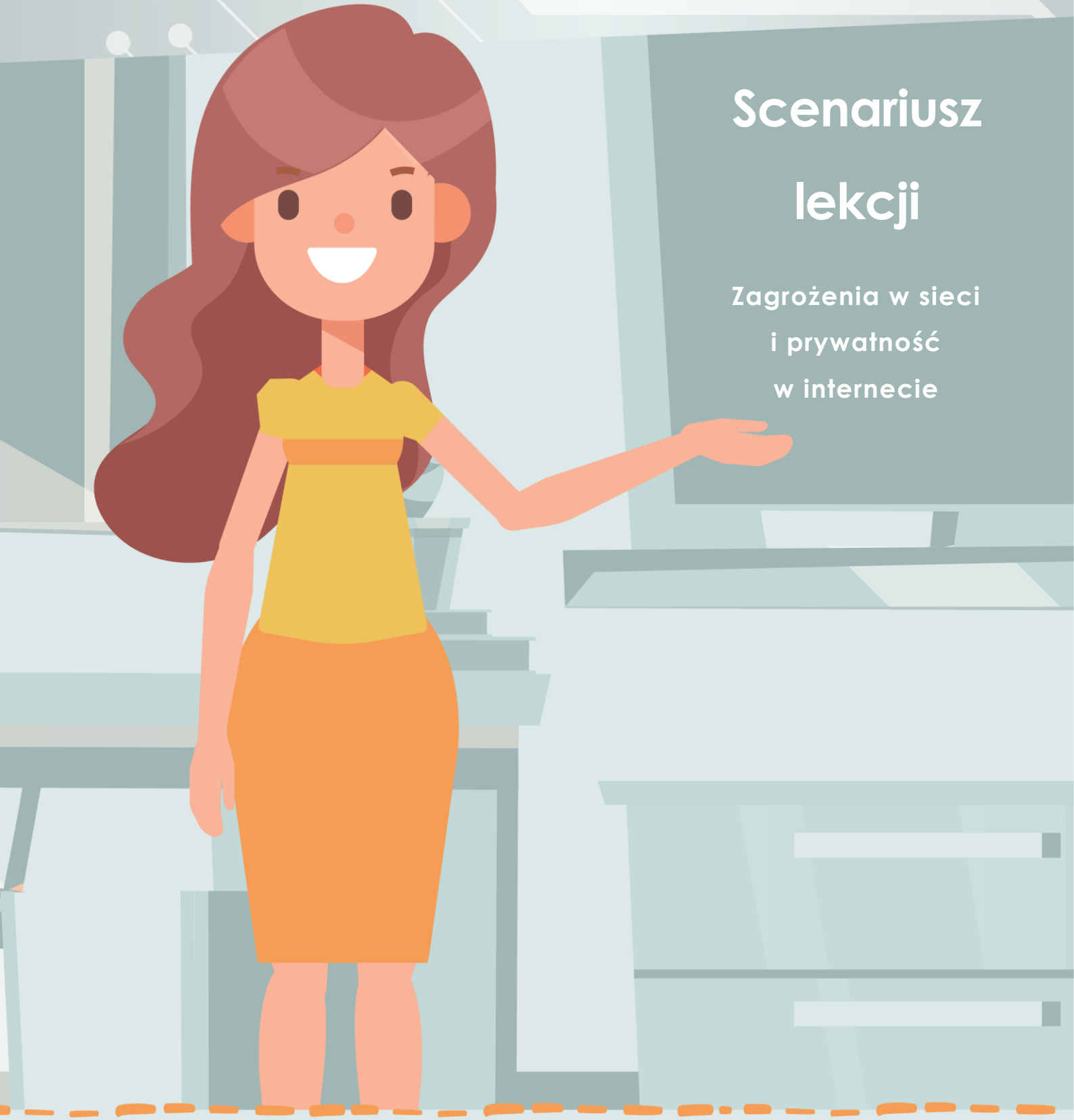
CYBER lekcje



Scenariusz lekcji

Zagrożenia w sieci
i prywatność
w internecie

NASK
NASK akademia
KPRM
GOV.pl CYFRYZACJA

CYBER lekcje

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

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

Redakcja językowa, dostępność (WCAG): Diana Kania

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

CYBER lekcje

Spis treści

CYBER lekcje

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

Klasa: **4–6 szkoły podstawowej**

Czas realizacji: **2 x 45 minut**

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 internami 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 osób dorosłych.

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.

CYBER lekcje

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**.

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;
- wykorzystuje technologie informacyjno-komunikacyjne w nabywaniu wiedzy.

