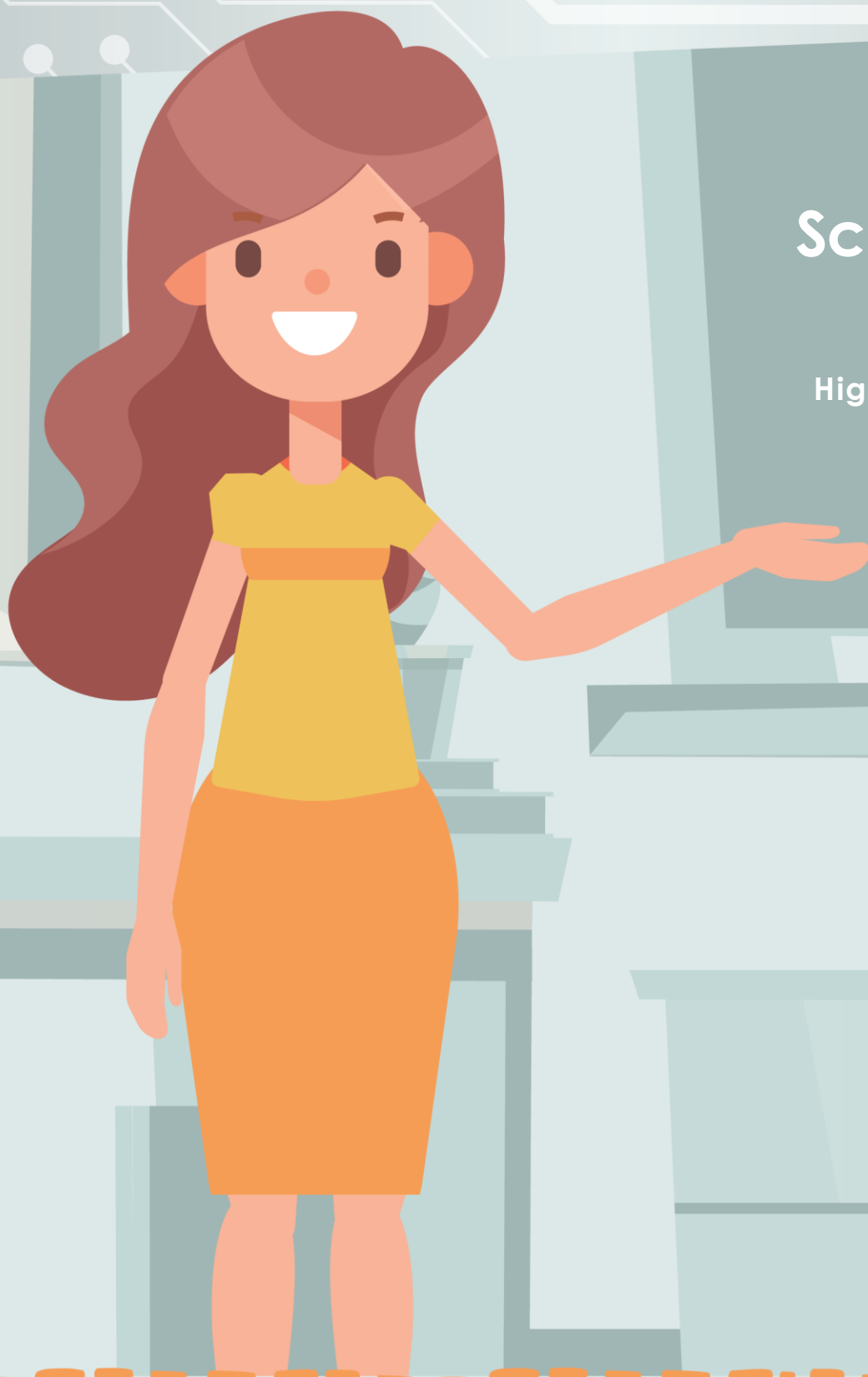


# CYBER lekcje



## Scenariusz lekcji

Higiena cyfrowa

## Higiena cyfrowa

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

Redakcja językowa, dostępność (WCAG): Diana Kania

© NASK – Państwowy Instytut Badawczy

Warszawa 2021

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe

NASK – Państwowy Instytut Badawczy

ul. Kolska 12

01-045 Warszawa

## Spis treści

Warto wiedzieć – wprowadzenie do zajęć .....	4
Informacje na temat zajęć .....	4
Cele ogólne powiązane z podstawą programową .....	4
Cele szczegółowe powiązane z podstawą programową .....	5
Kompetencje kluczowe .....	6
Metody/techniki pracy .....	6
Formy pracy .....	6
Środki dydaktyczne .....	6
Opis przebiegu zajęć/lekcji .....	7
Wprowadzenie .....	7
Część główna .....	7
Podsumowanie .....	9
Komentarz metodyczny .....	10
Uwagi do realizacji lekcji/zajęć .....	10
Sposoby oceniania .....	10
Praca z uczniem ze specjalnymi potrzebami edukacyjnymi (SPE): .....	10
Karta pracy „Umiejętności cyfrowe” – grupa 1 .....	11
Karta pracy „Umiejętności cyfrowe” – grupa 2 .....	12
Karta pracy „Zdrowie psychiczne a internet” .....	13
Karta pracy „Treści internetowe” .....	14
Karta pracy „Metody oszustw cyfrowych” .....	15
Bibliografia/Netografia .....	16
Opis projektu .....	17

Temat: **Higiena cyfrowa**

Etap: **szkoła ponadpodstawowa**

Czas realizacji: **2 x 45 minut**

