CYBER lekcje

Scenariusz lekcji

Prywatność w sieci

NASK
NASK akademia
KPRM
GOV.pl CYFRYZACJA

CYBER lekcje

Prywatność w sieci

Scenariusz lekcji dla szkól ponadpodstawowych

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

Autorka scenariusza: Agata Arkabus

Redakcja merytoryczna: Akademia NASK (Zespół Edukacji Cyfrowej), Zespół Budowania Świadomości Cyberbezpieczeństwa

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

CYBER lekcje

Spis treści

CYBER lekcje

Temat: **Prywatność w sieci**

Etap**: szkoła ponadpodstawowa**

Czas realizacji: **2 x 45 minut**

Warto wiedzieć – wprowadzenie do zajęć

Dbać o swoją prywatność trzeba zarówno w świecie realnym, jak i wirtualnym. Udostępnianie zbyt wielu informacji o sobie w internecie może być niebezpieczne: nasze dane mogą zostać wykradzione, a zdjęcia czy filmy – wykorzystane przeciwko nam. Na ten problem należy zwracać uwagę szczególnie młodym ludziom.

Uczniowie w internecie najczęściej korzystają z serwisów społecznościowych, co wiąże się z akceptacją regulaminów. Regulamin określa prawa i obowiązki użytkowników i administratora. Choć bywa długi i skomplikowany, warto się z nim zapoznać, aby w przyszłości uniknąć blokady konta przez nieświadome złamanie zawartych w nim postanowień. Tego typu przepisy rozszerzają i uzupełniają obowiązujące prawo, jednak nie zastępują go i mogą być dowolnie kształtowane, a także aktualizowane – pod warunkiem, że wszyscy użytkownicy otrzymają wcześniejsze powiadomienie o zmianach.

W sytuacji, w której ktoś bezprawnie wejdzie w posiadanie czyichś danych osobowych i wykorzysta je wbrew woli tej osoby, mówimy o kradzieży tożsamości. Każde podszywanie się pod kogoś innego (niezależnie, czy celem jest osiągnięcie korzyści majątkowej, zaliczenie sprawdzianu czy wyłącznie dowcip) jest karalne.

Przed analizą problemu prywatności w sieci warto zapoznać się z filmem „Prywatność: bezpieczne zarządzanie danymi".

Informacje na temat zajęć

Cele ogólne powiązane z podstawą programową

Informatyka

IV. Rozwijanie kompetencji społecznych, takich jak: **komunikacja i współpraca w grupie**, w tym w środowiskach wirtualnych, udział w projektach zespołowych oraz zarządzanie projektami.

V. Przestrzeganie prawa i zasad bezpieczeństwa. **Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego**, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych. Uczeń:

1) aktywnie uczestniczy w realizacji projektów informatycznych rozwiązujących problemy z różnych dziedzin, przyjmuje przy tym różne role w zespole realizującym projekt i **prezentuje efekty wspólnej pracy**;

2) podaje **przykłady wpływu informatyki i technologii komputerowej na najważniejsze sfery życia osobistego** i zawodowego;

4) **bezpiecznie buduje swój wizerunek w przestrzeni medialnej**;

Etyka

4. Etyka a nauka i technika. Uczeń:

1) **podaje przykłady właściwego i niewłaściwego wykorzystywania nowych technologii**, w szczególności technologii informatycznych;

2) **jest świadomy, że postęp cywilizacyjny dokonuje się dzięki wiedzy**; wyjaśnia, dlaczego wiedza jest dobrem (wartością);

3) identyfikuje i **analizuje wybrane problemy moralne związane z postępem naukowo-technicznym** (np. problem ochrony prywatności, ochrony praw autorskich, cyberprzemocy, rozwój sztucznej inteligencji, transhumanizm).

Cele szczegółowe powiązane z podstawą programową

Uczeń:

- zna pojęcie prywatności w sieci;
- jest świadomy zagrożeń wynikających z posiadania kont w portalach społecznościowych;
- zna sposoby chronienia prywatności w internecie;
- jest świadomy istnienia zalet i wad wykorzystania technologii informacyjno-komunikacyjnej w życiu codziennym.

Kompetencje kluczowe

- kompetencje w zakresie rozumienia i tworzenia informacji;
- kompetencje językowe;
- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie uczenia się;
- kompetencje w zakresie świadomości i ekspresji kulturalnej.

Metody/techniki pracy

- opis;
- rozmowa;

- dyskusja;
- metoda problemowa;
- metoda praktyczna.

Formy pracy

- indywidualna;
- grupowa.

