalsze działania: Prześlij **wskazówki dotyczące zapobiegania** do **wspólnej sieci ośrodków młodzieżowych**.

Pytania do refleksji:

- Jakie **emocje** sprawiają, że ludzie są podatni na **oszustwa lub phishing**?
- W jaki sposób **samokontrola** może pomóc komuś **uniknąć impulsywnych kliknięć**?
- Jaka jest jedna **strategia EI**, którą wykorzystasz, aby **chronić się w Internecie**?

Najważniejsze wnioski: Uznanie **emocjonalnego wymiaru** zagrożeń cybernetycznych pozwala młodzieży **reagować konstruktywnie, a nie impulsywnie**.

Ćwiczenie 3: Projektant sesji integracyjnych

Temat: zagrożenia dla prywatności, dezinformacja i **złośliwe oprogramowanie**

Overview: Laboratorium projektowe umożliwia nauczycielom **stworzenie 30-minutowej sesji mieszanej**, która jest **emocjonalnie inteligentna, integracyjna i dostosowana** do różnych profili młodzieży. Sesja musi poruszać tematykę **zagrożeń dla prywatności, dezinformacji lub złośliwego oprogramowania, wykorzystując zasady Uniwersalnego Projektu w Edukacji (UDL)**.

Cele nauczania:

- Zastosowanie **UDL** do projektowania **sesji integracyjnych** dotyczących **zagrożeń internetowych**.
- Zintegrować **kompetencje emocjonalne i cyfrowe** w spójnej lekcji.
- Zastanowić się nad **dostępnością, uczestnictwem i samopoczuciem uczniów**.

Czas trwania: 90 minut

Dofinansowane przez Unię Europejską

Wielkość grupy: 6–20 edukatorów

Materiały/narzędzia:

- **Załącznik A: szablon plany sesji integracyjnej** (zapewniony przez PRAMMER).
- Laptop/tablet.
- Przestrzeń do współpracy (**Miro** lub **Google Docs**).

Instrukcje:

1. **Połącz się (osobiście):**
    - Przedstaw **2–3 profile młodzieży** (np. młodzież wiejska z ograniczonym dostępem do technologii cyfrowych; uczniowie z zaburzeniami neurologicznymi; młodzież migrująca z barierami językowymi).
    - Zapytaj:, „Jakie *wyjątkowe wyzwania mogą napotkać ci młodzi ludzie w związku z* ***zagrożeniami dla prywatności, dezinformacją lub złośliwym oprogramowaniem****?”*
2. **Zbadaj (osobiście):**
    - Zespoły wybierają **jeden obszar ryzyka** (prywatność, dezinformacja lub złośliwe oprogramowanie) i **jeden profil młodzieży**.
    - Wypełnij **szablon planu sesji**, podając szczegółowe informacje:
        - **Cele** (np. „Naucz, jak weryfikować źródła, aby zwalczać dezinformację”).
        - **Połączone fazy** (Połącz – Odkrywaj – Ćwicz – Zastanów się – Podziel się).
        - **Narzędzia** (np. Padlet do dyskusji na temat prywatności, Kahoot do quizów dotyczących złośliwego oprogramowania).
        - **Pytania wywołujące emocje** (np. „Jak byś się czuł, gdyby Twoje prywatne dane zostały ujawnione?”).
        - **Działania związane z dostępnością** (np. napisy do filmów, materiały drukowane).
3. **Ćwiczenie (mieszane):**

Dofinansowane przez Unię Europejską

- Zespoły **przedstawiają swoje plany sesji** kolegom.
- Koledzy przekazują informacje zwrotne, korzystając z **załącznika B: UDL i lista kontrolna dostępności**.

4. **Refleksja (online):**
   - Pytanie do dziennika:, „W jaki *sposób Twój projekt spełnia **emocjonalne i cyfrowe potrzeby** wybranego przez Ciebie profilu młodzieży? Jakie dostosowania były najbardziej skuteczne?”*
5. **Podziel się (osobiście):**
   - Omówienie: *„Jak możemy zapewnić wszystkim młodym ludziom, niezależnie od ich pochodzenia, poczucie **bezpieczeństwa i możliwości** poznania tych zagrożeń?”*

Pytania do refleksji:

- W jaki sposób Twój projekt uwzględniał kwestie **prywatności, dezinformacji lub złośliwego oprogramowania** w odniesieniu do **różnorodnych uczniów**?
- Które **adaptacje integracyjne** (np. opcje low-tech, zasoby wielojęzyczne) miały największy wpływ?
- W jaki sposób będziesz **oceniać zaangażowanie emocjonalne** podczas sesji?

Najważniejsze wnioski: Projektowanie **integracyjne od samego początku** gwarantuje **dostępność i bezpieczeństwo psychologiczne** dla każdego uczestnika.

Ćwiczenie 4: Gamifikacja emocji w Internecie

Temat: Oszustwa (oparte na FOMO), fałszywe wiadomości i phishing

Omówienie: Ćwiczenie to wykorzystuje **gamifikację** w celu wzmocnienia **umiejętności emocjonalnych i cyfrowych**, jednocześnie zwiększając zaangażowanie i motywację. Uczestnicy biorą udział w **quizie**, który łączy czynniki wywołujące emocje z zagrożeniami w Internecie, a następnie zastanawiają się nad tym, jak **emocje wpływają na decyzje podejmowane w sieci**.

Cele nauczania:

Dofinansowane przez Unię Europejską

- Przegląd **zasad EI i cyberbezpieczeństwa** związanych z **oszustwami, fałszywymi wiadomościami i phishingiem**.
- Doświadczenie, w jaki sposób **zabawowa rywalizacja** wspiera **zapamiętywanie i motywację**.
- Refleksja nad tym, jak **emocje** (np. strach, ciekawość, poczucie pilności) wpływają na **podejmowanie decyzji**.

Czas trwania: 35 minut (online)

Wielkość grupy: do 30 uczestników

Materiały/narzędzia:

- Platforma **Kahoot/Quizizz**.
- Projektor (opcjonalnie).
- Miejsce do dalszej dyskusji (**Mentimeter** lub **Padlet**).

Instrukcje:

1. **Połącz się (online):**
    - Przedstaw grę: *„Dzisiaj sprawdzimy waszą wiedzę na temat **czynników wywołujących emocje** w **oszustwach, fałszywych wiadomościach i phishingu**!”*
2. **Zbadaj (online):**
    - Rozpocznij **quiz Kahoot/Quizizz** z pytaniami typu:
        - *„Jakie emocje mogą skłonić kogoś do kliknięcia **linku phishingowego**?” (Opcje: strach, ciekawość, poczucie pilności).*
        - *„Dlaczego **oszustwa FOMO** są tak skuteczne?” (Opcje: wywołują podekscytowanie, presję lub poczucie ekskluzywności).*
        - *„Jak można sprawdzić, czy wiadomość jest **fałszywa**?” (Opcje: sprawdź źródło, poszukaj stronniczości, skorzystaj z funkcji wyszukiwania obrazów).*
3. **Ćwiczenie (online):**
    - Po każdym pytaniu **podkreśl emocjonalny czynnik** stojący za prawidłową odpowiedzią.

Dofinansowane przez Unię Europejską

- Przykład; *„Strach przed przegapieniem czegoś (FOMO) może sprawić, że będziemy działać impulsywnie — na przykład klikając **link do oszustwa!”***

4. **Refleksja (online):**
    - Pytanie po zakończeniu gry na **Mentimeter/Padlet**:, „Jakie *emocje doprowadziły do ryzykownych odpowiedzi w grze? W jaki sposób zrozumienie emocji może poprawić Twoje **decyzje online**?”*
5. **Podziel się (online):**
    - Poproś uczestników, aby **podzielili się jedną zmianą**, którą wprowadzą, aby czuć się **bezpieczniej i spokojniej w Internecie** (np. „Zanim kliknę link, zatrzymam się na chwilę”).

Pytania do refleksji:

- Które **emocje** sprawiły, że byliście najbardziej podatni na **oszustwa lub fałszywe wiadomości** w grze?
- W jaki sposób **grywalizacja** może pomóc w normalizacji dyskusji na temat **uczuć i bezpieczeństwa w Internecie**?
- Jak można wykorzystać **gry** we własnej praktyce mieszanej, aby uczyć o **phishingu lub dezinformacji**?

Najważniejsze wnioski: Metody oparte na zabawie zwiększają **zaangażowanie emocjonalne** i pomagają **normalizować dyskusje** na temat **uczuć i bezpieczeństwa w Internecie.**.

Ćwiczenie 5: Refleksyjny dziennik elektroniczny

Temat: wszystkie osiem obszarów ryzyka w Internecie

Omówienie: Strukturalna praktyka refleksji, która jest kontynuowana między sesjami, zachęcająca młodzież i nauczycieli do **samowiedzy i długotrwałej zmiany zachowań**. Uczestnicy, co tydzień zapisują w dzienniku swoje **doświadczenia emocjonalne** związane z **ośmioma rodzajami ryzyka w Internecie**.

Cele nauczania:

- Wyrobienie **nawyku regularnej autorefleksji**.
- Powiązanie **doświadczeń emocjonalnych** z **zachowaniem w Internecie**.

Dofinansowane przez Unię Europejską

- Monitorowanie **osobistych postępów** w kierunku **empatycznego i bezpiecznego zachowania w sieci**.

Czas trwania: 4–6 tygodni (asynchronicznie)

Wielkość grupy: zadanie indywidualne

Materiały/narzędzia:

- **Padlet** lub **wspólny folder Google Docs**.
- **Załącznik C: cotygodniowe pytania do refleksji** (zapewnione przez PRAMMER).

Instrukcje:

1. **Połącz się (online):**
    - Przedstaw dziennik: *„To miejsce, w którym możesz zastanowić się nad emocjami i zagrożeniami w Internecie—bez oceniania, tylko rozwój!”*
2. **Zbadaj (Asynchronicznie):**
    - Co tydzień uczestnicy odpowiadają na **1–2 pytania**, np.:
        - *„Jaka **sytuacja cyfrowa** w tym tygodniu sprawiła, że poczułeś się **dumny, niespokojny lub zły**? (np. **próba oszustwa, fałszywe wiadomości lub cyberprzemoc**.)”*
        - *“ „Jak zareagowałeś na **wiadomość phishingową lub próbę podszycia się**? Co zrobiłbyś inaczej?”*
        - *“ „Opisz sytuację, w której **zweryfikowałeś informacje** przed ich udostępnieniem. Jakie to było uczucie?”*
3. **Ćwiczenie (Asynchronicznie):**
    - Moderatorzy, co **tydzień przeglądają wpisy** i udzielają **empatycznych informacji zwrotnych** (np. *„Zauważyłem, że poczułeś frustrację z powodu **oszustwa FOMO**—jak samokontrola mogłaby pomóc następnym razem?”*).
4. **Refleksja (osobiście/online):**
    - Ostatnia sesja grupowa:, „Jaka *jedna **wniosek** z twojego dziennika zmieniła **twoje nawyki** online?”*
5. **Podziel się (osobiście):**

Dofinansowane przez Unię Europejską

- Uczestnicy **dzielą się zobowiązaniami** (np. *„Przed udostępnieniem wiadomości sprawdzę jej prawdziwość”*) i świętują postępy.

Pytania do refleksji:

- W jaki sposób **świadomość swoich emocji** zmieniła Twoje **nawyki w Internecie**?
- Które **strategie EI** (np. empatia, samokontrola) były najbardziej przydatne w przypadku **oszustw, cyberprzemocy lub zagrożeń dla prywatności**?
- W jaki sposób **prowadzenie dziennika** może wspierać **ciągłą naukę** o **bezpieczeństwie cyfrowym**?

Najważniejsze wnioski: Refleksja przekształca naukę w nawyk — konsekwentne prowadzenie dziennika buduje **cyfrową odporność emocjonalną**.

Ćwiczenia modułu 4

Poniżej przedstawiono ćwiczenia z modułu 4, które nauczyciele mogą wykorzystać do osiągnięcia celów nauczania. Ćwiczenia te mają charakter wysoce interaktywny i opierają się na scenariuszach, dając młodzieży możliwość przećwiczenia rozpoznawania zagrożeń i bezpiecznych reakcji w kontrolowanym środowisku. Obejmują one szereg metod (quizy, odgrywanie ról, dyskusje itp.) i można je łączyć i dopasowywać w zależności od czasu i zasobów. Co ważne, każde ćwiczenie zawiera elementy inteligencji emocjonalnej, pomagając młodzieży nie tylko rozpoznawać techniczne sygnały ostrzegawcze, ale także kontrolować swoje reakcje. Wszystkie ćwiczenia można dostosować do warunków online lub offline.

Ćwiczenie 1: Rozpoznaj zagrożenie – interaktywny quiz

Cel: Nauczyć uczestników rozpoznawania sygnałów zagrożenia w codziennych sytuacjach związanych z technologią cyfrową i łączenia każdego sygnału z bezpieczną reakcją lub działaniem. Ponadto pokazać, jak reakcje emocjonalne mogą wpływać na osąd.
Format: Online (Kahoot/Quizizz, udostępnianie ekranu) lub offline (quiz wyświetlany lub wydrukowany; ręczne liczenie punktów).
Czas trwania: 20-30 min.

Dofinansowane przez Unię Europejską

Instrukcje:

1. **Przygotuj pytania quizu:** Stwórz około 15 krótkich pytań. Najlepiej użyj materiałów wizualnych: zrzutów ekranu lub makiet takich elementów, jak wiadomość e-mail, wiadomość tekstowa, post w mediach społecznościowych, ekran logowania itp. Każdy z nich powinien przedstawiać scenariusz, który jest bezpieczny lub ryzykowny. Przykłady:

- Zrzut ekranu wiadomości e-mail z nieznanego adresu z informacją „Dostawa Twojej paczki nie powiodła się, kliknij tutaj, aby zmienić termin".
- Wiadomość WhatsApp z nieznanego numeru od osoby podającej się za przyjaciela, który potrzebuje pieniędzy.
- Post w mediach społecznościowych z sensacyjnym nagłówkiem (może zawierać fałszywe informacje).
- Profil przyjaciela, który nagle ma tylko 2 zdjęcia i został utworzony wczoraj, (co sugeruje, że jest to fałszywy profil).
- Wyskakujące okienko z komunikatem „Wykryto wirusa! Kliknij, aby zainstalować program czyszczący" na telefonie.
- Wiadomość na Instagramie z tekstem „Zobacz ten zabawny filmik o tobie! [Link]".
- Dodaj też kilka naprawdę bezpiecznych przykładów, żeby nie było to zbyt oczywiste (może to być prawdziwa wiadomość e-mail od znanej firmy bez żadnych podejrzanych elementów lub normalna wiadomość od znajomego).
- Do każdego z nich dodaj pytanie typu „Bezpieczne czy ryzykowne?" lub „Co byś zrobił?" z kilkoma opcjami do wyboru.
- Dodatkowo dodaj około 3 specjalne pytania dotyczące uczuć: np. po szczególnie przerażającym przykładzie pytanie, „Jakie uczucia wywołała w Tobie ta wiadomość? A) Nie martwiłem się, B) Byłem trochę zaniepokojony, C) Bardzo się przestraszyłem, D) Byłem podekscytowany" – to skłania do refleksji nad emocjami.

2. **Przeprowadzenie quizu:**, Jeśli quiz odbywa się online, uruchom go na wybranej platformie i poproś uczestników, aby dołączyli za pomocą swoich urządzeń. Jeśli quiz odbywa się offline, możesz wyświetlić każdy obrazek i poprosić uczestników o podniesienie kolorowych kartek lub zapisanie odpowiedzi. Jeśli żadna z tych opcji nie jest możliwa, wystarczy opisać scenariusz i poprosić uczestników o głosowanie przez podniesienie ręki lub przejście do odpowiedniego rogu sali (jeden róg = „bezpieczny", drugi = „ryzykowny.

Dofinansowane przez Unię Europejską

3. **Uczestnicy podejmują decyzję i uzasadniają ją:** W przypadku każdego elementu uczestnicy wybierają odpowiedź (lub fizycznie przechodzą do strefy odpowiedzi). Zachęć ich, aby zastanowili się, dlaczego wybrali opcję bezpieczną lub ryzykowną. Na przykład, jeśli ktoś widzi przykładową wiadomość e-mail i wybiera opcję „Ryzykowne", może to wynikać z tego, że dostrzegł błąd ortograficzny lub pomyślał „Nie spodziewałem się przesyłki, to wygląda na phishing".
4. **Ujawnij odpowiedzi wraz z wyjaśnieniem:** Po każdym pytaniu ujawnij prawidłową odpowiedź (czy rzeczywiście była to wiadomość phishingowa itp.) i podaj krótkie wyjaśnienie dotyczące sygnałów ostrzegawczych lub ich braku. Co ważne, podaj również wskazówkę, „Co zrobić następnym razem". Przykład:

- W przypadku prośby o pieniądze w WhatsApp: Ryzykowne. Prawdopodobnie oszustwo lub zhakowany znajomy. Wskazówka: Zweryfikuj, dzwoniąc do znajomego lub zadając pytanie, na które tylko on zna odpowiedź. Nie wysyłaj pieniędzy bez potwierdzenia.
- W przypadku sensacyjnego nagłówka: prawdopodobnie ryzykowne (może to być dezinformacja). Wywołało to niepokój u wielu osób (zgodnie z ich emocjonalnymi odpowiedziami). Wskazówka: sprawdź, czy źródło jest wiarygodne; przed udostępnieniem lub podjęciem działania sprawdź, czy zaufane serwisy informacyjne podają tę informację.
- W przypadku wyskakującego okienka reklamowego: ryzykowne. Jest to scareware próbujące nakłonić do pobrania pliku. Wskazówka: nie klikaj wyskakujących okienek. Jeśli uważasz, że coś jest nie tak, skorzystaj z wbudowanych zabezpieczeń telefonu lub zaufanej aplikacji ze sklepu z aplikacjami.
- W przypadku bezpiecznego przykładu (np. prawdziwego ekranu logowania dwuskładnikowego z witryny, o którą prosiłeś): Bezpieczne. Powód: pojawia się zgodnie z oczekiwaniami, a nie poprzez losowy link; ma odpowiedni branding itp. Mimo to zawsze warto sprawdzić adres URL.

5. **Podkreśl wszelkie elementy emocjonalne:** np. „Zwróćcie uwagę, jak oszustwo próbowało wywołać u was poczucie presji lub strachu – wielu z was stwierdziło, że czuliście niepokój. To jest wskazówka. Wykorzystajcie ten niepokój, jako przypomnienie, aby zwolnić tempo"
6. **Podsumowanie i elementy gry:**, Jeśli korzystasz z Kahoot lub podobnej platformy, będzie ona rejestrować wyniki i wyświetlać tabelę wyników. Jeśli nie korzystasz z Internetu, możesz zapisywać wyniki ręcznie lub po prostu zorganizować przyjacielską rywalizację, nagradzając oklaskami.

