ERASMEDIAH – EDUCATIONAL REINFORCEMENT AGAINST THE SOCIAL MEDIA HYPERCONNECTIVITY
NUMER PROJEKTU: 2023-1-HU01-KA220-YOU-000161173

MODUŁ 5

CYBERBEZPIECZEŃSTWO I BEZPIECZNE KORZYSTANIE Z INTERNETU

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by the European Union

Lekcja 5.4

Rozpoznawanie zagrożeń cybernetycznych i strategie zapobiegania wystawianiu się na nieodpowiednie treści

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie ponoszą za nie odpowiedzialności.

Czas trwania: 40 minut

Lekcja 5.4

Rozpoznawanie zagrożeń cybernetycznych i strategie zapobiegania wystawianiu się na nieodpowiednie treści

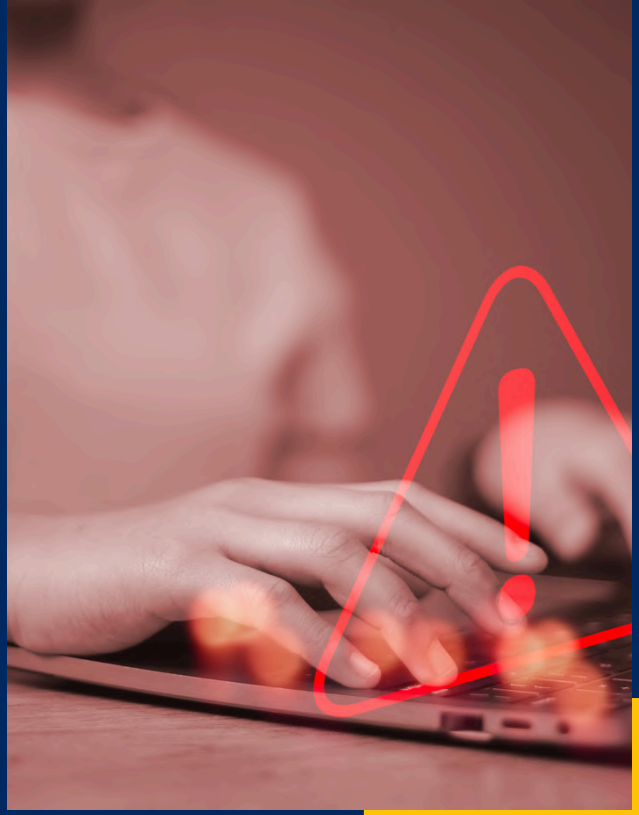
Cele:

- Rozwijanie świadomości powszechnych zagrożeń internetowych, takich jak narażenie na nieodpowiednie treści, cyberprzemoc i grooming, szczególnie skierowanych do wrażliwych użytkowników, takich jak dzieci i nastolatki.
- Zapewnienie uczniom umiejętności krytycznego rozpoznawania znaków ostrzegawczych zagrożeń cybernetycznych, takich jak podejrzane linki, drapieżne zachowania online i treści manipulacyjne.
- Promowanie aktywnych postaw w zarządzaniu interakcjami online poprzez wspieranie krytycznego myślenia, identyfikowanie bezpiecznych przestrzeni cyfrowych i utrzymywanie otwartej komunikacji na temat doświadczeń online.

Kluczowe przesłanie:

- Zagrożenia online często kryją się za niewinnie wyglądającymi platformami lub interakcjami. Rozpoznawanie znaków jest kluczem do zachowania bezpieczeństwa.
- Proste praktyki, takie jak korzystanie z filtrów treści i utrzymywanie silnej komunikacji, mogą pomóc w zapobieganiu narażeniu na szkodliwe treści i zagrożenia cybernetyczne.

RODZAJ LEKCJI:



Przegląd lekcji

W dzisiejszym hiperpołączonym środowisku cyfrowym narażenie na nieodpowiednie treści i zagrożenia cybernetyczne jest stale obecnym ryzykiem. Ta lekcja ma na celu zapewnienie kompleksowego zrozumienia charakteru i ryzyka tych zagrożeń, praktycznych narzędzi do ich łagodzenia oraz strategii sprzyjających bezpieczniejszym interakcjom online. Dzięki angażującym ćwiczeniom i praktycznym poradom opuścisz zajęcia lepiej przygotowanym do bezpiecznego i odpowiedzialnego poruszania się po cyfrowym świecie.