Środki dydaktyczne:

- karta pracy „Prywatność";
- karta pracy „Pozytywne i negatywne skutki wykorzystania technologii w życiu codziennym";
- karta ewaluacji „Podsumowanie zajęć";
- białe i czerwone kartki w formacie A4;
- kolorowe samoprzylepne karteczki;
- film „Bezpieczni w sieci: prywatność w internecie – dlaczego warto o nią zadbać?";
- film „Prywatność: bezpieczne zarządzanie danymi";
- białe kartki z bloku technicznego w formacie A3;
- pisaki;
- kredki pastelowe.

Opis przebiegu zajęć/lekcji

Wprowadzenie

Nauczyciel rozdaje czerwone i białe kartki. Uczniowie, którzy posiadają choć jedno konto w serwisie społecznościowym (np. Facebook, Instagram), podnoszą białe kartki, a nieposiadający takich kont – czerwone. Najprawdopodobniej w górze nie będzie ani jednej czerwonej kartki. Jeśli znajdzie się osoba nieposiadająca konta w portalu społecznościowym, warto zapytać ją o powody tej decyzji.

Uczniowie posiadający konta w portalach społecznościowych odpowiadają w formie luźnej dyskusji na pytania nauczyciela:

- Czy znasz treść regulamin portalu społecznościowego, do którego należysz?
- Co daje ci posiadanie konta w mediach społecznościowych?
- Jak daleko pozwalasz innym wkraczać w swoją prywatność?
- Czy wszystkie informacje publikowane na twoim koncie są zgodne z prawdą?
- Co ryzykujesz takimi działaniami?
- Jakie prywatne informacje o tobie tam się znajdują?
- Czy jest to dla ciebie forma komunikacji z rówieśnikami, przyjaciółmi, rodziną?

Część główna

- Nauczyciel dzieli uczniów na grupy i rozdaje mi karty pracy „Prywatność". Zadaniem każdej z grup jest stworzenie mapy myśli dotyczącej prywatności. Uczniowie na kolorowych karteczkach zapisują swoje skojarzenia związane z tym pojęciem i przyklejają na karcie. Przykładowe skojarzenia: prywatność korespondencji, prywatność informacji o sobie, prywatność komunikacji, prywatność wizerunku, prywatność danych osobowych, prywatność cielesna. Po zakończonej pracy jedna osoba z grupy prezentuje propozycje na forum klasy.
- Nauczyciel prosi uczniów, aby podali przykłady łamania zasad prywatności – po jednym do każdej z wcześniej zaprezentowanych propozycji. Jak zagrożona jest prywatność w sieci? Przykładowe odpowiedzi:
  - prywatność korespondencji – czytanie listów, maili, SMS-ów nieprzeznaczonych dla nas;
  - prywatność informacji o sobie – rozpowszechnianie informacji o naszej sytuacji rodzinnej;
  - prywatność wizerunku – publikowanie zdjęcia kolegi na naszym koncie społecznościowym bez jego zgody;
  - prywatność danych osobowych – podanie imienia i nazwiska kolegi bez jego zgody;
  - prywatność cielesna – niezachowywanie odpowiedniego dystansu fizycznego.
- Następnie nauczyciel wyświetla film „Bezpieczni w sieci: prywatność w internecie – dlaczego warto o nią zadbać?". Właściciele kanału na YouTube Komputer Świat dyskutują w nim na temat prywatności w sieci. Zadają sobie pytania dotyczące bezpieczeństwa. Rozmawiają z ekspertami o tym, dlaczego warto dbać o ochronę swoich danych osobowych i swojego wizerunku w internecie.

  Poruszane w filmie tematy:
  - reklama, miejsce dla przestępców, informacje dla złodziei;
  - dane z dowodów osobistych (ktoś bierze kredyt, wykorzystując nasze dane osobowe);
  - podawanie loginu i hasła bankowego (włamanie na konta bankowe, korzystanie z kart kredytowych);
  - świadomość, że Facebook to nie tylko krąg naszych znajomych, ale miejsce działań dla przestępców – przydaje się dobry program antywirusowy i dwuskładnikowy system logowania;
  - ciasteczka – dokładne identyfikowanie osoby lub firm,
  - możliwość usunięcia identyfikacji wyszukiwania jest bardzo utrudniona.