Dofinansowane przez Unię Europejską

Na koniec podziękuj zwycięzcom. Nie chodzi tu o wysokie stawki, tylko o odrobinę motywacji.

7. **Podsumowanie refleksji:** Po quizie zapytaj:, „Które elementy były najtrudniejsze do zidentyfikowania? Które były najłatwiejsze?" oraz „Które emocje najczęściej prowadziły do błędów?". Na przykład uczestnicy mogą powiedzieć: „Najbardziej podekscytowałem się nagrodą i prawie kliknąłem – moje podekscytowanie sprawiło, że zignorowałem podejrzany link". Omów, w jaki sposób zatrzymanie się i sprawdzenie może to złagodzić. Podkreśl, jeśli pojawiły się jakieś spostrzeżenia uczestników: „Jeden z was wspomniał, że przestraszył się fałszywego alertu – właśnie ten strach jest powodem, dla którego musimy się zatrzymać". Połącz to z świadomością → refleksją → regulacją: quiz był ćwiczeniem szybkiej świadomości; w prawdziwym życiu dodajemy etapy refleksji/regulacji.

Potrzebne narzędzia: W przypadku trybu online – platforma quizowa (Kahoot, Quizizz, tryb quizowy Mentimeter) oraz urządzenia uczestników. W przypadku trybu offline – wydrukowane zrzuty ekranu lub slajdy oraz sposób, w jaki uczestnicy mogą zaznaczać odpowiedzi (kartki, papiery, przemieszczanie się).

Adaptacja: W przypadku bardzo niskiego poziomu zaawansowania technologicznego można nawet przeprowadzić „quiz słowny": opisać scenariusz i poprosić uczestników, aby wykrzykiwali „Bezpieczne!" lub „Ryzykowne!", a następnie omówić wyniki. Można też przekształcić to zadanie w kontinuum ludzkie (ustawienie się w kolejce od oceny bezpiecznej do ryzykownej). Kluczem jest interakcja i natychmiastowa informacja zwrotna.

Ćwiczenie 2: Za kliknięciem – czynniki wywołujące emocje

Cel: Pomóc uczestnikom rozpoznać czynniki manipulacji w wiadomościach i przećwiczyć formułowanie spokojnych, asertywnych odpowiedzi na każdy rodzaj czynnika. Pozwala to stworzyć mentalną bibliotekę domyślnych odpowiedzi, z których można skorzystać w sytuacjach stresowych. **Format:** Można to zrobić online, korzystając z tablicy współpracy (Padlet lub Canva), na której dopasowuje się wyzwalacze i przykłady, lub offline, korzystając z wydrukowanych kart wyzwalaczy i pasków scenariuszy, nad którymi grupy pracują na papierze lub na ścianie. Obejmuje to dyskusje w małych grupach i wspólne tworzenie scenariuszy „bezpiecznych odpowiedzi".

Czas trwania: 30-40 min.

Instrukcje:

Dofinansowane przez Unię Europejską

1. **Rozdawanie kart wyzwalających:** Istnieje sześć klasycznych wyzwalaczy, które chcemy omówić (odzwierciedlając to, co zostało omówione w treści modułu 1): pilność, strach, empatia, okazja/nagroda, autorytet, ciekawość (można dodać siódmy, np. dowód społeczny/FOMO, jeśli jest to pożądane, lub połączyć go z ciekawością/nagrodą). Daj każdej małej grupie (3-4 osoby) jedną kartę wyzwalającą. Na przykład:

- Grupa 1 otrzymuje pilność (wiadomość grożąca szybkimi konsekwencjami).
- Grupa 2 otrzymuje strach (przerażająca wiadomość typu alert bezpieczeństwa).
- Grupa 3 otrzymuje empatię (prośba o wzruszającą historię).
- Grupa 4 otrzymuje Autorytet (ktoś udający, że jest szefem).
- Grupa 5 otrzymuje Szansę/Nagrodę (wygrałeś coś lub otrzymałeś coś ekskluzywnego).
- Grupa 6 otrzymuje Ciekawość (kusząca do kliknięcia, aby zobaczyć plotki lub tajne informacje).

Jeśli masz mniej uczestników, jedna grupa może obsłużyć dwa wyzwalacze lub pominąć jeden mniej powszechny wyzwalacz.

2. **Podaj przykłady:** Wraz z opisem wyzwalacza, przekaż każdej grupie jeden lub dwa przykładowe komunikaty (lub zapisz je na tablicy/kartkach papieru

- Przykład pilności: „Twoje konto zostanie zawieszone za 30 minut, jeśli nie potwierdzisz hasła tutaj [link]”.
- Przykład strachu: „Ostrzeżenie dotyczące bezpieczeństwa: ktoś próbował uzyskać dostęp do Twoich zdjęć! Wyślij ten kod TERAZ, aby zabezpieczyć swoje konto”.
- Przykład empatii: „Proszę, młodszy brat mojego przyjaciela jest w szpitalu. Pilnie potrzebujemy darowizn, każda kwota się przyda. Kliknij tutaj, aby wysłać pomoc”.
- Przykład autorytetu: „Administrator: Tu pomoc techniczna. Wykryliśmy złośliwe oprogramowanie na Twoim koncie. Odpowiedz, podając swoje dane logowania, abyśmy mogli to naprawić”.
- Przykład wykorzystujący okazję: „Gratulacje, zostałeś wybrany do testowania nowej gry w wersji beta i otrzymasz za to wynagrodzenie! Aby rozpocząć, wystarczy wypełnić ten formularz swoimi danymi”.
- Przykład wykorzystujący ciekawość: „O mój Boże, spójrz na to zdjęcie, które znalazłem w Internecie. Czy to ty? [Link] „ lub „W tej grupie mówią o tobie okropne rzeczy, pomyślałem, że powinieneś to zobaczyć [link]”.

Dofinansowane przez Unię Europejską

3. **Zadanie grupowe – dopasowanie wyzwalacza do przykładu i przygotowanie odpowiedzi:** Poproś grupy, aby najpierw potwierdziły, że ich przykłady rzeczywiście pasują do wyzwalacza (powinny, zgodnie z założeniem). Powinny one dokładnie określić, które słowa lub elementy w przykładzie ilustrują wyzwalacz. Na przykład, podkreślając „30 minut" i „zawieszony" dla pilności lub „młodszy brat…szpital" dla empatii. Następnie każda grupa przygotowuje krótki „scenariusz bezpiecznej odpowiedzi" dla swojego przykładu. Zazwyczaj jest to 1-3 zdania, spokojne i asertywne. Zachęć ich do użycia neutralnych zwrotów z modułu 1 (które możesz zapisać na tablicy, jako przypomnienie, np. „Nie udostępniam informacji za pośrednictwem linków; sprawdzę oficjalną stronę" lub „Nie mogę pomóc w ten sposób, przepraszam"). Ponadto uczniowie powinni uwzględnić w scenariuszu lub bezpośrednio po nim to, co faktycznie zrobiliby (krok weryfikacyjny lub alternatywne działanie).

- Przykład pilnej sprawy: dobrym scenariuszem może być „Nie będę się spieszył. Zaloguję się normalnie na swoje konto, aby sprawdzić, czy jest jakiś problem" (nie podając informacji w wiadomości).
- Przykład strachu: „Nie wyślę żadnego kodu. Sam sprawdzę ustawienia bezpieczeństwa mojego konta, – jeśli pojawił się alert, zobaczę go tam".
- Przykład empatii: „Przekazuję darowizny tylko za pośrednictwem znanych stron charytatywnych lub osobiście. Zweryfikuję tę historię za pomocą zaufanego źródła" lub po prostu „Przykro mi, nie mogę pomóc w ten sposób. Mam nadzieję, że Twój przyjaciel otrzyma pomoc" (i nie klikam w link).
- Przykład autorytetu: „Dziękuję, ale nie mogę podać swojego hasła. Skontaktuję się z oficjalną pomocą techniczną za pośrednictwem strony internetowej, aby to zweryfikować".
- Przykład wykorzystujący okazję: „Brzmi fajnie, ale nie podaję danych osobowych bez sprawdzenia. Najpierw sprawdzę tę firmę za pośrednictwem oficjalnych kanałów".
- Przykład wykorzystujący ciekawość: „Nie kliknę tego linku. Jeśli chodzi o mnie, dowiem się tego bezpośrednio lub zapytam znajomego – to wygląda podejrzanie".

4. **Podziel się wynikami:** oproś każdą grupę, aby przedstawiła swój bodziec, sposób, w jaki został on zilustrowany w przykładzie, oraz scenariusz odpowiedzi. Zachęć pozostałych uczestników do klaskania lub oklaskiwania dobrych odpowiedzi – dbaj o atmosferę wsparcia. W miarę jak poszczególne grupy dzielą się swoimi odpowiedziami, zbierz je w zbiorczą listę „Domyślnych odpowiedzi na bodźce" na tablicy lub

Dofinansowane przez Unię Europejską

slajdzie. Prawdopodobnie zauważysz powtarzające się odpowiedzi (wiele grup może odpowiedzieć „Nie klikam linków w wiadomościach"), co jest dobre – wzmacnia to kluczowe bezpieczne zachowania.
Jeśli w odpowiedzi grupy brakuje czegoś ważnego, delikatnie zapytaj: „Czy dodalibyście coś, aby odpowiedź była bezpieczniejsza?". Na przykład, jeśli nie uwzględnili etapu weryfikacji, zasugeruj to i sprawdź, czy zgodzą się to dodać.
Zwróć też uwagę na szczególnie sprytne lub empatyczne sformułowania. Na przykład, jeśli ktoś grzecznie odmówił, mówiąc „Przepraszam, nie mogę tego teraz zrobić", zaznacz, że nie zawsze trzeba się długo tłumaczyć – prosta odmowa jest w porządku.

5. **Stwórzcie wspólny zestaw odpowiedzi:** Na koniec powinniście mieć, co najmniej 6 przykładowych odpowiedzi na skrypty (po jednej na każdy bodziec). Warto to udostępnić/sfotografować i ewentualnie rozdać później, jako ściągawkę. Jest to w zasadzie stworzony przez młodzież „klucz odpowiedzi" na podejrzane wiadomości.
6. **Dodatkowa dyskusja - osobiste** wyzwalacze**:** Teraz zapytaj:, „Który wyzwalacz ma na ciebie największy wpływ? Na który najłatwiej się nabierzesz lub który jest dla ciebie najtrudniejszy do odparcia?" oraz „Jaka mogłaby być twoja osobista, wcześniej zaplanowana odpowiedź lub strategia w tej sytuacji?". Na przykład ktoś może powiedzieć: „Ciekawość mnie dopada. Jeśli widzę coś na swój temat, naprawdę chcę to kliknąć. Dlatego moim planem jest zawsze najpierw pokazać to znajomemu – to moja obecna zasada". Inny uczestnik może powiedzieć: „Przeraża mnie poczucie pilności; myślę, że pomocne będzie przygotowanie sobie w głowie frazy „Zaloguję się normalnie". Ta refleksja personalizuje lekcję – każdy uczestnik uznaje swoją własną podatność na zagrożenia i uzbraja się w odpowiedź.

Narzędzia: W przypadku pracy online – Padlet lub wspólny dokument Canva/Google Slide, w którym jedna kolumna zawiera listę wyzwalaczy, druga kolumna zawiera przykładowe zrzuty ekranu (można je przeciągnąć pod odpowiedni wyzwalacz), a trzecia kolumna służy do wpisywania odpowiedzi. W przypadku pracy offline – wydrukuj tytuły wyzwalaczy na kartonie, a przykładowe wiadomości na paskach papieru, pozwól uczestnikom fizycznie pogrupować je i napisać odpowiedzi na papierze, który następnie przykleją obok nich lub na tablicy flipchart.

Rezultat: Uczestnicy wychodzą z jasnymi przykładami tego, jak wyglądają oszukańcze lub manipulacyjne wiadomości, oraz konkretnymi, przećwiczonymi zwrotami lub działaniami, które należy podjąć. Zmniejsza to ryzyko, że w

Dofinansowane przez Unię Europejską

rzeczywistej sytuacji zaniemówią – przypomną sobie: „Widziałem to już wcześniej – to tylko próba wywarcia na mnie presji; wiem, co robić”.

Ćwiczenie 3: Cyberdetektyw – akta spraw

Cel: Daj uczestnikom możliwość przećwiczenia umiejętności weryfikacji i wykrywania zagrożeń w bardziej złożonych scenariuszach zawierających mieszane informacje. Muszą oni przeanalizować dowody, zidentyfikować sygnały ostrzegawcze, zweryfikować fakty w drugim źródle i podjąć decyzję o bezpiecznym sposobie postępowania (reagować, zgłosić lub zignorować). Symuluje to rzeczywiste sytuacje, w których nie wszystko jest jasne na pierwszy rzut oka.

Format: Zadanie dla małych zespołów, polegające na pracy z dostarczonymi „aktami sprawy”, które zawierają wiele dowodów (np. podejrzaną wiadomość prywatną, fragment profilu, podgląd linku itp.). Zadanie można wykonać online (za pośrednictwem systemu LMS lub folderów współdzielonych) lub offline (w formie wydrukowanych pakietów). Następnie zespoły przedstawiają swoje ustalenia.

Czas trwania: 45–60 min.

Instrukcje:

1. Przygotuj dokumentację spraw: Stwórz 2 lub 3 różne scenariusze spraw. Każda dokumentacja sprawy powinna zawierać:
- Krótki opis lub kontekst.
- Co najmniej 2-3 dowody, takie jak:
- Zrzut ekranu lub tekst podejrzanej wiadomości (np. powiadomienie o wygranej w konkursie lub wiadomość od znajomego z dziwną prośbą).
- Fragment profilu internetowego związanego z tą sprawą (np. profil osoby, która wysłała wiadomość, pokazujący coś, co wygląda na nowe lub nie ma wspólnych znajomych).
- Podgląd linku lub adres URL, który mogą rozważyć kliknąć (można podać tekst adresu URL i ewentualnie opisać, jak wygląda strona internetowa).
- Kilka wskazówek/pytań dla zespołu, np.: „Wymień trzy sygnały ostrzegawcze, które zauważyłeś”, „Jak można sprawdzić, czy jest to prawdziwa wiadomość?” oraz „Co postanowiłby zrobić Twój zespół: odpowiedzieć, zignorować, zgłosić lub coś innego?”.
2. Upewnij się, że przypadki obejmują **szereg zagrożeń**, np.:

Dofinansowane przez Unię Europejską

- Przypadek 1 może dotyczyć „wiadomości konkursowej” – klasycznego phishingu mającego na celu uzyskanie danych osobowych pod pozorem wygranej nagrody (obejmuje phishing/oszustwo).
- Przypadek 2: „przyjaciel w potrzebie” – prawdopodobnie podszywanie się pod przyjaciela potrzebującego pieniędzy za granicą (obejmuje fałszywe zaproszenia do grona znajomych/podszywanie się, wywoływanie empatii).
- Przypadek 3: „Fałszywa oferta pracy” lub „Wspaniała okazja” – nastolatek otrzymuje e-mail/wiadomość prywatną dotyczącą dobrze płatnej pracy, wymagającej podania danych bankowych (obejmuje oszustwo, być może również nadużycie władzy).
- Można również wyobrazić sobie przypadek 4 dotyczący cyberprzemocy lub scenariusza z udziałem przestępcy seksualnego (w zależności od czasu itp.), ale należy uważać, aby nie przeładować materiału. Pierwsze trzy przypadki obejmują dość szeroki zakres zagadnień.

3. **Przydział zespołu:** Podziel uczestników na zespoły po około 4 osoby. Przydziel każdemu zespołowi jedną sprawę, (jeśli jest mniej zespołów niż spraw, wykorzystaj tylko niektóre sprawy; jeśli jest więcej zespołów, dwa zespoły mogą zająć się tą samą sprawą i porównać wyniki). Przekaż im materiały dotyczące sprawy (za pośrednictwem wspólnego dokumentu online lub wydrukowanych materiałów z dołączonymi obrazami).
4. **Faza badania:** Zespoły wspólnie analizują materiały (ok. 15 minut). Powinny one:

- Przeczytaj opis, aby zrozumieć kontekst.
- Sprawdź każdy dowód pod kątem niespójności lub sygnałów ostrzegawczych (np. w przypadku konkursu mogą zwrócić uwagę, że wiadomość o nagrodzie pochodziła z ogólnego adresu Gmail, link jest typu bit.ly lub profil, z którego wysłano wiadomość, ma 0 obserwujących).
- Sporządź listę sygnałów ostrzegawczych: poproś jednego z członków, aby sporządził listę punktów.
- Spróbuj zweryfikować informacje:, jeśli masz dostęp do Internetu i jest to wykonalne, możesz poprosić członków grupy o przeprowadzenie szybkiego wyszukiwania lub sprawdzenia (np. wpisanie w wyszukiwarce Google hasła „nazwa konkursu + oszustwo” lub sprawdzenie, czy prawdziwy profil znajomego zawiera informację o włamaniu). Jeśli nie masz dostępu do Internetu, członkowie grupy mogą sformułować hipotezę dotyczącą sposobu weryfikacji (np. „Zadzwonimy do rodziny znajomego, aby sprawdzić, czy naprawdę jest za granicą”).

Dofinansowane przez Unię Europejską

- Na podstawie dowodów i weryfikacji uczestnicy decydują, jakie działanie jest najlepsze: np. zignorować/usunąć wiadomość, zgłosić konto platformie, odpowiedzieć z ostrożnością (w takich przypadkach prawdopodobnie rzadko się odpowiada) lub zebrać więcej informacji.
- Poproś ich również, aby zwrócili uwagę, czy podczas pracy zespołowej przydała się jakaś strategia EI: czy ktoś powiedział: „Hej, nie wyciągajmy pochopnych wniosków, co czujemy i co faktycznie wiemy?" lub czy poświęcenie chwili na dokładniejsze sprawdzenie uspokoiło osobę, która początkowo była spanikowana scenariuszem?

5. Prezentacje zespołów: Każdy zespół przedstawia grupie podsumowanie swojej sprawy:

- Krótkie streszczenie scenariusza („Nasza sprawa dotyczyła wygrania konkursu…").
- Zauważone przez nich sygnały ostrzegawcze („Wiadomość zawierała błędy ortograficzne i prośbę o przesłanie dokumentu tożsamości, co jest dziwne").
- Jak zweryfikowali lub zweryfikowaliby („Wyszukaliśmy konkurs w Internecie – nie znaleźliśmy żadnych oficjalnych informacji. Ponadto profil rzekomego organizatora konkursu został utworzony wczoraj, co jest podejrzane").
- Jak zweryfikowali lub zweryfikowaliby („Wyszukaliśmy konkurs w Internecie – nie znaleźliśmy żadnych oficjalnych informacji. Ponadto profil rzekomego organizatora konkursu został utworzony wczoraj, co jest podejrzane").
  Zachęć ich do wspomnienia o aspekcie emocjonalnym: „Na początku jeden z nas był naprawdę podekscytowany, myśląc, że to prawda, co pokazuje, jak oszustwo może cię wciągnąć. Ale inny członek zespołu był sceptyczny. Wspólna dyskusja pomogła – dobrą lekcją jest zapytanie kogoś innego, gdy nie jesteś pewien".