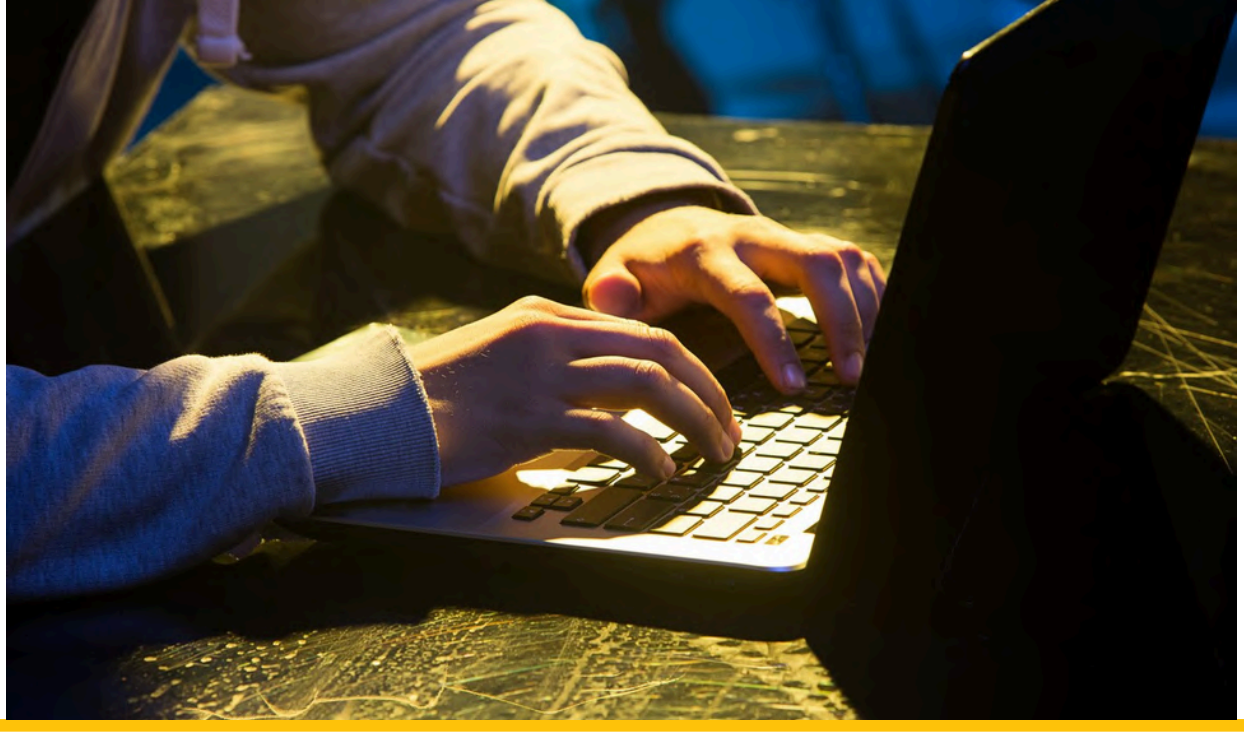
Warsztaty podzielone są na 4 etapy:

1: Podstawy zagrożeń cybernetycznych i nieodpowiednich treści (10 min)

2: Rozpoznawanie sygnałów ostrzegawczych i zagrożeń (15 min)

3: Metody zapobiegania i łagodzenia skutków (10 min)

4: Przemyślenia i zastosowanie (5 min)



Krok 1

Podstawy zagrożeń cybernetycznych i nieodpowiednich treści

Czy kiedykolwiek natknąłeś się w sieci na coś, co sprawiło, że poczułeś się niekomfortowo lub niepewnie?
Zagrożenia cybernetyczne to szkodliwe działania wymierzone w osoby lub systemy online, mające na celu kradzież informacji, wyrządzenie szkody lub wykorzystanie luk w zabezpieczeniach.
Przykłady obejmują:

- Cyberprzemoc: Wykorzystywanie platform internetowych do nękania lub zastraszania.
- Phishing: Wysyłanie fałszywych wiadomości w celu nakłonienia ludzi do ujawnienia danych osobowych.
- Grooming: Budowanie relacji z kimś w internecie w celu późniejszego wykorzystania go, często w niewłaściwy sposób.

Czym są **nieodpowiednie treści**?
Są to treści, które są szkodliwe, nieprzyzwoite lub nieodpowiednie dla określonych grup wiekowych, takie jak:

- Obrazy lub filmy o jednoznacznym charakterze.
- Manipulacyjne lub wykorzystujące wiadomości.
- Materiały zawierające przemoc lub nienawiść.

Krok 1

Podstawy zagrożeń cybernetycznych i nieodpowiednich treści

Narażenie na takie treści może powodować niepokój emocjonalny, szkodzić relacjom i prowadzić do długoterminowych konsekwencji, takich jak kradzież tożsamości lub wykorzystywanie.

Ćwiczenie

Teraz podzielimy się na małe grupy. Każda grupa otrzyma jeden scenariusz do przeanalizowania:

Scenariusz 1: Otrzymujesz wiadomość e-mail od nieznajomego, który prosi cię o podanie danych osobowych.

Scenariusz 2: Widzisz podejrzany link w wiadomości e-mail.

Scenariusz 3: Natrafiasz na nieodpowiedni komentarz w mediach społecznościowych.

Twoim zadaniem jest udzielenie odpowiedzi na pytania w grupie:

- Co jest ryzykowne w tej sytuacji?
- Jak można bezpiecznie zareagować?

Gdy wszystkie grupy skończą, wspólnie podzielcie się wnioskami.

Krok 2

Rozpoznawanie sygnałów ostrzegawczych i zagrożeń

Spójrz na poniższe przykłady i zastanów się, czy kiedykolwiek widziałeś coś podobnego w internecie. Podczas burzy mózgów przedyskutujcie w grupie, które z tych znaków ostrzegawczych są najczęstsze i jak można na nie zareagować.