## Warto wiedzieć – wprowadzenie do zajęć

Internet oraz urządzenia mobilne to narzędzia, które ułatwiają życie nam wszystkim. Młodzież bardzo chętnie sięga po zasoby online także w celach edukacyjnych oraz rozrywkowych. Niestety, często czas poświęcany na korzystanie z telefonu oraz materiałów dostępnych w sieci znacznie się wydłuża, co może mieć negatywne skutki dla zdrowia fizycznego i psychicznego. Nierzadko wpływ na samopoczucie i bezpieczeństwo młodzieży mają również treści szkodliwe i niebezpieczne zamieszczane online. Są one ogólnodostępne, ponadto mają z nimi kontakt coraz młodszy użytkownicy internetu. Skutki wywołane nadmiernym korzystaniem z sieci oraz dostępem do treści niebezpiecznych oddziałują na fizyczny, psychologiczny i społeczny obszar rozwoju młodego człowieka.

Rodzice nie są w stanie kontrolować czasu, jaki spędzają w sieci uczniowie szkół ponadpodstawowych. Opiekunowie bardzo często także nie wiedzą, co ich dziecko ogląda w internecie, z kim nawiązuje relacje, na jakich forach się udziela. Zapobieganie ewentualnym negatywnym skutkom, jakie mogą mieć dla uczniów szkodliwe treści oraz niebezpieczne kontakty nawiązywane online, jest ważnym zadaniem szkoły, w tym nauczycieli.

Istotnym elementem edukacji uczniów jest nabywanie przez nich odpowiednich umiejętności cyfrowych: rozpoznawania wartościowych treści oraz nauka krytycznej analizy informacji dostępnych w online. Należy polecać uczniom publikacje oraz materiały filmowe, w których eksperci, specjaliści, osoby zaangażowane w działania na rzecz bezpieczeństwa w sieci przekazują istotne informacje.