6. **Lista kontrolna dla moderatora:** Po zakończeniu zadania przez każdą z drużyn należy uzupełnić listę o wszelkie istotne kwestie, które zostały pominięte. Na przykład, jeśli drużyna nie wspomniała o tym, jak ważne jest, aby nie wysyłać zdjęcia z dowodu osobistego, (ponieważ może ono zostać wykorzystane do kradzieży tożsamości), należy zwrócić na to uwagę: „Zgadza się, wysłanie dowodu osobistego byłoby bardzo niebezpieczne, ponieważ oszuści mogliby go wykorzystać do podszywania się pod Ciebie – dobrze, że zdecydowałeś się tego nie robić". W każdym przypadku wyciągnij ogólną lekcję:

Dofinansowane przez Unię Europejską

- Oszustwo związane z konkursem: zbyt dobra, aby była prawdziwa oferta + prośba o podanie danych osobowych = prawdopodobne oszustwo. Emocjonalnym haczykiem było podekscytowanie/chciwość.
- Przyjaciel w potrzebie: zawsze weryfikuj poprzez drugi kanał, jeśli przyjaciel prosi o pieniądze lub kody. Emocjonalnym haczykiem była empatia/przyjaźń i pilność.
- Fałszywa oferta pracy: wysokie wynagrodzenie za niewielką pracę + prośba o podanie danych bankowych z góry = oszustwo. Emocjonalnym haczykiem było podekscytowanie i być może pochlebstwo (oni „wybrali" ciebie).
- Jeśli wystąpiła sytuacja uwodzenia przez przestępcę: szukaj oznak zbytniego zainteresowania, zbyt szybkiego działania, prośby o osobiste zdjęcia itp. Wniosek: nigdy nie kontynuuj, jeśli osoba poznana w Internecie zaczyna być zbyt osobista lub prosi o coś – poproś o pomoc zaufaną osobę dorosłą. Emocjonalnym haczykiem jest często uznanie i miłość, ale w prawdziwych związkach nie buduje się zaufania w ten sposób.
- Przypadek cyberprzemocy, (jeśli taki wystąpił): być może złośliwy post i fałszywy profil wywołujący dramatyczne wydarzenia. Wniosek: nie odpowiadaj gniewem (może to doprowadzić do eskalacji); zbierz dowody, zablokuj, zgłoś i porozmawiaj z kimś. Emocjonalnym haczykiem jest gniew/wstyd.

  Podsumowanie: Zespoły skutecznie pełniły rolę „cyberdetektywów", a najważniejszą umiejętnością była weryfikacja poprzez drugi kanał i komunikacja zespołowa. Często to, co jedna osoba przeoczy, zauważa inna, – dlatego zachęcaj młodzież do konsultowania się ze sobą również w prawdziwym życiu.

7. **Refleksja:** Zapytaj:, „Jakie strategie EI pomogły zespołowi zachować spokój i skupienie w obliczu niejasności lub presji związanych z tymi przypadkami?". Uczestnicy mogą odpowiedzieć: „Przypomnieliśmy sobie, że może to być podstęp, więc nie poddaliśmy się emocjom" (samoregulacja) lub „Podzieliliśmy się zadaniami, co pozwoliło nam zachować spokój" (umiejętności interpersonalne, praca zespołowa) lub „Poświęciliśmy chwilę, aby potwierdzić nasze przeczucia poprzez szybkie wyszukiwanie informacji" (świadomość i refleksja w działaniu). Zapytaj również:, „W jaki sposób praca zespołowa zmieniła wynik w porównaniu z sytuacją, gdybyś działał samodzielnie?". Prawdopodobnie wzmocni to wartość wsparcia rówieśników – osoba działająca samodzielnie mogłaby dać się nabrać, ale w zespole ktoś powiedział: „Chwileczkę, coś tu nie gra". Chcemy, aby młodzież zdała sobie sprawę, że w kwestiach bezpieczeństwa dwie głowy są lepsze niż jedna.

Dofinansowane przez Unię Europejską

Narzędzia:, Jeśli korzystasz z Internetu, możesz przesłać zdjęcia i teksty dotyczące spraw do Google Drive/OneDrive lub forum Moodle dla każdego zespołu. Możesz też skorzystać z pokoi do pracy w grupach. Jeśli nie korzystasz z Internetu, wydrukuj wszystko wyraźnie (może w kolorze, jeśli chodzi o zrzuty ekranu) i umieść w kopertach oznaczonych „Sprawa 1" itp., aby stworzyć atmosferę detektywistyczną.

Rezultat: Uczestnicy ćwiczą dogłębną analizę i zdają sobie sprawę, że zagrożenia często wiążą się z wieloma wskazówkami, jeśli przyjrzeć się im dokładniej. Ćwiczą również weryfikację (a nie tylko przyjmowanie rzeczy za dobrą monetę) – kluczową umiejętność cyfrową. Ponadto wzmacnia to emocjonalną pracę zespołową – nie dając się ponieść pierwszym wrażeniom, ale badając sprawę dokładniej.

Ćwiczenie 4: Moje cyfrowe lustro – samoocena

Cel: Zachęć uczestników (młodzież lub samych nauczycieli) do refleksji nad własnymi nawykami i emocjami w sieci poprzez wypełnienie krótkiej ankiety samooceny. Następnie poproś ich, aby wyznaczyli sobie jeden lub dwa mikro cele dotyczące poprawy swoich nawyków cyfrowych w nadchodzącym tygodniu. Dzięki temu nauka stanie się osobista i praktyczna.

Format: Zajęcia indywidualne, po których następuje opcjonalna wymiana doświadczeń w parach lub grupach. Można to zrobić za pomocą formularza online (anonimowego lub osobistego) lub drukowanego materiału informacyjnego. Jest to zadanie introspektywne i nie zajmuje zbyt wiele czasu, ale dyskusja może być tak głęboka, jak tylko zechcesz.

Czas trwania: 15-30 min.

Instrukcje:

1. **Rozprowadź samoocenę (np. Handout_M4):** Rozdaj uczestnikom kwestionariusz samooceny. Jeśli kurs odbywa się online, prześlij link do formularza Google, a jeśli offline, rozdaj wydrukowane kwestionariusze. Upewnij się, że uczestnicy rozumieją, że nie jest to test i powinni odpowiadać szczerze, kierując się własnymi odczuciami. Kwestionariusz zawiera takie stwierdzenia jak:

- „Kiedy otrzymuję nieoczekiwaną wiadomość lub powiadomienie, przed udzieleniem odpowiedzi robię sobie przerwę". (Prawie zawsze / Czasami / Rzadko / Nigdy)
- „Zanim kliknę link, zwracam uwagę na to, jak się czuję (ciekawość, niepokój, pośpiech)". (Skala Likerta)

Dofinansowane przez Unię Europejską

- „Weryfikuję nietypowe prośby, korzystając z drugiego źródła”.
- „Rozpoznaję sytuacje, w których emocje są wykorzystywane, aby skłonić mnie do szybkiego działania (strach, litość, nagroda)”.
- „Proszę o pomoc lub drugą opinię, gdy coś w Internecie wydaje mi się nieprawidłowe”.
- „Regularnie aktualizuję swoje urządzenia i aplikacje”.
- „Ograniczam ilość danych osobowych, które publikuję publicznie”.
- „Kiedy w sieci zdarza się błąd, potrafię zachować spokój i spróbować go naprawić, zamiast go ukrywać”.
- „Wspieram przyjaciół, gdy borykają się ze stresem lub oszustwami w Internecie”.
- „Robię krótkie przerwy od ekranów, aby zresetować emocje.”

Obejmują one kwestie techniczne (aktualizacje, prywatność), behawioralne (robienie przerw, weryfikacja, szukanie pomocy), emocjonalne (zwracanie uwagi na uczucia, zachowanie spokoju, robienie przerw) i społeczne (wspieranie przyjaciół).

2. **Wypełnienie:** Daj uczestnikom czas na spokojne wypełnienie ankiety. Jeśli wypełniają ją na papierze i nie jest ona anonimowa (tj. zostanie zachowana), zapewnij ich, że nie będą musieli pokazywać nikomu swoich odpowiedzi, chyba, że sami tego chcą. Jeśli korzystasz z formularza online i chcesz zachować anonimowość, możesz następnie przedstawić zbiorcze wyniki do dyskusji bez podawania nazwisk.
3. **Ocena/refleksja:** Wyjaśnij, że nie ma oceny pozytywnej/negatywnej. Jednym ze sposobów refleksji jest.

- Jeśli przeważają odpowiedzi „Prawie zawsze” lub „Czasami”, oznacza to, że mają wiele dobrych nawyków – zachęć ich, aby tak dalej postępowali i być może służyli innym, jako mentorzy
- Jeśli mają wiele odpowiedzi „Rzadko” lub „Nigdy”, są to obszary potencjalnego rozwoju. Jednak nawet jedna poprawa może znacznie zwiększyć ich bezpieczeństwo.

W materiałach informacyjnych powinna również pojawić się sekcja „Moje spostrzeżenia”:

- Emocja, która najczęściej kieruje moimi działaniami w Internecie to: _____ (być może złość? Ciekawość? Nuda?)
- Sytuacje, w której czuję, że najmniej kontroluje siebie: _____ (np. późno w nocy, przeglądając Internet lub podczas gorącej dyskusji na czacie grupowym itp.)
- Moim osobistym sygnałem „zatrzymaj się i sprawdź” będzie_____ (niektórzy decydują się, na „kiedy moje serce bije szybko, to jest to dla

Dofinansowane przez Unię Europejską

mnie sygnał, żeby się zatrzymać" lub „jeśli otrzymam dwie wiadomości z rzędu z dopiskiem „PILNE", to jest to dla mnie sygnał")

- Wspierający partner lub przyjaciel, który będzie mi o tym przypominał: _____ (zachęca to do wskazania konkretnej osoby, jako „kumpla odpowiedzialnego" lub po prostu kogoś, z kim można porozmawiać o tych celach).

4. **Wybierz mikro-cele:** W ulotce należy poprosić uczestników o zaznaczenie jednego lub dwóch mikro-celów na dany tydzień:

   ☐ Ćwicz zatrzymywanie się przed kliknięciem.

   ☐ Poproś kolegę o drugą opinię, (gdy nie masz pewności, co do czegoś).

   ☐ Dostosuj ustawienia prywatności (może ustaw jedno konto, jako bardziej prywatne lub usuń część danych osobowych).

   ☐ Spróbuj oddychać metodą 4-4-6 przed zareagowaniem w gorącej sytuacji.

   ☐ Inne: _____ (uczestnicy mogą wpisać własny mały cel, np. „włączyć dwuskładnikowe uwierzytelnianie na Instagramie" lub „robić codziennie 10-minutową przerwę od ekranu").
   Cel powinien być możliwy do osiągnięcia w ciągu tygodnia, a nie taki jak „nigdy więcej nie dać się nabrać" (zbyt ogólny). Małe kroki prowadzą do wielkich zmian.
5. **Opcjonalne dzielenie się:**, Jeśli to możliwe, poproś uczestników, aby podzielili się jedną spostrzeżeniem i wybranym celem z partnerem lub małą grupą. Alternatywnie możesz zebrać wybrane cele anonimowo i przeczytać kilka z nich, (aby pokazać różnorodność). Dzielenie się może stworzyć poczucie zaangażowania: głośne wypowiedzenie swojego celu często wzmacnia intencję. Pozwala to również kolegom wspierać się nawzajem („Hej, ja też postanowiłem robić więcej przerw; może będziemy sobie o tym przypominać na czacie grupowym").
6. **Sugestia dotycząca odpowiedzialności:** Zasugeruj, aby zapisali lub ustawili przypomnienie o swoim celu. Na przykład, umieszczenie na komputerze karteczki samoprzylepnej z napisem „Pauza?" lub umówienie się z przyjacielem na spotkanie („W następny piątek sprawdzimy, czy osiągnęliśmy nasze cele"). Jeśli jest to klasa lub grupa młodzieżowa, możesz zaplanować powrót do tych celów podczas następnej sesji – nawet, jeśli tylko po to, aby zapytać, kto uważa, że odniósł sukces lub jakie przeszkody napotkał.
7. **Refleksja:** Zachęć do krótkiej dyskusji:, „Jakie przypomnienie lub wsparcie pomoże wam utrzymać te dwie zmiany?". Uczestnicy mogą powiedzieć na przykład: „Zmienię ekran blokady telefonu na komunikat

Dofinansowane przez Unię Europejską

„Oddychaj” lub „Powiedziałem mojej siostrze o moim celu, a ona obiecała, że mnie szturchnie, jeśli zobaczy, że denerwuję się na telefon”. To skłania ich do praktycznego myślenia o utrzymaniu zmiany zachowania.

Zapytaj również: „Jak się czujecie z tymi wynikami? Czy któreś z waszych odpowiedzi was zaskoczyły?” oraz „Czy czujecie się zmotywowani do pracy nad jakimś konkretnym aspektem?”. Niektórzy mogą powiedzieć: „Zdałem sobie sprawę, że nigdy nie aktualizuję swoich aplikacji – łatwo to naprawić i zamierzam to zrobić”. Inni mogą powiedzieć: „Rzadko robię przerwy; widzę, jak to mnie denerwuje. W tym tygodniu spróbuję odłączyć się przed snem”.

Narzędzia: W przypadku zajęć online – formularz Google/Microsoft lub quiz Mentimeter (w przypadku quizu można następnie wyświetlić statystyki grupowe dla każdego pytania). W przypadku zajęć offline – wydrukowane materiały informacyjne i długopisy.

Rezultat: To ćwiczenie sprawia, że uczestnicy patrzą na siebie jak w lustrze, dzięki czemu wszystkie abstrakcyjne rozmowy stają się bardzo osobiste. Wzmacnia to samoświadomość i zaangażowanie w poprawę. Wyznaczając mikro cele, zwiększamy prawdopodobieństwo, że faktycznie zmienią oni, co najmniej jedno zachowanie, (co jest sukcesem!). Podkreśla to również szeroki zakres bezpieczeństwa cybernetycznego: nie chodzi tylko o to, aby „nie klikać złych linków”, ale także o dbanie o siebie emocjonalnie (przerwy, spokojne reakcje) i wspieranie innych.

Ćwiczenie 5: Cyberdziennik – jeden dzień w sieci

Cel: Zwiększ świadomość uczestników na temat czynników wywołujących emocje w ich codziennym życiu cyfrowym i powiąż te emocje z późniejszym zachowaniem w sieci. Prowadząc krótki dziennik z jednego dnia (lub kilku dni), uczestnicy zidentyfikują wzorce typu, „kiedy dzieje się X, czuję Y i robię Z”. Podczas podsumowania zgrupują wspólne czynniki wywołujące emocje i zdecydują się na zmianę jednego nawyku lub zwrócą uwagę na jeden sygnał emocjonalny.

Format: Indywidualny dziennik (w formie elektronicznej lub papierowej) prowadzony przez 1–3 dni, a następnie grupowa dyskusja na temat wzorców. Opcjonalnie można użyć chmury słów lub karteczek samoprzylepnych, aby zwizualizować wspólne odczucia/czynniki wyzwalające.

Czas trwania: 10 min dziennie przez 2–3 dni + 20 min podsumowania.

Dofinansowane przez Unię Europejską

Instrukcje:

1. **Szablon dziennika:** Zapewnij prosty szablon (może to być strona z małego notesu lub formularz Google, który uczniowie wypełniają codziennie) z kolumnami takimi jak:

- Czas/kontekst: (np. rano przed szkołą na Instagramie, po południu podczas odrabiania lekcji na YouTube, wieczorem podczas grania w gry itp.)
- Co wydarzyło się w sieci: (np. „Zobaczyłem złośliwy komentarz pod moim postem", „Dostałem 20 powiadomień ze Snapchata", „Przeczytałem wiadomość o...", „Znudziło mi się i przez godzinę przeglądałem TikToka", „Znajomy wysłał mi zabawny mem", „Ktoś przesłał mi przerażającą wiadomość łańcuchową" itp.)
- Emocje, które odczuwałem: (np. radość, irytacja, poczucie wykluczenia, niepokój, złość, podekscytowanie, zazdrość itp.)
- Co zrobiłem (zachowanie): (np. odpowiedziałem, kliknąłem link, przesłałem dalej, zignorowałem, zamknąłem aplikację, skonfrontowałem się z nimi, udostępniłem zbyt wiele informacji, a nawet coś w rodzaju „nie mogłem przestać o tym myśleć" – każde znaczące działanie lub brak działania).
- Można dodać wynik/refleksję: (opcjonalnie: „Patrząc wstecz, czy była to dobra decyzja? Czy następnym razem postąpiłbym inaczej?" – Można to zostawić do uzupełnienia podczas podsumowania).
  Zachęć ich, aby robili, co najmniej 3–5 wpisów dziennie (lub jeśli to trwa 2–3 dni, może 2 dziennie). Nie muszą zapisywać wszystkiego, tylko chwile, kiedy poczuli silne emocje podczas korzystania z Internetu lub urządzenia.

2. **Wytłumacz i motywuj:** Wyjaśnij, że jest to ćwiczenie mające na celu zwiększenie świadomości osobistej, a nie zadanie do oceny. Uczniowie mogą zachować szczegóły dla siebie, jeśli chcą (mogą używać skrótów lub omówić ogólnie później, jeśli coś jest delikatną kwestią). Podkreśl szczerość:, „Jeśli spędziłeś godzinę na przeglądaniu negatywnych wiadomości i wywołało to u Ciebie niepokój, zanotuj to. Jeśli jakiś post bardzo Cię podekscytował i skłonił do impulsywnego zakupu, zanotuj to. Nie ma tu miejsca na osądzanie, chodzi o poznanie samych siebie".
   Zapewnij ich również, że nawet „negatywne" emocje lub „złe" zachowania można zapisywać w dzienniku – każdy je ma.
3. **Czas trwania dziennika**: Poinformuj ich o terminie (np. do następnego spotkania). Jeśli to możliwe, wyślij przypomnienie w połowie okresu, np. SMS-em lub ogłoszeniem: „Nie zapomnijcie zapisać wszystkich ważnych wydarzeń online, które miały miejsce dzisiaj!"

Dofinansowane przez Unię Europejską

Jeśli to tylko jeden dzień, może powiedz im, żeby wybrali jutro, jako dzień skupienia i żeby zwracali uwagę na różne rzeczy tego dnia.