1. Nieznany lub podejrzany nadawca

- Otrzymujesz wiadomość od kogoś, kogo nie znasz, z prośbą o podanie danych osobowych lub z prośbą o kliknięcie linku.
- Adres e-mail wygląda nietypowo, na przykład „bank123przyklad@mail.com” zamiast oficjalnego adresu.
- *Pytanie do dyskusji*: „Co robisz, gdy otrzymujesz wiadomość od kogoś, kogo nie rozpoznajesz?”

2. Błędy ortograficzne lub gramatyczne

- Wiadomość jest pełna błędów ortograficznych lub dziwnych sformułowań.
- Przykład: "Twoj konto jest zablkowane! Klknij by aktywać"
- *Pytanie do dyskusji*: "Czy takie błędy w wiadomości wzbudzają u ciebie podejrzenia? Dlaczego lub dlaczego nie?"

Krok 2

Rozpoznawanie sygnałów ostrzegawczych i zagrożeń

3. Pilne prośby lub groźby

- Wiadomości takie jak: „Jeśli nie zapłacisz w ciągu 24 godzin, twoje konto zostanie dezaktywowane!”.=
- Treść próbuje przestraszyć użytkownika lub zmusić go do szybkiego działania.
- *Pytanie do dyskusji*: „Jak odróżnić prawdziwe ostrzeżenie od oszustwa?”

4. Oferty zbyt piękne, by mogły być prawdziwe

- Reklamy obiecujące niesamowite nagrody: "Wygrałeś nowiutkiego iPhone'a! Kliknij tutaj, aby odebrać nagrodę"
- Strony internetowe oferujące nierealistyczne korzyści przy niewielkim wysiłku.
- *Pytanie do dyskusji*: „Dlaczego tego rodzaju oferty są niebezpieczne?”

Krok 2

Rozpoznawanie sygnałów ostrzegawczych i zagrożeń

5. Nieznane linki lub załączniki

- Otrzymujesz link, który nie wygląda na godny zaufania, na przykład "www.darmowerzeczy.teraz".
- Załączniki od nieznanych nadawców, które mogą zawierać wirusy.
- *Pytanie do dyskusji*: „Jak sprawdzić, czy link lub załącznik jest bezpieczny?”

W swojej grupie wybierz jeden z tych znaków ostrzegawczych i przedyskutuj, jak poradziłbyś sobie z tą sytuacją.
Na koniec każda grupa podzieli się swoimi spostrzeżeniami i pomysłami, jak uniknąć tych zagrożeń w codziennych działaniach online.

Krok 3

Metody zapobiegania i łagodzenia skutków

Najlepszym sposobem na zachowanie bezpieczeństwa w internecie jest podjęcie aktywnej postawy, która chroni dane i zapobiega zagrożeniom, zanim do nich dojdzie. Przyjrzyjmy się prostym strategiom, które możesz zacząć stosować od razu.

Pozostańmy w tych samych grupach. Zapoznaj się z poniższą listą prostych działań, które możesz podjąć, aby zmniejszyć ryzyko online:

- **Używaj silnych, unikalnych haseł** i regularnie je aktualizuj.
- **Włącz uwierzytelnianie wieloskładnikowe** dla ważnych kont.
- **Unikaj podejrzanych linków i załączników** - zawsze weryfikuj źródło.
- **Zapoznaj się z ustawieniami prywatności** w mediach społecznościowych i aplikacjach, aby kontrolować, kto widzi twoje informacje.
- **Aktualizuj oprogramowanie**, aby łatać luki w zabezpieczeniach.

Przedyskutujcie w grupie, które z tych działań już praktykujecie, a których wdrożenie może być dla was wyzwaniem.
Odpowiedzcie wspólnie na te pytania:

- „Jak myślisz, która strategia jest najskuteczniejsza w zachowaniu bezpieczeństwa online?”

Krok 3

Metody zapobiegania i łagodzenia skutków

„Jak możesz przypominać sobie o budowaniu lepszych nawyków, takich jak sprawdzanie ustawień prywatności lub unikanie ryzykownych linków?”
Po burzy mózgów każda grupa dzieli się jedną **nową** strategią, którą planuje przyjąć i wyjaśnia w kilku słowach, dlaczego jest ona ważna.

W ramach końcowej refleksji, poświęć chwilę na zastanowienie się nad jednym konkretnym nawykiem lub narzędziem, którego będziesz używać natychmiast, aby poprawić swoje bezpieczeństwo w internecie. Zapisz go na karteczce samoprzylepnej i zastanów się, jak możesz pomóc innym przyjąć te same nawyki. Dzieląc się swoją wiedzą, możesz stworzyć bezpieczniejsze środowisko online nie tylko dla siebie, ale także dla swoich przyjaciół, rodziny i społeczności.

