3.0
CYBERLEKCJE

Scenariusz lekcji

Czy na pewno chronisz swoje dane w Internecie?

Zajęcia dla klas 4–6

NASK
cyber profilaktyka NASK
Ministerstwo Cyfryzacji
Projekt finansowany ze środków Ministerstwa Cyfryzacji.

1

Scenariusz lekcji dla klasy 4–6 szkół podstawowych

Scenariusz opracowany w ramach projektu „Działania wspierające nauczanie o cyberbezpieczeństwie"

Autorka scenariusza: Bernardetta Czerkawska

Redakcja merytoryczna: Cyberprofilaktyka NASK (Dział Profilaktyki Cyberzagrożeń)

Redakcja językowa, dostępność (WCAG):

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

KLASY 4–6

Temat: Czy na pewno chronisz swoje dane w Internecie?

Czas realizacji: 45 minut

Warto wiedzieć – wprowadzenie do zajęć

W wieku 10–12 lat dzieci najczęściej posiadają stały dostęp do urządzenia z dostępem do internetu, takiego jak smartfon. W tym czasie intensywnie eksplorują jego możliwości, grają w gry i poznają media społecznościowe (pomimo że zgodnie z regulaminami sieci społecznościowe powinny być wykorzystywane dopiero od 13. roku życia). Radość z poznawania nowego medium i satysfakcja z nawiązywania kontaktów są dla dzieci bardzo ważne, nie zdają sobie one jednak sprawy z ryzyka związanego z podawaniem wrażliwych informacji na swój temat w internecie.

Dorośli nierzadko nie zdają sobie sprawy z możliwości oferowanych przez te aplikacje i z tego, jak łatwo jest dziecku opublikować dowolne treści tekstowe, zdjęcia, a nawet filmy. W czasie, gdy sami uczęszczali do szkoły, internet wyglądał inaczej. Teraz muszą nadrabiać zaległości, aby zrozumieć wyzwania, przed jakim postawione jest ich potomstwo. Rolą nauczycieli i nauczycielek powinno być przekazywanie uczniom i uczennicom wiedzy na temat tych wyzwań oraz pokazywanie i utrwalanie dobrych wzorców zachowania, a także wspieranie rodziców w ochronie dzieci online.

Bardzo ważne jest, aby szkoła i dom w spójny sposób zapewniały ochronę prywatności dzieci – jeśli w jednym z tych miejsc nie są egzekwowane prawidłowe zasady ochrony informacji, będzie to działało na szkodę bezpieczeństwa młodej osoby. Widząc odmienne wzorce i normy zachowań, wybierze ona te wygodniejsze dla siebie. W efekcie będzie bardziej narażona na personalizowane reklamy, dostęp do nieodpowiednich treści, a nawet cyberprzemoc.

Brak odpowiedniej edukacji w zakresie prywatności prowadzi do pozostawiania wielu „cyfrowych śladów", które z czasem mogą być wykorzystane przeciwko użytkownikom. Internet stał się uniwersalnym medium wykorzystywanym powszechnie do kontaktu, odnajdowania informacji, w celach rozrywkowych oraz do pracy. Dobre praktyki zachowania się online (bez ujawniania swoich wrażliwych danych) są podstawą prawidłowego rozwoju człowieka w kontakcie z technologią.

Ten scenariusz kładzie nacisk na uświadomienie sobie, co wchodzi w skład cyfrowego śladu, w jaki sposób kształtują go wybory użytkowników, jakie ryzyko wiąże się z brakiem dbałości o pilnowanie go. Uczy, że treści raz umieszczone w internecie przestają być pod kontrolą udostępniającego i mogą pozostać tam na zawsze. Mogą także zostać wykorzystane przez osoby trzecie w celu wyrządzenia szkód – oszuści potrafią skutecznie polować na takie dane i używają ich z premedytacją, aby przykuć uwagę ofiar, zredukować ich nieufność i wykorzystać ich przyzwyczajenia oraz słabości.

