PFR Fundacja

Centralny Dom Technologii

CYBER BEZPIECZNI

SCENARIUSZE LEKCJI O CYBERBEZPIECZEŃSTWIE

Edukacja Jutra

WARSZAWA, 2022

Spis treści

CYBER BEZPIECZNI

SCENARIUSZE LEKCJI O CYBERBEZPIECZEŃSTWIE

CYBERBEZPIECZNI – PROJEKT EDUKACYJNY DLA UCZNIÓW I NAUCZYCIELI

Cyberbezpieczni to ogólnopolski program rozwoju kompetencji uczniów i nauczycieli realizowany przez zespół edukacyjny Centralnego Domu Technologii i Fundację Polskiego Funduszu Rozwoju. Projekt ma na celu na celu promowanie wiedzy z zakresu bezpieczeństwa w sieci. W efekcie działań edukacyjnych **już ponad 10 tysięcy osób miało szansę dowiedzieć się, jak być bezpiecznym w sieci i jak rozpoznawać nieprawdziwe treści publikowane w Internecie.**

Jednym z efektów projektu jest niniejsza publikacja, w której zebraliśmy scenariusze lekcji nadesłane i nagrodzone w ogólnopolskim konkursie „Edukacja Jutra". Scenariusze zostały przygotowane przez nauczycieli z całej Polski. Kryteria oceny najlepszych zgłoszeń stanowiły: umocowanie w podstawie programowej, **oryginalne i innowacyjne podejście do tematu,** ale także **popularyzowanie wiedzy z zakresu bezpieczeństwa w cyberprzestrzeni.**

Jesteśmy pewni, że publikacja stanie się dla każdego nauczyciela i edukatora inspiracją do wprowadzenia tematów związanych z bezpieczeństwem w sieci podczas lekcji szkolnych – online i stacjonarnie. Mamy nadzieję, iż dzięki wykorzystaniu przedstawionych podpowiedzi i porad autorów, każdy będzie miał możliwość zrealizowania wartościowych, angażujących zajęć, na których skorzysta z nowoczesnych narzędzi edukacji. – Karol Izdebski, koordynator projektu

Oprócz konkursu program „Cyberbezpieczni" składał się z dwóch ważnych komponentów – warsztatów dla uczniów i nauczycieli prowadzonych online i stacjonarnie oraz szerokich działań edukacyjnych takich, jak debata CDTalks „Jak uczyć cyberbezpieczeństwa?".

Podczas bezpłatnych kilkugodzinnych szkoleń, których przeprowadzono prawie 70 dla ponad 1500 uczestników w Warszawie, Wrocławiu i Białymstoku, była mowa o tym, jak unikać oszustw w Internecie, walczyć z dezinformacją i żyć w świecie mediów społecznościowych, żeby nie było to szkodliwe, a wspomagało procesy społeczne. Zajęcia miały charakter warsztatowy, dzięki czemu wszyscy mogli na realnych przykładach poznać istotę cyberbezpieczeństwa i dowiedzieć się, dlaczego jest to tak ważny i aktualny temat.

Debata CDTalks „Jak uczyć cyberbezpieczeństwa?" odbyła się 15 grudnia w Centralnym Domu Technologii w Warszawie. O podzielenie się wiedzą, doświadczeniem i rekomendacjami na temat cyberbezpieczeństwa poproszono pięcioro ekspertów: Annę Gwozdowską – redaktorkę portalu FakeHunter (PAP), Michała Krawczyka – analityka Instytutu Kościuszki, Aldonę Rumińską-Szalską – nauczycielkę i zwyciężczynię 3. edycji konkursu CDT „Edukacja Jutra", Annę Rywczyńską – kierowniczkę Zespołu Edukacji Cyfrowej w NASK oraz Tomasza Szporlendowskiego – prawnika i starszego specjalistę ds. współpracy z organami ścigania w Allegro. Moderatorką rozmowy została redaktorka

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

naczelna CyberDefence24.pl Nikola Bochyńska. Uczestnicy panelu wskazali **konieczność włączenia do procesu edukacji dyrektorów szkół, nauczycieli, rodziców oraz uczniów. Zgodzili się również, że temat bezpieczeństwa młodzieży w sieci wymaga włączenia go do podstawy programowej wszystkich przedmiotów szkolnych.** Pełne nagranie z debaty jest dostępne na kanale YouTube CDT.

Materiały edukacyjne stworzone w ramach projektu są udostępnione bezpłatnie na kanałach YouTube CDT oraz na stronie www.cdt.pl. Ze względu na ogromne zainteresowanie zajęciami zespół edukacyjny CDT będzie kontynuował działania dotyczące cyberbezpieczeństwa w kolejnym roku i nadal promował wiedzę w tym obszarze!

Życzymy inspirującej lektury,
Zespół Fundacji Polskiego Funduszu Rozwoju

Więcej informacji o projekcie Cyberbezpieczni znajduje się na stronie:
www.fundacjapfr.pl/cyberbezpieczni

Projekt jest finansowany ze środków Kancelarii Prezesa Rady Ministrów w ramach ogólnopolskiego programu rozwoju kompetencji uczniów i nauczycieli „Cyberbezpieczni”.

CYBER BEZPIECZNI

Centralny Dom Technologii

1. MIEJSCE
KLIK I ENTER Z NETI - CIEKAWEJ PLANETY: INTERAKTYWNE I INTERDYSCYPLINARNE ZAJĘCIA WPROWADZAJĄCE UCZNIÓW W ŚWIAT BEZPIECZNEGO KORZYSTANIA Z INTERNETU

autorka: Aldona Rumińska-Szalska

Biografia Autorki

Aldona Rumińska-Szalska jest nauczycielem współorganizującym proces kształcenia w Szkole Podstawowej z Oddziałami Integracyjnymi nr 105 w Krakowie. Autorka wielu scenariuszy zajęć oraz projektów edukacyjnych o tematyce ekologicznej, senioralnej (międzygeneracyjnej), przedsiębiorczej, historycznej, religijnej, prozdrowotnej i wolontaryjnej nagradzanych w konkursach ogólnopolskich (org.: Wydawnictwo Nowa Era, Polskie Stowarzyszenie Energetyki Wiatrowej, Winiary, NBP, Catalyst Education, Otrivin, ORE, Referat Prowincji Polski Południowej Towarzystwa Jezusowego, UMK- Klimat-Energia-Gospodarka Wodna, Kuratorium Oświaty w Krakowie itp.). Zdobywczyni tytułu: Nauczyciel Kreatywny (2013) i Nauczyciel Jutr@ (2022). Uczniowie o różnych potrzebach edukacyjnych pod opieką A. Rumińskiej-Szalskiej zdobywają nagrody w konkursach różnotematycznych na szczeblach międzynarodowych i ogólnopolskich. Nauczyciel promujący w działaniach kreatywny, zrównoważony rozwój uczniów w duchu szeroko rozumianych wartości humanistycznych.

Nawiązania do problematyki związanej z cyberbezpieczeństwem

- Wiek wczesnoszkolny uczniów (9 lat) jest okresem, w którym młody człowiek zaczyna lub zaczął już być użytkownikiem cyfrowego świata. Jest to pilny czas, by podjąć działania prewencyjne, ostrzegawcze w zakresie bezpiecznego korzystania z zasobów Sieci, ale przede wszystkim KREATYWNEGO I ROZWIJAJĄCEGO PRZETWARZANIA INFORMACJI CYFROWEJ.
- Uczniowie z niepełnosprawnością, zwłaszcza dysfunkcją intelektualną wymagają szczególnej czujności i ukierunkowania podczas korzystania z cyfrowych źródeł informacji, a także rozwijania świadomości, a następnie autokontroli w tym zakresie.
- Szerzące się nagminnie zjawisko cyberprzemocy oraz dynamiczny rozwój techniki, głośno wzywa do działań ostrzegawczych i automotywacyjnych.
- Potrzeba ukazania równoległych aktywnie przestrzeni: cyfrowej, ekologicznej (terenowej) i klasowej, które winny być ujmowane w sposób uzupełniający i równoważący się.
- Kształtowanie wśród uczniów alternatywnych aktywności, decyzyjności, odwagi do proszenia o pomoc, czujności na potencjalne zagrożenia, netykietyzacji własnych działań.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

• **Kształcenie ogólne w szkole podstawowej ma na celu:**
- rozwijanie kompetencji, takich jak: kreatywność, innowacyjność i przedsiębiorczość;
- wszechstronny rozwój osobowy ucznia przez pogłębianie wiedzy oraz zaspokajanie i rozbudzanie jego naturalnej ciekawości poznawczej;

Najważniejsze umiejętności rozwijane w ramach kształcenia ogólnego w szkole podstawowej to:
poszukiwanie, porządkowanie, krytyczna analiza oraz wykorzystanie informacji z różnych źródeł;

kreatywne rozwiązywanie problemów z różnych dziedzin ze świadomym wykorzystaniem metod i narzędzi wywodzących się z informatyki, w tym programowanie;

Szkoła ma przygotowywać [uczniów] do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w Internecie, krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci.

• Do zadań szkoły w zakresie edukacji wczesnoszkolnej należy: zapewnienie dostępu do wartościowych, w kontekście rozwoju ucznia, źródeł informacji i nowoczesnych technologii;

W zakresie społecznego rozwoju uczeń osiąga:
• umiejętność dbania o bezpieczeństwo własne i innych uczestników grupy, w tym bezpieczeństwo związane z komunikacją za pomocą nowych technologii.

W zakresie poznawczego rozwoju uczeń osiąga
• potrzebę i umiejętność samodzielnego, refleksyjnego, logicznego, krytycznego i twórczego myślenia;

OSIĄGNIĘCIA W ZAKRESIE EDUKACJI POLONISTYCZNEJ - Uczeń:
• słucha z uwagą (...) tekstów czytanych przez nauczyciela, uczniów i inne osoby;
• wykorzystuje nabyte umiejętności do rozwiązywania problemów i eksploracji świata, dbając o własny rozwój;

OSIĄGNIĘCIA W ZAKRESIE EDUKACJI INFORMATYCZNEJ, w tym w zakresie przestrzegania prawa i zasad bezpieczeństwa - Uczeń:
• posługuje się udostępnioną mu technologią zgodnie z ustalonymi zasadami;
• rozróżnia pożądane i niepożądane zachowania innych osób (również uczniów) korzystających z technologii, zwłaszcza w sieci Internet;
• przestrzega zasad dotyczących korzystania z efektów pracy innych osób i związanych z bezpieczeństwem w Internecie.

OSIĄGNIĘCIA W ZAKRESIE EDUKACJI SPOŁECZNEJ:
• ocenia swoje postępowanie (...);
• wykorzystuje pracę zespołową w procesie uczenia się, w tym przyjmując rolę lidera zespołu i komunikuje się za pomocą nowych technologii;
• ma świadomość obecności nieprawdziwych informacji, np. w przestrzeni wirtualnej (...);
• stosuje zasady bezpieczeństwa podczas korzystania z urządzeń cyfrowych;
• ma świadomość, iż nieodpowiedzialne korzystanie z technologii ma wpływ na utratę zdrowia człowieka.

