CYBERLEKCJE 3.0

Scenariusz lekcji

Zagrożenia w sieci i prywatność w Internecie

NASK

cyber profilaktyka NASK

Ministerstwo Cyfryzacji

Zagrożenia w sieci i prywatność w Internecie

Scenariusz lekcji dla klas 4–6 szkół podstawowych

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

Autorka scenariusza: Agata Arkabus, Bernardetta Czerkawska

Redakcja merytoryczna: Cyberprofilaktyka NASK (Dział Profilaktyki Cyberzagrożeń), Dział Budowania Świadomości Cyberbezpieczeństwa

Redakcja językowa, dostępność (WCAG): Diana Kania, Marta Danowska

Warszawa 2023

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

Spis treści

Temat: **Zagrożenia w sieci i prywatność w Internecie**

Klasa: **4–6 szkoły podstawowej**

Czas realizacji: **2 x 45 minut (1 x 45 minut – przygotowanie do przeprowadzenia badania między zajęciami, 1 x 45 – wnioskowanie z badań).**

Warto wiedzieć – wprowadzenie do zajęć

W Internecie znajduje się wiele programów i aplikacji przeznaczonych dla dzieci i młodzieży. Zawierają one treści i zasoby dostosowane do wieku psychofizycznego dziecka, są odpowiednio oznaczone oraz umożliwiają sprawowanie kontroli rodzicielskiej. Niestety, w sieci dostępne są także programy oraz gry online, z których młodzi odbiorcy nie powinni korzystać. Zawierają one szkodliwe i niebezpieczne treści, takie jak: przemoc, agresywne zachowania czy treści pornograficzne, które mogą wyzwalać w dzieciach destruktywne emocje.

Innym zagrożeniem, które czyha na dzieci i młodzież w grach online lub na portalach społecznościowych, są możliwe kontakty z nieznanymi osobami – głównie internautami udzielającymi się w grupach społecznościowych, na czatach lub forach dyskusyjnych. Wśród nich mogą znaleźć się osoby używające niecenzuralnych i obraźliwych słów, podszywające się pod osoby, którymi w rzeczywistości nie są, bądź mające negatywne intencje związane z relacjami z dziećmi korzystającymi z tego typu sieci społecznościowych.

Co 12 polski nastolatek (7,8%) doświadczył kradzieży dóbr wirtualnych (np. cennych wirtualnych przedmiotów czy zgromadzonych w aplikacjach punktów), prawie co 10 został oszukany przy transakcjach online (8,7%), a niemal co 15 padł ofiarą ataku hakerskiego (6,7%).

Aplikacje, aktualizacje czy rozszerzenia do gier pobierane z niezaufanych źródeł mogą przekierować dziecko na strony zawierające nielegalne lub szkodliwe treści czy zainfekować urządzenie złośliwym oprogramowaniem. Podobny skutek może mieć instalowanie oferowanych przez innych graczy cheatów, czyli dodatków/kodów, które mają ułatwić grę bądź wymianę czy kupno-sprzedaż wirtualnych dóbr.
W grach również działają oszuści. Nierozważna transakcja może nie tylko kosztować gracza utratę unikatowego majątku, ale też skutkować przejęciem danych logowania do bankowości elektronicznej i realną kradzieżą.

Od kilku lat można zaobserwować szybko rosnącą liczbę ataków socjotechnicznych, które wykorzystują niewiedzę, nieuwagę lub rutynowe zachowanie użytkownika, aby nakłonić go do określonych działań narażających bezpieczeństwo urządzenia lub konta. Popularną formą oszustw internetowych jest phishing (połączenie ang. słów *password harvesting* oraz *fishing* – łowienie haseł).

Sprawcy starannie preparują „zachętę", którą może być np. strona internetowa, wiadomość e-mail lub zwykła wiadomość przesyłana przez komunikator internetowy. Specyficzną cechą techniki phishingu jest wywołanie wrażenia pośpiechu, konieczności podjęcia natychmiastowego działania, które z reguły sprowadza się do kliknięcia w proponowany link.