Krok 4

Przemyślenia i zastosowanie

Teraz, gdy zbadaliśmy zagrożenia online i strategie zapobiegania im, nadszedł czas, aby zastanowić się nad tym, czego się nauczyłeś i pomyśleć o tym, jak możesz to zastosować w swoim codziennym cyfrowym życiu. Poświęć chwilę, aby po cichu odpowiedzieć na pytanie:

- „Jaki masz obecnie nawyk, który może narazić cię na ryzyko online?”

Zapisz swoją odpowiedź na karteczce samoprzylepnej.

Następnym krokiem jest dobranie się w pary z partnerem i podzielenie się swoimi refleksjami:

- Wyjaśnij, jaki ryzykowny nawyk zidentyfikowałeś i dlaczego może on stanowić problem.
- Podziel się działaniem lub narzędziem, które planujesz zastosować, aby zmniejszyć to ryzyko.
- Zaoferuj sobie nawzajem informacje zwrotne lub dodatkowe pomysły, aby wzmocnić swoje plany.
- Omów, w jaki sposób te strategie mogą być stosowane w różnych sytuacjach, takich jak korzystanie z publicznej sieci Wi-Fi, udostępnianie danych osobowych lub unikanie groomingu i phishingu.

Podsumowanie kluczowych wniosków

- **Świadomość jest pierwszym krokiem w kierunku ochrony.**
- **Znaki ostrzegawcze są wszędzie, ale gdy nauczysz się je rozpoznawać i odpowiednio reagować, możesz znacznie zwiększyć swoje bezpieczeństwo online!**
- **Zrozumienie zagrożeń cybernetycznych i nieodpowiednich treści pozwala zidentyfikować potencjalne ryzyko i odpowiednio zareagować.**
- **Rozpoznawanie zagrożeń w codziennych sytuacjach online pozwala działać szybko i unikać niebezpieczeństw.**
- **Szerząc świadomość, pomagasz stworzyć bezpieczniejszą społeczność online dla wszystkich.**

Instrukcje dla osób pracujących z młodzieżą, edukatorów i nauczycieli

Cel:
Ta lekcja ma na celu podniesienie świadomości na temat zagrożeń internetowych, w tym zagrożeń cybernetycznych i nieodpowiednich treści, oraz wyposażenie uczestników w praktyczne strategie sprzyjające bezpieczniejszym interakcjom online. Analizując rzeczywiste scenariusze, uczestnicy nauczą się identyfikować zagrożenia, rozpoznawać znaki ostrzegawcze i podejmować środki zapobiegawcze.

Potrzebne materiały:

- Flipchart lub narzędzie do prezentacji cyfrowej do przedstawiania kluczowych pojęć
- Długopisy i markery
- Puste kartki papieru do sporządzania notatek lub wykonywania ćwiczeń
- Dostęp do narzędzi takich jak CyberWise lub Malwarebytes Browser Guard (w przypadku prezentowania ich uczestnikom)
- Kolorowe karteczki samoprzylepne do burzy mózgów

Krok 1: Podstawy zagrożeń cybernetycznych i nieodpowiednich treści (10 min)

1. Zacznij od zapytania uczestników: „Czy kiedykolwiek spotkałeś się z czymś online, co wydawało się niebezpieczne lub podejrzane?”. Zachęć kilka osób do podzielenia się swoimi doświadczeniami lub podania krótkiego przykładu, takiego jak otrzymanie podejrzanej wiadomości e-mail lub zobaczenie obraźliwego komentarza. Wykorzystaj to, aby podkreślić znaczenie zrozumienia i radzenia sobie z zagrożeniami online.
2. Mini wykład - wyjaśnij kluczowe zagrożenia cybernetyczne: phishing, grooming itp. Zdefiniuj nieodpowiednie treści, w tym:
- Jednoznaczne materiały - Szkodliwe lub drastyczne zdjęcia i filmy.
- Wykorzystujące wiadomości - manipulacyjna lub szkodliwa komunikacja.
- Treści nieodpowiednie dla wieku - materiały nieodpowiednie dla określonych grup wiekowych.

3. Ćwiczenie: Podziel uczestników na grupy po 3-5 osób i przydziel każdej z nich jeden z trzech różnych scenariuszy.

Instrukcje dla grup:

1. Przeanalizuj ryzyko: Omów, co sprawia, że scenariusz jest ryzykowny (np. nieznany nadawca, pilny ton lub podejrzany link).
2. Zaproponuj bezpieczne działania: Przeprowadź burzę mózgów na temat praktycznych reakcji:

- W przypadku wiadomości e-mail: Unikaj klikania linków, zweryfikuj nadawcę za pośrednictwem oficjalnych kanałów lub zgłoś jako spam.
- W przypadku nieodpowiednich komentarzy: Zablokuj użytkownika, zgłoś komentarz i unikaj odpowiadania.
- W przypadku podejrzanych linków: Najedź kursorem, aby sprawdzić adres URL, nie klikaj, jeśli nie masz pewności, i skonsultuj się z zaufanym źródłem.

3. Podziel się wynikami: Grupy podsumowują swoją analizę i dzielą się nią z klasą. Podkreśl wspólne strategie i omów ich skuteczność.
4. Zakończ, wzmacniając kluczowe punkty, łącząc ćwiczenie z szerszymi strategiami bezpieczeństwa online, które zostaną omówione w kolejnych krokach.