4. **Zbieraj i reflektuj:** W przypadku korzystania z anonimowej ankiety można zebrać odpowiedzi dotyczące wzorców klasowych. Jeśli ankieta jest w formie papierowej, uczniowie zatrzymują ją, ale wykorzystują podczas dyskusji.
5. **Dyskusja podsumowująca:** Po zakończeniu wypełniania dzienników zbierz wszystkich razem. Zacznij od ogólnego pytania:, „Jakie sytuacje w sieci wywołały u was silne emocje?". Zapisz je w miarę jak uczestnicy będą je wymieniać (mogą to być takie rzeczy jak: brak polubień pod postem, widok znajomych spędzających czas beze mnie, przerażająca wiadomość, duże zaangażowanie w grę, brak szybkiej odpowiedzi od kogoś itp.). Następnie zapytaj:, „Jakie emocje pojawiały się najczęściej?". Możesz je policzyć lub poprosić uczestników, aby je wykrzykiwali: niepokój, radość, frustracja, zazdrość itp.

   Użyj narzędzia takiego jak chmura słów Mentimeter lub po prostu napisz na tablicy: „Emocje, które odczuwaliśmy w Internecie w tym tygodniu". Ta wizualizacja może być bardzo pomocna, aby dostrzec, że niepokój lub FOMO mogą być ogromne, a może radość i zabawa również są duże – to mieszanka.

   Następnie omów związek z zachowaniem:, „Kiedy czułeś [emocję], co zazwyczaj robiłeś zaraz potem?". Na przykład:, „Kiedy czułem złość z powodu komentarza, pisałem złośliwą odpowiedź (i być może potem tego żałowałem)". „Kiedy czułem się samotny, przez godzinę przeglądałem losowe profile". „Kiedy czułem podekscytowanie, klikałem wiele linków na ten temat".

   Możliwe, że podobne czynniki wyzwalające:

- Czynniki społeczne: np. widok postów, które wywołały zazdrość lub poczucie wykluczenia→ uczucia (niepewność) → zachowanie (być może publikowanie postów mających na celu zwrócenie na siebie uwagi lub po prostu złe samopoczucie).
- Czynniki związane z oszustwem/strachem: np. dziwne wiadomości→ uczucia (niepokój) → zachowanie (pośpieszne działanie lub poszukiwanie pomocy).
- Czynniki wywołujące przeciążenie informacyjne: np. zbyt wiele powiadomień→ uczucia (stres) → zachowanie (wyłączenie telefonu lub, przeciwnie, kompulsywne sprawdzanie wszystkich powiadomień).

   Można narysować prostą mapę na tablicy, łączącą czynniki wywołujące z uczuciami i działaniami, aby uzyskać powtarzające się wzorce.

6. **Wybierz jeden nawyk, który chcesz zmienić:** Teraz zapytaj każdego: „Z twojego dziennika, jaki wzorzec zauważyłeś, który chciałbyś zmienić?".

Dofinansowane przez Unię Europejską

Na przykład: „Widzę, że każdej nocy długo przeglądam internet i to mnie wyczerpuje – chcę to ograniczyć" lub „Kiedy widzę wiadomości o problemach na świecie, denerwuję się i psuje mi to nastrój – może powinienem ograniczyć częstotliwość sprawdzania wiadomości" lub „Zdałem sobie sprawę, że kiedy jestem podekscytowany, odpowiadam używając wielu wykrzykników i wyrażając pośpiech. Może powinienem się opanować przed wysłaniem wiadomości, aby nie dzielić się zbyt wieloma informacjami lub nie zgadzać się na rzeczy, których tak naprawdę nie chcę."

7. Jeśli są to jednorazowe warsztaty, a nie cykl, zachęć uczestników, aby opowiedzieli przyjacielowi lub rodzeństwu o swoim planie, aby poczuli się odpowiedzialni.

Narzędzia: Papierowe dzienniki lub wspólny szablon Google Doc; Mentimeter lub slido do tworzenia anonimowej chmury słów opisujących emocje (opcjonalnie).

Rezultat: Uczestnicy zwiększają swoją samoświadomość w zakresie nawyków cyfrowych. Często odkrywają: „O rany, nie zdawałem sobie sprawy, że tak często się denerwuję na X" lub „Sprawdzam telefon za każdym razem, gdy się nudzę". Ta świadomość jest pierwszym krokiem do zmiany. Dzięki publicznej (lub półpublicznej) refleksji dostrzegają również, że nie są osamotnieni w tych zmaganiach (inni też cierpią na FOMO lub stresują się powiadomieniami). Wybranie konkretnego nawyku do zmiany sprawia, że niejasna koncepcja „bycia lepszym w sieci" staje się namacalnym działaniem, takim jak „wyłączę powiadomienia podczas odrabiania lekcji" lub „nie będę odpowiadać na wiadomości, gdy jestem zdenerwowany; poczekam". A powiązanie tego z sygnałem (wyzwalaczem emocji) oznacza, że stosują cykl EI: zauważenie uczucia -> zmiana reakcji. Ten dziennik skutecznie łączy sygnały emocjonalne z zachowaniem związanym z cyberbezpieczeństwem w prawdziwym życiu.

Ćwiczenie 7: Mapa podatności– warsztaty

Cel: Uczestnicy stworzą wizualną mapę słabych punktów w czterech wymiarach (technicznym, behawioralnym, emocjonalnym i społecznym), a następnie przeprowadzą burzę mózgów w celu opracowania konkretnych środków zaradczych dla każdego z nich, wraz ze strategią wsparcia EI. Na koniec zobowiązują się do podjęcia jednego działania w każdym kwadrancie. Pozwala to na syntezę treści modułu poprzez zastosowanie jej do ogólnego obrazu ryzyka własnego lub ryzyka grupy.

Dofinansowane przez Unię Europejską

Format: Małe grupy lub osoby indywidualne rysują wykres kwadratowy (online za pomocą Canva/Miro lub offline na papierze plakatowym z karteczkami samoprzylepnymi). Wymieniają osobiste lub zaobserwowane słabe punkty w każdym obszarze, a następnie dla każdego z nich zapisują jeden sposób na zmniejszenie tej słabości (łagodzenie) i jedno wsparcie związane z inteligencją emocjonalną (np. nawyk lub przypomnienie dotyczące umiejętności emocjonalnych). Wynikiem jest rodzaj macierzy planu bezpieczeństwa.

Czas trwania: 40–50 min.

Instrukcje:

1. **Przygotuj kwadranty:** Niezależnie od tego, czy korzystasz z dużego plakatu, tablicy czy cyfrowego ekranu, narysuj kwadrat podzielony na cztery kwadranty z następującymi oznaczeniami:

- Techniczny
- Behawioralny
- Emocjonalny
- Społeczny

Krótko przypomnij wszystkim, co obejmuje każda z tych kategorii (na podstawie treści modułu i wcześniejszych ćwiczeń).

- Techniczny: problemy związane ze sprzętem/oprogramowaniem (hasła, aktualizacje, bezpieczeństwo sieci itp.)
- Behawioralny:, co robimy online (kliknięcie bez zastanowienia, nadmierne udostępnianie informacji itp.).
- Emocjonalny: jak nasze uczucia wpływają na nasze działania online (impulsywność, stres itp.).
- Społeczny: wpływ naszych uczuć na działania w Internecie (impulsywność, stres itp.).
  Jeśli pracujesz w małych grupach, każda grupa otrzymuje własną „mapę" do wypełnienia. Jeśli jest to jedna duża grupa, możecie wspólnie wypełnić jedną mapę na tablicy, a każdy może wnieść swój wkład, dodając karteczki samoprzylepne.

2. **Zidentyfikuj słabe punkty:** Poproś uczestników, aby zastanowili się nad osobistymi lub typowymi słabymi punktami młodzieży w każdej kategorii. Mogą oni odwołać się do zdobytej wiedzy, wpisów w dziennikach lub dyskusji:

- Przykłady techniczne: słabe hasła lub ponowne wykorzystywanie tych samych haseł; brak korzystania z uwierzytelniania dwuskładnikowego (2FA); korzystanie z publicznych sieci Wi-Fi bez zachowania

Dofinansowane przez Unię Europejską

ostrożności; pozostawianie urządzeń bez nadzoru; brak aktualizacji aplikacji; dzielenie się urządzeniami bez wylogowywania się; itp.

- Przykłady zachowań: klikanie linków w wiadomościach; nadmierne udostępnianie informacji w mediach społecznościowych; akceptowanie zaproszeń do grona znajomych od osób nieznanych w prawdziwym życiu; pobieranie pirackiego lub przypadkowego oprogramowania; nieczytanie uprawnień aplikacji; publikowanie postów w gniewie, (co może być również emocjonalne); padanie ofiarą oszustw, takich jak oferty nagród; itp.
- Przykłady emocji: działanie pod wpływem strachu lub gniewu (np. niegrzeczna odpowiedź lub panika i kliknięcie); zbytnia ciekawość (kliknięcie plotki); poczucie samotności i uwierzenie w przypadkowy flirt online; poczucie pewności siebie „wiem wszystko" i pomijanie ostrzeżeń; wstyd, który powstrzymuje Cię przed szukaniem pomocy, gdy dzieje się coś złego; itp.
- **Przykłady społeczne:** presja rówieśników, aby dołączyć do ryzykownych wyzwań online; ufanie rzeczom tylko, dlatego, że wiele osób je udostępniło; zakładanie, że ktoś w społeczności jest bezpieczny, ponieważ inni wydają się mu ufać; poddawanie się wpływowi myślenia grupowego na forach; dynamika cyberprzemocy (presja, aby się zjednoczyć lub milczeć); niechęć do bycia jedyną osobą z prywatnym kontem, gdy przyjaciele ujawniają swoje; itp.

  Poproś uczestników, aby zapisali każdą słabość na osobnej karteczce samoprzylepnej (w przypadku ćwiczenia fizycznego) lub w polu tekstowym (w przypadku ćwiczenia cyfrowego) i umieścili ją w odpowiednim kwadrancie. Postaraj się, aby każda grupa miała, co najmniej 3-4 pozycje w każdym kwadrancie. Zachęcaj do podawania konkretów („Używanie hasła „12345" zamiast po prostu „słabych haseł", – choć obie opcje są dopuszczalne).

3. **Burza mózgów dotycząca środków zaradczych:** Teraz do każdej uwagi dotyczącej podatności dodają środek zaradczy – konkretne działanie mające na celu zmniejszenie lub wyeliminowanie tego ryzyka:

- W przypadku słabych haseł: używaj menedżera haseł lub frazy hasła, włącz uwierzytelnianie dwuskładnikowe (2FA).
- W przypadku braku aktualizacji: włącz automatyczne aktualizacje, zaplanuj comiesięczną kontrolę.
- Publiczne sieci Wi-Fi: używaj VPN lub unikaj logowania się do serwisów wymagających podania poufnych danych w sieciach publicznych.
- Nadmierne udostępnianie: Przejrzyj ustawienia prywatności; zastanów się dwa razy przed opublikowaniem; stosuj zasadę typu, „jeśli nie

Dofinansowane przez Unię Europejską

powiedziałbym tego w pomieszczeniu pełnym nieznajomych, nie opublikuję tego publicznie".

- Impulsywne kliknięcia: Rutyna „zatrzymaj się i sprawdź".
- Akceptowanie nieznanych znajomych: Ustaw profil, jako prywatny; akceptuj tylko wtedy, gdy mogę zweryfikować, kim są, poprzez wspólnych znajomych.
- Pobieranie przypadkowych plików: Pobieraj tylko z oficjalnych sklepów z aplikacjami; sprawdzaj recenzje i uprawnienia.
- Emocjonalność: Działanie pod wpływem strachu: Wykonuj ćwiczenia oddechowe; odczekaj godzinę przed odpowiedzią na niepokojącą treść.
- Wiara w pochlebstwa: Przypominaj sobie, że „komplementy w Internecie mogą być fałszywe"; zweryfikuj tożsamość osoby poprzez rozmowę wideo w obecności rodzica lub wcale.
- Wstyd zgłaszania: Zapewnij anonimowy sposób zgłaszania w naszej grupie; pamiętaj, że to nie Twoja wina, jeśli padłeś ofiarą oszustwa.
- Społeczność: Wyzwania rówieśników: Oglądaj filmy z „wyzwaniami" krytycznie; jeśli są ryzykowne, porozmawiaj z dorosłym przed podjęciem jakichkolwiek działań.
- Zachowania stadne: Graj w myślach rolę adwokata diabła – zadaj sobie pytanie „czy to może być złe?", Nawet, jeśli coś jest często udostępniane; korzystaj z serwisów weryfikujących fakty.
- Zaufanie do społeczności: Stosuj podejście „zero zaufania": nawet w bezpiecznych społecznościach weryfikuj nowe osoby lub informacje.

  Każde środki zaradcze można zapisać obok lub na tej samej notatce, co podatność, na przykład innym kolorem. Zachęcaj do konkretów.

4. **Linia zobowiązania:** Na dole plakatu lub na osobnej kartce poproś każdego uczestnika (lub całą grupę) o zapisanie jednego działania, do którego osobiście się zobowiązuje w każdym kwadrancie na nadchodzący tydzień. Na przykład:

- Techniczne: „Włączyć 2FA na dwóch kontach do piątku".
- Behawioralne: „Nie będę już akceptować zaproszeń do grona znajomych od osób, których nie znam – najpierw zapytam je, kogo oboje znamy".
- Emocjonalne:, „Kiedy w sieci coś mnie zdenerwuje, zamiast odpowiadać, zrobię sobie 5-minutową przerwę."
- Społeczne:, „Jeśli zobaczę, że znajomy robi coś ryzykownego, delikatnie przypomnę mu o tym, czego się nauczyliśmy (będę osobą, która staje w obronie innych)".

  To coś w rodzaju mini-zobowiązań, które łączą warsztaty z przyszłym zachowaniem. Jeśli moduł jest częścią trwającego programu, możesz wrócić do tych zobowiązań później.

Dofinansowane przez Unię Europejską

5. **Spacer po galerii, (jeśli wystarczy czasu):**, Jeśli mapy zostały sporządzone przez wiele grup, niech wszyscy obejrzą mapy pozostałych grup lub zaprezentują najważniejsze informacje. Mogą oni nauczyć się od innych o słabościach i sposobach ich łagodzenia, o których sami nie pomyśleli.
6. **Refleksja podsumowująca:**, „Które z działań (z dowolnego kwadrantu) Twoim zdaniem będzie miało największy bezpośredni wpływ na bezpieczeństwo Twoje lub Twojej grupy?" Niektórzy mogą uznać, że rozwiązania techniczne, takie jak uwierzytelnianie dwuskładnikowe (2FA), zapewniają znaczną poprawę, podczas gdy inni mogą cenić sobie środki emocjonalne, takie jak wstrzymanie się z działaniem, ponieważ pozwalają ograniczyć liczbę kliknięć. Jest to sposób na podkreślenie, że wszystkie kwadranty mają znaczenie i często wzajemnie na siebie oddziałują (np. kontrola emocjonalna może zapobiec błędom behawioralnym, takim jak nadmierne ujawnianie informacji).
   Zapytaj również:, „W jaki sposób sporządzenie tego schematu pomogło ci wyobrazić sobie stan twojego bezpieczeństwa?". Ludzie mogą odpowiedzieć, że podział na kategorie pozwolił im dostrzec, gdzie są najsłabsi (być może w kwestiach behawioralnych w porównaniu z technicznymi), albo, że satysfakcjonujące było przekształcenie każdej budzącej obawy luki w konkretne działanie, dzięki czemu wydaje się to możliwe do rozwiązania.

Narzędzia: Duży papier i markery lub tablica do pracy offline; lub Miro/Canva/Google Jamboard do wspólnego tworzenia map online (z polami tekstowymi i ewentualnie obrazkami/ikonami, aby urozmaicić pracę).

Rezultat: Ćwiczenie polegające na sporządzeniu mapy podatności na zagrożenia utrwala zdobytą wiedzę. Uczestnicy przenoszą ryzyko z głowy na papier, dzięki czemu nie wydaje się ono już tak przytłaczające, a staje się czymś w rodzaju „obiektów", z którymi mogą się zmierzyć. Pokazuje ono również szeroki zakres cyberbezpieczeństwa – nie tylko rozwiązania techniczne, ale także nawyki, odczucia i aspekty społeczne. Zapisując środki ograniczające ryzyko, przekształcają abstrakcyjne zagrożenia w konkretne zadania do wykonania. Kolumna wsparcia EI gwarantuje, że w każdym rozwiązaniu uwzględniają czynnik ludzki. A zobowiązania sprawiają, że z teoretycznego planu staje się to osobistą listą zadań do wykonania, zwiększając szansę, że szkolenie zaowocuje rzeczywistą zmianą zachowań.

Najważniejsze wnioski dla pracowników młodzieżowych

- Inteligencja emocjonalna to broń obronna w cyberbezpieczeństwie. Nauczanie młodych ludzi rozpoznawania własnych wzorców

Dofinansowane przez Unię Europejską

emocjonalnych – takich jak stres, ciekawość czy empatia – jest równie ważne, jak przekazywanie im wiedzy o zaporach sieciowych i programach antywirusowych. Oszuści często wykorzystują nasze emocje, dlatego musimy je chronić.

- Rozpoznawanie czynników wywołujących emocje pomaga zapobiegać manipulacji. Młodzież, która potrafi powiedzieć: „ Jestem bardzo podekscytowany tą ofertą, co oznacza, że powinienem być ostrożny", są znacznie mniej narażeni na oszustwa lub presję rówieśników. Chodzi o to, aby emocje przestały być ślepym kierowcą, a stały się pomocnym pasażerem.
- Nauka oparta na grach i scenariuszach znacznie zwiększa zaangażowanie i zapamiętywanie. Kiedy lekcje zamieniają się w quizy, wyzwania lub odgrywanie ról, młodzież uczestniczy w nich bardziej aktywnie i dłużej zapamiętuje treści. Gry zachęcają również do współpracy i dyskusji między rówieśnikami, co wzmacnia naukę w kontekście społecznym.
- Połączenie oceny z refleksją prowadzi do trwałych zmian. Wykorzystanie narzędzi takich jak samooceny lub dzienniki, a następnie omówienie ich, pomaga młodzieży dostrzec obszary, w których mogą się rozwijać, bez poczucia bycia ocenianym. Sprawia to, że nauka staje się osobistą misją (np. „Zdaję sobie sprawę, że powinienem częściej aktualizować swój telefon; zrobię to teraz"). Refleksja gwarantuje, że młodzież zrozumie, dlaczego dane zachowanie jest ryzykowne lub bezpieczne, co zwiększa prawdopodobieństwo, że będą kontynuować dobre praktyki po zakończeniu warsztatów.
- Kluczowe znaczenie mają struktury wsparcia rówieśniczego. Kultura, w której młodzież pomaga sobie nawzajem (np. wspólne sprawdzanie wiadomości lub nie wyśmiewanie kogoś za ostrożność) może być jedną z najsilniejszych form obrony. Należy zachęcać do tworzenia systemów partnerskich, norm grupowych dotyczących weryfikacji informacji oraz otwartej komunikacji na temat błędów, (aby w przypadku oszukania kogoś, poinformował on o tym innych, aby zapobiec podobnej sytuacji w przyszłości, zamiast ukrywać to z powodu wstydu).