- Po zapoznaniu się z materiałem filmowym nauczyciel prosi uczniów, aby wykorzystując rozdane na początku lekcji białe i czerwone kartki, zabrali głos w dyskusji „Czy jesteśmy w stanie ryzykować utratę prywatności w sieci dla naszej wygody?" (tak – biała kartka, nie – czerwona).
- Nauczyciel prowadzi dyskusję moderowaną, podczas której uczniowie podają przykłady wykorzystywania technologii informacyjno-komunikacyjnych, ułatwiających załatwianie wielu osobistych, codziennych spraw: komunikacja elektroniczna w kontaktach z urzędami, sklepami internetowymi czy spotkania towarzyskie i służbowe online. Sytuacje te, choć z jednej strony pozwalają na różne oszczędności, z drugiej – wymagają podawania danych osobowych, a więc zagrażają naszej prywatności.
- Na koniec dyskusji nauczyciel rozdaje uczniom kartę pracy „Pozytywne i negatywne skutki wykorzystania technologii w życiu codziennym". Uczniowie opracowują kartę pracy w grupach.
- Drugą część zajęć stanowi praca w grupach, polegająca na przygotowaniu plakatu „Prywatność w sieci". Do jego wykonania uczniowie wykorzystują kartki A3 bloku technicznego, pisaki oraz kredki pastelowe.

Podsumowanie

Jedna osoba z grupy omawia wykonane plakaty na forum klasy. Pozostali uczniowie oceniają plakaty i prezentację w skali 1 do 5, gdzie 1 to ocena najniższa, 5 – najwyższa. Uczniowie z najwyżej ocenionej grupy otrzymują w nagrodę oceny bardzo dobre.

Nauczyciel podsumowuje zajęcia konkluzją: Wskazane jest bezpieczne korzystanie z sieci i rozważne podawanie swoich danych w internecie. Mimo pozytywnej opinii dotyczącej wykorzystania technologii informacyjno-komunikacyjnych w naszym życiu musimy pamiętać o wszystkich możliwych zabezpieczeniach, które mamy do dyspozycji. Prywatność jest bardzo ważną wartością.

Na koniec uczniowie wykonują kartę ewaluacji „Podsumowanie zajęć".

Komentarz metodyczny

Uwagi do realizacji lekcji/zajęć

Wskazane jest odpowiednie ustawienie stolików do pracy grupowej, tak aby zapewnić uczniom wygodne uzupełnianie kart pracy oraz wykonanie plakatów.

Jeśli dysponujemy tabletami lub laptopami, plakaty można wykonać w ogólnodostępnej aplikacji typu Canva.

Sposoby oceniania

- aktywność podczas lekcji;
- odpowiedzi na pytania;
- zadania wykonywane podczas lekcji;
- ćwiczenia i zadania praktyczne;
- umiejętność prowadzenia dyskusji;
- wykonanie plakatu.

Praca z uczniem ze specjalnymi potrzebami edukacyjnymi (SPE)

Uczniowie zdolni mogą zostać liderami grup. Uczniowie ze specyficznymi trudnościami edukacyjnymi są aktywizowani do pracy i odpowiedzi poprzez dodatkowe, pomocnicze pytania.

CYBER lekcje

Karta ewaluacji „Podsumowanie zajęć”

Odpowiedz na pytania.

Czy zajęcia Ci się podobały?

……

……

……

……

Czy dowiedziałeś/dowiedziałaś się czegoś nowego?

……

……

……

……

Jak i kiedy wykorzystasz nowo nabytą wiedzę?

……

……

……

……

Czy jest jeszcze jakiś problem z zakresu ochrony prywatności, który Cię nurtuje?

……

……

……

……

CYBER lekcje

Karta pracy „Pozytywne i negatywne skutki wykorzystania technologii w życiu codziennym”

Uzupełnij.

Pozytywne skutki wykorzystywania technologii w życiu codziennym

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Negatywne skutki wykorzystywania technologii w życiu codziennym

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Prywatność”

Stwórz mapę myśli z hasłem PRYWATNOŚĆ. Dookoła pojęcia doklej karteczki z Twoimi skojarzeniami.

PRYWATNOŚĆ

CYBER lekcje

Bibliografia/Netografia

- „Bezpieczne korzystanie z mediów społecznościowych – baza wiedzy" [online, dostęp z dn. 29.12.2021].
- Grygiel I.W., (2018), „Mamo, Tato – nie czytaj tego! Szanuj moją prywatność!" [online, dostęp z dn. 29.12.2021].
- Krzyżanowski P., (2020), „9 prostych sposobów na zapewnienie sobie prywatności w internecie" [online, dostęp z dn. 29.12.2021].
- Lekcja „Prawo do prywatności w sieci" [online, dostęp z dn. 29.12.2021].
- Lekcja „Ochrona prywatności w sieci" [online, dostęp z dn. 29.12.2021].

Powyższy scenariusz opracowany został w ramach projektu „Działania wspierające nauczanie o cyberbezpieczeństwie".