Krok 2: Rozpoznawanie sygnałów ostrzegawczych i zagrożeń (15 min)

1. Zapoznaj uczestników z typowymi sygnałami ostrzegawczymi zagrożeń cybernetycznych na konkretnych przykładach:

- Podejrzane linki lub nieznani nadawcy: Wiadomości od nieznanych kontaktów z linkami lub załącznikami (np. „www.darmowerzeczy.xyz”).
- Błędy ortograficzne lub pilne żądania: Wiadomości takie jak "Twoj konto jest zablkowany! rektywuj teraz", często źle napisane, aby nadać im pilny charakter.
- Oferty zbyt dobre, by mogły być prawdziwe: Obietnice nagród lub ofert, takie jak „Wygrałeś darmowego iPhone'a!”.

Możesz także użyć wizualizacji, takich jak zrzuty ekranu z prób phishingu, i zachęcić uczestników do dzielenia się przykładami w celu zwiększenia zaangażowania.

2. Następnym krokiem jest przeprowadzenie ćwiczenia grupowego. Podziel uczestników na małe grupy i przydziel każdej z nich konkretny znak ostrzegawczy do przeanalizowania (np. pilne wiadomości lub podejrzane linki). Wykonaj następujące kroki:

1. Przeanalizuj ostrzeżenie: Omów, co sprawia, że zagrożenie jest przekonujące (np. pilność lub podstęp).
2. Zaproponuj rozwiązania: Burza mózgów na temat odpowiedzi, takich jak weryfikacja źródeł, unikanie podejrzanych linków lub zgłaszanie oszustw.
3. Podsumuj ustalenia: Przygotuj praktyczne wskazówki dotyczące unikania przypisanego zagrożenia.

3. Na koniec każda grupa przedstawia swoje spostrzeżenia i strategie. Podsumuj je w postaci zbiorczej listy najlepszych rozwiązań na tablicy lub flipcharcie. Zakończ, podkreślając wartość ostrożności, weryfikacji i krytycznego myślenia w zachowaniu bezpieczeństwa w internecie.

Krok 3: Metody zapobiegania i łagodzenia skutków (10 min)

1. Rozpocznij od podkreślenia znaczenia aktywnej postawy w celu ochrony danych osobowych i zmniejszenia ryzyka online. Przedstaw listę prostych działań, które uczestnicy mogą podjąć natychmiast, takich jak:

- Używanie silnych, unikalnych haseł i regularne ich aktualizowanie.
- Włączenie uwierzytelniania wieloskładnikowego dla najważniejszych kont.
- Unikanie podejrzanych linków i załączników poprzez weryfikację ich źródeł.
- Sprawdzanie ustawień prywatności w mediach społecznościowych i aplikacjach.
- Aktualizowanie oprogramowania w celu wyeliminowania luk w zabezpieczeniach.

Wyjaśnij, w jaki sposób te działania mogą skutecznie ograniczyć powszechne zagrożenia online.

2. Pozostaw uczestników w ich istniejących grupach i przedstaw listę działań. Poproś ich o omówienie i wykonanie następujących zadań:

1. Dyskusja grupowa:

- Określ, które działania już stosują, a które stanowią dla nich wyzwanie.
- Przedyskutuj, dlaczego niektóre strategie mogą być trudniejsze do wdrożenia i przeprowadź burzę mózgów na temat sposobów przezwyciężenia tych wyzwań.

2. Odpowiedz na kluczowe pytania:

- „Jak myślisz, która strategia jest najskuteczniejsza w zachowaniu bezpieczeństwa online?”
- „Jak możesz przypomnieć sobie o budowaniu lepszych nawyków, takich jak regularne sprawdzanie ustawień prywatności lub unikanie ryzykownych linków?”

3. Podziel się nowymi strategiami:

- Każda grupa wybiera jedną nową strategię, którą planuje przyjąć, wyjaśnia, dlaczego jest ona ważna i dzieli się nią z innymi.

Krok 3: Metody zapobiegania i łagodzenia skutków (10 min)

3. Zakończ ćwiczenie, prosząc każdego uczestnika o indywidualne zastanowienie się nad jednym nawykiem lub narzędziem, którego będą używać natychmiast, aby poprawić swoje bezpieczeństwo w internecie. Niech zapiszą go na karteczce samoprzylepnej. Zachęć uczestników do zastanowienia się, w jaki sposób mogą podzielić się tym nawykiem z przyjaciółmi, rodziną lub współpracownikami, aby wspólnie promować bezpieczniejsze środowisko online.

Krok 4: Przemyślenia i zastosowanie (5 min)

1. Indywidualna refleksja:
   - Zapytaj uczniów: „Jaki jest jeden nawyk online, który możesz zmienić, aby poprawić bezpieczeństwo?”
   - Uczestnicy zapisują swoje odpowiedzi na karteczkach samoprzylepnych.
2. Dyskusja między rówieśnikami:
   - Uczestnicy w parach dzielą się swoimi celami i sugerują możliwe do podjęcia kroki.
3. Podsumowanie:
   - Zakończ motywującym podsumowaniem. Może to być na przykład: „Niewielkie zmiany w zachowaniu online mogą mieć duży wpływ na bezpieczeństwo twoje i twojej społeczności”.