Ćwiczenia modułu 5

Młodzi ambasadorzy mogą promować kulturę bezpieczeństwa poprzez kampanie uświadamiające, media społecznościowe oraz edukowanie rówieśników i społeczności w zakresie bezpiecznych praktyk online, uczestnicząc w wydarzeniach dotyczących cyberbezpieczeństwa i tworząc

Dofinansowane przez Unię Europejską

angażujące treści. Inne działania obejmują organizowanie warsztatów, prowadzenie kampanii dotyczących bezpieczeństwa oraz nawiązywanie kontaktów z profesjonalistami w dziedzinie cyberbezpieczeństwa w celu zdobycia doświadczenia i wiedzy.

Edukacja społeczna i rówieśnicza

- Organizuj warsztaty i wydarzenia:

Organizuj sesje, gry poświęcone cyberbezpieczeństwu lub wirtualne sesje pytań i odpowiedzi z ekspertami, aby uczyć rówieśników o zagrożeniach internetowych.

- Prowadź kampanie informacyjne:

Twórz plakaty, filmy i prezentacje, aby edukować innych na temat zagrożeń związanych z cyberbezpieczeństwem i środków zapobiegawczych.

- Angażuj się w działania społeczności internetowych:

Udostępniaj informacje i zasoby w mediach społecznościowych, aby szerzyć świadomość i zachęcać do bezpiecznego zachowania w Internecie.

- Twórz ogłoszenia społeczne (PSA):

Opracuj krótkie, wyraziste filmy lub komunikaty, aby zwrócić uwagę na kluczowe kwestie związane z cyberbezpieczeństwem.

- Weź udział w szkoleniach i webinarach:

Weź udział w programach oferujących szkolenia techniczne, warsztaty i dostęp do sieci specjalistów ds. cyberbezpieczeństwa

Kreatywne i angażujące ćwiczenia

- Rozpocznij konkurs na memy dotyczące cyberbezpieczeństwa:

Wykorzystaj humor, aby zwiększyć świadomość na temat kwestii związanych z cyberbezpieczeństwem i zachęcić do zaangażowania.

Networking i przywództwo

- Nawiąż kontakt z profesjonalistami i innymi osobami z branży:

Zbuduj sieć kontaktów zawodowych, uczestnicząc w wydarzeniach, dołączając do forów internetowych i nawiązując kontakty z ekspertami ds. cyberbezpieczeństwa.

- Inicjatywy wiodące:

Dofinansowane przez Unię Europejską

Przejmij inicjatywę w edukacji i wzmacnianiu pozycji następnego pokolenia poprzez proponowanie i wdrażanie nowych pomysłów i projektów w społeczności.

- Podziel się osobistymi historiami:

Zainspiruj innych, dzieląc się własnymi doświadczeniami i osiągnięciami w dziedzinie cyberbezpieczeństwa.

Praktyczne ćwiczenia do wykonania z młodzieżą

Ćwiczenie 1: drzewo zaufania cyfrowego

Cel:
Aby pomóc młodym ludziom i pracownikom młodzieżowym w zbadaniu, co sprawia, że czują się bezpiecznie lub niebezpiecznie w przestrzeni cyfrowej, oraz aby wspólnie wypracować wspólne rozumienie wartości, które budują kulturę zaufania i szacunku w sieci.

Czas trwania: 60–75 minut

Wielkość grupy: 8–20 uczestników

Materiały: Papier do tablicy flipchartowej lub duża tektura plakatowa, kolorowe markery, karteczki samoprzylepne, opcjonalnie tablica cyfrowa (np. Miro, Jamboard).

Instrukcje

1. **Wprowadzenie (10 min)**

   Wyjaśnij, że kultura bezpieczeństwa opiera się na wzajemnym zaufaniu. Zachęć uczestników do zastanowienia się, co sprawia, że czują się w sieci bezpieczni zarówno pod względem emocjonalnym, jak i cyfrowym.

2. **Rysowanie drzewa (10 min)**

   Na dużym arkuszu narysuj proste drzewo z korzeniami, pniem i gałęziami. Oznacz poszczególne części, jako:

   - *Korzenie = wartości sprzyjające poczuciu bezpieczeństwa (np. empatia, uczciwość, szacunek)*
   - *Pień = Nawyki lub zasady (np. weryfikacja faktów, ustawienia prywatności)*
   - *Gałęzie i liście = działania i postawy, które wyrastają z tych korzeni (np. pomaganie przyjaciołom, świadome publikowanie postów).*

Dofinansowane przez Unię Europejską

3. **Praca grupowa (25 min)**

Podziel uczestników na małe grupy, aby wypełnili każdą sekcję, używając karteczek samoprzylepnych lub wpisując informacje bezpośrednio na drzewie. Zachęć do swobodnej dyskusji.

4. **Dzielenie się(15 min)**

Grupy dzielą się swoimi drzewami i wskazują powtarzające się motywy.

5. **Synteza (10 min)**

Połącz wszystkie pomysły w jedno wspólne „Drzewo zaufania cyfrowego" i wyeksponuj je w przestrzeni edukacyjnej lub opublikuj w mediach społecznościowych, jako stworzoną przez młodzież deklarację wartości.

Refleksja

- Jakie wartości pojawiały się najczęściej?
- Jakie codzienne działania odzwierciedlają te wartości w sieci?
- Jak możemy wykorzystać to „drzewo zaufania" w naszym własnym zachowaniu w sieci?

Rezultaty nauczania:

- Rozpoznaje związek między wartościami a bezpieczeństwem w sieci.
- Wzmacnia umiejętności przywódcze poprzez dyskusję opartą na uczestnictwie.
- Wspiera empatię i wspólną odpowiedzialność w przestrzeni internetowej.

Ćwiczenie 2: Filtr emocji

Cel:
Aby pomóc uczestnikom w rozpoznawaniu emocji wywołanych interakcjami cyfrowymi oraz w opracowywaniu strategii regulacji emocjonalnej.

Czas trwania: 60 minut

Wielkość grupy: 6–15 uczestników

Dofinansowane przez Unię Europejską

Materiały: Karty emocji lub wydrukowane arkusze z emoji, karty scenariuszy przedstawiające typowe sytuacje w sieci (np. wykluczenie z grupy, fałszywe wiadomości, obraźliwy komentarz).

Instrukcje

1. **Rozgrzewka (10 min)**

   Omów, w jaki sposób emocje wpływają na decyzje podejmowane w sieci. Zapytaj:, „Kiedy silne emocje wpłynęły na to, co opublikowałeś lub powiedziałeś w sieci?"

2. **Praca nad scenariuszem (25 min)**

   Podzielcie się na małe grupy. Rozdajcie każdej grupie jedną kartę scenariusza. Poproście ich, aby:

   - Zastanów się, jakie emocje mogą się pojawić.
   - Omów, w jaki sposób każda z tych emocji może wpływać na zachowanie.
   - Zaproponuj konstruktywne sposoby reagowania z zachowaniem świadomości.

3. **Dzielenie się i dyskusja (15 min)**

Każda grupa przedstawia swoje przemyślenia. Proszę zwrócić uwagę na przykłady regulacji emocji lub empatii.

4. **Plan działania (10 min)**

Każdy uczestnik zapisuje sobie jedną osobistą wskazówkę dotyczącą „filtra emocji", na przykład: „Zanim coś opublikuję, nazwę swoje uczucie i odczekam 5 minut."

Refleksja

- Jakie emocje mają największy wpływ na Twoje zachowanie w sieci?
- W jaki sposób świadomość wpływa na Twoje reakcje?
- Jakie praktyczne strategie pomagają Ci opanować silne emocje?

Rezultaty nauczania:

- Rozwija samoświadomość i samokontrolę.
- Rozwija inteligencję emocjonalną w kontekście internetowym.
- Zachęca do rozwiązywania problemów w oparciu o empatię.

Dofinansowane przez Unię Europejską

Ćwiczenie 3: Mapa ambasadorów

Cel:
Aby pracownikom młodzieżowym oraz uczestnikom w zidentyfikowaniu i przedstawieniu istniejących sieci wsparcia, interesariuszy oraz sojuszników, którzy mogą promować kulturę bezpieczeństwa.

Czas trwania: 75 minut

Wielkość grupy: 8–20 uczestników

Materiały: Duży arkusz papieru lub płótno cyfrowe, flamastry i karteczki samoprzylepne.

Instrukcje

1. **Wprowadzenie (10 min)**

   Wyjaśnij, że żaden ambasador nie działa samodzielnie. Kultura bezpieczeństwa to wspólne przedsięwzięcie, w które zaangażowani są koledzy, organizacje i lokalne instytucje.

2. **Ćwiczenie z tworzenia map (30 min)**

   W środku kartki napisz „Ambasador młodzieży". Wokół tego napisu narysuj kółka symbolizujące:

   - *Rówieśnicy i przyjaciele*
   - *Rodzina i mentorzy*
   - *Szkoły i organizacje pozarządowe*
   - *Władze lub organizacje zajmujące się bezpieczeństwem w Internecie*

Poproś grupy, aby podały przykłady dla każdego obszaru i odnotowały, w jaki sposób każdy z podmiotów może wnieść swój wkład.

3. **Linie połączeń (15 min)**

   Narysujcie strzałki pokazujące istniejące powiązania i luki, („Kogo nam brakuje?").

4. **Planowanie działania (15 min)**

   Każda grupa proponuje jedno nowe partnerstwo lub działanie (np. zaproszenie funkcjonariusza policji lub psychologa do udziału w dyskusji, utworzenie grupy wsparcia rówieśniczego).

Dofinansowane przez Unię Europejską

Refleksja

- Kto jest obecnie Państwa partnerem w promowaniu kultury bezpieczeństwa?
- Jakie partnerstwa mogłyby wzmocnić Państwa działania?
- W jaki sposób osoby pracujące z młodzieżą mogą ułatwić nawiązywanie tych kontaktów?

Rezultaty nauczania:

- Rozwija umiejętności w zakresie nawiązywania kontaktów i rzecznictwa.
- Wspiera współpracę i buduje zaufanie między zainteresowanymi stronami.
- Promuje systemowe podejście do wsparcia młodzieży.

Ćwiczenie 4: kampania #MindfulMedia

Cel:
Aby umożliwić młodym ludziom opracowywanie i realizowanie krótkich kampanii uświadamiających, promujących kulturę bezpieczeństwa, inteligencję emocjonalną oraz świadome korzystanie z technologii cyfrowych.

Czas trwania: 2–3 sesje, każda po 90

Wielkość grupy: 6–12 uczestników

Materiały: Smartfony, dostęp do Internetu, szablony Canva/PosterMyWall, konta w mediach społecznościowych, arkusz kampanii.

Instrukcje

1. **Sesja 1 – generowanie pomysłów (90 min)**
    - Omówcie, która kwestia związana z cyfryzacją jest dla uczestników najważniejsza (np. dezinformacja, empatia w sieci, cyberprzemoc).
    - Wymyśl hasła reklamowe i hashtagi (np. #ThinkBeforeYouType, #MyDigitalMood).
    - Wybierz jeden główny temat kampanii i grupę docelową.
2. **Sesja 2 –projekt (90 min)**
    - Twórz krótkie materiały wizualne, relacje lub posty tekstowe.

Dofinansowane przez Unię Europejską

- Uzgodnijcie plan publikacji oraz podział ról (twórca treści, redaktor, weryfikator faktów, menedżer ds. mediów społecznościowych).

3. **Sesja 3 – rozpoczęcie i refleksja (90 min)**
    - Opublikuj materiały kampanii.
    - Śledź aktywność użytkowników (polubienia, komentarze, udostępnienia).
    - Zastanów się nad emocjonalnym oddziaływaniem i autentycznością przekazu.

Refleksja

- Która wiadomość wywarła największe wrażenie na odbiorcach?
- Czego nauczyłeś się o przywództwie i pracy zespołowej dzięki tej kampanii?
- W jaki sposób zadbałeś o to, by Twoje treści odzwierciedlały empatię i odpowiedzialność?

Rezultaty nauczania:

- Wzmacnia umiejętności przywódcze i komunikacyjne.
- Wspiera kreatywność i współpracę między rówieśnikami.
- Zachęca do aktywności obywatelskiej i odpowiedzialnego wyrażania opinii w sieci.

Ćwiczenie 5: zatrzymaj się – zastanów się - odpowiedz

Cel:
Szkolenie pracowników młodzieżowych oraz samych młodych ludzi w zakresie regulacji emocji i mediacji w sytuacjach konfliktowych, zarówno w środowisku internetowym, jak i w grupach.

Czas trwania: 75 minut

Wielkość grupy: 10–15 uczestników

Materiały: Karty scenariuszy, arkusze do refleksji, projektor (opcjonalnie).

Instrukcje

1. **Wprowadzenie (10 min)**

Dofinansowane przez Unię Europejską

Należy uświadomić, że impulsywne reakcje w sieci mogą doprowadzić do eskalacji konfliktów, podczas gdy świadomość emocjonalna może zapobiec wyrządzeniu krzywdy.

2. **Praca w grupach (30 min)**

   W grupach po 3–4 osoby przydzielcie scenariusze konfliktowe (np. wykluczenie z czatu, otrzymanie złośliwego komentarza, błędnie zinterpretowany post).
   Każda grupa odgrywa scenki:

   - **Zatrzymaj się:** określ związane z tym emocje.
   - **Zastanów się:** omów dostępne opcje.
   - **Odpowiedz:** wybierz stanowczą, pełną empatii odpowiedź.

3. **Dyskusja w grupie (20 min)**

   Zastanów się, które odpowiedzi były najbardziej konstruktywne i dlaczego.

4. **Zestaw narzędzi EI (15 min)**

   Wspólnie stwórzcie listę „narzędzi sprzyjających spokojnej komunikacji” (głęboki oddech, wyrażenie empatii, sprawdzenie faktów, szukanie wsparcia).

Refleksja

Jakie emocje wywołują u Ciebie najsilniejsze reakcje w sieci?

Jak przekształcić świadomość emocjonalną w cechy przywódcze?

Które umiejętności z zakresu inteligencji emocjonalnej najbardziej pomogły w rozwiązaniu konfliktu

Rezultaty nauczania:

- Wzmacnia zdolność do samokontroli i empatię.
- Rozwija umiejętności mediacyjne i komunikacyjne.
- Wspiera odpowiedzialne i oparte na inteligencji emocjonalnej zachowanie w sieci.

Ćwiczenie 6: Laboratorium dialogi młodzieżowo-dorosłego

Cel:
W celu pogłębienia międzypokoleniowego zrozumienia zagrożeń, wartości i

Dofinansowane przez Unię Europejską

zachowań w sieci oraz budowania wspólnego poczucia odpowiedzialności i zaufania między młodzieżą a dorosłymi.

Czas trwania: 90 minut

Wielkość grupy: 10–20 osób (zrównoważona grupa złożona z młodzieży oraz dorosłych/rodziców/nauczycieli)

Materiały: Karty do dyskusji, tablica flipchart, markery, neutralny moderator.

Instrukcje

1. **Wprowadzenie (15 min)**

   Wyjaśnij cel: zbliżenie poglądów różnych pokoleń na temat życia w sieci oraz omówienie, czym dla każdej z tych grup są „bezpieczeństwo" i „zaufanie".

2. **Osobna refleksja (20 min)**

   Młodzież i dorośli dyskutują osobno:

   - „Co najbardziej mnie niepokoi w Internecie?"
   - „Co sprawia, że czuję się bezpiecznie?"
   - „Co chciałbym, żeby ta druga grupa zrozumiała?"

3. **Wspólny dialog (40 min)**

   Zbierz obie grupy, aby podzieliły się swoimi przemyśleniami. Wskaż podobieństwa i różnice.

   Wspólnie opracujcie „Umowę o zaufaniu cyfrowym" – prosty dokument określający wzajemne oczekiwania.

4. **Zakończenie (15 min)**

   Podsumuj wnioski i podkreśl znaczenie stałej komunikacji oraz empatii.

Refleksja

- Co zaskoczyło cię w punkcie widzenia drugiej grupy?
- Jak można kontynuować tę dyskusję w twojej społeczności?
- W jaki sposób inteligencja emocjonalna wpłynęła na twoją komunikację?

Rezultaty nauczania:

- Buduje empatię i wzajemne zrozumienie między pokoleniami.

Dofinansowane przez Unię Europejską

- Wzmacnia umiejętności w zakresie facylitacji i przywództwa.
- Wspiera współpracę i działania na rzecz bezpieczniejszych społeczności cyfrowych.

Ćwiczenie 7: „Digital Bridge – dialog międzypokoleniowy"

Cel:
W celu pogłębienia wzajemnego zrozumienia między młodzieżą a ich rodzicami lub ogólnie rzecz biorąc dorosłymi w kwestiach dotyczących bezpieczeństwa w sieci, dezinformacji oraz reakcji emocjonalnych na zagrożenia cyfrowe.

Czas trwania: 50 minut

Wielkość grupy: 8–20 uczestników (najlepiej 50% młodzieży i 50% rodziców/osób dorosłych)

Materiały: Papier do tablicy flipchart, markery, „karty emocji", wydrukowane scenariusze, projektor (opcjonalnie).

Instrukcje

1. **Rozgrzewka – „Pokolenia w świecie cyfrowym" (10 min)**

- Pokaż dwa kontrastujące materiały cyfrowe (np. filmik z TikToka i artykuł prasowy).
- Zapytaj osobno młodzież i dorosłych:, „Jakie emocje lub obawy budzi w was ten materiał?"
- Podzielcie się spontanicznymi reakcjami, aby uwidocznić różnice w postrzeganiu.

2. **Symulacja zamiany ról (20 min)**

- Utwórzcie pary (młodzież i rodzic/osoba dorosła) i zamieńcie się rolami – młodzież wciela się w rolę rodzica, a rodzic w rolę młodzieży.
- Przedstawcie jeden krótki scenariusz (np. wiadomość phishingowa, przypadek cyberprzemocy, fałszywe wiadomości).
- Uczestnicy odgrywają rozmowę, próbując wspólnie znaleźć rozwiązanie.
- Obserwator odnotowuje przykłady empatii, tonu wypowiedzi i jasności wypowiedzi.

3. **Zakończenie (20 min)**

Dofinansowane przez Unię Europejską

Podsumuj, jakie to uczucie próbować działać z innej perspektywy i w innym wieku oraz w jaki sposób ta odmienna perspektywa wpłynęła na dialog i reakcje.