Uświadamiając młodych internautów, należy pamiętać o przekazywaniu im wartościowych treści dotyczących zachowywania bezpieczeństwa w sieci. Należą do nich m.in. metody tworzenia haseł, do których zaliczamy następujące zasady:

- długość hasła (minimum 8 znaków zawierających małe i wielkie litery, cyfry i znaki specjalne) – dobrą metodą na długie hasło jest wymyślenie całej frazy;
- używanie różnych haseł do różnych aplikacji;

- niezapisywanie haseł w przeglądarkach ani na kartkach;
- używanie sprawdzonych managerów haseł;
- niepodawanie haseł obcym osobom;
- stosowanie uwierzytelniania dwuskładnikowego.

Nauczenie młodych odbiorców tych istotnych zasad wpłynie korzystnie na ich bezpieczeństwo w sieci.

Kolejnym ważnym aspektem korzystania z zasobów Internetu jest znajomość zasad bezpieczeństwa stosowanych na urządzeniach, do których dzieci i młodzież mają dostęp. Najlepszą obroną przed działaniem złośliwego oprogramowania jest posiadanie na każdym urządzeniu aktualnego programu antywirusowego, które chroni system i wykrywa złośliwe pliki. Antywirusy to programy, których zadaniem jest analiza plików w momencie ich pojawienia się (pobranie/włożenie nośnika zewnętrznego) na komputerze lub przed uruchomieniem. Pliki są sprawdzane pod względem podobieństwa do znanego złośliwego oprogramowania. Należy jednak pamiętać, że programy antywirusowe nie gwarantują nam stuprocentowej ochrony – muszą posiadać informacje o konkretnym wariancie złośliwego oprogramowania, żeby móc go rozpoznać. Dodatkowo są one obarczone błędem fałszywego rozpoznania, czyli potrafią zakwalifikować bezpieczne pliki jako groźne. Nie jest to argument przeciwko stosowaniu antywirusów, ale należy mieć tego świadomość. Jest to niezbędna wiedza dla każdego internauty – zarówno młodego, jak i osoby dorosłej.

Rola rodziców oraz nauczycieli w zakresie edukowania na temat zagrożeń w sieci i prywatności w Internecie jest bardzo istotna. Szczególnie w młodym wieku, gdy dzieci są chłonne nowości, a wpływ rówieśników na ich zachowania jest bardzo duży, potrzebna jest opieka i nadzór ze strony osób dorosłych.

Informacje na temat zajęć

Cele ogólne powiązane z podstawą programową

Informatyka

IV. Rozwijanie kompetencji społecznych. Uczeń:

1. uczestniczy w zespołowym rozwiązaniu problemu, posługując się technologią taką jak: poczta elektroniczna, forum, wirtualne środowisko kształcenia, dedykowany portal edukacyjny.

V. Przestrzeganie prawa i zasad bezpieczeństwa. Uczeń:

3. wymienia zagrożenia związane z powszechnym dostępem do technologii oraz do informacji i opisuje metody wystrzegania się ich.

Etyka

II. Człowiek wobec innych ludzi. Uczeń:

3. okazuje szacunek innym osobom;

17. wyjaśnia, na czym polega zasada fair play.

V. Człowiek a świat ludzkich wytworów. Uczeń:

6. podaje przykłady właściwego i niewłaściwego wykorzystywania nowoczesnych technologii informacyjnych.

Godziny wychowawcze

Tematyka może wynikać z obowiązującego w szkole Programu Wychowawczo-Profilaktycznego. Zawsze zakłada on wsparcie uczniów i uczennic w rozwoju kompetencji społecznych i umożliwieniu bezpiecznego korzystania z sieci.