Kluczowe wnioski:
Uczestnicy powinni opuścić sesję z jasnym zrozumieniem, jak identyfikować zagrożenia cybernetyczne i nieodpowiednie treści, takie jak próby phishingu, wiadomości manipulacyjne lub podejrzane linki. Podkreśl znaczenie praktycznych strategii bezpieczeństwa, takich jak używanie silnych haseł, włączanie uwierzytelniania wieloskładnikowego i dostosowywanie ustawień prywatności w celu ochrony danych osobowych.
Zachęć uczestników do przyjęcia aktywnej postawy w sposobie myślenia poprzez wspieranie krytycznego myślenia i prowadzenie otwartych dyskusji na temat zagrożeń online. Wspieraj te zasady poprzez regularne działania i dzielenie się wiedzą z innymi, które promują bezpieczniejsze nawyki online w ich społecznościach.

Działania uzupełniające i zadanie domowe:
Poproś uczestników o:

- Przejrzenie osobistych ustawień mediów społecznościowych.
- Przetestowanie narzędzi takich jak Malwarebytes Browser Guard lub filtry treści.
- Podzielenie się jedną z poznanych strategii z przyjacielem lub członkiem rodziny.

Wskazówki dla nauczycieli:
Spraw, by lekcje były angażujące, wykorzystując rzeczywiste przykłady i przejrzyste wizualizacje w celu wyjaśnienia zagrożeń online i praktycznych strategii bezpieczeństwa. Zachęcaj do interaktywnych dyskusji, aby pomóc uczestnikom zapoznać się z materiałem. Praktyczne działania, takie jak tworzenie przewodników bezpieczeństwa, pomagają utrwalić koncepcje. Utrzymuj wspierające i otwarte środowisko, w którym pytania są mile widziane, i podkreślaj długoterminowe korzyści płynące z bezpiecznych nawyków online. Podkreśl kluczowe lekcje poprzez zadania uzupełniające lub refleksje grupowe, aby upewnić się, że uczestnicy zachowają i zastosują to, czego się nauczyli.

Działania uzupełniające i zadanie domowe:

Poproś uczestników o:

- Sprawdzenie ich osobistych ustawień mediów społecznościowych.
- Przetestowanie narzędzi takich jak Malwarebytes Browser Guard lub filtrów treści.
- Podzielenie się jedną z poznanych strategii z przyjacielem lub członkiem rodziny.

Wskazówki dla nauczycieli:

Spraw, by lekcja była angażująca, wykorzystując rzeczywiste przykłady i przejrzyste wizualizacje w celu wyjaśnienia zagrożeń online i praktycznych strategii bezpieczeństwa. Zachęcaj do interaktywnych dyskusji, aby pomóc uczestnikom zrozumieć materiał. Praktyczne działania, takie jak tworzenie przewodników bezpieczeństwa, pomagają utrwalić koncepcje. Utrzymuj wspierające i otwarte środowisko, w którym pytania są mile widziane, i podkreślaj długoterminowe korzyści płynące z bezpiecznych nawyków online. Podkreślaj kluczowe lekcje poprzez zadania uzupełniające lub refleksje grupowe, aby upewnić się, że uczestnicy zachowują i stosują to, czego się nauczyli.

Narzędzia

CyberWise

CyberWise to platforma edukacyjna, która oferuje narzędzia, zasoby i przewodniki pomagające osobom, w szczególności rodzicom, nauczycielom i uczniom, zrozumieć bezpieczeństwo w internecie. Zawiera moduły dotyczące rozpoznawania zagrożeń cybernetycznych, takich jak phishing, cyberprzemoc i nieodpowiednie treści, a także strategie ograniczania ryzyka.

www.cyberwise.org

Malwarebytes Browser Guard

To bezpłatne rozszerzenie przeglądarki, które chroni użytkowników przed phishingiem, oszustwami, złośliwym oprogramowaniem i nieodpowiednimi treściami. Aktywnie blokuje szkodliwe strony internetowe i reklamy, zapewniając bezpieczniejsze przeglądanie dla wszystkich użytkowników, nie tylko dzieci.

www.malwarebytes.com

Referencje

- CyberWise. (n.d.). Pozyskano z https://www.cyberwise.org
- Dalby, J. (2021, Styczeń 15). How to Avoid Inappropriate Content. Gabb Now. Pozyskano z https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (2023, Wrzesień 25). Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. Pozyskano z https://figshare.com/ndownloader/files/42443952
- Lynch, M. (2024, Kwiecień 5). 19 simple ways to block inappropriate content. The Tech Edvocate. Pozyskano z https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (2024, Luty 21). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. Pozyskano z https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (n.d.). Pozyskano z https://www.malwarebytes.com/browserguard
- Roy, R. (2021, Siespień 23). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples. Pozyskano z https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (n.d.). 10 Types of Cyber Security Threats and Solutions. Pozyskano z https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