Refleksja

- Jakie to było uczucie, wyjaśniać zagrożenie cyfrowe osobie z innego pokolenia?
- Jakie emocje pojawiły się po obu stronach?
- Jakie techniki słuchania lub sformułowania wypowiedzi pomogły złagodzić napięcie?
- Jak możemy utrzymać tę rozmowę na żywo po zakończeniu sesji?

Rezultaty nauczania

- Większa empatia i lepsza kontrola emocji międzypokoleniowa.
- Większa pewność siebie młodzieży w rozmowach na temat bezpieczeństwa w sieci w domu.
- Lepsze zrozumienie przez rodziców zagrożeń emocjonalnych, a nie tylko technicznych.

Dofinansowane przez Unię Europejską

Źródła

Moduł 1

Komisja Europejska. (2020). *Digital Education Action Plan 2021–2027: Resetting education and training for the digital age* (COM(2020) 624 final). Urząd Publikacji Unii Europejskiej.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa. (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies.* ENISA.

Mayer, J. D., & Salovey, P. (1997). What is emotional intelligence? In P. Salovey & D. Sluyter (Eds.), *Emotional development and emotional intelligence: Educational implications* (pp. 3–31). Podręczniki.

Collaborative for Academic, Social, and Emotional Learning. (2020). *SEL framework: What are the core competencies?* CASEL.

Moduł 2

Nauczanie mieszane i podologia

Garrison, D. R., & Vaughan, N. D. (2008). *Blended learning in higher education: Framework, principles, and guidelines*. Jossey-Bass. https://doi.org/10.1002/9781118269558

UNESCO. (2022). *Guidelines on blended learning for quality education*. Wydawnictwo UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380609

OECD. (2023). *Teaching for the digital era: Effective strategies for blended and online learning*. Wydawnictwo OECD. https://www.oecd.org/education/teaching-for-the-digital-era.htm

Inteligencja emocjonalna

Salovey, P., & Mayer, J. D. (1990). Emotional intelligence. *Imagination, Cognition and Personality, 9*(3), 185–211. https://doi.org/10.2190/DUGG-P24E-52WK-6CDG

Wong, C. S., & Law, K. S. (2002). The effects of leader and follower emotional intelligence on performance and attitude. *The Leadership Quarterly, 13*(3), 243–274. https://doi.org/10.1016/S1048-9843(02)00099-2

Uniwersalne podejście do nauczania i integracja

Dofinansowane przez Unię Europejską

CAST. (2018). *Universal design for learning guidelines version 2.2*. CAST, Inc. https://udlguidelines.cast.org/static/udlg2.2-text-a11y.pdf

European Agency for Special Needs and Inclusive Education. (2022). *Inclusive digital education: Project examples*. EASNIE. https://www.european-agency.org/sites/default/files/_Inclusive_Digital_Education_Project_Examples.pdf

Obywatelstwo cyfrowe, praca z młodzieżą i umiejętności cyfrowe

Rada Europy. (2022). *Digital citizenship education handbook*. Urząd Publikacji Rady Europy. https://www.coe.int/en/web/digital-citizenship-education

Wspólne Centrum Badawcze Rady Europy. (2022). *DigComp 2.2: The digital competence framework for citizens*. Urząd Publikacji Unii Europejskiej. https://joint-research-centre.ec.europa.eu/digcomp_en

Vermeire, L., & Van den Broeck, W. (2024). Digital futures: A signal-based approach to inclusive digital youth work for socially vulnerable youth. *Media and Communication, 12*(2), 63–80. https://doi.org/10.17645/mac.i446

SALTO-YOUTH. (2023). *Curriculum for youth workers: Competence framework and training resources*. SALTO. https://www.salto-youth.net/downloads/toolbox_tool_download-file-3965/PR2_Final.pdf

Moduł 3

CAST Inc. (2018). Universal Design for Learning Guidelines Version 2.2. Wakefield, MA: CAST. https://udlguidelines.cast.org/static/udlg2.2-text-a11y.pdf

Rada Europy (2022). Digital Citizenship Education Handbook. Strasbourg: Urząd Publikacji Rady Europy. https://www.coe.int/en/web/digital-citizenship-education

European Agency for Special Needs and Inclusive Education (2022). Inclusive Digital Education: Project Examples. Odense: EASNIE. https://www.european-agency.org/sites/default/files/_Inclusive_Digital_Education_Project_Examples.pdf

Wspólne Centrum Badawcze Rady Europy (2022). DigComp 2.2: The Digital Competence Framework for Citizens. Luxembourg: Urząd Publikacji Unii Europejskiej. https://joint-research-centre.ec.europa.eu/digcomp_en

Garrison, D. R., & Vaughan, N. D. (2008). Blended Learning in Higher Education: Framework, Principles and Guidelines. San Francisco: Jossey-Bass / Wiley. https://onlinelibrary.wiley.com/doi/book/10.1002/9781118269558

Dofinansowane przez Unię Europejską

OECD (2023). Teaching for the Digital Era: Effective Strategies for Blended and Online Learning. Paris: OECD Publishing.

https://www.oecd.org/education/teaching-for-the-digital-era.htm

Salovey, P., & Mayer, J. D. (1990). Emotional Intelligence. Imagination, Cognition and Personality, 9(3), 185–211.

https://doi.org/10.2190/DUGG-P24E-52WK-6CDG
SALTO-YOUTH (2023). Curriculum for Youth Workers: Competence Framework and Training Resources. Bonn: SALTO.

https://www.salto-youth.net/downloads/toolbox_tool_download-file-3965/PR2_Final.pdf

UNESCO (2022). Guidelines on Blended Learning for Quality Education. Paris: UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380609

Vermeire, L., & Van den Broeck, W. (2024). Digital Futures: A Signal-Based Approach to Inclusive Digital Youth Work for Socially Vulnerable Youth. Media & Communication, 12(2), 63–80. https://doi.org/10.17645/mac.i446

Wong, C. S., & Law, K. S. (2002). The Effects of Leader and Follower Emotional Intelligence on Performance and Attitude. The Leadership Quarterly, 13(3), 243–274. https://doi.org/10.1016/S1048-9843(02)00099-2

Moduł 4

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming, 51*(5), 586–611. https://doi.org/10.1177/1046878120933312

Komisja Europejska. (2020). *Digital Education Action Plan 2021–2027: Resetting education and training for the digital age* (COM(2020) 624 final). Urząd Publikacji Unii Europejskiej.

Komisja Europejska. (2023). *Proposal for a Council Recommendation on improving the provision of digital skills and competences in education and training.* Komisja Europejska.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies.* ENISA.

Dofinansowane przez Unię Europejską

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Dofinansowane przez Unię Europejską

Załączniki

Załączniki modułu 1

Załącznik A – Arkusz ćwiczeniowy z mapą pojęciową

Instrukcje (dla uczestników)

Wpisz w środku jedną codzienną sytuację związaną z technologią cyfrową (np. „Pilna wiadomość dotycząca mojego konta").

Wokół niego dodaj następujące węzły i połącz je strzałkami:

• Zagrożenie

• Słaby punkt

• Zachowanie, (co mógłbym zrobić)

• Emocje, (co czuję)

• Bezpieczniejsza reakcja, (co zrobię zamiast tego)

• Etap weryfikacji (jak to sprawdzę)

Dodaj krótkie zdanie wyjaśniające znaczenie każdej strzałki (np. „Poczucie pośpiechu może skłonić mnie do kliknięcia bez sprawdzenia").

Przykład z rozwiązaniem

Kluczowy moment: „DM informuje, że moje konto zostanie usunięte za 30 minut".

Zagrożenie: Próba wyłudzenia danych.

Słabe punkty: Pośpiech; używanie tych samych haseł.

Zachowanie: Kliknięcie linku, aby „to naprawić".

Emocje: Niepokój, strach przed utratą.

Bezpieczniejsza reakcja: Zatrzymaj się, weź głęboki oddech, otwórz bezpośrednio oficjalną aplikację (nie link).

Krok weryfikacyjny: Sprawdź powiadomienia w aplikacji; poproś zaufaną osobę o dodatkowe sprawdzenie.

Puste pola do wypełnienia

Moment kluczowy: _____

Zagrożenie: _____

Dofinansowane przez Unię Europejską

Słabość: _____

Zachowanie: _____

Emocja: _____

Bezpieczna reakcja: _____

Krok weryfikacji: _____

Załącznik B – Arkusz opisów przypadków

Instrukcje (dla par lub małych grup)

Przeczytaj każdy krótki scenariusz. Podkreśl sygnały ostrzegawcze, zakreśl słowa wywołujące emocje i przygotuj spokojną, dwuzdaniową odpowiedź wraz z jednym krokiem weryfikacyjnym.

Scenka 1 – „Kontakt z obsługą klienta"

„Naruszyłeś zasady społeczności. Kliknij tutaj, aby potwierdzić swoją tożsamość, w przeciwnym razie Twoje konto zostanie dzisiaj zawieszone."

• Prawdopodobny czynnik wyzwalający: Pilność / strach.

• Sygnały ostrzegawcze (miejsce): _____

• Spokojna odpowiedź (dwa zdania): _____

• Etap weryfikacji: _____

Scenka 2 – „Przyjaciel w pośpiechu"

„Hej, to ja. Zmieniłem numer. Czy możesz mi przesłać swój kod logowania, żebym mógł się znowu zalogować?"

• Prawdopodobny czynnik wyzwalający: Empatia / presja, by pomóc.

• Sygnały ostrzegawcze (miejsce): _____

• Spokojna odpowiedź (dwa zdania): _____

• Etap weryfikacji: _____

Scenka 3 – „Rozdanie nagród"

„Gratulacje! Wygrałeś nowy telefon. Wpłać tutaj 2 € za wysyłkę, aby odebrać nagrodę w ciągu najbliższej godziny."

Dofinansowane przez Unię Europejską

• Prawdopodobny czynnik wyzwalający: Podekscytowanie / nagroda.

• Sygnały ostrzegawcze (miejsce): _____

• Spokojna odpowiedź (dwa zdania): _____

• Etap weryfikacji: _____

Przykłady odpowiedzi, z których możesz skorzystać

„Nie klikam w linki w wiadomościach. Sprawdzę to w oficjalnej aplikacji".

„Nigdy nie udostępniam kodów ani haseł. Zweryfikuję to inną drogą".

„Jeśli to prawdziwa oferta, znajdę ją na oficjalnej stronie firmy".

Załącznik C – EI – umiejętności mikro: strona informacyjna

Cel: Proste czynności, które uczniowie mogą wykonać przed kliknięciem lub udzieleniem odpowiedzi.

1) Zatrzymaj się – Weź głęboki oddech – Sprawdź (10–20 sekund)

Zatrzymaj się: Odłóż ręce od klawiatury/telefonu na 3 sekundy.

Oddychaj: Wdech na 4 – wstrzymaj oddech na 2 – wydech na 6 (jeden lub dwa cykle).

Sprawdź:, Co czuję? O co prosi ta wiadomość? Jaki jest jeden bezpieczny krok weryfikacyjny?

2) 4-4-6 oddychanie (20–30 sekund)

Wdychaj powietrze przez nos przez 4 sekundy.

Wstrzymaj oddech na 4 sekundy.

Wydychaj powietrze przez usta przez 6 sekund (dłuższy wydech).

Powtórz dwa razy. Zwróć uwagę, jak rozluźniają się Twoje ramiona i szczęka.

3) Weryfikacja wiadomości przez rówieśnika (mniej niż minuta)

Prześlij zrzut ekranu lub opisz wiadomość zaufanemu przyjacielowi lub osobie dorosłej.

Zapytaj: „Czy coś wygląda podejrzanie? Co byś zrobił?"

Podejmij działanie dopiero po zasięgnięciu drugiej opinii.

Dofinansowane przez Unię Europejską

4) Weryfikacja dwuetapowa (zasada nawyku)

Nigdy nie klikaj w link zawarty w wiadomości, która wywiera presję.

Samodzielnie otwórz oficjalną aplikację lub stronę internetową albo skorzystaj z zapisanej zakładki.

W razie wątpliwości skontaktuj się z pomocą techniczną za pośrednictwem oficjalnych stron pomocy.

Wskazówki dotyczące pozytywnego myślenia dla młodzieży

„Nie muszę się spieszyć".

„Najpierw mogę to sprawdzić".

„Można grzecznie odmówić.

Załącznik D – Szablon scenariusza myślenia na głos

Instrukcje (dla edukatorów)

Skorzystaj z tego szablonu, aby na głos przedstawić przebieg wewnętrznego procesu podczas obsługi wiadomości o podwyższonym ryzyku. Postaraj się, aby trwało to około 60 sekund.

Wskazówki dotyczące skryptu

Określenie uczucia: „Zauważam, że czuję się_____ (np. pośpieszony/ciekawy)."

Zidentyfikowany bodziec: „Ta wiadomość wykorzystuje_____ (poczucie pilności/autorytet/nagrodę)."

Przerwa: „Wezmę jeden spokojny oddech, żeby się zastanowić".

Pytanie o ryzyko:, „O co mnie prosi i dlaczego?"

Krok weryfikacyjny: „Zamiast klikać tutaj, otworzę oficjalną aplikację/stronę".

Spokojna odpowiedź (opcjonalnie): „Nie udostępniam kodów ani danych osobowych. Sprawdzę to przez oficjalne kanały".

Decyzja: „Najpierw to zweryfikuję, a potem zdecyduję".

Monolog wewnętrzny: „Zwolnienie tempa pomaga mi zachować bezpieczeństwo".

Twój scenariusz (wypełnij)

Dofinansowane przez Unię Europejską

Typ wiadomości: _____

Uczucie, które nazywam: _____

Wyzwalacz, który dostrzegam: _____

Moja pauza: _____

Mój krok weryfikacyjny: _____

Moje zdanie odpowiedzi: _____

Ostateczna decyzja: _____

Załącznik E – Karty z błędnymi przekonaniami

Instrukcje (dla grupy)

Oznacz każde stwierdzenie, jako „Prawda", „Fałsz" lub „To zależy", a następnie napisz jedno zdanie wyjaśniające to w języku przystępnym dla młodzieży.

„Jeśli moje hasło jest silne, nie potrzebuję uwierzytelniania dwuskładnikowego".

P / F / Zależy – Wyjaśnij:_____

„Jeśli wiadomość pochodzi z konta znajomego, jest bezpieczna".

P / F / Zależy – Wyjaśnij: _____

„Tylko osoby starsze dają się nabrać na oszustwa".

P / F / Zależy – Wyjaśnij: _____

„Jeśli czuję niepokój, powinienem zignorować swoje odczucia i po prostu działać".

P / F / Zależy – Wyjaśnij: _____

„Oficjalna pomoc techniczna może poprosić mnie o podanie hasła, aby mi pomóc".

P / F / Zależy – Wyjaśnij: _____

„Jeśli to pilne, powinienem najpierw kliknąć, a potem pomyśleć".

P / F / Zależy – Wyjaśnij: _____

„Korzystanie z publicznej sieci Wi-Fi jest zawsze bezpieczne, jeśli strona korzysta z protokołu HTTPS".

Dofinansowane przez Unię Europejską

P / F / Zależy – Wyjaśnij: _____

„Ustawienia prywatności nie mają znaczenia, jeśli nie jestem sławny”.

P / F / Zależy – Wyjaśnij: _____

„Jeśli nagroda wiąże się z niewielką opłatą za wysyłkę, to prawdopodobnie jest to oferta wiarygodna”.

P / F / Zależy – Wyjaśnij: _____

„W sieci emocje sprawiają, że stajesz się bezsilny”.

P / F / Zależy – Wyjaśnij: _____

Uwagi dla prowadzącego (przydatne wskazówki)

„Silne hasła pomagają, ale uwierzytelnianie dwuskładnikowe (2FA) stanowi dodatkowe zabezpieczenie”.

„Konta mogą zostać zhakowane; zweryfikuj dane za pomocą innego kanału”.

„Oszustwa dotykają wszystkich; taktyki są dostosowywane również do młodzieży”.

„Uczucia są sygnałami; zwróć na nie uwagę, a następnie spokojnie zweryfikuj sytuację”.

„Prawdziwe wsparcie nigdy nie prosi o hasła ani kody”.

„Pilność to sygnał ostrzegawczy; zatrzymaj się i sprawdź w oficjalnej aplikacji”.

„HTTPS pomaga, ale publiczne Wi-Fi nadal wiąże się z ryzykiem; unikaj wykonywania wrażliwych czynności”.

„Ustawienia prywatności ograniczają narażenie i przyszłe szkody”.

„Opłaty i liczniki czasu to klasyczne taktyki oszustów”.

„Inteligencja emocjonalna wzmacnia bezpieczeństwo i decyzje”.

Załączniki modułu 2

Załącznik 1: Lista kontrolna cyberhigieny

Ta lista kontrolna pomaga młodzieży ocenić swoje codzienne zachowania w sieci i zachować bezpieczeństwo, radząc sobie z czynnikami wywołującymi emocje.

Codzienne środki bezpieczeństwa:

Dofinansowane przez Unię Europejską

☐ Zanim kliknę w link, zatrzymuję się na chwilę – zwłaszcza, gdy czuję się pod presją lub jestem zestresowany.

☐ Przed zaakceptowaniem zaproszenia sprawdzam nieznane profile.

☐ Unikam publikowania postów, gdy jestem zły, podekscytowany lub czuję presję.

☐ Dbam o aktualizację mojego urządzenia (aplikacji, przeglądarki, systemu operacyjnego).

☐ Sprawdzam ustawienia prywatności na wszystkich kontach w mediach społecznościowych.

☐ Pobieram pliki wyłącznie z zaufanych, zweryfikowanych źródeł.

☐ Używam silnych haseł i, w miarę możliwości, uwierzytelniania dwuskładnikowego.

☐ Sprawdzam informacje przed ich udostępnieniem.

☐ Zastanawiam się, jak wpływają na mnie interakcje w sieci.

Załącznik 2: Przewodnik po technikach radzenia sobie z emocjami

Niniejszy przewodnik pomaga młodzieży radzić sobie ze stresem, impulsywnością i wrażliwością emocjonalną wynikającymi z zagrożeń w sieci.

Szybkie narzędzia EI:

- Oddychanie 4-6: Wdech przez 4 sekundy → Wstrzymaj oddech przez 4 sekundy → Wydech przez 6 sekund. Świetna metoda na opieranie się presji związanej z oszustwami i phishingiem.
- Nazywanie emocji: „Czuję się ___, ponieważ ___”. Pomaga uniknąć impulsywnych postów i reakcji.
- Ćwiczenie uziemiające: Wymień 5 rzeczy, które widzisz, 4, które czujesz, i 3, które słyszysz – przydatne w przypadku cyberprzemocy lub stresu.
- Technika pauzy: Przed udzieleniem odpowiedzi zapytaj: „Czy to bezpieczne? Czy to prawda? Jakie emocje odczuwam?”
- Pozytywna reinterpretacja: Zastąp myśli wywołujące panikę („To wygląda na pilne!”) spokojnymi („Mogę to spokojnie sprawdzić".).
- Cyfrowa przerwa: Odsuń się, gdy czujesz się przytłoczony w sieci.