Cele szczegółowe powiązane z podstawą programową

Uczeń:

- zna zasady bezpiecznego korzystania z gier online;
- potrafi chronić swoją prywatność w Internecie;
- zna zagrożenia związane z nadmiernym korzystaniem z gier cyfrowych;
- zna zalety gier online.

Kompetencje kluczowe

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

Cele zajęć w języku ucznia:

1. Dowiem się, jakie są bezpieczne zasady korzystania z gier komputerowych.

2. Przeprowadzę badanie ankietowe na temat korzystania przez uczniów z gier komputerowych, a wnioski zaprezentuję w czasie dyskusji w klasie.

Kryteria sukcesu dla ucznia/uczennicy:

1. Potrafię wyjaśnić cztery zasady bezpiecznego korzystania z gier komputerowych.

2. Umiem wyjaśnić dwa powody, dlaczego gry na komputerze/smartfonie lub innym urządzeniu mogą uzależniać.

3. Potrafię podać dwa wnioski z przeprowadzonych przeze mnie badań ankietowych.

4. W czasie dyskusji na temat zalet i szkodliwości gier komputerowych potrafię uzasadnić i zaprezentować swoją opinię w oparciu o wniosek z badań.

Wskazówki do przeprowadzenia zajęć:

- zajęcia są pretekstem do zaproszenia uczniów do bycia badaczami w swojej społeczności szkolnej, do przeprowadzenia badań i wyciągania wniosków;
- ROZSZERZENIE:
  - uzyskane wyniki można zaprezentować w szkole, wykorzystując np. prezentację w canva.com lub app.genial.ly;
  - na kolejnej lekcji można zaprosić uczniów do nakręcenia filmu/spotu społecznego dla pozostałych uczniów i uczennic na temat bezpiecznego korzystania z gier komputerowych. Punktem wyjścia mogą być hasła, które młodzież wypracowała na pierwszych zajęciach. Film można nakręcić smartfonem i poprosić uczniów o jego edycję.

Metody/techniki pracy

- zabawa dydaktyczna – test ruchowy;
- rozmowa;
- dyskusja – w trójkach i na forum klasy;
- metoda problemowa – planowanie i przeprowadzenie badania;
- praca z tekstem;
- praca z filmem.

Formy pracy

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

Środki dydaktyczne

- film „Uzależnienia Behawioralne – Gry";
- Co to są gry komputerowe? - Infografika;
- Zadania dla trójek – Karta pracy;
- Kwestionariusz badania ankietowego – Karta pracy;
- Dlaczego gry uzależniają.

Pomoce dydaktyczne

- kartki samoprzylepne;
- kartki A4;
- mazaki.

Przebieg zajęć pierwszych

Wprowadzenie

1. Nauczyciel zaprasza młodzież na lekcję. Pyta: Czy jest w klasie ktoś, kto nie wie, czym są gry na smartfonie, konsoli lub komputerze?
2. Nauczyciel rozdaje każdej osobie po 3 kartki samoprzylepne i prosi, by młodzież na każdej napisała nazwę gry, w którą lubi grać. Kartki przylepiają na tablicy, nauczyciel je kategoryzuje wg nazw gier. Która gra jest najbardziej lubiana w tej grupie? Która najmniej?
3. **Zabawa dydaktyczna** – test – nauczyciel prosi uczniów, aby wstali. Mówi: Zadam wam 10 pytań. Jeśli zgadzacie się z twierdzeniem – kucnijcie; jeśli nie – podskoczcie. I tak dziesięć razy. Przypatrujcie się sobie, potem będziemy wspólnie wyciągać wnioski.

   TAK – kucanie **NIE** – podskok

1) Gram w gry na smartfonie/konsoli lub innym urządzeniu.
2) Mam swoje konto na jednym z portali społecznościowych np. Facebook, Instagram, TikTok itp.
3) Kiedy się nudzę, gram.
4) Gry to moja pasja.
5) Gram codziennie.
6) Gram kilka razy w tygodniu.
7) Gram do godz. 22.00.
8) Kiedy gram, zdarza mi się denerwować, np. na innych graczy lub gdy coś mi nie wyjdzie.
9) Zdarza mi się grać, zamiast wykonywać różne obowiązki.
10) Mógłbym/mogłabym nie mieć smartfona/konsoli lub innego urządzenia do gier.