QUIZ

1. Co jest główną oznaką próby phishingu?
A. Otrzymanie wiadomości z nieznanego, ale zweryfikowanego konta
B. Wiadomość e-mail bez linków, obrazów lub załączników
C. Wiadomość e-mail ponaglająca do natychmiastowego działania, często ze słabą gramatyką
D. Wiadomość od znanego nadawcy z prośbą o rutynowe informacje

2. Które zachowanie może zwiększyć ryzyko zagrożeń cybernetycznych?
A. Regularne aktualizowanie urządzeń i aplikacji
B. Klikanie linków w wiadomościach e-mail bez weryfikacji nadawcy
C. Korzystanie z uwierzytelniania dwuskładnikowego dla kont online
D. Sprawdzanie ustawień prywatności w mediach społecznościowych raz w miesiącu

3. Który nawyk pomaga uniknąć stania się ofiarą zagrożeń cybernetycznych?
A. Używanie menedżera haseł do tworzenia i przechowywania unikalnych haseł
B. Akceptowanie wszystkich uprawnień podczas instalowania aplikacji dla wygody
C. Udostępnianie haseł zaufanym przyjaciołom lub członkom rodziny, aby mieć zapasowe hasło na wypadek ich zapomnienia.
D. Lekceważenie ostrzeżeń dotyczących bezpieczeństwa w przeglądarce

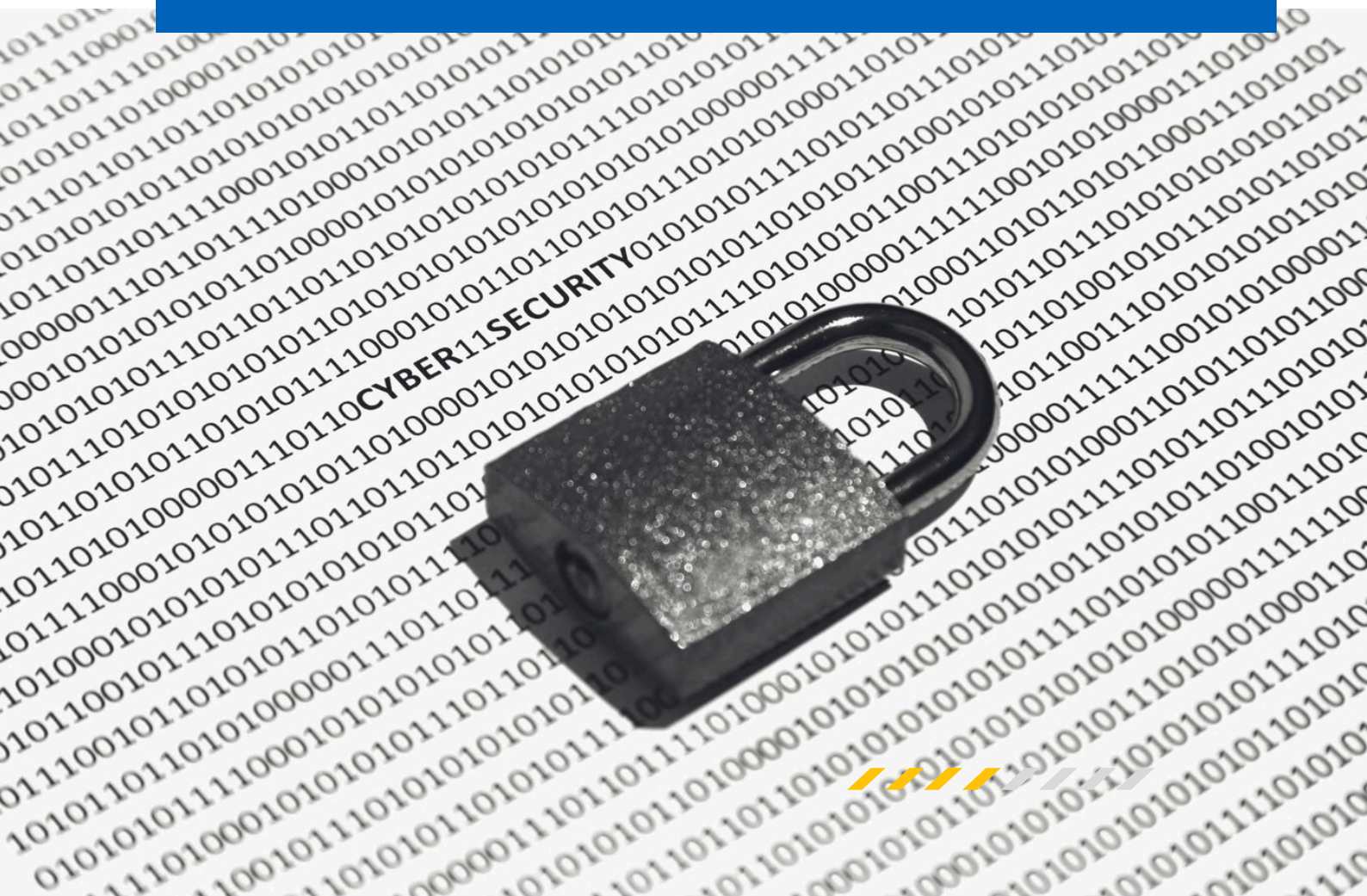
QUIZ

4. Co sprawia, że link jest podejrzany i potencjalnie szkodliwy?
A. Używa szyfrowania HTTPS
B. Przekierowuje na inną stronę internetową
C. Zawiera nietypowe znaki lub domeny
D. Został udostępniony przez znajomego w bezpośredniej wiadomości