## Informacje na temat zajęć

### Cele ogólne powiązane z podstawą programową

#### Język polski

IV. Samokształcenie. Uczeń:

- 1) **rozwija umiejętność pracy samodzielnej między innymi przez przygotowanie różnorodnych form prezentacji własnego stanowiska;**
- 2) **porządkuje informacje w problemowe całości poprzez ich wartościowanie; syntetyzuje poznawane treści wokół problemu, tematu, zagadnienia oraz wykorzystuje je w swoich wypowiedziach;**

## Informatyka

IV. Rozwijanie kompetencji społecznych. Zakres podstawowy. Uczeń:

- 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;**
- 4) **bezpiecznie buduje swój wizerunek w przestrzeni medialnej;**
- 6) **poszerza i uzupełnia swoją wiedzę, korzystając z zasobów udostępnionych na platformach do e-nauczania.**

V. Przestrzeganie prawa i zasad bezpieczeństwa. Zakres podstawowy. Uczeń:

- 4) **opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.**

## Edukacja dla bezpieczeństwa

IV. Edukacja zdrowotna. Zdrowie w wymiarze indywidualnym oraz zbiorowym. Zachowania prozdrowotne.

2. Elementy zdrowia psychicznego. Uczeń:

- 1) **wyjaśnia zależności między zdrowiem fizycznym, psychicznym, emocjonalnym a społecznym; wyjaśnia wpływ stresu na zdrowie;**
- 3) **ocenia własne zachowania związane ze zdrowiem, ustala indywidualny plan działania na rzecz własnego zdrowia;**
- 4) **zna podstawowe sygnały i objawy problemów ze zdrowiem psychicznym (stres fizyczny i emocjonalny, zaburzenia odżywiania, depresja kliniczna);**
- 5) **opisuje konstruktywne i niekonstruktywne sposoby radzenia sobie z emocjami, w tym negatywnymi.**

## Cele szczegółowe powiązane z podstawą programową

Uczeń:

- definiuje termin „zdrowie psychiczne”;
- ocenia wpływ internetu na zdrowie psychiczne;
- zna treści szkodliwe dostępne w internecie;
- aktywnie uczestniczy w dyskusji;
- wyszukuje informacje na temat bezpieczeństwa urządzeń i zasobów sieciowych;

- zna metody kontrolowania czasu spędzanego w internecie;
- wykorzystuje sprawdzone aplikacje do planowania czasu online;
- korzysta z kwestionariuszy psychologicznych w celu ochrony zdrowia.

## Kompetencje kluczowe

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

## Metody/techniki pracy

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

## Formy pracy

- indywidualna;
- grupowa.

## Środki dydaktyczne

- definicja terminu [„zdrowie psychiczne”](#);
- karta pracy „Zdrowie psychiczne a internet”;
- karta pracy „Treści internetowe”;
- karta pracy „Metody oszustw cyfrowych”;
- karty pracy „Umiejętności cyfrowe”;
- [film „Największe zagrożenia w Internecie”](#);
- [infografika „Co nas martwi w sieci – czas poświęcany nowym technologiom”](#);
- karteczki, np. samoprzylepne;
- [film „Phishing/Socjotechnika”](#) – wywiad z ekspertem;
- [przesiewowy kwestionariusz ryzyka uzależnienia od Internetu wg Kimberly Young](#);
- kody QR, telefony komórkowe;
- komputer z dostępem do internetu, ekran/tablica.

## Opis przebiegu zajęć/lekcji

### Wprowadzenie

Nauczyciel wyświetla lub zapisuje na tablicy hasło: „Zdrowie psychiczne”. Prosi uczniów o zastanowienie się, z czym kojarzą podany termin. Zaprasza do dyskusji i dzielenia się własnymi doświadczeniami. Podczas wspólnej rozmowy nauczyciel zapisuje na tablicy najważniejsze elementy zdrowia psychicznego wymieniane przez uczniów (np. dobre samopoczucie; brak problemów; brak stanów lękowych itp.). Następnie omawia definicję [„zdrowia psychicznego”](#), zwracając uwagę na wpływ różnych czynników (fizycznych, psychologicznych i społecznych) na dobrostan człowieka.

### Część główna

1. Nauczyciel zadaje uczniom pytanie: „Czy korzystanie z technologii informacyjno-komunikacyjnych (TIK) i internetu może wpływać na zdrowie psychiczne?”. Prosi uczniów o zastanowienie się nad odpowiedzią. Następnie dzieli klasę na grupy. Każda z nich otrzymuje kartę pracy „Zdrowie psychiczne a internet”.