OSIĄGNIĘCIA W ZAKRESIE EDUKACJI PLASTYCZNEJ (EKSPRESJI TWÓRCZEJ) - Uczeń:
maluje farbami (...) rysuje kredką, kredą, ołówkiem.

OSIĄGNIĘCIA W ZAKRESIE WYCHOWANIA FIZYCZNEGO:
• uczestniczy w zabawach i grach zespołowych, respektuje przepisy, reguły zabaw i gier ruchowych.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

Edukacje: polonistyczna, społeczna, artystyczna, informatyczna, elementy wychowania fizycznego

Adresaci lekcji (wiek, klasa)

Koncepcja lekcji opracowana jest wielopoziomowo ze względu na kompetencje rozwojowe uczniów.

Dotyczy ona:
- uczniów z klasy integracyjnej III szkoły podstawowej (pełnosprawnych, z dysfunkcjami rozwojowymi oraz zdolnych/uzdolnionych)
- uczniów z trudnościami rozwojowymi szkół i placówek specjalnych (III –V kl. SP)
- uczniów wykazujących szczególne zainteresowanie tematem w powyższych specyfikacjach.

Cel ogólny lekcji i cele szczegółowe

I. Cel ogólny:
Poznanie i zapobieganie zagrożeniom w cyber- przestrzeni wśród najmłodszych uczestników Sieci, poprzez motywacyjne spotkanie z Suberbohaterami – przewodnikami lekcji : Klikiem i Enterem na podstawie wirtualnej książeczki.

Cele szczegółowe:
- Wymieni skojarzenie związane z rysunkiem umieszczonym na bilecie wstępu na lekcję;
- Słucha uważnie tekst czytany przez nauczyciela/kolegę, samodzielnie odczytuje fragment tekstu;
- Wykona ćwiczenie dydaktyczno-ruchowe: W sieci – rety! I wyjaśni jego znaczenie;
- Wyjaśnia kim jest haker i czym jest hejt;
- Wymienia potencjalne zagrożenia w świecie cyfrowym;
- Wykona ćwiczenie na karcie pracy;
- Wyjaśnia w jaki sposób można przeciwdziałać cyberprzemocy;
- Wyjaśnia czym jest Helpline i czym się zajmuje;
- Udziela prawidłowej odpowiedzi na pytania interaktywnej gry: „Milionerzy”;
- Zapisuje swój nick na balonie;
- Wykona pracę twórczą zgodnie ze swoimi predyspozycjami;
- Oceni swoje zainteresowanie lekcją.

Metody pracy

- **Metody pracy:** aktywne (burza mózgów, metoda skojarzeń, sztafeta pytań, ćw. interaktywne (quiz, e-książeczka) i integracyjne; waloryzacyjne (ekspresyjna, impresyjna); asymilacyjne wiedzę, (wyjaśnienie, omówienie, pokaz, praca w oparciu kartę pracy); praktyczna w plenerze (zrównoważona edukacja).
- **Formy pracy:** indywidualna– (jednolita, zróżnicowana), grupowa– (zróżnicowana), zbiorowa (jednolita).
- **Typ lekcji:** lekcja rozwijająco-problemowa.

UWAGI REALIZACYJNE: bohaterami przewodnimi podczas lekcji są: Klik i Enter. Towarzyszą oni ucz-

niom podczas wykonywania zadań na stronach zwanych: Neto Kroki. Bohaterowie oprowadzają uczniów po planecie Neti zwracając uwagę na niebezpieczeństwa, na które mogą napotkać. Nauczyciel zapoznaje uczniów z konkretnymi ćwiczeniami w oparciu o elektroniczną książeczkę – „nawigatora" kolejnych etapów lekcji. Uczniowie wykonując zadania, wspólnie z nauczycielem tworzą e-książkę. Docelowo, może ona zostać wydrukowana i uzupełniona fotorelacją z lekcji oraz pracą uczniów (zad. domowe). Mając na uwadze zalety edukacji zrównoważonej, zastosowano różnorodne metody i formy prac, w tym aktywne tematyczne zagospodarowanie przerwy lekcyjnej na świeżym powietrzu. Scenariusz ma charakter otwarty, można go uzupełniać, modyfikować i kontynuować. Wprowadzenie wielopoziomowości w zakresie opracowanych pomocy dydaktycznych umożliwia przeprowadzenie lekcji z uczniami o różnym poziomie intelektualno-rozwojowym. Scenariusz ma charakter interdyscyplinarny, korelujący różne dziedziny wiedzy. Został uzupełniony dodatkowymi ćwiczeniami, w tym interaktywnymi, które można wykorzystać wymiennie (rotacyjnie) lub kontynuując tematykę zajęć.

Link do e-książeczki: https://www.storyjumper.com/book/read/143158051/6368182d6eb64
Uwaga: książeczka zawiera nagrane teksty. Należy włączyć przycisk: „play" zatrzymując w odpowiednim miejscu.

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

dziurkacz, bilety wstępu na lekcję dla każdego ucznia, motek włóczki, tablica interaktywna, komputer, rzutnik, poziomowe karty pracy, 3 szt. toreb płóciennych, szablony – propozycja zał. 3, kredki i pisaki do materiału, plansza strzelnicy dla uczniów, wykałaczki dla każdego ucznia, karta ewaluacji dla nauczycieli, materiały papiernicze, kolorowe balony dla każdego ucznia.

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

I. WPROWADZENIE Klik i Enter zapraszają do przygody, by przełamać pierwsze lody!

Czynności nauczyciela: nauczyciel odtwarza nagranie z e-książeczki – str. 1 i dedykacja.
1. Neto Krok. Bilet wstępu na planetę Klika i Entera (czas: 5 min.)
Czynności nauczyciela: nauczyciel odtwarza nagranie z e-książeczki – str. 2.
UWAGA: uczniowie wykazujący umiejętności czytelnicze, mogą odczytywać na głos fragmenty tekstu.
Zgodnie z poleceniem Klika i Entera nauczyciel rozdaje każdemu uczniowi Bilet wstępu (zał. 1a – najłatwiejszy poziom trudności , 1b - średni, 1c - najtrudniejszy).
Czynności uczniów: uczniowie na podstawie rysunków na bilecie odgadują do jakiej planety zostali zaproszeni podczas lekcji. Po udzielonej odpowiedzi nauczyciel „kasuje" bilet dziurkując go.
Czynności nauczyciela: nauczyciel odtwarza nagranie z e-książeczki – str. 3.
Konkluzja: Witajcie na planecie Neti!

II. ROZWINIĘCIE
2. Neto Krok. W sieci - o rety! zabawa dydaktyczno-ruchowa - (czas: 5 min.)
Czynności nauczyciela: odtwarza nagranie z e-książeczki – str. 4.
Zgodnie z zadaniem wyznaczonym przez Klika i Entera, nauczyciel prosi uczniów o ustawienie się

w okręgu. Do środka okręgu wchodzi jeden uczeń.
Czynności uczniów: uczniowie wzajemnie podają sobie motek wełny zakręcając na palcu włóczkę przed jego podaniem. Zostaje utworzona sieć. Zadaniem ucznia w środku sieci jest wydostać się z niej niestosując przemocy. W omówieniu uczeń relacjonuje swoje samopoczucie będąc „uwięzionym" w sieci. Nauczyciel zwraca uwagę, że korzystając z Internetu również jesteśmy narażeni na niebezpieczeństwa, dlatego należy im przeciwdziałać.
Konkluzja: Czujny i uważny musi być każdy.

3. Neto Krok. *Co w sieci brzęczy i nas dręczy* – aktywne słuchanie e-książeczki i wykonanie ćwiczenia (czas: 10 min.)
Czynności nauczyciela: odtwarza nagranie z e-książeczki – str. 5.
a) *Wykonanie ćwiczeń na karcie pracy* (zał. 2a – najłatwiejszy poziom trudności , **2b** - średni, **2c** - najtrudniejszy); **b) *Prezentacja pracy przez uczniów.***
Czynności nauczyciela: odtwarza nagranie z e-książeczki – str. 6 i 7.
Konkluzja: Chroń siebie i innych.

4. Neto Krok: Sklepik Bezpiecznego Internetu – Twórcza Misja Ostrzegawcza – 15 min.
Czynności nauczyciela: odtwarza nagranie z e-książeczki – str. 8.
Prowadzący dokonuje podziału uczniów na 4 grupy (można przyjąć zasadę, w zależności od poziomu reprezentowanych przez uczniów umiejętności/predyspozycji/zainteresowań).
Czynności uczniów: uczniowie pracują w grupach kreatywnych wyzwań nt. przeciwdziałania przemocy internetowej wykonując: I gr.- tematyczne rysunki pisakami materiałowymi na torbach płóciennych; II gr.: Zakładki do książek; III gr.: breloczki na klucze; IV gr.: ulotki informacyjne – rysunkowo-słowne (najtrudniejszy poziom). **Propozycja zał. 3. Uwaga: gadżety zostaną rozdane seniorom ze środowiska lokalnego w ramach akcji cyberostrzegawczej.**
Konkluzja: Bądź świadomy zagrożeń w Internecie i uświadamiaj innych!

III. PODSUMOWANIE ZAJĘĆ

9. Neto Krok. „Milionerzy" – interaktywna gra sprawdzająca wiedzę uczniów (czas: ok. 5 min.).
Czynności nauczyciela: nauczyciel odtwarza nagranie z e-książeczki – str. 9.
Po wysłuchaniu nagrania zaprasza uczniów do gry podsumowującej wiedzę z zajęć (link: https://learningapps.org/display?v=put6329m322)
Czynności uczniów: uczniowie udzielają odpowiedzi na pytania w grze o milion.
Konkluzja: Wiedza znaczy najwięcej wtedy, kiedy potrafimy ją wykorzystać w życiu. To warte jest miliony!

10. Neto Krok. Spotkanie z Klikiem i Enterem na planecie Neti – rodzinne zadanie dla chętnych.
Czynności nauczyciela: nauczyciel odtwarza nagranie z e-książeczki – str. 10, następnie rozdaje kartki z zadaniem (zał. 4.)

IV. ZAKOŃCZENIE ZAJĘĆ

11. Neto Krok. Akcja plenerowa -Bezpieczni: w Chmury do góry! - aktywna przerwa (czas trwania przerwy – minimum 10 min.)
Czynności nauczyciela: odtwarza nagranie z e-książeczki – str. 11.

