



Konspekt # 2

Poziom 6 klasy szkoły podstawowej

Temat - Bezpieczeństwo w sieci: Jak chronić siebie i pomagać innym?

Włączenie do przedmiotów szkolnych – Informatyka, Edukacja dla bezpieczeństwa, Wiedza o społeczeństwie

Grupa docelowa	Szkoła podstawowa Klasa 6
Liczba uczniów	Minimalna liczba uczniów: 10 Maksymalna liczba uczniów: 30
Przygotowanie do lekcji	Dostęp do projektora oraz komputera z Internetem. Zapoznanie się z proponowanymi zasobami edukacyjnymi. Research w zakresie dostępnych polityk prywatności, uproszczone treściowo dla uczniów szkoły podstawowej.
Cele nauczania na podstawie programu nauczania DataPro	A. Jak chronić swoje dane (i zaufanie do informacji)? A.2 Ochrona własna: Nauka stosowania narzędzi do ochrony komunikacji (filtry antyspamowe, ustawienia poczty e-mail). Wprowadzenie zasad bezpieczeństwa, takich jak różne hasła do różnych serwisów, aktualizacje oprogramowania. A.5 Ochrona innych: Zrozumienie konsekwencji udostępniania danych innych osób bez ich zgody. Nauka odpowiedzialnego korzystania z platform społecznościowych i dzielenia się treściami. B. Co sprawia, że ochrona danych jest prawem człowieka? B.4 Poszanowanie praw człowieka: Świadomość, że ochrona prywatności w Internecie jest częścią godności człowieka i jego praw. Nauka cyfrowej odpowiedzialności wobec innych użytkowników. B.7 Polityka prywatności: Proste wprowadzenie do czytania polityk prywatności i zrozumienia, jakie dane są gromadzone przez aplikacje i serwisy.

	C. Co sprawia, że dane są wartościowe (ekonomicznie)? Sprzedaż danych: Wyjaśnienie, w jaki sposób dane uczniów mogą być wykorzystywane w celach reklamowych lub komercyjnych. Nauka o zagrożeniach związanych z udostępnianiem zbyt dużej ilości danych w sieci.
Inne efekty uczenia się, jeśli dotyczy	Rozwój umiejętności krytycznego myślenia i rozwiązywania problemów. Rozwój kreatywności u uczniów poprzez aktywności przygotowania plakatu.
Czas trwania lekcji z uwzględnieniem czasu na zadanie domowe	Konspekt na 3 lekcje szkolne po 45 minut. Łącznie 135 minut lekcji. Dodatkowy czas na zadania domowe w ramach pierwszej i drugiej propozycji metodologii, po 45 minut.
Wymagania techniczne/Pomoce	Laptopy lub komputer z dostępem do Internetu. Projektor. Smartfony.
Zasoby DataPro, które można wykorzystać do lekcji	Program nauczania dotyczący ochrony danych. Asystent DataPro (Chatbot). Edytowalny link do szablonu plakatu „Bezpieczeństwo online” w Canvie
Dodatkowe zasoby edukacyjne	Quizy online: Nt. hejtu ; Nt. phishingu Przykłady polityk prywatności, uproszczone treściowo dla uczniów szkoły podstawowej (nauczyciel robi własny research przygotowując się do lekcji.). Materiały wideo: Asy Internetu - Bezpieczeństwo dzieci w Internecie (kanał Smart Kids Planet) Kreskówki nt. zasad bezpieczeństwa w sieci (Sieciaki.pl) Film edukacyjny dla dzieci Rety rety internety, surfuj bezpiecznie w sieci Phishing, czyli kłopoty to nasza specjalność

Propozycja metodologii lub sposobu przeprowadzenia lekcji	Propozycja 1 1. Wprowadzenie: „<i>Kim jestem w Internecie?</i>” – krótka rozmowa o tym, jakie dane uczniowie udostępniają w sieci (np. imię, zdjęcia, lokalizację). Nauczyciel może posłużyć się kreskówkami audiowizualnymi nt. zasad bezpieczeństwa w sieci. 2. Ćwiczenie grupowe ze scenariuszami/pytaniem w oparciu o materiał wideo „<i>Bezpieczeństwo dzieci w Internecie</i>” – uczniowie analizując poszczególne sytuacje z materiału wideo (np. odpowiadanie na wiadomości od nieznajomych), odpowiadają na pytania. Nauczyciel zatrzymuje film w odpowiednich momentach, aby umożliwić uczniom swobodną wypowiedź. 2. Ćwiczenie w formie warsztatu (praca w parach lub w trójkach). Nauczyciel wyświetla dalszą część filmu nt. tworzenia silnych haseł online. Uczniowie mają za zadanie utworzenie silnych haseł. Przedstawiciel grupy zapisuje proponowane hasło na tablicy. Uczniowie głosują za wyborem najsilniejszego hasła. 3. Podsumowanie oraz zadanie domowe. Zadanie domowe: Przygotowanie plakatu promującego bezpieczeństwo online i przestrzeganie praw innych w sieci. Propozycja 2 1. Wprowadzenie o zagrożeniach w sieci. Nauczyciel może do tego celu posłużyć się materiałami wideo podanymi w sekcji dodatkowe zasoby edukacyjne. 2. Ćwiczenie: „<i>Rozpoznaj zagrożenie</i>” – uczniowie mają za zadanie rozpoznać rodzaj ataku w następującej sytuacji: <i>Julia otrzymała e-mail z informacją, że jej konto bankowe zostało naruszone, a ona musi natychmiast zmienić hasło. W e-mailu znajduje się link do fałszywej strony banku.</i> Nauczyciel podaje rozwiązanie i następuje dyskusja o tym czym jest phishing: <i>Phishing – Próba wyłudzenia danych logowania do konta bankowego przez podszywanie się pod zaufaną instytucję.</i> 3. Podsumowanie od nauczyciela o sposobach obrony przed phishingiem: <i>Nie klikać w linki w podejrzanych e-mailach. Zawsze logować się bezpośrednio przez oficjalną stronę banku, wpisując jej adres ręcznie</i>



	<i>w przeglądarce. Zainstalować program antywirusowy z funkcją ochrony przed phishingiem.</i> 4. Zadanie domowe za aktywność/dla chętnych. Zadanie domowe: Przygotowanie plakatu o potencjalnych niebezpieczeństwach w sieci. Propozycja 3 1. Moje pytania do chatbota nt. bezpieczeństwa w sieci, mojej i kolegów/koleżanek. Uczniowie korzystają z Asystenta DataPro (Chatbota). 2. Podsumowanie odpowiedzi chatbota na forum klasy. 3. Mini wykład: Polityki prywatności w praktyce. Wyjaśnienie, w jaki sposób dane uczniów mogą być wykorzystywane w celach reklamowych lub komercyjnych.
--	---



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.