Zadaniem uczniów jest wpisanie negatywnych konsekwencji korzystania z TIK oraz internetu, np. nadwaga, bezsenność, zmęczenie, podrażnienie oczu, zachwiane relacje z rówieśnikami, rozdrażnienie, zespół cieśni nadgarstka, brak akceptacji, obniżenie poczucia własnej wartości itp.

2. Po zakończonej pracy lider grupy odczytuje zapisane odpowiedzi. Nauczyciel zwraca uczniom uwagę, że wymienione przez nich symptomy mogą prowadzić do poważnych problemów zdrowotnych – fizycznych i psychicznych. Mogą one się nasilać pod wpływem kontaktu z treściami online i podczas czynności związanych z użytkowaniem internetu.
3. „Treści internetowe” – karta pracy. Nauczyciel rozdaje uczniom karty pracy, na których zostały zawarte różne szkodliwe i niebezpieczne treści dostępne w internecie. Prosi uczniów o wybranie pięciu obszarów tematycznych wpływających negatywnie na zdrowie młodzieży, przy czym pierwszy obszar to treści najmniej szkodliwe, a piąty – najbardziej szkodliwe.

Obszary tematyczne:

- Pornografia;
- Przemoc, obrażenia fizyczne;
- Samobójstwa bądź śmierć;
- Przyjmowanie środków odurzających;
- Samookaleczenia;
- Restrykcyjne i wyniszczające diety;

- Rasizm i nienawiść klasowa;
  - Nietypowe i dewiacyjne zachowania seksualne;
  - Wykorzystywanie seksualne dzieci;
  - Fałszywe wiadomości (tzw. fake news);
  - Patostreamy;
  - Online challenge;
  - Inne.
4. Uczniowie wieszają kartki w widocznym miejscu. Nauczyciel komentuje zaznaczone przez młodzież obszary tematyczne obejmujące treści szkodliwe i niebezpieczne. Następnie wyświetla [film „Największe zagrożenia w Internecie”](#).
5. Nauczyciel dzieli uczniów na grupy. Każda z nich otrzymuje kartę pracy „Umiejętności cyfrowe” i wyszukuje jeden obszar tematyczny (bezpieczeństwo urządzeń lub bezpieczeństwo zasobów), sporządzając na jego temat krótkie notatki. Uczniowie do wyszukania informacji wykorzystują swoje telefony komórkowe.

Obszary tematyczne:

- Grupa 1. Bezpieczeństwo urządzeń (np. aktualizowanie systemu operacyjnego urządzenia oraz zainstalowanych na nim aplikacji; instalowanie oprogramowania antywirusowego; ustawienia dotyczące uprawnień nadawanym aplikacjom).
- Grupa 2. Bezpieczeństwo zasobów (np. zarządzanie danymi, kopie zapasowe; szyfrowanie wiadomości; ustawianie blokady PIN lub hasła).

Po wykonaniu zadania uczniowie prezentują opracowany materiał. Nauczyciel zwraca uwagę, że bardzo ważne jest zwiększanie poziomu świadomości mające na celu zapobieganie sytuacjom, w których użytkownik podejmuje błędne decyzje. Mogą one skutkować np. utratą danych.

Następnie nauczyciel wskazuje, jak można podnieść poziom świadomości: zapoznać się z metodami ataków kierowanych na użytkowników oraz zobaczyć, jak wyglądają przykładowe fałszywe wiadomości i metody stosowane przez przestępców. Najlepszymi miejscami do zdobywania takich informacji są strony internetowe zespołów reagowania na incydenty komputerowe (CSIRT/CERT) oraz blogi i konta na serwisach społecznościowych prowadzone przez specjalistów od bezpieczeństwa sieciowego.

6. Następnie nauczyciel wyświetla [film „Phising/Socjotechnika”](#). Po jego zakończeniu nauczyciel pyta uczniów, czy w swoim życiu doświadczyli działania przestępców internetowych, zostali pokrzywdzeni przez oszustów stosujących atak socjotechniczny. Zachęca młodzież do dyskusji.