Nauczyciel rozdaje każdemu uczniowi nadmuchany balon. Uczniowie podpisują balon swoim nickiem /pseudonimem. Podczas przerwy śródlekcyjnej udają się z prowadzącym przed szkołę lub na boisko szkolne. Na znak nauczyciela wypuszczają balony do góry. **Prowadzący uświadamia, że od tej chwili korzystając z szerokiego świata wiedzy, zabawy i rozrywki w Internecie, muszą być czujni i ostrożni. Ich zadaniem jest troszczyć się o bezpieczeństwo swoje i innych.**
Czynności uczniów: uczniowie wypuszczają swoje balony wykrzykując równocześnie swój nick.

12. Neto Krok. *Strzelnic@* - ocena zainteresowania zajęciami (czas: 2 min.) Nauczyciel przyczepia na tablicy planszę **(zał. 5)**, celem dokonania przez uczniów oceny zainteresowania zajęciami.
Czynności uczniów: Zadaniem uczniów jest wbić wykałaczkę na kręgu Strzelnicy oceny (plansza), którego numer odpowiada ich zainteresowaniu zajęciami. (Cyfra 6 - zainteresowanie największe). Po wykonaniu zadania następuje przeliczenie „strzał".
Konkluzja końcowa: Zachowanie bezpieczeństwa w Internecie to strzał w dziesiątkę!
Na do widzenia: uczniowie otrzymują zawieszkę do umieszczenia nad biurkiem (zał. 6).
Uwaga: Nauczyciel dokonuje autooceny z przeprowadzonych zajęć. Propozycja szablonu – (zał.7).

PROPOZYCJA ĆWICZEŃ KONTYNUACYJNYCH LUB WYMIENNYCH:
- interaktywne:

https://www.jigsawplanet.com/?rc=play&pid=1335a7cca871 – puzzle interaktywne (obraz stanowi praca konkursowa ucznia: Żyj zdrowo, a komputer używaj z głową!). Dla ułatwienia używamy podkładu – „duszka" – ikonka: lewy dolny róg.
https://learningapps.org/display?v=pfdmydde522 – wyścig wiedzy (sugerowany: jeden gracz)
- problemowe:
- Tworzenie *Kodeksu Super Internauty – Savoir-vivre* (rysunek, opis);
- *W pokojach eksperckich:* uczniowie w grupach podejmują się udzielenia rad w sytuacji cyberprzemocy: I- obrażania, wyśmiewania; II-namawiania na spotkanie; III-wyłudzania pieniędzy lub danych osobowych.

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

- M. Górka, *Cyberbezpieczeństwo dzieci i młodzieży.* Realny i wirtualny problem polityki bezpieczeństwa, Wyd. Difin, Warszawa 2017
- P. Sajkowski, *Sieci@ki.pl - 2 - Stop cyberprzemocy*, Nasza Księgarnia, Fundacja Dzieci Niczyje, Warszawa 2008

Lista dodatkowych plików, będących integralną częścią scenariusza

LINKI DO ĆWICZEŃ INTERAKTYWNYCH:
https://www.storyjumper.com/book/read/143158051/6368182d6eb64 - link do autorskiej książeczki elektronicznej
https://learningapps.org/display?v=put6329m322 – gra interaktywna „Milionerzy"

ZAŁĄCZNIKI DO LEKCJI: (nr: 1-7)
Nr: 1-5 – wykorzystywane typowo na lekcji;
6 – „przypominajka ostrzegawcza"dla ucznia;
7 – Karta refleksji dla Nauczyciela
8 - Model wizualizacyjny lekcji

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Załączniki do lekcji

Zał. 1a

Zał. 1b

Zał. 1c

Zał. 2a

Otocz czerwoną pętlą rysunki z prawidłowymi podpisami zachowań internautów.

- Ufam każdej osobie piszącej do nas w Internecie.
- Wylogowuję się z komputera po zakończonej pracy.
- Ustalam łatwe hasło do komputera.
- Miło komentuję zdjęcia innych.
- Zawsze rozmawiam z rodzicami o tym, co mnie matwi.

Zał. 2b

Przyporządkuj do rysunków podpisy z prawidłowymi zachowaniami internautów.

- Ostrożnie zawieram znajomości w Internecie. Rozmawiam o tym z rodzcami.
- Wylogowuję się z komputera po zakończonej pracy.
- Ustalam trudniejsze hasło do komputera i zapamiętuję je.
- Nie przekazuję innym swojego hasła do komputera.
- Miło komentuję zdjęcia innych.

Zał. 2c

Uzupełnij zdania związane z bezpiecznym poruszaniem się w Internecie. Stwierdzenia ze znakiem zakazu rozpocznij od słowa NIE.

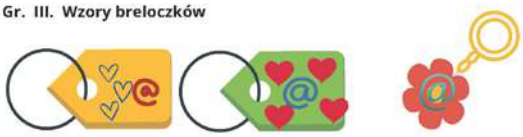
- ..... innym swojego hasła do komputera.
- W Internecie nie podaję danych osobowych takich jak: ....
- ..... komentuję zdjęcia innych osób.
- Jestem ..... podczas ..... nowych znajomości. Gdy coś mnie zaniepokoi .....
- ..... łatwego hasła do komputera.
- Używam programu: ..... chroniącego dane w komputerze.

Zał. 3 Propozycja szablonów

Gr. I. Wzory toreb

Gr. II. Wzory zakładek do książek

Gr. III. Wzory breloczków



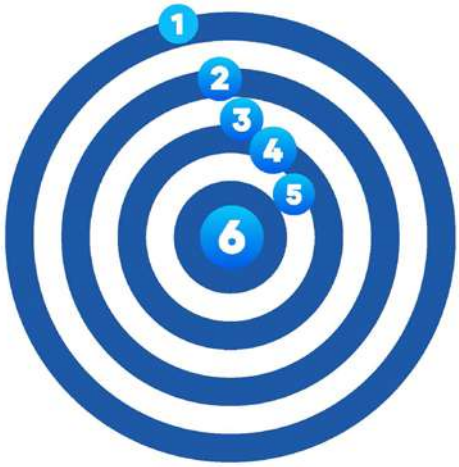
Gr. IV. Wzór ulotki informacyjnej

Zał. 4

Zadanie domowe dla chętnych od Klika i Entera

Jesteś autorem dalszej części naszej książeczki: "Klik i Enter z Neti - ciekawej planety". Na kartce z bloku narysuj swoje spotkanie oraz Twojej rodziny z Klikiem i Enterem na planecie Neti. Pracę możesz wykonać wspólnie ze swoją rodziną. Ustalcie nick dla każdego członka rodziny. Powodzenia!

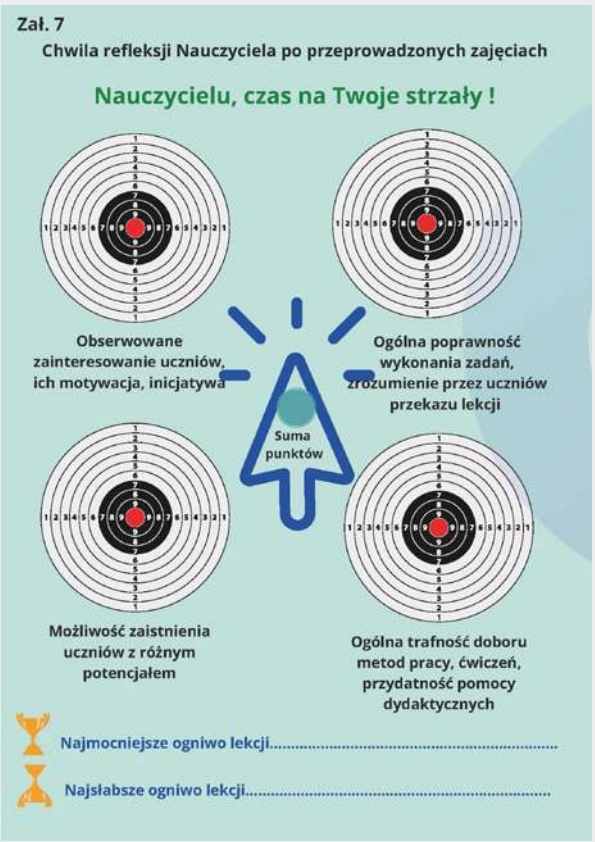
Zał. 5 Strzelnica oceny zainteresowania zajęciami



Zał. 6

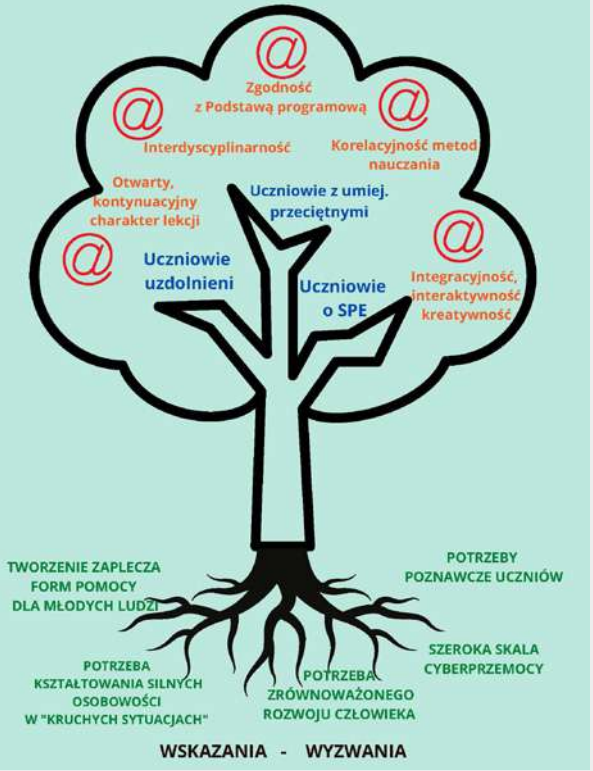
Zał. 7

Chwila refleksji Nauczyciela po przeprowadzonych zajęciach



Zał. 8

Model wizualizacyjny lekcji z zakresu cyberprzemocy



2. MIEJSCE

CYBERSAFE, CZYLI O BEZPIECZEŃSTWIE W INTERNECIE Z ESCAPE ROOMEM

autor: Marek Grzywna

Biografia Autora

Zwycięzca etapu globalnego AI Impact Shapers 2021, zwycięzca Global Principal Award 2022 dla najlepszych dyrektorów na świecie, zwycięzca Global Edu Leader 2021, wyróżniony (ex aequo 2 msc) w konkursie Nauczyciel Roku 2022, wykładowca MBA Szkoła Główna Krajowa, wykładowca Akademicki, trener, nauczyciel informatyki i biologii, dyrektor szkoły, superbelfer RP, finalista ogólnopolskiego konkursu Nauczyciel Jutr@, lider programu Mobilny Informatyk w wydawnictwie Operon, laureat Listy 100 2020 SPRUC, MIE Expert, pomysłodawca i współorganizator Ogólnopolskiego Projektu Emp@tyczna Klasa, trener regionalny i lokalny w projekcie Lekcja: Enter (ponad 1000 przeszkolonych nauczycieli!, grantobiorca w Centrum Mistrzostwa Informatycznego, coach programu Intel AI4Youth, laureat plebiscytu „Nauczyciel na Medal" pod patronatem Marszałka Woj. Kujawsko-Pomorskiego, "Przyjaciel SuperKoderów" Fundacji Orange, autor innowacyjnego programu zajęć w przyrodniczych „Science", lider programu #SuperKoderzy i Mega Misja, członek inicjatywy społecznej W.I.E.M zrzeszającej nauczycieli pasjonatów, koordynator projektu Lekcje w sieci, autor innowacyjnego programu „ZArdiunowani", uczestnik „Projektu z klasą", finalista ogólnopolskiego konkursu "Nauczyciel Jutr@" 2021.