4. **Dyskusja** – nauczyciel zaprasza uczniów, by wrócili na miejsca i pyta: Czego dowiedzieliśmy się o nas? Co nas cieszy z tego mikrobadania? Co może nas niepokoić i dlaczego?

Część główna

1. **Praca indywidualna i w parach** – nauczyciel wprowadza uczniów w tematykę gier online. Rozdaje materiał o grach – Co to są gry komputerowe?
2. Prosi, by każda osoba przeczytała go, a następnie w parze uczniowie ustalają 3 informacje, które ich zdaniem powinien posiadać każdy gracz. Pary kolejno prezentują po jednej swojej wybranej informacji.

3. **Praca w trójkach** – Co czyha na gracza? – Nauczyciel mówi, że osoby, które świetnie znają zasady, jak działają różne gry, mogą je wykorzystać przeciwko tym, którzy po prostu grają i nie zdają sobie sprawy z ewentualnych niebezpiecznych sytuacji. Każda trójka dostaje do omówienia jedno zachowanie (Karta pracy), które może się zdarzyć w sieci w czasie grania na wybranym urządzeniu.
   Młodzież przygotowuje wypowiedź, dlaczego to zachowanie jest niebezpieczne i proponuje zasadę bezpiecznego zachowania, które pomoże się przed nim ustrzec. Zasadę grupa zapisuje dużymi literami na kartce A4.
   Po kilku minutach nauczyciel zaprasza trójki do prezentacji swoich haseł dotyczących bezpieczeństwa i ochrony prywatności w sieci.
   Hasła zbiera i wiesza w widocznym miejscu w klasie.
   Ważne: nauczyciel zwraca uwagę, czy pojawiły się takie hasła jak:

   - Pamiętanie o prywatności konta, haśle oraz wylogowaniu się po zakończonej grze;
   - Nie należy umieszczać zdjęć w sieci, które identyfikują gracza;
   - Ograniczenia wiekowe związane z uczestnictwem nastolatków w mediach społecznościowych i grach online;
   - Nie należy odpowiadać na propozycje spotkań i bliższych konwersacji;
   - Nie wolno klikać w linki umieszczane na czacie, mogą one zawierać złośliwe oprogramowanie lub szkodliwe treści.

4. **Planowanie badania ankietowego** – nauczyciel prosi uczniów, by dobrali się w pary z osobą, z którą będą chcieli wykonać zadanie na następne zajęcia.
   Następnie mówi, że wspólnie – jako klasa, przeprowadzą badanie ankietowe wśród swoich rówieśników na temat korzystania przez nich z gier komputerowych.

Nauczyciel rozdaje każdej parze kwestionariusz badania ankietowego – Karta pracy ankiety, prosi uczniów o zapoznanie się z treścią i chwilę refleksji, jak i kiedy mogą przeprowadzić badanie.
Ważne: zachęcamy uczniów, by ustalili, kiedy to zrobią, kto będzie za co odpowiedzialny.

Podsumowanie

Nauczyciel zaprasza uczniów do wspólnego podsumowania zajęć.
Prosi, aby każda osoba podzieliła się jedną informacją, która jej zdaniem jest ważna w związku z dzisiejszymi zajęciami. Nauczyciel zaprasza do słuchania wypowiedzi i niepowtarzania informacji.

Przebieg zajęć drugich

Wprowadzenie

Prezentacja wyników badań – nauczyciel łączy pary po dwie (czwórki), w których uczniowie omawiają swoje badania. Następnie na forum nauczyciel zadaje ogólne pytania: ilu uczniów udało nam się zbadać? Jak często młodzież gra? Czy zdarza się uczniom i uczennicom grać mimo zakazu? Co lubią robić młodzi ludzie w czasie wolnym? Czego dowiadujemy się z tego badania o naszych uczniach i uczennicach?

