CYBER lekcje

Scenariusz lekcji

Zagrożenia w sieci

NASK

NASK akademia

KPRM

GOV.pl CYFRYZACJA

CYBER lekcje

Zagrożenia w sieci

Scenariusz lekcji dla szkół 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: **Zagrożenia w sieci**

Etap: **szkoła ponadpodstawowa**

Czas realizacji: **2 x 45 minut**

Warto wiedzieć – wprowadzenie do zajęć

Internet jest dla współczesnej młodzieży miejscem spotkań towarzyskich, rozrywki i nauki. Korzystanie z sieci niesie jednak za sobą również zagrożenia. Nastolatkom czasem trudno jest określić granice bezpieczeństwa. Wiążą się one również z zarządzaniem zasobami sieci, takimi jak muzyka czy zdjęcia. Młodzi ludzie nie zawsze wiedzą, jak korzystać z tych materiałów zgodnie z prawem.

Rolą nauczyciela jest wskazanie i uświadomienie młodemu człowiekowi ryzyka, z jakimi może się wiązać korzystanie z internetu. Warto ugruntować wiedzę z tego zakresu, zwracając szczególną uwagę na sposoby radzenia sobie z tymi zagrożeniami. Z pomocą przychodzą nam tutaj otwarte zasoby edukacyjne, możliwość zgłaszania nieodpowiednich zachowań administratorom, dbanie o prywatność kont internetowych czy też uważne czytanie regulaminów sklepów sieciowych.

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**.

IV. Rozwijanie kompetencji społecznych.

Zakres podstawowy. 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; korzysta z wybranych e-usług; przedstawia **wpływ technologii** na dobrobyt społeczeństw i **komunikację społeczną**;

CYBER lekcje

Etyka

4. Etyka a nauka i technika. Uczeń:

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

Cele szczegółowe powiązane z podstawą programową

Uczeń:

- zna zagrożenia związane z korzystaniem z internetu;
- wykorzystuje aplikacje komputerowe w celu poszerzania wiedzy;
- pełni rolę lidera w zespole;
- zna sposoby zapobiegania zagrożeniom internetowym.

Kompetencje kluczowe

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

Metody/techniki pracy

- prezentacja;
- dyskusja;
- metoda problemowa;
- metoda praktyczna;
- praca z komputerem, tabletem/smatfonem.

Formy pracy

- indywidualna;
- grupowa.

Środki dydaktyczne

- komputery z dostępem do internetu lub laptopy/tablety;
- karteczki samoprzylepne,
- prezentacja multimedialna „Zagrożenia w sieci",
- karta pracy „Jak dbać o bezpieczeństwo w sieci" (różne rodzaje) – przykłady kart pracy w załącznikach;
- infografika „Nielegalne i szkodliwe treści";
- aplikacje internetowe do tworzenia testów/quizów, np. Learning Apps, Kahoot, Quzzlet;

- karty do głosowania;
- smartfony.

Opis przebiegu zajęć/lekcji

Wprowadzenie

Nauczyciel rozdaje uczniom karteczki samoprzylepne. Prosi uczniów o napisanie na nich, z jakich treści/zasobów najczęściej korzystają w sieci. Następnie uczniowie przyklejają karteczki w wyznaczonym miejscu, np. na tablicy. Wybrani uczniowie grupują zapisane odpowiedzi, tworząc obszary treści czy zasobów, np. Rozwój zainteresowań; Edukacja i dokształcanie się; Celebryci i influencerzy itp. Nauczyciel podsumowuje udzielone przez uczniów odpowiedzi. Zwraca uwagę, że niektóre z tych treści mogą należeć do tzw. treści szkodliwych i niebezpiecznych.