Kompetencje kluczowe

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

Metody/techniki pracy

- opis;
- zabawa dydaktyczna;
- rozmowa;
- dyskusja;
- metoda problemowa;
- metoda praktyczna.

Formy pracy

- indywidualna;
- grupowa.

Środki dydaktyczne

- film „Uzależnienia Behawioralne – Gry";
- karta pracy „Model gracza";
- aplikacja Mentimeter;
- prezentacja multimedialna „Prywatność gracza";
- tablica (interaktywna);
- telefony komórkowe z dostępem do internetu;
- infografika „Prywatność w grach";
- infografika „Pozytywne i negatywne aspekty grania";
- infografika „Uzależnienie od gier";
- quiz „Prywatność w internecie 4–6";
- karta pracy „Gra online";
- karta pracy „Profil gracza".

Opis przebiegu zajęć/lekcji

Wprowadzenie

Nauczyciel wyświetla na ekranie chmurę wyrazów składającą się z nazw popularnych gier online, w tym gier sieciowych oraz gier MMORPG (skrót od ang. *Massively multiplayer online role-playing game*). Zadaje uczniom pytanie, z czym kojarzą im się te nazwy. Następnie kontynuuje rozmowę, zadając pytanie: Kto z was lubi grać w tego typu gry? Zachęca wszystkich do krótkiej dyskusji na temat znanych gier online.

Nauczyciel może także wykorzystać aplikację, np. Mentimeter, i przeprowadzić głosowanie, które wskaże wyniki i zachęci do dyskusji. Przykładowe pytania:

- W jakie gry online grasz?
- Ile czasu grasz na komputerze/konsoli?
- Czy znasz osoby, z którymi grasz?

Ważne! W tym przypadku uczniowie muszą posiadać telefony komórkowe z dostępem do internetu.

Część główna

1. Nauczyciel wprowadza uczniów w tematykę gier online. Omawia pokrótce rodzaje gier. Następnie prezentuje film „Uzależnienia Behawioralne – Gry" oraz infografikę „Pozytywne i negatywne aspekty grania". Omawia rodzaje gier oraz ich pozytywny wpływ na rozwój.
2. Nauczyciel wspólnie z uczniami wskazuje na wady i zalety korzystania z gier. Na tablicy zapisuje podawane przez uczniów propozycje:
   - Zalety – rozrywka, dokonywanie wyborów, pomysłowość, koncentracja, sprawność fizyczna (gry sportowe), rozwój umiejętności, logiczne myślenie, zdobywanie wiedzy, zdolności motoryczne (koordynacja ręka–oko);
   - Wady – nerwowość, agresywne treści, brak ruchu, nadwaga, wady postawy, problemy ze zdrowiem psychicznym, problemy ze zdrowiem fizycznym (ból głowy, oczu), uzależnienia, brak więzi z rówieśnikami.

   Nauczyciel uzupełnia propozycje uczniów, odwołując się do infografiki „Uzależnienie od gier".
3. Nauczyciel zwraca uczniom uwagę, że bardzo ważne jest, aby korzystając z gier cyfrowych, pamiętać o zachowaniu prywatności oraz przestrzegać zasad netykiety wśród graczy. Nauczyciel prezentuje uczniom infografikę „Prywatność w grach". Porusza również inne problemy występujące podczas użytkowania gier, np. przejmowanie kont.
4. Karta pracy „Model gracza" – nauczyciel dzieli uczniów na grupy. Każda z grup otrzymuje kartę, którą wypełnia, wpisując zachowania cechującego dobrego gracza, np. Gracz: stosuje się do regulaminów; nie poniża słabszych graczy; nie używa niecenzuralnych słów; nie wykorzystuje zakazanych kodów do gier (cheata); nie oszukuje; dba o swoją prywatność.
5. Prywatność gracza – nauczyciel przy wykorzystaniu prezentacji multimedialnej omawia najczęstsze zagrożenia, które mogą wystąpić przed uruchomieniem gry online lub w trakcie rozgrywki:
   - phishing – wysyłanie fałszywych wiadomości z linkiem w celu wyłudzenia danych;
   - ukryte koszty, wyłudzanie opłat – niektóre gry posiadają mechanizmy, które wyłudzają od gracza nakłady finansowe, tzw. mikropłatności;
   - kontakty, znajomości z innymi graczami – niektóre gry tworzą wielkie społeczności graczy, które wymieniają się doświadczeniami i poradami. Również nastolatki są ich członkami, przez co często nawiązują kontakty z nieznanymi osobami;
   - kradzież tożsamości – posługiwanie się w sieci fałszywym nazwiskiem lub pseudonimem, które zostało skradzione (wykradanie danych osobowych);