Opis projektu

Projekt „Działania wspierające nauczanie o cyberbezpieczeństwie", zwany dalej „Cyberlekcje", jest współfinansowany ze środków budżetu państwa otrzymanych od Kancelarii Prezesa Rady Ministrów i wpisuje się w Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

Opracowane scenariusze „Cyberlekcji" wpisują się w obowiązki wynikające z podstawy programowej. Tematyka scenariuszy odpowiada rosnącemu zapotrzebowaniu na wiedzę i kompetencje z zakresu efektywnego wykorzystywania mediów cyfrowych, co jest konsekwencją rewolucji cyfrowej postępującej również w podstawowych dziedzinach życia społecznego.

Korzystanie z własnego telefonu komórkowego najczęściej rozpoczyna się w wieku 7–8 lat Ponad 80% uczniów posiada telefon komórkowy – w tym 64% dzieci w wieku 7–9 lat. Przeważająca większość dzieci używa telefonu typu smartfon, prawie wszystkie osoby w wieku szkolnym (97%) korzystają też z internetu. Podobnie jak w przypadku telefonu komórkowego podróże po wirtualnym świecie rozpoczynają się najczęściej w wieku 7–8 lat. Dwie trzecie rodziców deklaruje stosowanie kontroli nad korzystaniem przez dziecko z telefonu i internetu. Najczęściej jest to wspólne ustalenie zasad korzystania z telefonu, rzadziej – korzystanie z ustawień bezpieczeństwa czy specjalnych aplikacji służących do kontroli rodzicielskiej (39% rodziców). Aż 80% rodziców przyznaje, że ich dziecko samodzielnie instaluje aplikacje na telefon*. Warto podkreślić, że przed pandemią łączny, średni czas dobowy korzystania z sieci przez dzieci i młodzież (w wieku 13–17 lat) wynosił 4 godziny**. Obecnie sięga on 6, a nawet 8 godzin dziennie spędzonych na lekcjach zdalnych (44,3% respondentów) oraz do 4 godzin w czasie wolnym (31,7%)***.

Młodzi ludzie wykorzystują internet najczęściej w celu budowania oraz podtrzymywania relacji społecznych – znakomita większość jest aktywna na portalach społecznościowych oraz korzysta z komunikatorów i chatów. Poza poszukiwaniem informacji i rozwijaniem zainteresowań internet to dla młodych ludzi główne miejsce rozrywki – źródło gier i aplikacji, które wymagają wiedzy o bezpieczeństwie teleinformatycznym, w szczególności mając na względzie fakt znacznego nasilenia się cyberataków wykorzystujących socjotechniki oraz braki w zabezpieczeniach urządzeń domowych. Warto tutaj zaznaczyć, że zgodnie z raportem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z 2020 r. liczba incydentów phishingowych – czyli mających na celu wyłudzenie danych – wzrosła w ostatnich miesiącach nawet sześciokrotnie.

Tematyka projektu edukacyjnego obejmuje następujące obszary:

- bezpieczeństwo sieci i systemów;
- zarządzanie informacją;

- wizerunek i tożsamość online;
- prywatność – bezpieczne zarządzanie danymi personalnymi;
- zdrowie, dobrostan psychiczny i cyberhigiena.

W ramach projektu opracowanych zostanie łącznie 18 scenariuszy lekcyjnych dla poszczególnych grup wiekowych uczniów w podziale na:

- dwa scenariusze dla klas 1–3 szkoły podstawowej;
- dwa scenariusze dla klas 4–6 szkoły podstawowej;
- cztery scenariusze dla klas 7–8 szkoły podstawowej;
- dziewięć scenariuszy dla klas szkół ponadpodstawowych.

Wykorzystanie przez nauczycieli przygotowanych w ramach działania scenariuszy może wpłynąć na lepszą profilaktykę w zakresie najważniejszych wyzwań związanych z zagrożeniami w sieci, jakimi są: przeciwdziałanie cyberprzemocy, patostreamingowi, przygotowanie dzieci i młodzieży do właściwej ochrony prywatności online, zapobieganie uzależnieniu od internetu oraz ochrona przed cyberprzestępczością, w tym ryzykiem wykorzystania dziecka w celach seksualnych czy finansowych.

* Urząd Komunikacji Elektronicznej (2020), „Badanie ankietowe opinii publicznej w zakresie funkcjonowania rynku usług telekomunikacyjnych oraz oceny preferencji konsumentów. Raport z badania dzieci i rodziców" [online, dostęp z dn. 13.12.2021].

** Bochenek, M., Lange, R., (2019), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów", Warszawa: NASK – Państwowy Instytut Badawczy, s. 15 [online, dostęp z dn. 10.12.2021].

*** Lange R. (red.), (2021), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów", Warszawa: NASK – Państwowy Instytut Badawczy, s. 6 [online, dostęp z dn. 10.12.2021].