Część główna

1. Nauczyciel dzieli uczniów na grupy. Zachęca ich, aby zastanowili się, czy w internecie można natknąć się na zagrożenia. Uczniowie na kartkach dokonują próby stworzenia definicji zagrożeń internetowych.
2. Nauczyciel omawia zagrożenia internetowe, korzystając z prezentacji multimedialnej o tej tematyce. Przykładowe zagadnienia:
    a. **Slajd 1. Cyberprzemoc**. Obecność młodzieży w sieci niesie za sobą ryzyko włamania się oszustów na konto (w celu kradzieży tożsamości i podszywania się) czy wzajemnego ośmieszania. Prześladowcami są zazwyczaj rówieśnicy. Rodzaje cyberprzemocy: cybermobbing, cyberbullying, trolling.
    b. **Slajd 2. Naruszanie praw autorskich**. Korzystanie z internetowych źródeł informacji jest powszechne. Młodzież na co dzień, np. przygotowując się do zajęć, korzysta z internetu. Nie zawsze uczniowie są świadomi łamania praw autorskich.
    c. **Slajd 3. Kradzież danych osobowych**. Dane osobowe bardzo często są udostępniane przez uczniów w portalach społecznościowych czy komunikatorach. Dane mogą być również podstępnie wyłudzane przez przestępców.
    d. **Slajd 4. Wyłudzenia finansowe**. Internet jest dla współczesnej młodzieży m.in. miejscem rozrywki i zabawy. Dla relaksu uczniowie często grają w multimedialne gry – darmowe lub świadomie zakupione. Może tak się jednak zdarzyć, że nastolatek padnie ofiarą wyłudzenia finansowego, np. w przypadku nieświadomości zakupu cyklicznego, kiedy opłata pobierana jest wielokrotnie zamiast jednorazowo.
    e. **Slajd 5. Niebezpieczne znajomości**. Korzystając z internetu, możemy spotkać się ze zjawiskiem groomingu, czyli uwodzeniem w sieci w celu nawiązania więzi emocjonalnej i późniejszego wykorzystania seksualnego.

f. **Slajd 6. Piractwo**. W ramach rozrywki uczniowie często słuchają muzyki czy oglądają filmy z internetu. Czasem materiały te zapisują na dysku komputera. Działanie to nie jest zgodne z prawem.
g. **Slajd 7. Sexting**. To forma komunikacji elektronicznej, w której przekazem jest seksualnie sugestywny obraz lub treść.
h. **Slajd 8. Uzależnienie od internetu**. Korzystając z internetu w domu, w szkole, podczas nauki i rozrywki, łatwo można się od niego uzależnić. Bardzo trudno zauważyć granicę bezpieczeństwa przy korzystaniu z sieci.
i. **Slajd 9. Phishing.** To metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.
j. **Slajd 10. Vishing**. Oszustwo polegające na wyłudzaniu danych (ang. phishing) w wersji głosowej, w trakcie rozmowy telefonicznej.
k. **Slajd 11. Smishing**. Rodzaj phishingu skierowanego na telefony komórkowe. Celem przestępcy jest zgromadzenie danych osobowych, takich jak np. numer ubezpieczenia społecznego lub numer karty kredytowej. Drogą ataku są wiadomości tekstowe lub SMS.

3. Po omówieniu zagadnień nauczyciel rozdaje uczniom karty pracy „Jak dbać o bezpieczeństwo w sieci". Każda grupa pracuje nad jednym przykładowym zagrożeniu: np. Cyberprzemoc; Naruszenie praw autorskich; Kradzież danych finansowych; Wyłudzenia finansowe; Niebezpieczne znajomości; Piractwo, Sexting; Uzależnienie od internetu.
   Propozycje odpowiedzi uczniów:
   a. Cyberprzemoc: brak reakcji na nękanie, zachowywanie dowodów, blokowanie nękającej osoby, zgłoszenie nieodpowiednich zachowań administratorowi strony, poinformowanie o przykrej sytuacji rodziców/nauczycieli.
   b. Naruszenie praw autorskich: świadomość istnienia praw autorskich, otwarte zasoby edukacyjne, licencje Creative Commons, ochrona wizerunku.
   c. Kradzież danych osobowych: dbanie o prywatność kont internetowych, nieujawnianie w internecie danych osobowych, zakładanie odpowiednich haseł dostępu.
   d. Wyłudzenia finansowe: uważne czytanie regulaminu zakupu, niepodawanie w sieci numerów kont bankowych, stosowanie zapór internetowych (ogniowych).
   e. Niebezpieczne znajomości: świadomość anonimowości osoby z kontaktu internetowego.
   f. Piractwo: słuchanie muzyki online, oglądanie filmów w streamingu, ponoszenie opłat.
   g. Sexting: niewysyłanie nagich zdjęć, niepublikowanie nagich zdjęć.
   h. Uzależnienie od internetu: ograniczanie czasu spędzanego przed komputerem, kontakty „na żywo" z rówieśnikami, rozwijanie zainteresowań niezwiązanych z internetem.