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Pojęcie cyberbezpieczeństwa ze względu na swoją złożoność powinno omawiać się zwracając uwagę nie tylko na bezpieczeństwo w sieci, ale również kwestie dotyczące komunikacji, etyki oraz oprogramowania i licencji.

Scenariusz lekcji obejmuje wszystkie powyższe zagadnienia. Podczas lekcji wykorzystywane są innowacyjne metody nauczania oparte na WebQuescie i lekcji odwróconej. Zastosowanie pracy w grupie i elementów gamifikacji pozwala na rozwój kompetencji społecznych.

Zastosowane metody i formy pracy angażują uczniów do pracy. Natomiast nauczyciel pełni rolę mentora, obserwatora procesu.

Scenariusz oparty jest na filarach edukacji STEAM, połączenie wiedzy, technologii, inżynierii, sztuki i matematyki, co pozwala na lepsze zrozumienie złożonych zagadnień dotyczących cyberbezpieczeństwa w odniesieniu do świata określonego akronimem BANI (kruchym, niespokojnym, nieliniowym i niezrozumiałym).

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Podstawa programowa Informatyka klasy 7-8 V.1-V.3 Przestrzeganie prawa i zasad bezpieczeństwa:
Uczeń
1. opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją;
2. postępuje etycznie w pracy z informacjami;
3. rozróżnia typy licencji na oprogramowanie oraz na zasoby w sieci.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

Godziny wychowawcze, Informatyka.

Adresaci lekcji (wiek, klasa)

Uczniowie klas 7-8 (scenariusz można dostosować również dla klas 4-6 oraz uczniów szkół ponad-podstawowych).

Cel ogólny lekcji i cele szczegółowe

Cel ogólny:
Celem zajęć jest przedstawienie zagrożeń wynikających z korzystania z sieci Internet oraz przedstawienie działań, które chronią użytkownika sieci przed nimi.

Cele szczegółowe:
Uczeń:
- opisuje złożoność pojęcia cyberbezpieczeństwa
- potrafi opisać zagrożenia wynikające z korzystania z sieci Internet
- zna zasady bezpiecznego korzystania z Internetu
- wie jak reagować na przejawy hejtu
- rozpoznaje wirusy internetowe

Metody pracy

- Praca w grupach
- WebQuest z elementami Escape Roomu
- Gamifikacja
- Lekcja Odwrócona

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

1. Specjalnie przygotowana strona internetowa
https://sites.google.com/view/cyberniaki/strona-g%C5%82%C3%B3wna?authuser=0
2. Załącznik 1 Dla ucznia przed lekcją
3. ZAŁĄCZNIK 2 KARTA STARTOWA DLA GRUPY Escape room
4. ZAŁĄCZNIK 3 Odpowiedź KARTA STARTOWA DLA GRUPY Escape room
5. Załącznik 4 Dyplom dla ucznia
UWAGA: Wszystkie załączniki dostępne na stronie: https://sites.google.com/view/cyberniaki/nauczyciel/materia%C5%82y-do-pobrania-i-wydrukowania?authuser=0
Ograniczona możliwość dodania większej ilości załączników w formularzu.

6. Kolorowe karteczki- po 5 w danym kolorze (można zastąpić kartkami z wpisanymi cyframi, które będą wskazywać przynależność do grupy- 5 kartek z numerem 1, 5 kartek z numerem 2 itd.)
7. Karteczki samoprzylepne
8. Tablet lub telefon z dostępem do sieci- przynajmniej jeden na 5cio osobową grupę.
9. Czarny flamaster- przynajmniej jeden na grupę

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

Przed lekcją przekaż uczniom kartę z kodem QR do strony dla ucznia- **ZAŁĄCZNIK 1**
(Zadbaj o dostępność sartfona lub tabletu z dostępem do sieci- przynajmniej po 1 na grupę).
(ELEMENTY LEKCJI ODWRÓCONEJ)

Uczeń przed lekcją zapoznaje się z treściami dostępnymi na stronie
https://sites.google.com/view/cyberniaki/ucze%C5%84?authuser=0

Materiały dla nauczyciela dostępne są pod linkami:
Potrzebne materiały na lekcje:
https://sites.google.com/view/cyberniaki/nauczyciel/potrzebne-materia%C5%82y
Materiały do pobrania i wydrukowania
https://sites.google.com/view/cyberniaki/nauczyciel/materia%C5%82y-do-pobrania-i-wydrukowania

Część wstępna (5min):
Przed wejściem do klasy rozdaj losowo swoim uczniom karteczki w różnych kolorach.
Uczniowie siadają w grupach zgodnie z otrzymanym/wylosowanym kolorem kartki.
Sprawdź obecność, podaj temat lekcji: CybERsafe- czyli o bezpieczeństwie w internecie oraz omów cele lekcji.
Poinformuj uczniów, że podczas lekcji będziecie korzystać z przygotowanego escape roomu.

Część główna lekcji: (35min)
1. Przeprowadź z uczniami krótką dyskusję dotyczącą zagrożeń w Internecie. Wypiszcie je w widocznym miejscu **(10min)**:
Zagrożenia w Internecie
- Hejt
- Cyberprzemoc
- Niebezpieczne treści
- Hazard
- Kradzież danych osobowych
- Włamania komputerowe
- Wyłudzanie poufnych informacji
- Wirusy

2. Poinformuj uczniów, że od tej pory będą pracować metodą WebQuestu i pozyskiwać wiedzę z Internetu, która pozwoli Im rozwiązać zadania
3. Rozdaj uczniom "dziurawy kod QR z instrukcją", czarny flamaster, oraz kartę z zadaniami dla ucznia.
ZAŁĄCZNIK 2 KARTA STARTOWA DLA GRUPY Escape room

UWAGA- Uczniowie zamalowują kratki w kodzie czarnym flamastrem. W przypadku problemów nauczyciel może skorzystać z odpowiedzi
ZAŁĄCZNIK 3.
4. Uczniowie rozwiązują kolejne zadania. Poinformuj uczniów, że na wykonanie zadań mają **25 minut**.

Opis działań uczniów

- Uzupełnienie kodu QR: uczniowie rozwiązują 3 zadania:

Pierwsza cyfra do zamalowania wskazuje, w której połowie lutego odbywa się Dzień Bezpiecznego Internetu. Druga cyfra do zamalowania wskazuje na ilość liter "W" w skrócie najpopularniejszej z dostępnych usług w sieci Internet. Trzecia i zarazem ostatnia cyfra do zamalowania to iloczyn dwóch dwójek

- Po uzupełnieniu kodu qr, uczniowie skanują go za pomocą smartfona lub tabletu i przekierowani są na stronę, na której grają w grę Milioner. Pytania:

Pyt.1 Proces przekształcania informacji w taki sposób, że jej odczytanie nie jest możliwe bez znajomości tzw. klucza odszyfrującego to:
Odp1. Szyfrowanie
Pyt.2 Czym jest phishing?
Odp.2 Metoda oszustwa, w której przestępca podszywa się pod inną osobę
Pyt.3 Na czym zarabia twórca Adware?
Odp.3 Na reklamach
Pyt. 4 Malware to:
Odp.4 Złośliwe oprogramowanie
Pyt. 5 Błąd w oprogramowaniu, który ma wpływ na bezpieczeństwo jego użytkowania to
Odp.5 Luka
Pyt.6 Połączenie przez sieć VPN
Odp. 6 Umożliwia bezpieczne korzystanie z sieci wifi
Pyt.7 Czym się charakteryzuje shareware?
Odp.7. oprogramowanie zamknięte i bezpłatne
Pyt. 8 Która z tych licencji istnieje?
Odp. 8. Trial
Pyt. 9 Zaznacz informację fałszywą o GNU.
Odp. 9 GNU - Genius Private License
Pyt.10 Jakiego rodzaj phishingu nie występuje?
Odp.10 Virus phishing

Uczniowie wyszukują informację w sieci Internet - zgodnie z zasadą pracy metodą WebQuest.
Podsumowanie lekcji: **5 minut**
1. Ostatnim etapem pracy grup jest wypełnienie ankiety oceniającej lekcję https://sites.google.com/view/cyberniaki/ucze%C5%84/ankieta
2. Poproś uczniów, aby napisali na kartkach samoprzylepnych co im się podobało na lekcji i przyczepili do tablicy.
3. Na zakończenie lekcji przeczytaj odpowiedzi uczniów i zapytaj czego nauczyli się dzięki dzisiejszej lekcji.
Uwaga! Po zakończeniu pracy z Escape roomem uczeń otrzymuje dyplom do wydrukowania w wersji online. Nauczyciel może również wydrukować dyplomy (załącznik 4).

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

1. Paweł Tkaczyk, *Grywalizacja* Wydawnictwo OnePress, 2012
2. https://www.gov.pl/web/mswia/cyberbezpieczenstwo dostęp 29.10.2022
3. Sabina Furgoł, Lechosław Hojnacki, *Metoda Webquest Poradnik Nauczyciela*, Think- wirtualna biblioteka nowoczesnego nauczyciela

Lista dodatkowych plików, będących integralną częścią scenariusza

1. Specjalnie przygotowana strona internetowa https://sites.google.com/view/cyberniaki/strona-g%C5%82%C3%B3wna?authuser=0
2. Załącznik 1 Dla ucznia przed lekcją
3. ZAŁĄCZNIK 2 KARTA STARTOWA DLA GRUPY Escape room
4. ZAŁĄCZNIK 3 Odpowiedź KARTA STARTOWA DLA GRUPY Escape room
5. Załącznik 4 Dyplom dla ucznia

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".


PRZED LEKCJĄ
Czeka Cię niezwykła przygoda w świecie gry. Przed lekcją zapoznaj się z materiałami na stronie
https://tiny.pl/w9vqh


ESCAPE ROOM
Zamaluj odpowiednie cyfry, zeskanuj kod qr i przejdź dalej
Pierwsza cyfra do zamalowania wskazuje, w której połowie lutego odbywa się Dzień Bezpiecznego Internetu. Druga cyfra do zamalowania wskazuje na ilość liter "W" w skrócie najpopularniejszej z dostępnych usług w sieci Internet. Trzecia i zarazem ostatnia cyfra do zamalowania to iloczyn dwóch dwójek.