7. Nauczyciel rozdaje uczniom karty pracy „Metody oszustw cyfrowych”. Uczniowie dopasowują opisy metod oszustw z ich nazwami. Ćwiczenie można również wykonać przy wykorzystaniu tablicy interaktywnej:
  - Phishing – rodzaj cyberataku polegający na podszyciu się pod zaufany z punktu widzenia ofiary podmiot (np. pośrednik płatności, bank, kurier).
  - Smishing – ataki tekstowe polegające na tym, że treści nakłaniające do podjęcia określonego działania rozpowszechniane są za pośrednictwem wiadomości tekstowych (SMS-ów).
  - Vishing – ataki telefoniczne polegające na wyłudzeniu informacji prywatnych bądź finansowych.
  - Smishing – to rodzaj ataku phishingowego ukierunkowanego na komunikatory typu Messenger.
8. Nauczyciel prezentuje uczniom infografikę „Co nas martwi w sieci – czas poświęcany nowym technologiom”. Wskazuje, że zbyt długie korzystanie z internetu oraz urządzeń mobilnych przyczynia się do zaniedbywania innych obowiązków, wpływa na pogorszenie bezpośrednich relacji międzyludzkich, powoduje spadek motywacji do rozwoju zainteresowań i pasji, destrukcyjnie oddziałuje na zdrowie fizyczne i psychiczne.
9. „Kontroluję swój czas w internecie” – nauczyciel prosi uczniów o zapisanie na karteczce jednej propozycji dotyczącej kontrolowania własnego czasu spędzonego w sieci: „Jak spędzasz czas bez dostępu do internetu?”, „Co tracę, korzystając zbyt długo z internetu i urządzeń mobilnych?”. Uczniowie przypinają karteczki w wyznaczonym miejscu. Nauczyciel lub wskazany uczeń odczytuje odpowiedzi.
10. Nauczyciel omawia aplikacje i ustawienia, które pomagają w zachowaniu higieny cyfrowej. Należą do nich np. aplikacja Cyfrowa równowaga w systemie Android lub ustawienia czasu ekranowego w systemie operacyjnym iOS.

## Podsumowanie

Nauczyciel zwraca uwagę, że zbyt częste korzystanie z internetu prowadzi nie tylko do zaburzeń fizycznych i psychicznych, ale również do poważnych uzależnień od internetu lub treści dostępnych online. Na zakończenie demonstruje [przesiewowy kwestionariusz ryzyka uzależnienia od internetu według Kimberly Young](#). Zaprasza wszystkich do jego wykonania. Uczniowie przy wykorzystaniu telefonów komórkowych skanują kod QR odsyłający do testu Kimberly Young.

## Komentarz metodyczny

### Uwagi do realizacji lekcji/zajęć

W sytuacji zainteresowania uczniów omawianą tematyką warto wydłużyć zajęcia do trzech godzin dydaktycznych. Spotkanie można uzupełnić o szersze poruszenie wiadomości dotyczących treści szkodliwych i niebezpiecznych dostępnych w internecie.

Podczas spotkania uczniowie mogą zainstalować aplikację, która pomoże im kontrolować czas spędzany w sieci, np. Cyfrowa równowaga.

Jeśli nauczyciel wie, że nie wszyscy uczniowie będą mogli korzystać z telefonów komórkowych, planuje przeprowadzenie zajęć w pracowni komputerowej.

### Sposoby oceniania

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

### Praca z uczniem ze specjalnymi potrzebami edukacyjnymi (SPE):

Uczniowie zdolni – interesujący się tematyką nowoczesnych technologii – mogą zaprezentować podczas zajęć wykorzystanie aplikacji mobilnych pomocnych w zachowaniu cyfrowej higieny.

## Karta pracy „Umiejętności cyfrowe” – grupa 1

Wyszukaj w zasobach internetowych informacje na temat bezpieczeństwa urządzeń cyfrowych. Sporządź notatki na podstawie pozyskanych wiadomości.

