ZESTAW ĆWICZEŃ KREATYWNYCH UNPLUGGED

„Czy to bezpieczne?" – Zrozumieć zagrożenia w sieci

W tym ćwiczeniu uczestnicy analizują codzienne sytuacje cyfrowe, w których pojawiają się podejrzane wiadomości, e-maile i połączenia telefoniczne. Pracując wspólnie, oceniają poziom ryzyka, identyfikują sygnały ostrzegawcze i decydują o najbezpieczniejszym sposobie postępowania. Uczą się również, jak chronić swoje dane osobowe i finansowe oraz jak weryfikować prośby przed udzieleniem odpowiedzi. Do końca zajęć uczestnicy wypracują proste, praktyczne i powtarzalne zasady bezpieczniejszego i pewniejszego korzystania z usług cyfrowych

Co-funded by the European Union

CC BY NC SA

Projekt ten został współfinansowany ze środków programu ERASMUS+ Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie stanowisko jej autorów, a Komisja Europejska oraz SEPIE nie ponoszą odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Zakres tematyczny

Kompetencje informacyjne

Czas trawania

90-120 min

Poziom

Zaawansowany

Wykorzystane elementy myślenia komputacyjnego

Dekompozycja
Rozpoznawanie

Grupa docelowa

Nisko wykwalifikowane osoby dorosłe o niskich kompetencjach cyfrowych
Nisko wykwalifikowane osoby dorosłe z ograniczonym formalnym wykształceniem lub kwalifikacjami
Nisko wykwalifikowane osoby dorosłe o niskim poziomie uczestnictwa w uczeniu się przez całe życie

Cele kształcenia

- Dzielenie komunikacji lub zapytań cyfrowych na jasne i łatwe do zarządzania kroki.
- Rozpoznawanie typowych sygnałów ostrzegawczych świadczących o podejrzanej lub niebezpiecznej komunikacji cyfrowej.
- Identyfikowanie poufnych informacji, które muszą być chronione, takich jak hasła, dane bankowe i dane osobowe.
- Stosowanie prostych reguł decyzyjnych w celu określenia prawdopodobnie najbezpieczniejszej reakcji.

wzorców
Abstrahowanie
Myślenie algorytmiczne

Podejście metodologiczne

Gamifikacja
Nauczanie oparte na wyzwaniach
Uczenie się we współpracy
Uczenie się przez doświadczenie

- Jasne wyjaśnianie i demonstrowanie bezpiecznych decyzji podczas ćwiczeń opartych na odgrywaniu ról.

Obszar kompetencji

a) Kompetencje innowacyjne

Kreatywność
Myslenie krytyczne
Rozwiązywanie problemów
Komunikacja
Praca zespołowa

b) Kompetencje w zakresie umiejętności informacyjnych

Zdolność do uzyskiwania dostępu do informacji, ich rozumienia oraz krytycznej analizy
Interpretacja treści cyfrowych i wizualnych
Świadomość wpływu mediów i stronniczości przekazu biases

c) Kompetencje życiowe I zawodowe

Elastyczność i możliwości adaptacji
Inicjatywa i autonomia
Umiejętności społeczne i kompetencje międzykulturowe
Produktywność
Przywództwo i odpowiedzialność

Efekty uczenia się:

Po zakończeniu zajęć uczestnicy będą potrafili:

- Dzielić sytuacje cyfrowe na jasne i łatwe do zarządzania kroki;
- Rozpoznawać typowe sygnały ostrzegawcze w podejrzanych lub niebezpiecznych wiadomościach, e-mailach i połączeniach telefonicznych;
- Odróżniać działania prawdopodobnie bezpieczne, potencjalnie ryzykowne oraz niebezpieczne;
- Stosować proste algorytmy bezpieczeństwa w celu ochrony danych osobowych, finansowych oraz danych logowania;
- Wybierać i wyjaśniać właściwe reakcje na codzienne

		zagrożenia cyfrowe; ● Demonstrować podejmowanie prawdopodobnie bezpieczniejszych decyzji podczas ćwiczeń opartych na odgrywaniu ról. Uwagi: ● Używaj prostych i realistycznych przykładów, takich jak wiadomości tekstowe, e-maile, połączenia telefoniczne oraz zapytania online. ● Wybieraj sytuacje, które są znane uczestnikom i mają bezpośredni związek z ich codziennym życiem. ● Zachęcaj do dyskusji i dobrowolnego dzielenia się doświadczeniami, bez wywierania presji na ujawnianie prywatnych informacji. ● Udzielaj wskazówek w razie potrzeby, pozwalając jednocześnie uczestnikom na samodzielną analizę sytuacji i podejmowanie własnych decyzji. ● Używaj jasnego, przystępnego języka i wyjaśniać wszelkie nieznane pojęcia z zakresu technologii cyfrowych. ● Podkreślaj, że każdy może zostać oszukany przez przekonującą wiadomość, a proszenie o pomoc jest rozsądną strategią bezpieczeństwa. ● Wzmacniaj znaczenie zatrzymania się, sprawdzenia i zweryfikowania prośby przed udzieleniem odpowiedzi, kliknięciem w link lub udostępnieniem informacji.