Każda informacja pozwalająca na osobistą identyfikację powinna być udostępniana jedynie osobom zasługującym na pełne zaufanie. Informacje takie jak adres e-mail, miejsce zamieszkania, data urodzenia czy osobiste preferencje nie powinny być publicznie rozpowszechniane. Właściwe decyzje i wybory w kwestii

ograniczenia ich widoczności stanowią zabezpieczenie przed przykrymi konsekwencjami w przyszłości.

Cele szczegółowe:

Uczeń/uczennica:

- wymienia dane osobowe i rozumie, dlaczego należy je chronić;
- identyfikuje cyfrowe ślady i ryzyka z nimi związane;
- rozumie zasadę działania i skutki wyboru różnych poziomów ustawień prywatności w popularnych aplikacjach.

Kompetencje kluczowe

- kompetencje w zakresie rozumienia i tworzenia informacji,
- kompetencje cyfrowe,
- kompetencje osobiste, społeczne i w zakresie uczenia się.

Cele w języku ucznia/uczennicy:

1. Poszerzę moją wiedzę na temat dbania o prywatność w Internecie.
2. Dowiem się, w jaki sposób mogę chronić dane moje i znajomych w Internecie.

Kryteria sukcesu dla ucznia/uczennicy:

1. Potrafię wyjaśnić, dlaczego należy chronić dane osobowe w Internecie.
2. Potrafię podać dwa przykłady zasad ustawiania poziomu prywatności w aplikacjach i sposób ich działania.

Wskazówki do przeprowadzenia zajęć:

- Lekcja została oparta na zasadach **Problem Based Learning (PBL) – Uczenie się oparte na problemach**. Celem metody jest zaangażowanie uczniów i uczennic w rozwiązanie realistycznego, otwartego problemu, aby wzmacniać ich samodzielność i zdolność krytycznego myślenia. Młodzież w czasie lekcji odwołuje się do swoich doświadczeń, ale na potrzeby zajęć został opracowany materiał ze studium przypadku – przykładowymi postami ich rówieśniczki. Istotą lekcji jest rozmowa o ochronie prywatności w sieci, a nie analiza indywidualnych zachowań poszczególnych dzieci.
- Lekcja porusza bardzo ważny wątek. Aby maksymalnie podnieść świadomość uczniów i uczennic, warto w czasie lekcji inicjować jak najwięcej okazji do wymiany opinii. W czasie pracy grup nauczyciel/nauczycielka może, chodząc po grupach, dopytywać młodzież o uzasadnienie swoich wniosków.
- Finalna lista „Naszych złotych zasad bezpieczeństwa w interecie" może zostać spisana na plakacie lub grafice stworzonej w aplikacji canva.com i upowszechniona w społeczności szkolnej.

Metody/techniki pracy:

- pogadanka,
- PBL – uczenie się oparte na rozwiązywaniu problemu,
- dyskusja – w trójkach i na forum klasy.

Formy pracy:

- indywidualna,
- grupowa – praca w parach, trójkach i grupach.

Środki dydaktyczne:

- Załącznik nr 1 – cyfrowy ślad,
- Załącznik nr 2 – studium przypadku.

Pomoce dydaktyczne:

- flipchart lub szary papier,
- mazaki.

Opis przebiegu zajęć/lekcji

Wprowadzenie

1. Pogadanka – nauczyciel/nauczycielka zaprasza uczniów i uczennice do rozmowy o prywatności:
    - Co to jest?
    - Dlaczego jest dla nas ważna?
    - Jak ją chronimy w domu? (Np. zamykamy drzwi na klucz, wieczorem można zasłonić okna, sadzimy drzewa/ tuje na posesjach.)
    - Jak ją chronimy w szkole? (Nie czytamy na głos ocen, nie rozmawiamy o innych uczniach itp.)
    - Nauczyciel/nauczycielka może omówić kwestię bezpiecznych haseł – uczniowie powinni wiedzieć, że dobre hasło:
        - Nie jest wykorzystywane w różnych miejscach. Każda usługa i konto powinno mieć swoje unikalne hasło;
        - Jest długie – obecnie eksperci zalecają używanie przynajmniej 14 znaków;
        - Nie powinno składać się z łatwych do znalezienia fraz, np. być znanym cytatem;
        - Nie powinno zawierać danych osobowych, jak np. numer telefonu, data urodzin, imię ulubionego zwierzaka.