Ważne: badanie to jest tylko pretekstem do pogłębienia świadomości zagrożeń uzależnieniem grami, nie musi to być bardzo precyzyjne badanie.

Część główna

1. **Dyskusja za i przeciw** – nauczyciel dzieli klasę na pół. Jedna część, pracując w parach, musi znaleźć argumenty za graniem w gry komputerowe, druga część klasy musi znaleźć argumenty przeciwko. Nauczyciel zachęca uczniów, by korzystali z wniosków ze swoich badań. Warto, by każda strona miała przygotowanych kilka argumentów, które wygłoszą inne osoby.

Prezentacja argumentów stron trwa aż do wyczerpania argumentacji.

2. **Praca z filmem** – Nauczyciel w ramach podsumowania dyskusji zaprasza na film „Uzależnienia Behawioralne – Gry" i prosi, by zwrócić uwagę, czy wystąpią jakieś argumenty, które nie pojawiły się w klasie.
3. **Praca indywidualna i w parach** – nauczyciel rozdaje uczniom Dlaczego gry uzależniają. Zaprasza młodzież do przeczytania i sformułowanie wniosku – dlaczego, wg tej wiedzy oni sami i ich rówieśnicy są narażeni na uzależnienie od gier?

   Nauczyciel zachęca do zaprezentowania wniosków par na forum klasy. Warto dopytywać uczniów, którzy nie byli jeszcze aktywni.

Podsumowanie

Nauczyciel przypomina cele i kryteria sukcesu zajęć. Zaprasza uczniów i uczennice, by w ramach podsumowania obu lekcji odpowiedzieli sobie na pytanie: czego się o sobie dowiedziałam/dowiedziałem? Chętne osoby wypowiadają się na forum.

Komentarz metodyczny

Sposoby oceniania

Ocenie podlegają:

- ćwiczenia pisemne wykonywane podczas lekcji;
- aktywność podczas lekcji;
- quizy i gry interaktywne;
- odpowiedzi na pytania;
- zadania wykonywane podczas lekcji (indywidualne i grupowe).

Praca z uczniem ze specjalnymi potrzebami edukacyjnymi (SPE)

Uczniowie z SPE mogą pracować w grupie z uczniami zdolnymi.

Uczniowie wykazujący się dużą wiedzą na temat gier komputerowych mogą podzielić się nią podczas godziny wychowawczej lub spotkania w ramach kół zainteresowań w szkole.

Bibliografia/Netografia

- Borkowska A., Witkowska M., (2017), „Media społecznościowe w szkole", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 28.06.2023].
- „Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?" [online, dostęp z dn. 28.06.2023].
- „Gry online: korzyści i zagrożenia" [online, dostęp z dn. 28.06.2023].
- „Owce w sieci": materiały edukacyjne [online, dostęp z dn. 28.06.2023].
- Rywczyńska A., Wójcik Sz. (red.), (2019), „Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów", Warszawa: NASK – Państwowy Instytut Badawczy, Fundacja Dajemy Dzieciom Siłę [online, dostęp z dn. 28.06.2023].
- Sowala M., Wrońska A., (2020), „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 28.06.2023].
- „Ścieżki nauczania (11–13 lat)" [online, dostęp z dn. 28.06.2023].
- „Uzależnienia Behawioralne – Gry", film ExplainVisually zrealizowany w ramach akcji „Uzależnieniom behawioralnym mówię STOP!" [online, dostęp z dn. 28.06.2023].
- Witkowska M.,(2021), „Nastolatki i gry cyfrowe. Poradnik dla rodziców", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 28.06.2023].
- Wojtas M., (2020), „W świecie gier komputerowych – szanse i zagrożenia" [online, dostęp z dn. 28.06.2023].