Dofinansowane przez Unię Europejską

Załącznik 3: Karty scenariuszy do gier fabularnych

Wykorzystaj poniższe scenariusze podczas zajęć mieszanych lub stacjonarnych.

Scenariusz 1: Cyberprzemoc na czacie grupowym

- Sprawca: Napisz krzywdzącą wiadomość.
- Ofiara: Opisz, jak się czujesz.
- Obserwator: Zaproponuj alternatywne rozwiązania.
- Mediator: Pokaż, jak okazywać empatię i rozwiązywać konflikty.

Scenariusz 2: Fałszywa prośba o dodanie do znajomych

- Nowy profil zachowuje się przyjaźnie, ale prosi o podanie danych osobowych.
- Młodzież rozpoznaje sygnały ostrzegawcze i ćwiczy ustalanie bezpiecznych granic.

Scenariusz 3: E-mail Phishingowy z pilną prośbą

- „Administrator szkoły" grozi usunięciem konta.
- Młodzież ćwiczy zatrzymanie się, oddychanie i weryfikację.

Scenariusz 4: Oszustwo FOMO („Wygrałeś nagrodę!")

- Zbadaj emocjonalne czynniki wyzwalające związane z nagrodami.
- Młodzież rozpoznaje taktyki manipulacyjne..

Scenariusz 5: Post dezinformacyjny

- Wirusowa wiadomość informuje o szokującym wydarzeniu.
- Młodzież analizuje emocjonalne czynniki wyzwalające i weryfikuje fakty.

Scenariusz 6: Pobieranie plików narażonych na złośliwe oprogramowanie

- „Darmowy link do streamingu" obiecuje treści premium.
- Młodzież omawia kwestię ciekawości kontra ostrożność.

Załącznik 4: Przewodnik po kręgach rówieśniczych

Grupy wsparcia rówieśniczego wzmacniają odporność psychiczną młodzieży.

Struktura:

- Utwórzcie grupy po 3–4 osoby.

Dofinansowane przez Unię Europejską

- Co miesiąc zmieniajcie osobę pełniącą rolę cyberambasadora.
- Spotykajcie się, co dwa tygodnie lub co miesiąc.

Każda sekcja obejmuje:

1. W centrum uwagi: omów jedno z niedawno napotkanych zagrożeń cybernetycznych.
2. Refleksja emocjonalna:, Jakie wywołało to w Tobie uczucia? (Skorzystaj z narzędzi inteligencji emocjonalnej.)
3. Strategie radzenia sobie:, co można zrobić inaczej?
4. Wyzwanie związane z profilaktyką: Każdy członek zobowiązuje się do wyrobienia jednego nawyku związanego z bezpieczeństwem w sieci.

Obowiązki ambasadora:

- Zachęcaj do prowadzenia dialogu opartego na szacunku.
- Informuj o aktualnych zagrożeniach w sieci.
- Wspieraj rówieśników borykających się z problemami w sieci.
- Promuj empatię i bezpieczne nawyki w sieci.

Załączniki modułu 3

Załącznik A: Szablon planu zajęć integracyjnych

Cel: Szablon krok po kroku do opracowywania **30–60-minutowych zajęć mieszanych,** które uwzględniają **osiem obszarów ryzyka związanych z nauką online,** a jednocześnie łączą **inteligencję emocjonalną, uniwersalne projektowanie nauczania oraz narzędzia cyfrowe**.

Treści:

Sekcja	**Wskazówki**
Tytuł sekcji	Przykład: „Rozpoznawanie i reagowanie na **phishing i oszustwa** z empatią”.
Obszar ryzyka	Wybierz 1–2 obszary ryzyka (np. **phishing, cyberprzemoc, dezinformacja**).
Profil młodzieży	Opisz grupę docelową (np. młodzież z obszarów wiejskich, uczniowie z zaburzeniami neurorozwojowymi, młodzież migrująca).

Dofinansowane przez Unię Europejską

Cele nauczania	Przykład: „Pod koniec tej sesji uczestnicy będą potrafili **rozpoznać sygnały ostrzegawcze phishingu** i **ćwiczyć samokontrolę**, aby uniknąć impulsywnego klikania”..”
Fazy mieszane	Nakreśl działania w ramach **Nawiąż kontakt – Odkrywaj – Ćwicz – Zastanów się – Podziel się**, w tym **narzędzia** (np. Kahoot do quizów, Padlet do refleksji) oraz **pytania dotyczące EI** (np. „Jak byś się czuł, gdybyś dał się nabrać na to oszustwo?”).
Działania na rzecz dostępności	Wymień dostosowania (np. napisy do filmów, materiały drukowane do dyskusji na temat **złośliwego oprogramowania/prywatności**, zasoby wielojęzyczne).
Metody oceny	Określ, w jaki sposób będziesz oceniać **wiedzę** (quiz), **umiejętności** (odgrywanie ról) oraz **efekty emocjonalne** (dziennik refleksji).

Przykładowe zastosowanie: Facylitator planujący sesję poświęconą **cyberprzemocy i empatii cyfrowej** mógłby skorzystać z tego szablonu, aby upewnić się, że sesja obejmuje **techniki EI, dostosowania zgodne z zasadami UDL oraz zajęcia mieszane**.

Załącznik B: Lista kontrolna UDL i dostępności

Cel: Lista kontrolna mająca na celu zapewnienie, że wszystkie zajęcia są **integracyjne i dostępne** dla różnorodnych uczestników, w tym osób z **niepełnosprawnościami, ograniczonym dostępem do technologii cyfrowych lub barierami językowymi**.

Treści:

Kryteria	Tak/nie	Uwagi/adaptacje
Różnorodne sposoby angażowania		Czy dostępne są **interaktywne, oparte na współpracy i dostosowane do indywidualnego tempa nauki** opcje ćwiczeń dotyczących **phishingu i oszustw**?

Dofinansowane przez Unię Europejską

Różnorodne sposoby przedstawienia		Czy materiały są dostępne w **formacie tekstowym, audio i wizualnym** (np. filmy z napisami do dyskusji na temat **fałszywych wiadomości**)?
Różnorodne sposoby wyrażania się		Czy uczestnicy mogą **dzielić się swoimi przemyśleniami** poprzez pisanie, wypowiedzi ustne lub twórczość artystyczną (np. na platformie Padlet w przypadku historii dotyczących **cyberprzemocy**)?
Alternatywne zastosowanie low-tech		Czy dostępne są **wydrukowane arkusze ćwiczeń** lub **dyskusje offline** na tematy związane **ze złośliwym oprogramowaniem/prywatnością**?
Znaczenie kulturowe		Czy przykłady odzwierciedlają **różnorodne doświadczenia** związane z **podszywaniem się lub cyberprzestępcami**?
Bezpieczeństwo emocjonalne		Czy istnieją **możliwości rezygnacji** z udziału w dyskusjach na drażliwe tematy (np. **posty, których się żałuje, cyberprzemoc**)?
Przejrzystość językowa		Czy język używany w dyskusjach na **temat oszustw lub fałszywych zaproszeń do grona znajomych** jest **prosty i neutralny**?

Przykładowe zastosowanie: Przed rozpoczęciem sesji poświęconej **dezinformacji** prowadzący korzystałby z tej listy kontrolnej, aby upewnić się, że **filmy mają napisy, dyskusje przewidują możliwość rezygnacji z udziału** oraz **przykłady są dostosowane do kontekstu kulturowego**.

Załącznik C: Tematy do dziennika refleksji

Cel: Zestaw pytań, które mają pomóc uczestnikom w **cotygodniowej refleksji** nad ich **doświadczeniami emocjonalnymi** związanymi z **ośmioma obszarami ryzyka w sieci**.

Treści:

Tydzień 1: Cyberprzemoc i empatia cyfrowa

Dofinansowane przez Unię Europejską

- *“ Opisz sytuację, w której widziałeś lub doświadczyłeś **cyberprzemocy**. Jak się wtedy czułeś? Co zrobiłbyś teraz inaczej?”*
- *„W jaki sposób empatia może zmienić sposób, w jaki komunikujemy się w sieci?”*

Tydzień 2: Phishing i oszustwa

- *„Jakie emocje mogą sprawić, że ktoś stanie się podatny na **wiadomość phishingową lub oszustwo**? W jaki sposób samokontrola może w tym pomóc?”*
- *„Opowiedz o sytuacji, w której prawie kliknąłeś podejrzany link. Co Cię powstrzymało?”*

Tydzień 3: Fałszywe wiadomości i dezinformacja

- *“ W jaki sposób zweryfikowałeś jakąś informację w tym tygodniu? Z jakimi trudnościami się spotkałeś?*
- *„Jak myślisz, dlaczego **fałszywe wiadomości** rozprzestrzeniają się tak szybko? Jak możemy to spowolnić??”*

Tydzień 4: Prywatność i posty, których żałujemy

- *“ Jaka jest jedna informacja osobista, której ujawnienia żałujesz? Jak to na ciebie wpłynęło?”*
- *“ Jak możemy wesprzeć znajomych, którzy opowiedzieli o czymś, czego teraz żałują?”*

Tydzień 5: Złośliwe oprogramowanie i cyberprzestępcy

- *„Jakie kroki podejmujesz, aby uniknąć **przypadkowego pobrania złośliwego oprogramowania**? Jak się czujesz, gdy nie masz pewności, co do linku?”*
- *„Jak rozpoznać **cyberprzestępcę** i jak na niego zareagować?”*

Przykładowe użycie: Uczestnicy wykorzystują te pytania w swoich **dziennikach internetowych**, aby zastanowić się nad swoimi **reakcjami emocjonalnymi** na zagrożenia w sieci, co sprzyja **samoświadomości i bezpieczniejszym zachowaniem**.

Dofinansowane przez Unię Europejską

Załącznik D: Tabela oceny i integracji

Cel: Tabela służąca do oceny **skuteczności, otwartości i oddziaływania emocjonalnego** sesji poświęconych **ośmiu obszarom zagrożeń w sieci**.

Treści:

Obszar oceny	Wskaźniki	Narzędzia/metody
Wiedza	Czy uczestnicy potrafią **rozpoznać sygnały ostrzegawcze związane z phishingiem** lub **wykryć fałszywe wiadomości**?	Quizy przed i po zajęciach, wyniki w Kahoot.
Umiejętności	Czy uczestnicy potrafią **z empatią reagować na cyberprzemoc** lub **weryfikować źródła informacji**?	Obserwacje podczas odgrywania ról, odpowiedzi na Padlet.
Postawy	Czy uczestnicy wykazują **większą empatię** lub **krytyczne myślenie** w odniesieniu do zagrożeń internetowych?	Dzienniki refleksji, dyskusje grupowe.
Integracja	Czy **wszyscy uczestnicy byli zaangażowani**, niezależnie od pochodzenia lub umiejętności?	Lista kontrolna UDL, rejestry uczestnictwa.
Wpływ emocjonalny	Sprawdzanie samopoczucia emocjonalnego, anonimowe opinie.	Sprawdzanie samopoczucia emocjonalnego, anonimowe opinie.
Kompetencje cyfrowe	Czy uczestnicy potrafią **korzystać z narzędzi cyfrowych** (np. Padlet, Kahoot) w celu zdobywania wiedzy na temat zagrożeń internetowych?	Analizy platformy, samooceny.

Przykładowe zastosowanie: Po sesji poświęconej **podszywaniu się i oszustwom** prowadzący wykorzystałby tę tabelę, aby ocenić, czy uczestnicy **rozpoznali oszustwa, zareagowali z empatią** oraz **czuli się włączeni w zajęcia**.

Dofinansowane przez Unię Europejską

Załącznik E: Przykłady profili młodzieżowych

Cel: Przykładowe profile młodych ludzi o różnym pochodzeniu, umiejętnościach i stopniu dostępu do technologii cyfrowych, które pomogą prowadzącym w **opracowywaniu sesji sprzyjających integracji**.

Treści:

1. **Młodzież z obszarów wiejskich o ograniczonym dostępie do technologii cyfrowych**
    - **Wyzwania:** Powolny internet, ograniczona liczba urządzeń.
    - **Adaptacje:** Materiały drukowane, dyskusje poza Internetem na temat **zagrożeń związanych z prywatnością lub złośliwego oprogramowania**.
2. **Uczeń o odmiennej neurologii**
    - **Wyzwania:** Przeciążenie sensoryczne, potrzeba jasnych wskazówek.
    - **Adaptacje:** Wizualne harmonogramy, spokojne miejsca przeznaczone do zajęć związanych z **cyberprzemocą lub oszustwami**.
3. **Młodzież migrująca borykająca się z barierami językowymi**
    - **Wyzwania:** Ograniczona znajomość języka, w którym odbywa się sesja.
    - **Adaptacje:** Materiały w wielu językach, partnerzy do rozmów na temat **fałszywych wiadomości lub phishingu**.
4. **Młodzież miejska o wysokim poziomie umiejętności cyfrowych**
    - **Wyzwania:** Zbytnia pewność siebie w kwestii bezpieczeństwa w sieci.
    - **Adaptacje:** Zaawansowane scenariusze (np. **podszywanie się za inne osoby za pomocą deepfake'ów, skomplikowane oszustwa**).

Przykładowe zastosowanie: Prowadzący, który planuje sesję poświęconą **fałszywym zaproszeniom do grona znajomych**, powinien zapoznać się z tymi profilami, aby mieć pewność, że zadania będą **przystępne i angażujące** dla wszystkich uczestników.

Dofinansowane przez Unię Europejską

Załącznik F: Przewodnik dla mentorów rówieśniczych / ambasadorów młodzieżowy

Cel: Przewodnik służący do szkolenia **mentorów rówieśniczych lub ambasadorów młodzieży** w zakresie wspierania rówieśników w **rozpoznawaniu i reagowaniu na osiem obszarów zagrożeń w sieci**.

Treści:

Sekcja	Wskazówki
Rola mentorów rówieśniczych	*„Jesteś wzorem do naśladowania! Twoim zadaniem jest **dzielenie się wiedzą, słuchanie i wspieranie** rówieśników w zapewnieniu im bezpieczeństwa w sieci.*
Główne obszary ryzyka	Przegląd zagadnień takich jak **cyberprzemoc, phishing, oszustwa, fałszywe wiadomości itp**. wraz z **przystępnymi objaśnieniami**.
Techniki EI	Jak wykorzystać **empatię, samokontrolę i krytyczne myślenie** podczas dyskusji w grupie rówieśniczej.
Wskazówki dotyczące facylitacji	*„Zadaj **pytania otwarte**, na przykład: »Jak się czułeś po tej **próbie oszustwa**?”*
Materiały pomocnicze	Linki **do filmów, quizów i numerów telefonów zaufania**, które pomogą w dalszej nauce.
Protokoły bezpieczeństwa	*„Jeśli znajomy opowie Ci o **cyberprzemocy**, wysłuchaj go bez osądzania i zaproponuj pomoc w zgłoszeniu tego przypadku.”*

Przykładowe zastosowanie: Ambasador młodzieży mógłby skorzystać z tego przewodnika, aby poprowadzić dyskusję na temat zagrożeń związanych z podszywaniem się pod inne osoby lub udzielić wsparcia rówieśnikowi, który padł ofiarą cyberprzemocy .

Dofinansowane przez Unię Europejską

Załączniki modułu 4

Załącznik 1: Arkusz_M4

Instrukcje dla uczestników:

Przeczytaj każde stwierdzenie i zaznacz opcję, która najlepiej Cię opisuje. Bądź szczery – to ćwiczenie służy Twojej własnej refleksji, a nie jest testem. Po wypełnieniu zastanów się, co Cię zaskoczyło i co chciałbyś poprawić. Jeśli czujesz się na siłach, podziel się swoimi spostrzeżeniami z kolegą lub prowadzącym.

Kiedy otrzymuję nieoczekiwaną wiadomość lub powiadomienie, zanim odpowiem, robię chwilę przerwy..

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Zanim kliknę w link, zwracam uwagę na to, jak się czuję (jestem ciekawy, zaniepokojony, spieszy mi się).

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

W przypadku nietypowych próśb sprawdzam je w innym źródle (u znajomego, w oficjalnym dziale pomocy itp.), zamiast po prostu wierzyć w treść wiadomości.

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Potrafię rozpoznać, kiedy emocje są wykorzystywane, by skłonić mnie do podjęcia szybkiej decyzji (na przykład wiadomość, która ma mnie przestraszyć lub podekscytować).

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Proszę o pomoc lub drugą opinię, gdy coś w sieci wydaje mi się „nie tak”.

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Regularnie aktualizuję swoje urządzenia i aplikacje (instaluję aktualizacje, poprawki).

Dofinansowane przez Unię Europejską

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Ograniczam zakres danych osobowych, które udostępniam publicznie (np. zdjęcia o charakterze intymnym, pełne imię i nazwisko, dane kontaktowe).

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Kiedy popełnię błąd w sieci (na przykład kliknę coś, czego nie powinienem), potrafię zachować spokój i spróbować to naprawić, zamiast ukrywać to ze strachu.

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Wspieram znajomych, gdy borykają się ze stresem w sieci lub padają ofiarą oszustw (na przykład pomagam im zgłosić nadużycie lub ostrzegam ich, jeśli zauważę coś podejrzanego).

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Robię sobie krótkie przerwy od ekranów, żeby się emocjonalnie zresetować, zwłaszcza, gdy czuję, że jestem zestresowany lub zdenerwowany.

☐ Prawie zawsze ☐ Czasami ☐ Rzadko ☐ Nigdy

Wyjaśnienie (To nie jest „ocena", a jedynie wskazówka):

- Jeśli w przypadku większości pytań zaznaczyłeś opcję „Prawie zawsze" lub „Czasami", oznacza to, że wykazujesz już dobrą świadomość i masz dobre nawyki w wielu obszarach. Sprawdź, w których przypadkach zaznaczyłeś „Rzadko/Nigdy", i skup się na nich, jako na obszarach wymagających poprawy.
- Jeśli w kilku punktach zaznaczyłeś „Rzadko" lub „Nigdy", to nic strasznego – oznacza to po prostu, że masz jasno określone obszary, nad którymi warto popracować. Wybierz jeden lub dwa, nad którymi zaczniesz pracować w pierwszej kolejności (próba zmiany wszystkiego naraz może być trudna).

Moje spostrzeżenia: (wypełnij po ukończeniu powyższego)

Dofinansowane przez Unię Europejską

Emocją, która najczęściej skłania mnie do korzystania z Internetu, jest: _____ (np., ciekawość, nuda, FOMO, złość...).

Sytuacją, w której czuję się najmniej panem sytuacji w sieci, jest: _____ (np. późno w nocy na portalach społecznościowych, podczas kłótni w komentarzach, gdy widzę najświeższe wiadomości...).