Po zakończonej pracy jeden uczeń z grupy omawia wykonane zadanie. Uczniowie z pozostałych grup ewentualnie uzupełniają odpowiedzi.

4. Nauczyciel prezentuje infografikę pokazującą zgłaszanie nielegalnych i szkodliwych treści – „Nielegalne i szkodliwe treści".

Podsumowanie

„Bezpieczny internet" – praca w grupach. Uczniowie w zespołach tworzą quiz/test zawierający pytania i odpowiedzi jednokrotnego wyboru, wykorzystując wiadomości nabyte podczas lekcji. Po wykonaniu zadania:

- Opcja 1. Lider grupy odczytuje pytanie wraz z odpowiedziami uczniom z innych grup. Uczniowie udzielają odpowiedzi słownie lub przez tzw. głosowanie – podnosząc kartę z odpowiedzią A, B, C, D.
- Opcja 2. Uczniowie tworzą quiz przy wykorzystaniu aplikacji typu Learning Apps, Kahoot lub Quzzlet. Po utworzeniu interaktywnego quizu udostępniają go nauczycielowi i innym uczniom.

Komentarz metodyczny

Uwagi do realizacji lekcji/zajęć

Warto zaplanować zajęcia w sali komputerowej lub wykorzystywać laptopy/tablety do tworzenia quizu dla lidera grupy. Jeśli nie mamy dostępu do urządzeń mobilnych, uczniowie test podsumowujący zajęcia mogą otrzymać w formie linku na skrzynki pocztowe i rozwiązać go w ramach zadania domowego.

Sposoby oceniania

- aktywność;
- udział w dyskusji;
- wykonanie kart pracy;
- umiejętność wykorzystania aplikacji internetowych;
- rozwiązanie testu interaktywnego.

Praca z uczniem ze specjalnymi potrzebami edukacyjnymi (SPE)

Uczniowie zdolni mogą przygotować na zajęcia prezentację dotyczącą zagrożeń internetowych, którą omówią we współpracy z nauczycielem.

Warto zaangażować uczniów zdolnych do przeprowadzenia instruktażu korzystania z aplikacji do tworzenia testów/quizów.

Uczniowie z SPE mogą pracować w parach z innymi uczniami podczas udzielania odpowiedzi na pytania testu.

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 1

Bazując na własnej wiedzy i doświadczeniach, utwórz definicję zagrożeń internetowych.

Zagrożenia internetowe to:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 2

Zaproponuj sposoby zapobiegania cyberprzemocy.

Możliwe sposoby zapobiegania cyberprzemocy:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 3

Zaproponuj sposoby zapobiegania naruszeniu praw autorskich

Możliwe sposoby zapobiegania naruszeniu praw autorskich:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 4

Zaproponuj sposoby zapobiegania kradzieży danych finansowych.

Możliwe sposoby zapobiegania kradzieży danych finansowych:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 5

Zaproponuj sposoby zapobiegania wyłudzeniom finansowym.

Możliwe sposoby zapobiegania wyłudzeniom finansowym:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 6

Zaproponuj sposoby zapobiegania niebezpiecznym znajomościom.

Możliwe sposoby zapobiegania niebezpiecznym znajomościom:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 7

Zaproponuj sposoby zapobiegania piractwu internetowemu.

Możliwe sposoby zapobiegania piractwu internetowemu:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

CYBER lekcje

Karta pracy „Jak dbać o bezpieczeństwo w sieci" cz. 8

Zaproponuj sposoby zapobiegania uzależnieniu od internetu.

Możliwe sposoby zapobiegania uzależnieniu od internetu:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Bibliografia/Netografia

- Borkowska A., (2019), „Cyberprzemoc włącz blokadę na nękanie", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 13.12.2021].
- Fundacja Dajemy Dzieciom Siłę, (2015), film „Seksting: rejestrowanie, wysyłanie, upublicznianie nagich zdjęć przez młodzież" [online, dostęp z dn. 13.12.2021].
- Infografika „Phishing"
- Minitest „Bezpieczny internet" – LearninApps [online, dostęp z dn. 13.12.2021].
- Zintegrowana Platforma Edukacyjna, „Bezpieczeństwo w sieci – rodzaje zagrożeń" [online, dostęp z dn. 22.12.2021].

CYBER lekcje

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].