3. MIEJSCE
W KRAINIE NETUSI JESTEŚMY BEZPIECZNI

autorka: Edyta Korzeniowska

Biografia Autorki

Pedagog z 22-letnim stażem. Specjalizuje się w pedagogice wczesnoszkolnej, a także terapii ucznia ze specjalnymi potrzebami edukacyjnymi. Absolwentka Wyższej Szkoły Pedagogicznej w Krakowie na kierunkach: Pedagogika Specjalna i Przyroda oraz Akademii WSB w Dąbrowie Górniczej na kierunku Zintegrowana Edukacja Przedszkolna i Wczesnoszkolna. Pracuje jako nauczyciel edukacji wczesnoszkolnej, pedagog specjalny i surdopedagog. Z pasją i poświęceniem oddaje się swojej pracy podnosząc kompetencje w zakresie TIK oraz aktywnie uczestnicząc w sieciach współpracy i samokształcenia dla wychowawców klas I-III, nauczycieli szkolnictwa specjalnego oraz szkolnych specjalistów pracujących z dziećmi z niepełnosprawnościami. Z sukcesami przygotowuje uczniów do ogólnopolskich konkursów i sama bierze udział w konkursach dla nauczycieli. Jest zdobywcą głównej nagrody w ogólnopolskim konkursie dla nauczycieli na scenariusz zajęć o elektryczności, którego organizatorem był TAURON Dystrybucja S.A. Ponadto jest laureatką konkursu NBP na najlepszy scenariusz i realizację zajęć edukacyjnych pt. „Zanim wydam... O finansach w przedszkolach i szkołach". Jest także autorką zwycięskiego filmu krótkometrażowego z przebiegu lekcji zapoznającej uczniów z tematyką suszy i sposobami na jej przeciwdziałanie – organizatorem konkursu było Państwowe Gospodarstwo Wodne Wody Polskie. Uzyskała także trzecie miejsce, w organizowanym przez Fundację PFR, konkursie na scenariusz lekcji z zakresu cyberbezpieczeństwa. Uczniowie pracujący pod jej kierunkiem uzyskali wyróżnienie za makietę miasteczka Peronowo przygotowaną na konkurs „Kierunek – Bezpieczeństwo". Kocha przyrodę, dba o ekologię, pasjonuje się turystyką górską, jej poświęca każdą wolną chwilę i tą pasją stara się zarażać innych.

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Rzeczywistość, w której żyjemy staje się hybrydowa. Świat realny często miesza się z wirtualnym, a to co do tej pory odbywało się tradycyjnie – przeniosło się do Internetu. I choć zmianę tę odczuwamy wszyscy, w sposób szczególny musimy się skupić na dzieciach i młodzieży. Internet i sieć komórkowa stały się dla nich podstawową formą spędzania wolnego czasu. Pojawiły się również nowe wyzwania, takie jak m.in. zdalna edukacja. Niestety Sieć często jest także narzędziem agresji i przemocy, wzrosła liczba cyberataków i przestępstw. Wszystkie te okoliczności skłoniły mnie do opracowania scenariusza zajęć na temat cyberbezpieczeństwa, by minimalizować ryzyko zagrożeń związanych z korzystaniem z Internetu. Istotny jest również fakt, że lekcje o tej tematyce realizują jeden z podstawowych kierunków polityki oświatowej państwa w roku szkolnym 2022/23 oraz jeden z celów Strategii Cyberbezpieczeństwa RP na lata 2019-2024, którym jest wsparcie nauczycieli w realizacji podstawy programowej w obszarze bezpiecznego korzystania z nowoczesnych technologii.

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Podstawa programowa
Treści nauczania – wymagania szczegółowe:

I Edukacja polonistyczna
1. Osiągnięcia w zakresie słuchania. Uczeń:
1) Słucha z uwagą wypowiedzi nauczyciela, innych osób z otoczenia, w różnych sytuacjach życiowych, wymagających komunikacji i wzajemnego zrozumienia; okazuje szacunek wypowiadającej się osobie;
2) wykonuje zadanie według usłyszanej instrukcji; zadaje pytania w sytuacji braku rozumienia lub braku pewności zrozumienia słuchanej wypowiedzi;

V Edukacja plastyczna
1. Osiągnięcia w zakresie działalności ekspresji twórczej. Uczeń:
1) rysuje kredką, kredą, ołówkiem, patykiem (płaskim i okrągłym), piórem, węglem, mazakiem;

VII Edukacja informatyczna
1. Osiągnięcia w zakresie rozumienia, analizowania i rozwiązywania problemów. Uczeń:
3) rozwiązuje zadania, zagadki i łamigłówki prowadzące do odkrywania algorytmów.
2. Osiągnięcia w zakresie posługiwania się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi. Uczeń:
1) posługuje się komputerem lub innym urządzeniem cyfrowym oraz urządzeniami zewnętrznymi przy wykonywaniu zadania;
2) kojarzy działanie komputera lub innego urządzenia cyfrowego z efektami pracy zoprogramowaniem;
3) korzysta z udostępnionych mu stron i zasobów internetowych.
4.Osiągnięcia w zakresie rozwijania kompetencji społecznych. Uczeń:
1) współpracuje z uczniami, wymienia się z nimi pomysłami i doświadczeniami, wykorzystując technologię;
5. Osiągnięcia w zakresie przestrzegania prawa i zasad bezpieczeństwa. Uczeń:
1) posługuje się udostępnioną mu technologią zgodnie z ustalonymi zasadami;
2) rozróżnia pożądane i niepożądane zachowania innych osób (również uczniów) korzystających z technologii, zwłaszcza w sieci internetowej;
3) przestrzega zasad dotyczących korzystania z efektów pracy innych osób i związanych z bezpieczeństwem w Internecie.
zgodnie z podstawą programową z 2017 r.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

Edukacja informatyczna/ edukacja wczesnoszkolna

Adresaci lekcji (wiek, klasa)

uczniowie klas I-III

Cel ogólny lekcji i cele szczegółowe

Cel ogólny:
Zwiększenie świadomości na temat zagrożeń, na które jesteśmy narażeni w wirtualnym świecie.

Cele szczegółowe:
Uczeń :

- wie czym jest Internet i jakie korzyści z niego płyną,
- wymienia rodzaje zagrożeń w Internecie,
- zna zasady bezpiecznego poruszania się w cyberprzestrzeni,
- stosuje zasadę ograniczonego zaufania do osób poznanych w sieci,
- zna reguły Netykiety, podczas korzystania z Internetu,
- zna zagrożenia wynikające z nadmiernego korzystania z komputera, smartfona i tabletu.

Metody pracy

Gry dydaktyczno-interaktywne, w tym:

- samodzielnego dochodzenia do wiedzy – klasyczna metoda problemowa, burze mózgów
- asymilacji wiedzy – tekst audio, pogadanka
- metoda przypadków, gry dydaktyczne

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

- prezentacja multimedialna
- pliki dźwiękowe nr 1-12 z komentarzami Netusi, która jest bohaterką przewodnią,
- karty pracy nr 1-9
- ćwiczenia interaktywne: puzzle, krzyżówka, plątanina sylabowa, kodowanka, rozsypanka wyrazowa, łączenie zdań z odpowiadającymi im obrazkami, gram Milionerzy
- plakietki członków Klubu Netusi
- certyfikaty uczestnictwa w warsztatach „W Krainie Netusi”

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

Scenariusz został tak skonstruowany, aby sprawnie „prowadzić” nauczyciela przez poszczególne części lekcji i by był spójny narracyjnie. W tym celu przygotowano prezentację multimedialną oraz wprowadzono bohatea przewodniego – Netkę, która pomaga usystematyzować wiedzę z zakresu cyberbezpieczeństwa. Scenariusz umożliwia przeprowadzenie lekcji zarówno w formie stacjonarnej jak i zdalnej. Niemal wszystkie ćwiczenia zostały przygotowane w dwóch wersjach: w postaci tradycyjnych kart pracy oraz w formie narzędzi interaktywnych. Pod opisem każdego ćwiczenia w wersji papierowej znajduje się link do odpowiadającego mu ćwiczenia interaktywnego. Do nauczyciela prowadzącego zajęcia należy decyzja którą wersję ćwiczenia wykorzysta. W scenariuszu umieszczone są także linki do plików dźwiękowych, w których bohater przewodni Netka prowadzi przez kolejne etapy zajęć i zapoznaje uczniów z zasadami bezpiecznego zachowania w Internecie. Załączona prezentacja pomaga sprawnie przejść przez cały scenariusz.

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI”.

LINK DO PREZENTACJI MULTIMEDIALNEJ
https://view.genial.ly/62deb2071dec650011a97848/presentationcyberbezpieczenstwo

1. Wprowadzenie do tematu zajęć – układanie puzzli (5 min.)
Nauczyciel włącza PLIK NR 1:
https://drive.google.com/file/d/11hU_rlpzNJIEHLZkXvJ7XSjJ3qZqBxUJ/view?usp=sharing
Po wysłuchaniu nagrania nauczyciel rozdaje uczniom karty pracy nr 1 i prosi o rozwiązanie zadania.
KARTA PRACY NR 1 – puzzle
https://drive.google.com/file/d/1LvCod-xyB4H9AEv_na2N1vn4fA-C7Y0v/view?usp=sharing
Dzieci układają puzzle i głośno czytają rozwiązanie.
Rozwiązanie: Bądź bezpieczny w sieci.
Te same puzzle są dostępne w wersji elektronicznej.
LINK DO INTERAKTYWNYCH PUZZLI
https://www.jigsawplanet.com/?rc=play&pid=25ff3ac8e420

2. Krzyżówka - Chroń prywatność (5 min.)
Nauczyciel włącza PLIK NR 2:
Link do pliku dźwiękowego nr 2:
https://drive.google.com/file/d/1MrrSK14juTtJdmKcd5i_jvLkFwgxxwv8/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 2 i prosi o rozwiązanie krzyżówki.
KARTA PRACY NR 2 – krzyżówka
https://drive.google.com/file/d/1qVqAX4uWElU4tDluksPnEEbqlgvd9Jd0/view?usp=sharing
Nauczyciel po wykonaniu zadania sprawdza czy uczniowie poprawnie je wykonali. Wspólnie odczytują hasła w krzyżówce i rozwiązanie.
1. CZCIONKA 6. PLIK 11.LAPTOP
2. SŁUCHAWKI 7. FOLDER 12. MONITOR
3. DRUKARKA 8. MYSZKA 13. KOMPUTER
4. KURSOR 9. KLAWIATURA 14. ROZDZIELCZOŚĆ
5. BEZPIECZEŃSTWO 10. PŁYTA 15. SIEĆ
Hasło: CHROŃ PRYWATNOŚĆ
Ta sama krzyżówka jest dostępna w wersji elektronicznej.
LINK DO INTERAKTYWNEJ KRZYŻÓWKI
https://learningapps.org/display?v=p2hkyp2g322

