Konspekt # 6

Poziom 8 klasy szkoły podstawowej

Temat - Zrozumienie polityk prywatności i uprawnień aplikacji

Włączenie do przedmiotów szkolnych – Informatyka, Podstawy przedsiębiorczości, Wiedza o społeczeństwie

Grupa docelowa	Szkoła podstawowa Klasa 8
Liczba uczniów	Minimalna liczba uczniów: 10 Maksymalna liczba uczniów: 30
Przygotowanie do lekcji	Przygotowanie przykładów polityk prywatności popularnych aplikacji i platform społecznościowych. Przygotowanie przykładów komunikatów dotyczących zgody na pliki cookies i uprawnień aplikacji. Przygotowanie przykładów aplikacji wymagających różnych poziomów dostępu do danych użytkownika. Przygotowanie zasobów technicznych, w tym projektora, laptopów albo tabletów z dostępem do Internetu.
Cele nauczania na podstawie programu nauczania DataPro	**Jak chronić swoje dane (i zaufanie do informacji)?** **A.1 Zarządzanie tożsamością:** Rozwijanie świadomości dotyczącej danych udostępnianych aplikacjom i serwisom internetowym. Nauka bezpiecznego zarządzania kontami użytkownika oraz ustawieniami prywatności. Rozumienie znaczenia silnych haseł i uwierzytelniania wieloskładnikowego. **A.2 Ochrona własna:** Nauka identyfikowania nadmiernych uprawnień aplikacji. Rozwijanie umiejętności ograniczania dostępu aplikacji do danych użytkownika. Zrozumienie zagrożeń wynikających z nieświadomego udostępniania danych. **A.4 Sprawdzanie informacji:**

	Rozwijanie umiejętności analizy polityk prywatności i regulaminów usług. Nauka wyszukiwania najważniejszych informacji dotyczących przetwarzania danych. **A.6 Minimalizacja danych:** Nauka ograniczania ilości udostępnianych danych osobowych. Rozwijanie nawyku świadomego udzielania zgód na przetwarzanie danych. Rozpoznawanie sytuacji, w których aplikacje żądają zbędnych uprawnień. **B. Co sprawia, że ochrona danych jest prawem człowieka?** **B.2 Prywatność – Samostanowienie:** Zrozumienie prawa użytkownika do kontrolowania własnych danych osobowych. Rozwijanie świadomości dotyczącej wpływu technologii cyfrowych na prywatność. **B.3 Siła prywatności:** Poznanie podstawowych praw użytkowników wynikających z ochrony danych osobowych. Nauka korzystania z prawa dostępu do danych, poprawiania ich i usuwania. Rozwijanie umiejętności świadomego wyrażania zgody na przetwarzanie danych. **B.7 Polityka prywatności:** Nauka krytycznej analizy polityk prywatności aplikacji i usług cyfrowych. Rozumienie pojęć takich jak: dane osobowe, profilowanie, cookies, zgoda użytkownika. Rozwijanie umiejętności oceny, czy aplikacja przetwarza dane w sposób odpowiedzialny. **C. Co sprawia, że dane są wartościowe (ekonomicznie)?** **Zarabianie na danych:** Zrozumienie, że wiele bezpłatnych aplikacji i usług internetowych zarabia dzięki danym użytkowników.

	Poznanie podstaw reklamy internetowej i profilowania użytkowników. **Zachowanie jako identyfikator:** Rozpoznawanie sposobów śledzenia aktywności użytkowników online. Nauka ograniczania śledzenia poprzez ustawienia prywatności i zarządzanie zgodami. **Sprzedaż danych:** Rozwijanie świadomości dotyczącej ekonomicznej wartości danych osobowych. Zrozumienie, w jaki sposób firmy wykorzystują dane użytkowników do personalizacji usług i reklam.
Inne efekty uczenia się, jeśli dotyczy	Rozwój kompetencji cyfrowych. Rozwijanie krytycznego myślenia. Rozwijanie świadomości prawnej i obywatelskiej. Doskonalenie umiejętności pracy zespołowej. Rozwijanie odpowiedzialnych postaw wobec korzystania z technologii cyfrowych.
Czas trwania lekcji z uwzględnieniem czasu na zadanie domowe	Konspekt na 2–3 lekcje szkolne po 45 minut. Łącznie od 90 do 135 minut lekcji. Praca nad zadaniem projektowym zajmie około 45 minut.
Wymagania techniczne/Pomoce	Laptopy lub tablety z dostępem do Internetu. Projektor. Przykładowe polityki prywatności aplikacji. Karty pracy dotyczące analizy uprawnień aplikacji. Dostęp do ustawień prywatności wybranych aplikacji lub urządzeń.
Zasoby DataPro, które można wykorzystać do lekcji	Jak firmy wykorzystują dane i jak je odpowiednio chronić - Kahoot Prywatność jako prawo człowieka - Kahoot
Dodatkowe zasoby edukacyjne	Cyberprzezorny - uprawnienia aplikacji a zagrożenia Why Do Apps Ask for Permission? | Fun Tech Lesson for Kids

Propozycje metodologii lub sposobu przeprowadzenia lekcji	Propozycja 1 Dyskusja wprowadzająca: jakie dane aplikacje zbierają o użytkownikach? Nauczyciel prezentuje przykłady komunikatów cookies oraz próśb o dostęp do lokalizacji, mikrofonu lub kontaktów. Uczniowie analizują, które zgody są niezbędne, a które mogą być nadmiarowe. Omówienie pojęć: dane osobowe, polityka prywatności, zgoda użytkownika, profilowanie. Propozycja 2 Praca w grupach: analiza polityki prywatności wybranej aplikacji lub serwisu internetowego. Uczniowie wyszukują informacje dotyczące: • jakie dane są zbierane, • komu mogą być udostępniane, • jak długo są przechowywane, • jakie prawa posiada użytkownik. Prezentacja wyników przez grupy. Dyskusja: czy użytkownicy świadomie akceptują warunki korzystania z aplikacji? Propozycja 3 Ćwiczenie praktyczne: uczniowie sprawdzają ustawienia prywatności na swoich urządzeniach lub w wybranych aplikacjach. Uczniowie identyfikują aplikacje posiadające szerokie uprawnienia i proponują sposoby ograniczenia dostępu do danych. Zadanie projektowe: przygotowanie plakatu lub prezentacji „Jak świadomie chronić swoje dane?”. Podsumowanie najważniejszych zasad bezpiecznego korzystania z aplikacji i usług cyfrowych. Zadanie domowe

	Uczniowie wybierają jedną aplikację używaną na co dzień i przygotowują krótką analizę jej polityki prywatności oraz listę uprawnień, do których aplikacja ma dostęp.

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.