NASK cyber profilaktyka NASK Ministerstwo Cyfryzacji Projekt finansowany ze środków Ministerstwa Cyfryzacji.

- Warto przypomnieć uczniom i uczennicom, aby nie pozostawiali swoich urządzeń odblokowanych – każde powinno być chronione hasłem, pinem, a także, jeśli to możliwe, biometrią (odcisk palca lub rozpoznawanie twarzy). Smartfony przed odłożeniem zawsze wygaszamy (blokada ekranu)!

2. Wprowadzenie do tematu – nauczyciel/nauczycielka omawia cele lekcji i wprowadza pojęcie – „cyfrowy ślad". Rozdaje uczniom i uczennicom *Załącznik nr 1 – cyfrowy ślad* i prosi o chwilę refleksji:

   - W jakich sytuacjach nie zostawiam swojego cyfrowego śladu?
   - Kiedy go zostawiam?

Część główna

1. Praca w grupach – Wprowadzenie problemu

Nauczyciel/nauczycielka informuje uczniów i uczennice, że będą pracowali w grupach. Dostaną analizę przypadku – kilka postów swojej rówieśniczki, które zamieściła na swoim TikToku. Ich zadaniem będzie przeanalizowanie wpisów i zastanowienie się, czy koleżanka odpowiednio dba o swoją prywatność w internecie i czy zostawia ślady, a jeśli tak, to jakie i jak je zatrzeć.

Nauczyciel/nauczycielka łączy dzieci w czteroosobowe grupy i rozdaje *Załącznik nr 2 – studium przypadku*. Młodzież analizuje wpisy koleżanki i zapisuje propozycje rozwiązań.

Po upływie wyznaczonego czasu osoba prowadząca zajęcia zaprasza uczniów i uczennice do odczytania swoich notatek. Warto zachęcać kolejne grupy do prezentacji refleksji.

2. Praca w tych samych grupach – Synteza rozwiązań – zaproponowanie 3–4 zasad bezpieczeństwa

Nauczyciel/nauczycielka rozdaje flipcharty i mazaki i prosi uczniów oraz uczennice o zapisanie propozycji zasad. Następnie wiesza plakaty w widocznym miejscu lub rozkłada na podłodze.

Podsumowanie

1. Tworzenie listy „Naszych złotych zasad bezpieczeństwa w Internecie" – nauczyciel/nauczycielka prosi dzieci, by zastanowiły się, które z propozycji zasad zapisanych na wszystkich plakatach są dla nich osobiście najważniejsze. Następnie prosi każdą osobę o zagłosowanie na dwie zasady – pod uwagę bierzemy zapisy wszystkich grup. Uczniowie i uczennice głosują, rysując kropkę przy wybranej przez siebie zasadzie. Osoba prowadząca zajęcia zlicza głosy i odczytuje 3–4 zasady uznane przez klasę za najważniejsze.

2. Omówienie – nauczyciel/nauczycielka zaprasza uczniów i uczennice do dyskusji wokół pytań: co było dziś dla mnie najważniejsze, o jaką zasadę ja osobiście powinnam/powinienem zadbać.

Sposoby oceniania

Ocenie mogą podlegać:

- aktywność podczas lekcji,
- udział w pracach grupy.

Praca z uczniem ze zróżnicowanymi potrzebami edukacyjnymi:

Duża część lekcji ma formę pracy w grupach. Warto więc zadbać o uczniów lub uczennice z trudnościami w przemieszczaniu się i zaproponować im prace w takiej konfiguracji, żeby mieli swobodę przemieszczania się. Podobnie w przypadku osób z trudnościami społecznymi – warto dać im możliwość wyboru grupy, pracy w mniej licznym zespole lub indywidualnie.

W trakcie korzystania przez dzieci z materiałów, a zwłaszcza z załącznika nr 2, warto upewnić się, że jest on czytelny i zrozumiały dla każdego ucznia i uczennicy. W razie wątpliwości materiał można oczytać na głos w klasie. W przypadku dzieci z doświadczeniem migracyjnym, można również skorzystać z tłumacza wbudowanego w smartfon.