3. Dopasowanie zdań do obrazków - Jak chronić prywatność? (5min.)
Nauczyciel włącza PLIK NR 3:
https://drive.google.com/file/d/13rWas5PLTqzpFtnkDvQe9054jN1oFR56/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 3 i prosi o dopasowanie zdań do obrazków.
KARTA PRACY NR 3 – łączenie w pary
https://drive.google.com/file/d/1NBggL_Lyfnr9wCXIuVAAEyf807u02ipc/view?usp=sharing
To samo ćwiczenie jest dostępne w wersji elektronicznej.
LINK DO INTERAKTYWNEGO ĆWICZENIA POŁĄCZ W PARY
https://wordwall.net/pl/resource/28133768
Dzieci dopasowują zdania do informacji na monitorach.
4. Plątaninka sylabowa - Zasada ograniczonego zaufania. (5 min.)
Nauczyciel włącza PLIK NR 4:

https://drive.google.com/file/d/1wImme7UHNuB00uyQisRA3bpdr9zm-PL5J/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 4 i prosi o rozwiązanie zadania.
KARTA PRACY NR 4 – plątaninka sylabowa
https://drive.google.com/file/d/1-vFV-LDQrSihbeEhEh-lQAy21pqFLAYu/view?usp=sharing
Dzieci głośno czytają rozwiązanie.
Rozwiązanie: Nie ufaj osobom poznanym w sieci!
To samo ćwiczenie jest dostępne w wersji elektronicznej.
LINK DO INTERAKTYWNEJ PLĄTANINKI SYLABOWEJ
https://view.genial.ly/61f57efbb021450012aefaec/presentation-zen-presentation

5. Kodowanka – Co zrobić, gdy coś nas zaniepokoi? (5 min.)
Nauczyciel włącza PLIK NR 5:
https://drive.google.com/file/d/10JB1HKyRQjSXTwkhQcd0Tq0xLQKd8Yhk/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 5 i prosi o odkodowanie hasła.
KARTA PRACY NR 5 – kodowanka
https://drive.google.com/file/d/1BaPlnsBV859cFwy4eVkAtPJxYKlsQlcQ/view?usp=sharing
Dzieci głośno czytają rozwiązanie.
Rozwiązanie: Mów, jeśli coś cię zaniepokoi!
Ta sama kodowanka jest dostępna w wersji elektronicznej.
LINK DO INTERAKTYWNEJ KODOWANKI
https://view.genial.ly/61f540c5ff07d7001933a00d/presentation-zen-presentation

6. Rebus – szacunek do innych. (4 min.)
Nauczyciel włącza PLIK NR 6:
https://drive.google.com/file/d/1PnDFpPsrJFt5SByYTh8TQmMbB5fbHs0c/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 6 i prosi o wykonanie rebusu.
KARTA PRACY NR 6 – rebus
https://drive.google.com/file/d/1zbNH8LI_qXswPvdGZwWPkiWp0QzYQy4R/view?usp=sharing
Dzieci głośno czytają rozwiązanie.
Rozwiązanie: Szanuj innych w sieci!

7. Rozsypanka wyrazowa – Zachowujemy umiar. (4 min.)
Nauczyciel włącza PLIK NR 7:
https://drive.google.com/file/d/1HjE406RjBQW2IxxMaJmr9yl35gHj_wkK/view?usp=sharing
KARTA PRACY NR 7 – rozsypanka wyrazowa
https://drive.google.com/file/d/1EudHLQI_pwYXtif03et3z0hmGzJ0h2LS/view?usp=sharing
Dzieci głośno czytają rozwiązanie.
Rozwiązanie: Zachowaj umiar korzystając z Internetu.
To samo ćwiczenie jest dostępne w wersji elektronicznej.
LINK DO INTERAKTYWNEJ ROZSYPANKI WYRAZOWEJ
https://wordwall.net/pl/resource/28133334

8. Plakat – zadanie domowe (2 min.)
Nauczyciel włacza PLIK NR 8:
https://drive.google.com/file/d/1ZF1-Nm5w2kMB9TCsKFNT1_4RwWBVt1MJ/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 8 i prosi o wykonanie w domu plakatu.
KARTA PRACY NR 8 – plakat
https://drive.google.com/file/d/1ZsseInhx67fMWrqI2K0a5KHrHFsKFf_J/view?usp=sharing
Dzieci zabierają karty pracy do wykonania w domu.

9. Podsumowanie wiadomości (5 min.)
Nauczyciel włącza PLIK NR 9:
https://drive.google.com/file/d/1ZF0QWi65B-qBT2zGARnbzcf_YdL6t8Cc/view?usp=sharing
Nauczyciel rozdaje uczniom karty pracy nr 9 i prosi o narysowanie buziek.
KARTA PRACY NR 9 – Czy przestrzegasz zasady bezpiecznego zachowania w Internecie?
https://drive.google.com/file/d/11Wv9R87iaz-fpEvLFsZMrUIh5F5E6H6f/view?usp=sharing
Dzieci uzupełniają karty pracy wesołymi lub smutnymi buźkami.

10. Założenie Klubu Netusi – wręczenie klubowych plakietek i certyfikatów. (4 min.)
Nauczyciel włącza PLIK NR 10:
https://drive.google.com/file/d/1ZColiPwee-5TMprACVDqRt8cvcxj_GkL/view?usp=sharing
Nauczyciel wręcza uczniom plakietkę (załącznik nr 1) i certyfikat (załącznik nr 2)
ZAŁĄCZNIK NR 1 – plakietka
https://drive.google.com/file/d/1cgmFbmKutU08sc5eQws_cmpEqq-bzFRe/view?usp=sharing
ZAŁĄCZNIK NR 2 – certyfikat
https://drive.google.com/file/d/1iPUFUYRWK0GK0Cv0I8H-wZDE-9bc8852/view?usp=sharing

11. Zakończenie zajęć (1 min.)
Nauczyciel włącza PLIK NR 11:
https://drive.google.com/file/d/1ZAZrT15czDRkPza2YXK9L9AWPgGKuDly/view?usp=sharing

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

1. Borkowska Anna, Cyberprzemoc. *Włącz blokadę na nękanie. Poradnik dla rodziców.*, Warszawa: NASK Państwowy Instytut Badawczy, 2019
2. Borkowska Anna, *Cyberprzemoc w szkole. Poradnik dla nauczycieli*, Warszawa: Nask Państwowy Instytut Badawczy, 2021
3. *Cyberbezpieczeństwo dzieci i młodzieży : realny i wirtualny problem polityki bezpieczeństwa* / red. Marek Górka. - Warszawa : Difin, 2017
4. *Cyfrowe dzieci : zjawisko, uwarunkowania, kluczowe problemy* / red. Mariusz Jędrzejko [et al.]. - Warszawa : Oficyna Wydawnicza ASPRA-JR ; Milanówek : Oficyna Wydawnicza von Velke, 2017

Lista dodatkowych plików, będących integralną częścią scenariusza

Karty pracy nr 1-9 oraz załączniki nr 1-2
- Prezentacja multimedialna

https://view.genial.ly/62deb2071dec650011a97848/presentation-cyberbezpieczenstwo

KARTA PRACY NR 1

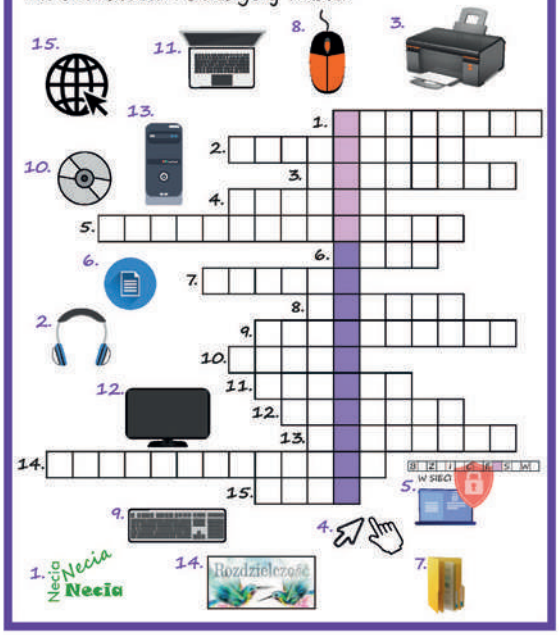
PUZZLE

Wytnij puzzle i ułóż obrazek, a dowiesz się o czym będziemy się uczyć na dzisiejszych warsztatach.

KARTA PRACY NR 2

Rozwiąż krzyżówkę.

Wpisz nazwy przedmiotów znajdujących się na obrazkach. Odczytaj hasło.



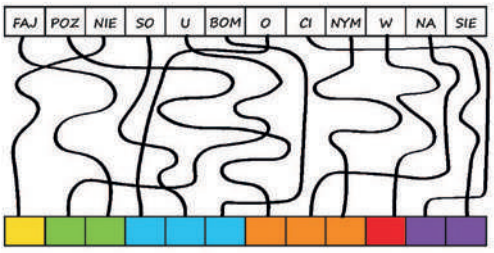
KARTA PRACY NR 3

Jak chronić swoją prywatność w Internecie?
Wytnij podpisy i wklej pod odpowiednimi obrazkami.

W adresie swojej poczty elektronicznej nie używaj własnego imienia i nazwiska.	Nie udostępniaj swojego numeru telefonu.	Nigdy nie podawaj adresu domowego.
Posługuj się nickiem.	Nie umieszczaj swoich zdjęć na profilach publicznych.	Nikomu nie zdradzaj swojego hasła internetowego.

KARTA PRACY NR 4

Ułóż plątaninkę sylabową,a poznasz kolejną zasadę bezpiecznego zachowania w Internecie.



Rozwiązanie:_____

_____

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

KARTA PRACY NR 5

Kodowanka

Odkoduj hasło poruszając się po planszy zgodnie z kierunkiem strzałek. Pierwsza litera znajduje się na pomarańczowym polu. Rozwiązanie zapisz pod strzałkami.

	A	B	C	D	E	F	G	H	I	J
1.	Z		B	Y	A	Ł	D	F	G	H
2.	M	O	R	S	T	U	E	A		I
3.	Ś	O	Y	T	I	D	E	H	Y	O
4.		T	E	M	A	Z	Ę	I	C	E
5.	T	Y	E	I	N	O		A	Ś	H
6.	H	O	P	A	D	H	M	Ś	O	Y
7.	D	K	T		Y	O	L	I	C	E
8.	Y	O	I	D	H	T	Ś	A	T	
9.	O	Ś	D	E	O	Y	E	J	W	D
10.		A	H	T	I	D	E	Y	Ó	M

KARTA PRACY NR 6

Rozwiąż rebus.