Co-funded by the European Union

Czy to bezpieczne?" – Zrozumieć zagrożenia w sieci

Krok 1. Dekompozycja

Uczestnicy otrzymują wydrukowane karty opisujące proste i realistyczne scenariusze cyfrowe, na przykład: „Otrzymujesz wiadomość z prośbą o podanie danych bankowych", „Otrzymujesz połączenie telefoniczne z prośbą o podanie hasła"

Uczestnicy są proszeni o:

- Podział każdej sytuacji na mniejsze i łatwiejsze do zarządzania kroki;
- Zidentyfikowanie, kto zainicjował komunikację i w jaki sposób nawiązano kontakt;
- Określenie, jakie informacje lub działania są przedmiotem prośby;
- Wskazanie, co odbiorca powinien zrobić według oczekiwań nadawcy;
- Rozważenie możliwych konsekwencji spełnienia tej prośby.

Wsparcie prowadzącego:

- Prowadzący może wspierać pytaniami: „Co wydarzyło się najpierw?", „Czego chce ta osoba?", „Co może się stać, jeśli odbiorca spełni tę prośbę?"
- Pomagaj dorosłym uczestnikom skupić się na jednym aspekcie naraz;
- Kładź nacisk na jasne zrozumienie sytuacji.

Ten krok pomaga dorosłym uczestnikom zrozumieć sytuacje cyfrowe w prosty i ustrukturyzowany sposób.

Krok 2: Rozpoznawanie wzorców

Dorośli uczestnicy otrzymują dodatkowe przykłady wiadomości cyfrowych, e-maili, połączeń telefonicznych oraz zapytań online.

Są oni proszeni o porównanie różnych sytuacji oraz o zidentyfikowanie podobieństw i różnic, a także o:

- Rozpoznawanie powtarzających się sygnałów ostrzegawczych, takich jak:
  - Prośby o podanie danych osobowych, finansowych lub danych logowania;
  - Język wyrażający pośpiech lub groźbę, na przykład „działaj natychmiast!”;
  - Nieznani lub nieoczekiwani nadawcy;
  - Podejrzane linki lub załączniki;
  - Oferty, nagrody lub obietnice, które wydają się nierealistyczne;
  - Wywieranie presji na udzielenie odpowiedzi bez sprawdzenia informacji.

Wsparcie prowadzącego:

- Prowadzący może wspierać pytaniami: „Co wygląda podejrzanie?”, „Czy widzieliście już wcześniej coś podobnego?”
- Wskazuj na powtarzające się sygnały ostrzegawcze;
- Zachęcaj do dzielenia się osobistymi doświadczeniami.

Ten krok pomaga dorosłym uczestnikom rozpoznawać powtarzające się schematy w podejrzanej komunikacji cyfrowej i stosować tę wiedzę podczas oceny nieznanych sytuacji.

Krok 3: Abstrahowanie

Dorośli uczestnicy skupiają się na kluczowych elementach niezbędnych do oceny, czy sytuacja cyfrowa jest prawdopodobnie bezpieczna, podejrzana czy niebezpieczna.

Są oni proszeni o:

- Identyfikowanie poufnych informacji, które muszą być chronione, takich jak hasła, dane bankowe, kody weryfikacyjne i dane osobowe;
- Odróżnianie istotnych sygnałów ostrzegawczych od mniej ważnych szczegółów;
- Określenie głównego ryzyka występującego

w każdej sytuacji;
- Decydowanie, czy komunikacja jest prawdopodobnie bezpieczna, czy wymaga dalszej weryfikacji, czy też jest niebezpieczna;
- Formułowanie prostych zasad bezpieczeństwa, które można zastosować w podobnych sytuacjach.

Wsparcie prowadzącego:

- Prowadzący może wspierać pytaniami: „Jakich informacji nigdy nie należy udostępniać?", „Który szczegół jest najważniejszy przy ocenie ryzyka?", „Co można zignorować, ponieważ nie wpływa to na decyzję?"
- Kładź nacisk na proste zasady bezpieczeństwa;
- Pomagaj dorosłym uczestnikom skupić się na kluczowych zagrożeniach.

Ten krok pomaga dorosłym uczestnikom upraszczać złożone sytuacje cyfrowe, skupiać się na informacjach, które mają największe znaczenie, oraz podejmować bardziej świadome decyzje dotyczące bezpieczeństwa.

