Konspekt # 4

Poziom 7 klasy szkoły podstawowej

Temat - Rozpoznawanie phishingu, oszustw i socjotechniki w Internecie

Włączenie do przedmiotów szkolnych – Informatyka, Edukacja dla bezpieczeństwa

Grupa docelowa	Szkoła podstawowa Klasa 7
Liczba uczniów	Minimalna liczba uczniów: 10 Maksymalna liczba uczniów: 30
Przygotowanie do lekcji	Przygotowanie przykładów wiadomości phishingowych (e-mail, SMS, komunikatory). Przygotowanie przykładów bezpiecznych i niebezpiecznych stron internetowych. Przygotowanie zasobów technicznych, w tym projektora, laptopów albo tabletów z dostępem do Internetu.
Cele nauczania na podstawie programu nauczania DataPro	**A. Jak chronić swoje dane (i zaufanie do informacji)?** **A.1 Zarządzanie tożsamością:** Nauka tworzenia silnych i unikalnych haseł. Rozwijanie świadomości dotyczącej ochrony danych logowania i danych osobowych. Zrozumienie znaczenia uwierzytelniania dwuskładnikowego. **A.2 Ochrona własna:** Rozpoznawanie niebezpiecznych wiadomości e-mail, SMS-ów i linków. Poznanie podstawowych zasad bezpiecznego korzystania z Internetu. Nauka korzystania z filtrów bezpieczeństwa i aktualizacji systemów. **A.3 Przeciwko dezinformacji:** Rozwijanie umiejętności krytycznej oceny informacji znalezionych w Internecie. Rozpoznawanie prób manipulacji i fałszywych komunikatów.

	A.4 Sprawdzanie informacji: Nauka sprawdzania wiarygodności źródeł. Umiejętność porównywania informacji z kilku źródeł. **A.5 Ochrona innych:** Zrozumienie konsekwencji udostępniania danych innych osób. Rozwijanie odpowiedzialnych zachowań online. **A.7 Przeciwko oszustwu:** Poznanie metod stosowanych przez cyberprzestępców. Rozpoznawanie phishingu, fałszywych konkursów i prób wyłudzania danych. Nauka reagowania na podejrzane sytuacje w sieci. **B. Co sprawia, że ochrona danych jest prawem człowieka?** **B.1 Prywatność to wolność:** Zrozumienie, że ochrona prywatności pozwala użytkownikom bezpiecznie korzystać z Internetu. Rozwijanie świadomości zagrożeń wynikających z utraty kontroli nad swoimi danymi. **B.3 Siła prywatności:** Poznanie praw użytkowników związanych z ochroną danych. Rozwijanie umiejętności świadomego wyrażania zgody na przetwarzanie danych. **C. Co sprawia, że dane są wartościowe (ekonomicznie)?** **Zachowanie jako identyfikator:** Zrozumienie, że aktywność online może być wykorzystywana do profilowania użytkowników. Nauka ograniczania śledzenia aktywności w Internecie. **Przeciwko kontrolowaniu zachowań:** Rozpoznawanie technik manipulacyjnych stosowanych w reklamach i mediach społecznościowych. Rozwijanie krytycznego myślenia wobec treści internetowych.
Inne efekty uczenia się, jeśli dotyczy	Rozwój kompetencji cyfrowych.

	Rozwijanie umiejętności pracy zespołowej. Doskonalenie umiejętności analitycznych i krytycznego myślenia. Rozwijanie odpowiedzialności za własne działania online.
Czas trwania lekcji z uwzględnieniem czasu na zadanie domowe	Konspekt na 2 lekcje szkolne po 45 minut. Łącznie 90 minut lekcji. Praca nad zadaniem domowym zajmie około 30 minut.
Wymagania techniczne/Pomoce	Laptopy lub tablety z dostępem do Internetu. Projektor. Materiały z przykładami wiadomości phishingowych. Karty pracy dla uczniów.
Zasoby DataPro, które można wykorzystać do lekcji	Znajdź phishing - InstaPik - aktywność w Interacty Znajdź phishing - Bank Czeski - aktywność w Interacty
Dodatkowe zasoby edukacyjne	Filmy edukacyjne (np. z YouTube) na temat ochrony danych i prywatności w sieci: Twoje dane – Twoja sprawa | Jak chronić prywatność w sieci i poza nią | UODO Zasady bezpiecznego korzystania z Internetu: Szanuj innych w sieci (Sieciaki.pl) Inne: Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y? - gov.pl
Propozycje metodologii lub sposobu przeprowadzenia lekcji	Propozycja 1 Dyskusja wprowadzająca: jakie zagrożenia mogą spotkać użytkowników Internetu? Nauczyciel prezentuje przykłady wiadomości phishingowych oraz fałszywych stron internetowych. Uczniowie w parach analizują przykłady i wskazują elementy świadczące o oszustwie. Omówienie wyników i stworzenie wspólnej listy zasad bezpiecznego zachowania online.

	Propozycja 2 Krótkie przypomnienie zasad bezpieczeństwa online. Ćwiczenie praktyczne: uczniowie otrzymują scenariusze sytuacji online i decydują, jak powinni zareagować. Dyskusja: dlaczego cyberprzestępcy stosują manipulację i jakie emocje próbują wywołać? Nauczyciel przedstawia sposoby zgłaszania oszustw internetowych i reagowania na incydenty. Propozycja 3 Praca projektowa w grupach: stworzenie plakatu lub infografiki „Jak nie dać się oszukać w Internecie?”. Prezentacja projektów przez uczniów. Podsumowanie najważniejszych zasad bezpieczeństwa. Zadanie domowe Uczniowie przygotowują krótką listę zasad bezpiecznego korzystania z Internetu dla młodszych uczniów lub członków rodziny.

Sylabus DataPro Polska/CWEP

Druga paczka pracy

Kontakt	Joanna Bać
Instytucja	CWEP
E-Mail	joanna.bac@cwep.eu
Telefon	+48 17 853 66 72

Projekt	DataPro
Poziom rozpowszechniania	Publiczny
Data utworzenia	Grudzień 2024-Luty 2025
Autor	Joanna Bać

Co-funded by the European Union

Disclaimer
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.