## Karta pracy „Umiejętności cyfrowe” – grupa 2

Wyszukaj w zasobach internetowych informacje na temat bezpieczeństwa zasobów cyfrowych. Sporządź notatki na podstawie pozyskanych wiadomości.

## Karta pracy „Zdrowie psychiczne a internet”

Wypisz negatywne konsekwencje korzystania z technologii informacyjno-komunikacyjnych oraz internetu.

### **Negatywne skutki korzystania z technologii informacyjno-komunikacyjnych oraz internetu**

Skutki fizyczne

.....

.....

.....

.....

.....

.....

.....

Skutki psychologiczne

.....

.....

.....

.....

.....

.....

.....

Skutki społeczne

.....

.....

.....

.....

.....

.....

## Karta pracy „Treści internetowe”

Wybierz pięć obszarów tematycznych obejmujących treści szkodliwe i niebezpieczne dostępne w internecie, które wpływają negatywnie na zdrowie młodzieży, i oznacz je cyframi od 1 do 5 (przy czym 1 to treści najmniej szkodliwe, a 5 – najbardziej szkodliwe).

Obszar tematyczny	Skala od 1 do 5
Pornografia	
Przemoc, obrażenia fizyczne	
Samobójstwa bądź śmierć	
Przyjmowanie środków odurzających	
Samookaleczenia	
Restrykcyjne i wyniszczające diety	
Rasizm i nienawiść klasowa	
Nietypowe i dewiacyjne zachowania seksualne	
Wykorzystywanie seksualne dzieci	
Fałszywe wiadomości (tzw. fake news)	
Patostreamy	
Online challenge	
Inne	

## Karta pracy „Metody oszustw cyfrowych”

1. Połącz w pary metody oszustw z odpowiednimi opisami.
2. Na podstawie prezentowanego filmu wymień sposoby obrony przed atakami socjotechnicznymi.

### SPOSOBY OBRONY PRZED ATAKAMI SOCJOTECHNICZNYMI

.....

.....

.....

.....

.....

Phishing

Ataki tekstowe, polegające na tym, że wiadomości rozpowszechniane są za pośrednictwem wiadomości tekstowych (SMS-ów).

Smishing

Rodzaj cyberataku polegający na podszyciu się pod zaufany z punktu widzenia ofiary podmiot (np. pośrednik płatności, bank, kurier).

Smishing

Ataki telefoniczne polegające na wyłudzeniu informacji prywatnych bądź finansowych

Vishing

To rodzaj ataku phishingowego ukierunkowanego na komunikatory typu Messenger

## Bibliografia/Netografia

- [„Bezpieczne korzystanie ze smartfonów, tabletów i komputerów przez dzieci i młodzież”](#) [online, dostęp z dn. 28.12.2021].
- Broszura [„Jak osiągnąć cyfrowy dobrostan”](#) [online, dostęp z dn. 28.12.2021].
- Crognale D., (2021), [„Bezpieczne korzystanie z aplikacji mobilnych”](#), tłum. Wnuk B., Węgrzynowicz A., „OUCH!” nr 6 [online, dostęp z dn. 28.12.2021].
- [„Europejski Miesiąc Cyberbezpieczeństwa – baza wiedzy”](#) [online, dostęp z dn. 28.12.2021].
- [„Internetowe porady dotyczące bezpieczeństwa”](#) [online, dostęp z dn. 28.12.2021].
- [„Jak ograniczyć czas spędzany ze smartfonem? Z technologii warto korzystać rozsądnie”](#) [online, dostęp z dn. 28.12.2021].
- Trailer filmu [„Zdrowie psychiczne – jak o nie dbać w wieku szkolnym”](#) [online, dostęp z dn. 28.12.2021].
- [„Zdrowie psychiczne dzieci i młodzieży – materiały do pobrania”](#) [online, dostęp z dn. 28.12.2021].



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;

# CYBER lekcje

- 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].