Moim osobistym sygnałem „zatrzymaj się i sprawdź" będzie: _____ (Jaki sygnał przypomni Ci, żeby się zatrzymać? np. „Kiedy zauważę, że czuję się zdenerwowany/podekscytowany, wezmę głęboki oddech" lub „Jeśli coś jest oznaczone, jako „pilne", to dla mnie znak, żeby to dokładnie sprawdzić.").

Osobą wspierającą lub przyjacielem, który będzie mi przypominał o zachowaniu bezpieczeństwa, jest: _____ (podaj imię osoby, której ufasz i która będzie cię delikatnie motywować, np. „Poprosiłem brata, żeby mi przypominał, jeśli zbytnio się denerwuję podczas gier.").

Mój mikro-cel na ten tydzień: (wybierz jedno lub dwa proste działania do przećwiczenia)

☐ Postaram się zatrzymać na chwilę, zanim kliknę na coś podejrzanego lub ekscytującego.

☐ Poproszę kolegę lub osobę dorosłą o opinię na temat czegoś dziwnego, co otrzymałem.

☐ Zmienię jedno ustawienie prywatności w mediach społecznościowych (lub usunę coś, czego żałuję, że opublikowałem).

☐ Wypróbuję ćwiczenie oddechowe 4-4-6, gdy poczuję stres związany z sytuacją w sieci.

☐ Inne: _____ (bądź konkretny: np. „Włącz uwierzytelnianie dwuskładnikowe na moich głównych kontach", „Rób sobie codziennie wieczorem godzinę przerwy od Instagrama" itp.)

(Trzymaj to w miejscu, gdzie będziesz to widzieć. Możesz nawet podzielić się swoim celem z przyjacielem, żeby mógł sprawdzić, jak sobie radzisz. Małe kroki prowadzą do wielkich zmian!)

Załącznik 2: Karty scenariuszy rozpoznawania zagrożeń

Cel: Karty te przedstawiają krótkie scenariusze ilustrujące manipulację emocjonalną w komunikacji cyfrowej. Wykorzystaj je, aby pomóc uczestnikom

Dofinansowane przez Unię Europejską

zidentyfikować czynniki wywołujące emocje i sformułować bezpieczne reakcje.

(Na każdej karcie podano kategorię zdarzenia wywołującego, przykładową wiadomość, zamierzoną reakcję emocjonalną oraz wzorcową, bezpieczną odpowiedź.)

Czynnik wyzwalający 1 – Pilność

- Wiadomość: „Twoje konto zostanie zablokowane za 30 minut, jeśli nie potwierdzisz tutaj swojego hasła: [złośliwy link]”
- Wykorzystywane emocje: Niepokój / strach przed utratą
- Bezpieczna odpowiedź: „Wygląda to na pilną sprawę, ale nie będę się spieszyć. Wejdę bezpośrednio do aplikacji/na stronę internetową, żeby sprawdzić stan mojego konta – nie kliknę tego linku.”

Czynnik wyzwalający 2 – Strach

- Wiadomość: „⚠ Ostrzeżenie dotyczące bezpieczeństwa: Ktoś próbował uzyskać dostęp do Twoich zdjęć! Wyślij TERAZ ten 6-cyfrowy kod, aby zabezpieczyć swoje dane”.
- Wykorzystywane emocje: Panika / strach
- Bezpieczna odpowiedź: „Martwię się, ale nie wyślę żadnego kodu w wiadomości. Sam sprawdzę w ustawieniach konta, czy pojawiło się jakieś powiadomienie. Prawdziwe serwisy nie proszą o podawanie kodów w ten sposób w prywatnych wiadomościach”.

Czynnik wyzwalający 3 – Empatia

- Wiadomość: „Proszę, dziecko mojego przyjaciela jest w szpitalu i potrzebuje pilnej operacji. Zbieramy datki – wystarczy kliknąć tutaj, aby pomóc; nawet 5 euro będzie miało ogromne znaczenie”.
- Wykorzystywane emocje: Współczucie / poczucie winy
- Bezpieczna odpowiedź: „Przykro mi to słyszeć. Przekazuję darowizny wyłącznie na rzecz sprawdzonych organizacji charytatywnych lub osób, które osobiście znam. Nie kliknę w ten link – rozważę inne sposoby pomocy, jeśli uda mi się zweryfikować tę historię”.

Czynnik wyzwalający 4 – Autorytet

- Widomość: “[Admin]: Tu dział IT szkoły. Twoje konto zostało zablokowane. Prześlij nam swoje hasło, abyśmy mogli rozwiązać ten problem, w przeciwnym razie utracisz dostęp do konta”.
- Wykorzystywane emocje: Posłuszeństwo / Presja ze strony autorytetu

Dofinansowane przez Unię Europejską

- Bezpieczna odpowiedź: „Nie mogę podać swojego hasła. Jeśli pojawi się jakiś problem, skontaktuję się bezpośrednio z działem IT, korzystając z oficjalnych kanałów. (Warto też zauważyć, że prawdziwi administratorzy nigdy nie proszą o podanie hasła)".

Czynnik wyzwalający 5 – Możliwość/nagroda

- Wiadomość: „🎉 Gratulacje! Wygrałeś nowego iPhone'a w naszym konkursie! Wystarczy, że pokryjesz tutaj koszt wysyłki w wysokości 2 euro, aby odebrać nagrodę w ciągu godziny."
- Wykorzystywane emocje: Podekscytowanie / chciwość (oraz FOMO – strach przed przegapieniem czegoś)
- Bezpieczna odpowiedź: „Gdyby to była prawda, nie musiałbym płacić. Brzmi zbyt pięknie, żeby mogło być prawdziwe, więc pewnie tak właśnie jest. Nie kliknę niczego ani nie wyślę żadnych pieniędzy".

Czynnik wyzwalający 6 – Ciekawość

- Wiadomość: „Hej, zobacz to! Ktoś wrzucił naprawdę żenujące wideo z tobą 😳. Robi furorę: [link]".
- Wykorzystywane emocje: Ciekawość /niepewność
- Bezpieczna odpowiedź: „Ta wiadomość próbuje mnie wystraszyć. Nie kliknę w link. Skontaktuję się z moim znajomym albo wejdę bezpośrednio na platformę, żeby sprawdzić, czy rzeczywiście jest tam jakiś film, – ale podejrzewam, że to fałszywa wiadomość".

(Wskazówka dla moderatora: Zachęć uczestników do uogólnienia tych odpowiedzi. Dokładne sformułowania mogą się różnić, ale schemat jest następujący: nie ulegaj emocjonalnemu naciskowi, zweryfikuj sytuację w inny sposób i zareaguj (lub nie reaguj) w sposób, który nie da napastnikowi tego, czego chce.)

Załącznik 3: Akta spraw cyberdetektywa

Cel

Każdy plik zawiera opis sytuacji oraz materiały dowodowe. Należy dać zespołom czas na przeanalizowanie tych materiałów i udzielenie odpowiedzi.

Sprawa 1 – Komunikat dotyczący konkursu

Opis: Otrzymujesz prywatną wiadomość na Instagramie od konta o nazwie „Natl_TalentAwards2025" z następującą treścią: „Gratulacje! Zostałeś finalistą Krajowego Konkursu Talentów Młodzieżowych. Aby odebrać nagrodę,

Dofinansowane przez Unię Europejską

potwierdź swoją tożsamość, klikając w link i przesyłając zdjęcie dokumentu tożsamości w ciągu 24 godzin". Niejasno pamiętasz, że brałeś udział w internetowym konkursie wokalnym, ale nie masz pewności, czy to ten sam konkurs. Wiadomość zawiera krzykliwe emotikony, a konto nie ma odznaki zweryfikowanego użytkownika.

Dowód: (a) Zrzut ekranu z treścią wiadomości prywatnej. (b) Fragment profilu „Natl_TalentAwards2025" – 3 posty, 0 obserwujących, obserwuje 200 osób. (c) Link w wiadomości to skrócony adres URL typu bit.ly.

Zadanie dla zespołu:

- Wymień, co najmniej 3 sygnały ostrzegawcze zawarte w wiadomości lub profilu (np. niezweryfikowane konto, mała liczba obserwujących jak na konkurs o zasięgu ogólnokrajowym, skrócony link, wywoływanie poczucia pilności, prośba o przesłanie dokumentu tożsamości w prywatnej wiadomości, czego konkursy zazwyczaj nie wymagają).
- Jak sprawdzić, czy ten konkurs jest prawdziwy? (np. zajrzyj na oficjalną stronę Krajowego Konkursu Młodych Talentów – czy taki konkurs w ogóle się odbył? Czy ogłoszono publicznie listę finalistów? Czy na oficjalnej stronie znajduje się link do tego konta na Instagramie? Albo napisz do znajomego, który też brał udział w konkursie.)
- Zdecyduj: czy kliknąć w link, czy nie? Czy odpowiedzieć, a jeśli tak, to, co napisać? A może zgłosić to? (Najprawdopodobniej: nie klikaj, nie podawaj danych osobowych. Prawdopodobnie fałszywa wiadomość/phishing. Bezpieczne rozwiązanie:, jeśli naprawdę uważasz, że to może być prawdziwe, poszukaj oficjalnych danych kontaktowych organizatorów konkursu i zapytaj ich. Odpowiedź może być skąpa lub może jej w ogóle nie być. Zgłoszenie konta do Instagrama, jako spam może być dobrym rozwiązaniem.)
- Refleksja po rozwiązaniu zadania:, Jakie emocje towarzyszyły tej próbie? (Być może podekscytowanie/duma z „wygranej" oraz poczucie pilności.) W jaki sposób wasz zespół zdołał opanować te emocje?

Sprawa 2 – Przyjaciel w potrzebie

Opis: Otrzymujesz wiadomość od swojej przyjaciółki Jenny na Instagramie: „Hej... Jestem w podróży i zgubiłam portfel😣. Utknęłam i potrzebuję trochę pieniędzy na bilet powrotny do domu. Czy mogłabyś przelać mi jakieś 100 dolarów przez PayPal? Oddam ci w przyszłym tygodniu, obiecuję!" To rzeczywiście nazwa użytkownika Jenny na Instagramie i rozpoznajesz jej zdjęcie profilowe. Ale coś tu nie gra – Jenny zazwyczaj pisze bardzo formalnie,

Dofinansowane przez Unię Europejską

a ta wiadomość wydaje się nieco niepasująca do jej charakteru (poza tym nie wiedziałeś, że jest za granicą).

Dowód: (a) Zrzut ekranu z rozmowy na Instagramie w prywatnych wiadomościach – „Jenny" pisze tam również, żeby do niej nie dzwonić, bo skradziono jej telefon (kolejna wymówka). (b) Na profilu na Instagramie Twojej prawdziwej przyjaciółki Jenny widnieje nieco inna nazwa użytkownika (ta, która do Ciebie pisze, ma dodatkowy podkreślnik). (c) Wpis na WhatsAppie: masz osobną rozmowę z prawdziwą Jenny z wczoraj, w której nie wspomniała nic o podróży.

Zadanie dla zespołu:

- Zauważ różnice, które mogą wskazywać, że to nie jest Twój znajomy (fałszywe konto o niemal identycznej nazwie użytkownika? Zhakowane konto? Sprawdź szczegóły profilu, ostatnie posty itp.).
- Jakie kroki podejmujesz, aby upewnić się, czy Jenny naprawdę ma kłopoty? (np. spróbuj zadzwonić lub wysłać SMS-a na jej zwykły numer; skontaktuj się ze wspólnym znajomym lub jej rodzicami; zadaj pytanie, na które odpowiedź znałaby tylko prawdziwa Jenny; sprawdź, czy styl wiadomości wydaje się odpowiedni.)
- Przygotuj uprzejmą odmowę lub bezpieczną odpowiedź na wiadomość na Instagramie (lub po prostu nie odpowiadaj), która nie zepsuje waszych relacji, na wypadek gdyby to naprawdę była ona, a jednocześnie zapewni ci bezpieczeństwo. Na przykład: „Jenny, tak mi przykro! Szkoda, że nie mogę pomóc. Czy mogę skontaktować się z twoją mamą?" (Oszust może się wycofać lub się zdenerwować; prawdziwa przyjaciółka powiedziałaby „jasne" lub wyjaśniła więcej.) Albo po prostu: „Nie mogę wysłać pieniędzy, ale spróbuję skontaktować się w inny sposób, żeby sprawdzić, czy wszystko z tobą w porządku".
- Czy należy zgłosić to konto lub tę sytuację? (Tak, po potwierdzeniu, że jest to fałszywe konto, należy zgłosić przypadek podszywania się lub oszustwa do platformy.)
- Refleksja:, Jaki czynnik emocjonalny tu zadziałał? (Empatia i poczucie pilności). W jaki sposób nawyk sprawdzania informacji uchronił cię przed potencjalną stratą pieniędzy? Jak byś się czuł, gdybyś wysłał pieniądze, a potem dowiedział się, że to oszustwo – czy to motywuje cię do zachowania ostrożności?

Dofinansowane przez Unię Europejską

Sprawa 3 – Fałszywa oferta pracy

Opis: Otrzymujesz wiadomość e-mail, która na pierwszy rzut oka wygląda dość profesjonalnie: pochodzi od firmy „GlobalDataEntry Inc." i zawiera ofertę pracy zdalnej w niepełnym wymiarze godzin za 500 dolarów tygodniowo, z elastycznym harmonogramem. Firma znalazła Twój profil na LinkedIn (wskazałeś tam, że szukasz nowych możliwości). Twierdzą, że aby kontynuować proces, musisz wypełnić formularz (w załączniku), a także przesłać zeskanowaną kopię dowodu tożsamości oraz unieważniony czek w celu skonfigurowania przelewu bezpośredniego. W wiadomości e-mail znajdują się ogólne sformułowania i kilka błędów gramatycznych. Adres e-mail nadawcy to [adres e-mail].

Dowód: (a) Zrzut ekranu z treścią wiadomości e-mail. (b) Załącznik „JobApplicationForm.pdf" (jeśli go załączysz, może to być bardzo prosty formularz zawierający pytania o imię i nazwisko, adres, numer konta bankowego itp.). (c) Jeśli wpiszesz w wyszukiwarce „GlobalDataEntry Inc.", nie pojawią się żadne wiarygodne wyniki, a jedynie posty na forach dotyczące oszustw związanych z ofertami pracy. (W przypadku spotkania offline możesz przedstawić wydruk z fikcyjnymi „wynikami wyszukiwania", pokazujący, że firma nie figuruje na LinkedIn lub że istnieją doniesienia o oszustwach.)

Zadanie dla zespołu:

- Zwróć uwagę na nieścisłości lub sygnały ostrzegawcze w wiadomości e-mail (np. zbyt wysokie wynagrodzenie w stosunku do prostych zadań, nietypowa prośba o podanie danych osobowych i bankowych na tak wczesnym etapie, adres Gmaila niebędący adresem firmowym, błędy gramatyczne, brak informacji o firmie w Internecie, brak osobistego powitania lub etapu rozmowy kwalifikacyjnej).
- Jak sprawdzić, czy ta oferta pracy jest prawdziwa? (np. wpisz nazwę firmy + „oszustwo"; sprawdź domenę rzekomej strony internetowej firmy – o, nie ma żadnej; przyjrzyj się domenie adresu e-mail nadawcy, – dlaczego Gmail, skoro to firma? Zapytaj na LinkedIn lub forach, czy ktoś o niej słyszał). Można nawet odpowiedzieć e-mailem z pytaniem, – ale to może tylko zachęcić oszusta do dalszych prób, więc prawdopodobnie lepiej nie wdawać się w kontakt.
- Decyzja: Czy odpowiedzieć, prosząc o potwierdzenie (np. „Czy możemy umówić się na rozmowę telefoniczną? Czy mogą Państwo przesłać oficjalną umowę?"), czy też zignorować wiadomość? Jeśli masz pewność, że to oszustwo, możesz nie odpowiadać lub grzecznie odmówić, a także zgłosić wiadomość, jako próbę wyłudzenia danych. Jeśli nie masz pewności, postępuj z najwyższą ostrożnością i nie

Dofinansowane przez Unię Europejską

wysyłaj żadnych dokumentów osobistych, dopóki nie upewnisz się – jednak generalnie ten scenariusz stanowi znany schemat oszustwa.

- Co zrobić z załącznikiem? (Najlepiej go nie otwierać – może to być złośliwe oprogramowanie. Można też otworzyć go w bezpieczny sposób – w środowisku izolowanym lub na telefonie, – ale lepiej tego unikać.)
- Refleksja: Omówcie, w jaki sposób chciwość/podekscytowanie (łatwa, wysoka pensja) oraz być może pochlebstwa („to ciebie znaleźliśmy, to ciebie wybraliśmy") mogą zaciemnić osąd. Jakich sztuczek psychologicznych używali oszuści? (Wywieranie presji poprzez nakłanianie do szybkiego działania w celu zapewnienia sobie stanowiska, odwoływanie się do potrzeb finansowych.) W jaki sposób weryfikacja informacji i poświęcenie czasu chronią cię w tym przypadku przed kradzieżą tożsamości?

(Możecie śmiało wymyślać dodatkowe scenariusze, np. stronę phishingową, znalezienie pendrive'a zainfekowanego złośliwym oprogramowaniem, próbę szantażu seksualnego itp., w zależności od tego, jakie zagrożenia chcecie przećwiczyć. Pamiętajcie o poziomie zaawansowania i poczuciu komfortu uczestników.)

Dofinansowane przez Unię Europejską

EM&M

EMotional intelligence & cybersecurity environMents in youth education

Partnerzy:

Asociatia De Dezvoltare Economico-Sociala (**ADES)** - Koordynator, Rumunia

KAINOTOMIA & SIA EE - Partner, Grecja

LABC S.R.L. - Partner, Włochy

STOWARZYSZENIE CENTRUM WSPIERANIA EDUKACJI I PRZEDSIEBIORCZOSCI (**CWEP**) - Partner, Polska

E&D KNOWLEDGE CONSULTING, LDA - Partner, Portugalia

"**PRAMMER**" Wissens Stadtinstitut Zur Sozialforschung Verein Zur Förderung Der Partizipativen, Mediativen Und Sozialen Entwicklung Und Die Vermittlung Von Künstlerischen, Sportlichen, Gesundheitlichen, Kulturellen, Wirtschaftlichen, Wissenschaftlichen - Partner, Austria

Dofinansowane przez Unię Europejską

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Niniejszy dokument został opracowany przy udziale zespołu projektowego. Niektóre fragmenty tekstu zostały zweryfikowane i zredagowane przy pomocy narzędzi opartych na sztucznej inteligencji (AI) w celu poprawy przejrzystości i spójności. Ostateczna odpowiedzialność za treść spoczywa na autorach

EM&M

EMotional intelligence & cybersecurity environMents in youth education

Numer referencyjny projektu: 2024-2-RO01-KA220-YOU-000293190

Dofinansowane przez Unię Europejską