Rozwiązanie: _____

KARTA PRACY NR 7

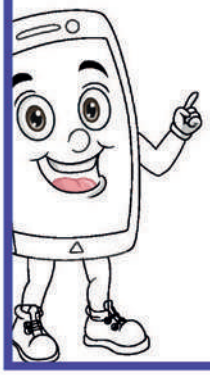
Rozsypanka wyrazowa

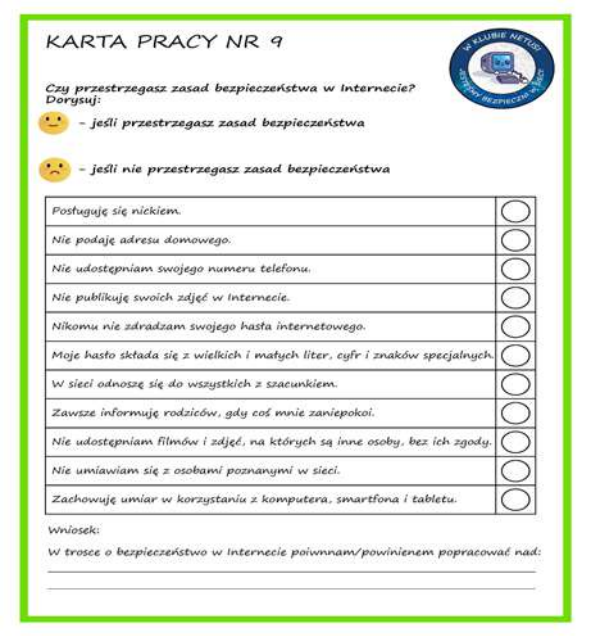
Wytnij i ułóż z rozsypanki zdanie, a poznasz kolejną zasadę korzystania z Internetu.

Internetu.	Zachowaj
korzystając	umiar
z	

KARTA PRACY NR 8

Plakat





KARTA PRACY NR 9

Czy przestrzegasz zasad bezpieczeństwa w Internecie? Dorysuj:

- jeśli przestrzegasz zasad bezpieczeństwa

- jeśli nie przestrzegasz zasad bezpieczeństwa

Posługuję się nickiem.	
Nie podaję adresu domowego.	
Nie udostępniam swojego numeru telefonu.	
Nie publikuję swoich zdjęć w Internecie.	
Nikomu nie zdradzam swojego hasła internetowego.	
Moje hasło składa się z wielkich i małych liter, cyfr i znaków specjalnych.	
W sieci odnoszę się do wszystkich z szacunkiem.	
Zawsze informuję rodziców, gdy coś mnie zaniepokoi.	
Nie udostępniam filmów i zdjęć, na których są inne osoby, bez ich zgody.	
Nie umawiam się z osobami poznanymi w sieci.	
Zachowuję umiar w korzystaniu z komputera, smartfona i tabletu.	

Wniosek:

W trosce o bezpieczeństwo w Internecie powinnam/powinienem popracować nad:

ZAŁĄCZNIK NR 1

Plakietka

CERTYFIKAT

Potwierdza udział ucznia

.....

w warsztatach

„W Krainie Netusi”.

Dziękujemy za udział w naszych zajęciach i życzymy bezpiecznego surfowania po Internecie.

Dyrektor szkoły

Wychowawca klasy

miejscowość, data

KOLEJNE WYZWANIA DLA BEZPIECZNEGO SERFOWANIA W SIECI

autorka: Grażyna Modrzewska

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Dzieci korzystają z sieci już od najmłodszych lat. Dostęp do sieci to szansa dla młodego człowieka na rozwój, która może jednak okazać się zagrożeniem. Statystyki pokazują, że ponad 60% dzieci w wieku od 6 miesięcy do 6,5 lat używa urządzeń mobilnych takich jak tablet czy smartfon, w tym 25% z nich codziennie. Dlatego warto zadbać o to, aby dzieci mogły korzystać z zasobów internetu w sposób bezpieczny (https://www.gov.pl/web/edukacja-i-nauka/cyberprzemoc--poradnik-dla-rodzicow).

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

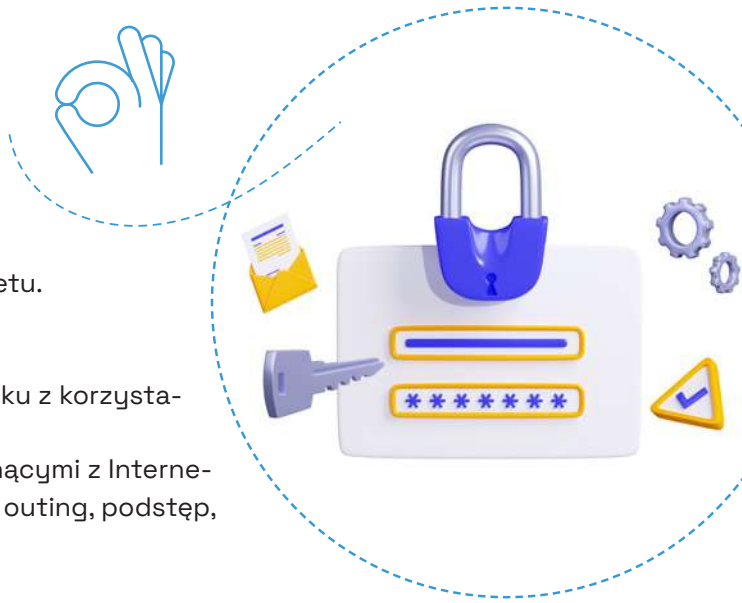
Celem kształcenia ogólnego Informatyki w klasach 6-8 szkoły podstawowej jest, m.in. :
- przestrzeganie prawa i zasad bezpieczeństwa,
- respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych. Treści podstawy programowej dotyczą klas 7-8/ Dział 5. Przestrzeganie prawa i zasad bezpieczeństwa. Uczeń: opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

Godzina wychowawcza, lekcja informatyki, zajęcia pozalekcyjne, zajęcia rewalidacyjne

Adresaci lekcji (wiek, klasa)

Uczniowie klasy 7-8



Cel ogólny lekcji i cele szczegółowe

Cel ogólny:
Promowanie zasad bezpiecznego korzystania z Internetu.

Cele szczegółowe:
- uczeń wie, jakie zagrożenia mogą go spotkać w związku z korzystaniem z sieci internetowej,
- uczeń wyjaśnia pojęcia związane z zagrożeniami płynącymi z Internetu (haker, hejter, cyberprzemoc, wykluczenie, nękanie, outing, podstęp, cyberstalking, fraping, maskarada, dissing, trolling)
- uczeń rozsądnie korzysta z zasobów sieci,
- uczeń korzysta z nowoczesnych technik pracy na lekcji, współpracuje w zespole.

Metody pracy

Podejście **STEAM**: gamifikacja, edukacja mobilna, gry interaktywne, zadania logiczne, elementy Metody WebQuestu - uczniowie rozwiązują problemy z wykorzystaniem bazy internetowej; Edukacja filmowa - kształtowanie kompetencji audiowizualnych oraz przygotowanie młodych ludzi do krytycznego tworzenia i odbioru mediów. Z wykorzystaniem aplikacji Flipgrid uczniowie stworzą własne filmiki odpowiadające na zadane pytanie;

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

Zadania Hakera (Kod Polibiusza do rozszyfrowania, zaszyfrowana wykreślanka, strony internetowe ukryte w kodach QR), smartfony lub tablety z zainstalowaną aplikacją do odczytywania kodów QR, aplikacja Kahoot; Quiz przygotowany w aplikacji Kahoot udostępniony w linku:
https://create.kahoot.it/creator/4fc90560-83d3-4f72-8397-f63004fe681b
Praca domowa z wykorzystaniem multimediów: https://flip.com/60ca5718; projektor, ekran lub tv

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

WPROWADZENIE
1. Nauczyciel informuje uczniów, że doszło do bardzo niepokojącej sytuacji, gdyż nieznany sprawca włamał się na do szkolnego i-Dziennika, pozmieniał w nim oceny oraz zamieścił tam zakodowane wiadomości. Trzeba jak najszybciej odczytać je, bo nie wiadomo co się w nich kryje. Nauczyciele nie wiedzą jak to zrobić, więc to uczniowie na dzisiejszych zajęciach mogą uratować sytuację.

2. Nauczyciel prosi uczniów o dobranie się w pary, którym przekazuje wyzwania do rozwiązania. Zaznacza, że dzisiejsze zajęcia wymagają szybkich działań, więc mogą korzystać z telefonów komórkowych i Internetu.

3. Uczniowie otrzymują Wyzwanie Hakera nr 1-zadanie zaszyfrowane za pomocą kodu Polibiusza. Gdy zespoły zgłaszają, że już odszyfrowali informację, nauczyciel pyta, jaki przekaz dostali od Hakera. Uczniowie podają: „Ktoś tu nawalił. Hasła bezpieczeństwa były za słabe, więc łatwo mogłem wkraść się do dziennika i pozmieniać oceny. Naprawcie to! Haker”

CZĘŚĆ ZASADNICZA
4. Podczas swobodnych wypowiedzi klasa interpretuje odczytaną informację. Nauczyciel pyta, czy wiedzą, jak się nazywa takie włamanie do cudzej własności w świecie cyfrowym. Uczniowie odpowiadają, że cyberprzemoc. My, jako użytkownicy Internetu, możemy jej przeciwdziałać. Chcąc zadbać o bezpieczeństwo w sieci, należy w jak największym stopniu utrudnić cyberprzestępcom proces rozszyfrowywania haseł, np. do systemu bankowości elektronicznej, poczty, routera czy sieci Wi-Fi.

5. Uczniowie podczas swobodnych wypowiedzi podają, o czym należy pamiętać podczas tworzenia haseł: przede wszystkim nie używać tych samych loginów i haseł w różnych miejscach sieci. Wyjątkowo łatwe do odgadnięcia są hasła w formie daty urodzenia, imienia czy innych krótkich słów. Znacznie więcej czasu zajmie hakerowi rozszyfrowanie hasła składającego się z wielu znaków – liczb, małych i wielkich liter oraz symboli specjalnych. W prosty sposób można je również utworzyć,

korzystając z darmowych generatorów online.
6. Każda para tworzy propozycję hasła do szkolnego I-Dziennika. Następuje prezentacja i ocena, które z nich jest najsilniejsze.

7. Nauczyciel pyta uczniów, czy włamanie Hakera do szkolnego I-Dziennika spowodowało, że zastanowili się na bezpieczeństwem korzystania z Internetu.