Krok 4: Myślenie algorytmiczne

Uczestnicy opracowują (indywidualnie lub w grupach) jasny, uporządkowany krok po kroku algorytm bezpiecznego reagowania na podejrzaną komunikację cyfrową. Algorytm powinien prowadzić użytkownika od momentu otrzymania wiadomości, e-maila lub połączenia telefonicznego, aż do podjęcia ostatecznej decyzji i właściwego działania.

Uczestnicy są proszeni o:

- Zdefiniowanie głównych kroków procesu podejmowania decyzji;
- Uporządkowanie kroków w logicznej sekwencji;
- Uwzględnienie punktów decyzyjnych z wykorzystaniem reguł „jeśli–to" (if-then);
- Określenie, jakie działania należy podjąć w każdej sytuacji;
- Zwizualizowanie algorytmu za pomocą kart, strzałek,

		symboli lub prostego schematu blokowego. Algorytm może obejmować następującą sekwencję: 1. Otrzymanie komunikatu. 2. Identyfikacja nadawcy oraz kanału komunikacji. 3. Określenie, jakie informacje lub działania są przedmiotem prośby. 4. Sprawdzenie sygnałów ostrzegawczych, takich jak presja czasu, groźby, podejrzane linki, nieoczekiwane prośby lub prośby o poufne dane. 5. Podjęcie decyzji, czy nadawcę można zweryfikować. 6. Wybór właściwej reakcji. Przykładowe reguły decyzyjne: ● Jeśli nadawca jest nieznany, to nie odpowiadaj natychmiast. ● Jeśli komunikat zawiera prośbę o hasło, kod weryfikacyjny lub informacje bankowe, to nie udostępniaj ich. Na koniec dorośli uczestnicy: ● Testują swoje algorytmy zapewniania bezpieczeństwa poprzez ćwiczenia oparte na odgrywaniu ról (role-play); ● Wyjaśniają i uzasadniają swoje decyzje; ● Porównują różne algorytmy opracowane przez grupy; ● Identyfikują, które zasady są najbardziej przydatne w rzeczywistych sytuacjach; ● Modyfikują swój proces podejmowania decyzji, gdy jest to konieczne. Wsparcie prowadzącego: ● Prowadzący wspierać pytaniami: „Co użytkownik powinien zrobić najpierw?”, „Jaką decyzję należy podjąć w tym momencie?” ● Zachęcaj do krytycznego myślenia podczas podejmowania decyzji. ● Wzmacniaj nawyki związane z zapewnianiem bezpieczeństwa.

Przykład

Nadawca: Zespół ds. wsparcia Global Prize
Temat: PILNE: Odbierz swoją nagrodę w wysokości 5 000 € już dziś!

Szanowny użytkowniku,
Gratulujemy! Zostałeś wybrany do otrzymania nagrody w wysokości 5 000 € w ramach pomocy w nagłych wypadkach. Oferta ta jest dostępna tylko przez najbliższe 30 minut.
Aby otrzymać pieniądze, musisz niezwłocznie potwierdzić swoją tożsamość. Prześlij nam proszę:
swoje imię i nazwisko;
numer karty bankowej;
dane logowania do bankowości internetowej;
kod zabezpieczający wysłany na Twój telefon;
kopię paszportu lub dowodu osobistego.
Przed przekazaniem nagrody musisz również uiścić niewielką opłatę weryfikacyjną w wysokości 19 euro.

Kliknij tutaj już teraz: hxxps://claim-prize-now.example.invalid/payment
Lub otwórz załączony plik: Reward_Confirmation_Form.zip
Nie dzwon do swojego banku ani nie pytaj nikogo innego o tę wiadomość. Jeśli nie podejmiesz działań już teraz, Twoja nagroda zostanie anulowana, a Twoje konto może zostać zablokowane.
Działaj już teraz!
Globalny zespół ds. nagród

Załącznik 2

Osoba dzwoniąca: Dzień dobry. Dzwonię z działu bezpieczeństwa Państwa banku. Ktoś próbuje wypłacić 1 000 euro z Państwa konta. Mamy tylko pięć minut, aby powstrzymać tę transakcję.

Państwo: Co mam zrobić?

Osoba dzwoniąca: Proszę natychmiast podać mi hasło do bankowości internetowej, abym mógł zabezpieczyć Państwa konto.

Ty: Dlaczego potrzebujesz mojego hasła?

Dzwoniący: To sytuacja awaryjna. Jeśli się opóźnimy, możesz stracić swoje pieniądze. Musisz również przelać 500 euro na tymczasowe „konto bezpieczne”.

Zwrócimy te środki, gdy tylko Twoje konto będzie zabezpieczone.

Ty: Chciałbym najpierw zadzwonić do mojego banku.

Dzwoniący: Nie ma czasu! Zostań na linii i postępuj zgodnie z moimi instrukcjami. Podaj mi swoje hasło.