- pamiętanie o prywatności konta, haśle oraz wylogowaniu się po zakończonej grze;
- wizerunek i zdjęcia gracza – nie należy umieszczać zdjęć w sieci, które identyfikują gracza;
- ograniczenia wiekowe związane z uczestnictwem nastolatków w mediach społecznościowych i grach online;
- podłączanie aplikacji i portali społecznościowych do konta gracza;
- czaty, komunikatory – nie należy odpowiadać na propozycje spotkań i bliższych konwersacji; nie wolno też klikać w linki umieszczane na czacie, mogą one zawierać złośliwe oprogramowanie lub szkodliwe treści.

6. Karta pracy „Profil gracza" – uczniowie otrzymują kartę, na której wypełniają okienka: Login; Ulubiony typ gier; Gram w…; Dzienny czas przeznaczony na gry; Podczas gry pamiętam o…; Dbam o prywatność w sieci…; Awatar.
7. Nauczyciel uruchamia na tablicy quiz, który wykonuje wspólnie z uczniami. Może również udostępnić im kody QR, wówczas uczniowie wykonują zadanie przy wykorzystaniu swoich telefonów komórkowych.

Podsumowanie

Uczniowie dobierają się w grupy lub podziału dokonuje nauczyciel. Wspólnie wymyślają fabułę gry komputerowej, którą opisują na karcie zadań „Gra online". Karta zawiera następujące kategorie: Tytuł gry; Rodzaj gry; Grupa wiekowa; Przydatne umiejętności; Dodatkowe oprogramowanie; Czas potrzebny na przejście gry; Ukryte koszty (tak lub nie); Potrzebne dane; Bohaterowie; Opis gry (fabuła).

Komentarz metodyczny

Uwagi do realizacji lekcji/zajęć

Jeżeli wiemy, że nie wszyscy uczniowie w klasie posiadają telefony komórkowe, należy połączyć ich w pary tak, aby osoby nieposiadające urządzenia mogły pracować z uczniami, którzy mają dostęp do telefonu.

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).

CYBER lekcje

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.

CYBER lekcje

Karta pracy „Model gracza”

GRUPA .....

Wpisz w puste okienka pozytywne zachowania cechujące osobę, która często gra w gry online.

Wzorowy gracz

CYBER lekcje

Karta pracy „Profil gracza”

Uzupełnij poszczególne pola, opierając się na własnych doświadczeniach oraz zasadach bezpieczeństwa w sieci.

Mój login

.....

Ulubiony typ gier

.....

Gram w (nazwa gry lub gier)

.....

Dzienny czas przeznaczony na gry

.....

Podczas gry pamiętam o…

.....

.....

.....

Dbam o prywatność w sieci (jak?)

.....

.....

.....

Mój awatar (opisz)

.....

.....

.....

CYBER lekcje

Karta pracy „Gra online”

Wymyśl i opisz fabułę gry komputerowej.

Poniższe zagadnienia pomogą uszeregować najważniejsze aspekty gry. Powodzenia!

Tytuł gry

.....

Rodzaj gry

.....

Grupa wiekowa

.....

Przydatne umiejętności

.....

Dodatkowe oprogramowanie

.....

Czas potrzebny na przejście gry

.....

Ukryte koszty (tak lub nie)

.....

Potrzebne dane

.....

Bohaterowie

.....

.....

.....

Opis gry (fabuła)

.....

.....

.....

Bibliografia/Netografia

- Borkowska A., Witkowska M., (2017), „Media społecznościowe w szkole", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 21.12.2021].
- „Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?" [online, dostęp z dn. 21.12.2021].
- „Gry online: korzyści i zagrożenia" [online, dostęp z dn. 21.12.2021].
- Infografika „Phishing".
- „Owce w sieci": materiały edukacyjne [online, dostęp z dn. 21.12.2021].

  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. 21.12.2021].
- Sowala M., Wrońska A., (2020), „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 21.12.2021].
- „Ścieżki nauczania (11–13 lat)" [online, dostęp z dn. 21.12.2021].
- „Uzależnienia Behawioralne – Gry", film ExplainVisually zrealizowany w ramach akcji „Uzależnieniom behawioralnym mówię STOP!".
- Witkowska M.,(2021), „Nastolatki i gry cyfrowe. Poradnik dla rodziców", Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 21.12.2021].
- Wojtas M., (2020), „W świecie gier komputerowych – szanse i zagrożenia" [online, dostęp z dn. 21.12.2021].

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 czatów. 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].