5. Która strategia jest najskuteczniejsza w zapobieganiu narażeniu na nieodpowiednie treści?
A. Ograniczenie interakcji online do minimum
B. Wyłączenie wszystkich powiadomień na urządzeniach
C. Poleganie wyłącznie na oprogramowaniu antywirusowym
D. Korzystanie z filtrów treści i dostosowywanie ustawień prywatności

Rozwiązania

Pytanie 1: C
Pytanie 2: B
Pytanie 3: A
Pytanie 4: C
Pytanie 5: D



ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

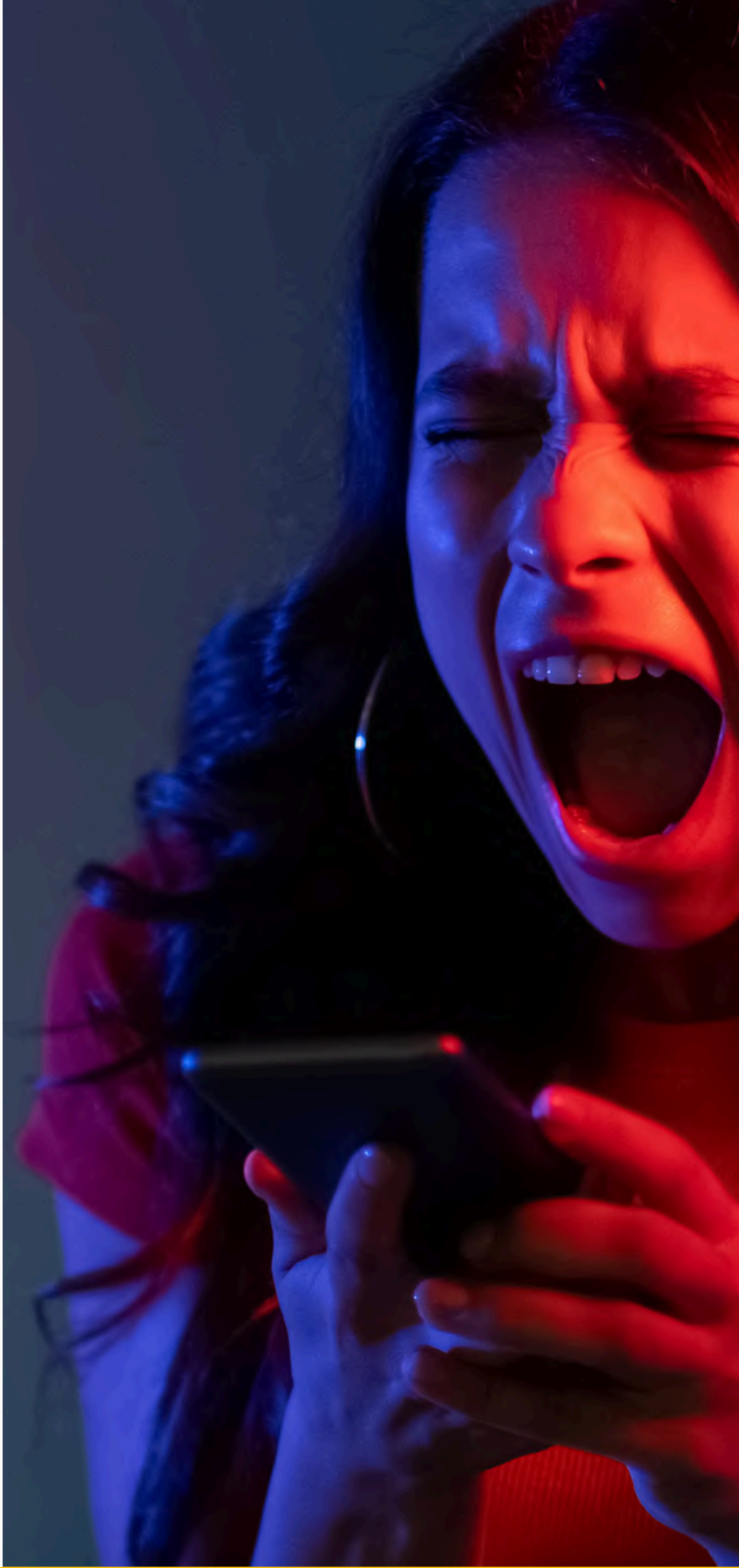
LABC

CWEP Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



Co-funded by the European Union

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie ponoszą za nie odpowiedzialności.