8. Znany nam Haker zostawił kolejną wiadomość, zapoznajcie się z nią. Uczniowie otrzymują Wyzwanie Hakera nr 2. W kodzie QR jest link do strony, na której wskazane są typy cyberprzemocy. Uczniowie swobodnie wypowiadają się, że istnieją różne rodzaje cyberprzemocy (wykluczenie, nękanie, outing, podstęp, cyberstalking, fraping, maskarada, dissing, trolling), ale wszystkie mają jeden cel – skrzywdzenie kogoś.

9. Nauczyciel dodaje, że zjawisko cyberprzemocy jest powszechne i może dotknąć każdego z nas. Może nawet większość z obecnych w tej sali już go doświadczyła. Ale wracamy do ratowania szkolnego dokumentu, bo nasz Haker nie odpuszcza. Niestety, dziennik dalej jest zablokowany, więc trzeba wykonać kolejne zadanie- Wyzwanie Hakera nr 3.

10. Uczniowie odczytują zaszyfrowane hasła poruszając się zgodnie z wytycznymi Hakera. Odczytują wyrazy: depresja, wycofanie, przygnębienie.

11. Nauczyciel pyta, co te słowa mogą oznaczać w kontekście omawianych problemów. Uczniowie w swobodnej rozmowie wyjaśniają, że tak mogą się czuć ofiary przemocy w sieci.

12. Nauczyciel mówi, Haker jeszcze chce od uczniów dalszej współpracy – Wyzwanie Hakera nr 4. Młodzież relacjonuje wrażenia po zapoznaniu się z materiałem o samobójstwach nastolatków, których dotknęła cyberprzemoc. Po wysłuchaniu odpowiedzi nauczyciel zauważa, że większość opisanych tutaj sytuacji dotyczy zagranicy, ale w Polsce również występują takie zdarzenia. Pyta uczniów, czy spotkali się w sieci z podobnymi sytuacjami? Uczniowie swobodnie się wypowiadają.

13. Zapytaj uczniów, czy potrafią nazwać, jaki typ cyberprzemocy dotknął bohaterów ich artykułów.

14. W otrzymanych materiałach przeczytali, do czego może doprowadzić stosowanie cyberprzemocy. Ważne jest, żeby nikt z nas nie stał się ani ofiarą ani prześladowcą w Internecie.

15. Znany nam już Haker najlepiej wie, ile nielegalnych rzeczy można zrobić w sieci. Dzisiaj z nami współpracuje, bo chce nas przestrzec, więc zobaczmy, co chce nam jeszcze przekazać. Zapoznajcie się z Wyzwaniem Hakera nr 5. Uczniowie za pomocą kodu QR znajdują właściwą stronę internetową, następnie identyfikując odpowiednie ikony zapoznają się z treściami na niej zamieszczonymi. Uzupełniają zdania brakującymi informacjami.

16. Po zakończeniu zadania uczniowie prezentują uzupełnione zdania. Następuje krótka dyskusja na temat hejtu, netykiety, udostępniania danych w Internecie oraz szukania pomocy w przypadku poczucia zagrożenia płynącego z sieci.
ZAKOŃCZENIE ZAJĘĆ

17. Nauczyciel prosi zespoły o otwarcie strony Kahoot. Uruchomia grę tak, żeby była widoczna na dużym ekranie, np. ekranie, telewizorze poprzez link: https://create.kahoot.it/creator/4fc90560-83d3-4f72-8397-f63004fe681b. Żeby rozpocząć grę należy zaznacz na ekranie, że chce się grę kontynuować jako gość, w wersji klasycznej. Zostanie wygenerowany kod PIN dla danej gry. Uczniowie wpisują go na swoich urządzaniach w aplikacji Kahoot. Zespoły muszą podać także swoje pseudonimy. Nauczyciel klika „początek", wtedy rozpoczyna się quiz. Polega na szybkim wybraniu właściwej odpowiedzi spośród zaproponowanych. Uczniowie w aplikacjach na swoich urządzeniach klikają dany kolor. Mają 30 sekund na podanie każdej odpowiedzi. Po każdym pytaniu pojawia się ranking (punktowany jest czas i poprawność odpowiedzi). Po przejściu przez wszystkie pytania pojawia się lista zwycięzców – załącznik nr 1 (screen gry Kahoot).

18. Nauczyciel zauważa, że młodzież świetnie poradziła sobie z pokonaniem Hakera. I-Dziennik został odkodowany, a oceny przywrócone. Nagrodź uczniów, którzy poradzili sobie z quizem i zadaniami. Podziękuj za udział i zachęć do zagłębienia się w problematykę bezpieczeństwa w sieci, bo dotyczy ona każdego użytkownika Internetu.

19. Zachęć młodzież do wykonania multimedialnej pracy we Flipgrid, znanym jako narzędzie do zadawania pytań i nagrywania wypowiedzi ustnych w formie wideo.

20. Podaj uczniom link do strony https://flip.com/60ca5718 oraz hasło dla gościa: Bezpieczniwsieci. Po wejściu na stronę uczniowie muszą nagrać w aplikacji video odpowiedź. Na następnych zajęciach zapoznamy się z treścią powstałych materiałów.

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

https://virtualmich.com/pl/co-to-jest-cyberprzemoc-learn-types-examples-and-scales/#Typy_cyberprzemocy
https://sieciaki.pl/warto-wiedziec/porady
https://www.gov.pl/web/edukacja-i-nauka/cyberprzemoc--poradnik-dla-rodzicow
https://pixabay.com/pl/

Lista dodatkowych plików, będących integralną częścią scenariusza

Wyzwanie Hakera nr 1
Wyzwanie Hakera nr 2
Wyzwanie Hakera nr 3
Wyzwanie Hakera nr 4
Wyzwanie Hakera nr 5w
Załącznik nr 1- Screeny quizu w Kahoot
Załącznik nr 2- Screen filmu we Flipgrip

WYZWANIE HAKERA NUMER 1

W II w. p.n.e. grecki pisarz Polibiusz wymyślił stosowany do dziś sposób szyfrowania. Spróbujcie go rozkodować, żeby odczytać moją wiadomość – podpowiadam, że na pewno przyda Wam się umiejętność korzystania z tabliczki mnożenia.

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	Ć	G	H	I	K	Ń
3	L	Ę	M	N	O	Ł
4	P	R	S	T	U	Ś
5	Ż	W	Ą	Y	Z	Ó

Myśl zapisana szyfrem:

25-44-35-46	44-45	34-11-52-11-31-24-36	
23-11-43-36-11	12-15-55-41-24-15-13-15-26-43-44-52-11		
12-54-36-54	55-11	43-36-11-12-15	52-24-32-13
36-11-44-52-35	33-35-22-36-15-33	52-25-42-11-46-21	
43-24-32	14-35	14-55-24-15-34-34-24-25-11	
24	41-35-55-33-24-15-34-11-21	35-13-15-34-54	
34-11-41-42-11-52-13-24-15		44-35	23-11-25-15-42

Rozwiązanie dla prowadzącego: W II w. p.n.e. grecki pisarz Polibiusz wymyślił stosowany do dziś sposób szyfrowania. Ułożył litery w kwadrat, a rzędy i kolumny ponumerował. Numer kolumny i wiersza, czyli współrzędne, kodowały konkretną wiadomość: **Ktoś tu nawalił. Hasła bezpieczeństwa były za słabe, więc łatwo mogłem wkraść się do dziennika i pozmieniać oceny. Naprawcie to! Haker**

Wyzwanie Hakera nr 2

Do czego służą te figurki ????
Pokombinujcie, może do czegoś dojdziecie. Powodzenia!
Ha ha ha ha……..

Wyzwanie Hakera nr 3

Poserfujcie sobie, tym razem po tabeli… Odczytane wyrazy niech was skłonią do refleksji. A jak je odczytać? Pomyślcie trochę, musicie sobie radzić:)

Wasz Haker

P	S	T	E	M	A	Ż	E	K	L	I	D	E
O	T	E	Y	R	F	G	Z	E	H	K	L	S
S	W	N	I	Y	O	B	V	C	A	I	N	O
O	C	T	G	Ę	L	O	R	M	Ó	H	F	S
B	W	M	E	T	M	S	A	G	H	L	E	J
R	P	U	Z	E	F	S	A	Ę	C	B	K	I
D	S	L	Ż	S	Ż	➡	L	O	S	D	Ł	R
C	V	I	Ś	A	O	B	N	I	W	Q	L	E
T	Y	S	Z	G	N	B	W	E	U	M	W	S
E	H	R	Y	C	Ó	M	K	S	V	Ń	E	I
W	U	M	L	N	Z	F	A	D	U	K	A	E
R	T	B	J	P	O	Ę	G	Ż	S	E	W	Y
I	N	W	G	S	Ą	Ż	F	N	L	O	N	T

PRZESUŃ SIĘ :

Wyraz 1
- 4 pola na wschód
- 5 pól na południe
- 6 pól na zachód
- 10 pól na północ
- 4 pola na wschód
- 4 pola na wschód
- 3 pola na południe
- 5 pól na zachód

Wyraz 2
- 4 pola na południe
- 6 pól na zachód
- 5 pól na północ
- 5 pól na wschód
- 7 pól na południe
- 5 pól na wschód
- 8 pól na północ
- 8 pól na zachód
- 2 pola na północ

Wyraz 3
- 3 pola na zachód
- 5 pól na południe
- 3 pola na wschód
- 4 pola na południe
- 3 pola na południe
- 5 pól na wschód
- 7 pól na północ
- 2 pola na wschód
- 5 pól na północ
- 3 pola na zachód
- 7 pól na południe
- 5 pól na zachód
- 6 pól na północ

Rozwiązanie dla prowadzącego zajęcia:
depresja, wycofanie, przygnębienie

WYZWANIE HAKERA NR 4

WYZWANIE HAKERA NR 4

Grupa 1

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

"Olka ona jest oblesna, jedzie jej z gęby" - taką opinię o sobie przeczytała na popularnym portalu społecznościowym Grono.pl 12-letnia Ola, uczennica jednej z podwarszawskich podstawówek. Dziewczynka jest typową ofiarą internetowej przemocy. Zaczęło się niewinnie: od śmiechu i szeptów, gdy odpowiadała przy tablicy. Wkrótce trzy klasowe prowodyrki drwiły z niej otwarcie: "Jesteś ohydna, śmierdzisz". Jeszcze później nękanie przeniosło się do sieci. Nauczyciele o niczym nie widzieli, a Ola bała się mówić. Prawdę wyciągnęli z niej rodzice, których zaniepokoiło, że córka ciągle narzeka na ból brzucha i nie chce chodzić do szkoły. Okazało się, że jest przerażona, bo jedna z koleżanek zagroziła, że wytnie jej twarz z klasowego zdjęcia, przyklei do fotografii o charakterze pornograficznym i zamieści na portalu razem z komentarzem, że właśnie tym Ola zajmuje się po lekcjach.

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku.

WYZWANIE HAKERA NR 4

Grupa 2

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

Koledzy lubili wyśmiewać się z 13-letniego Ryana z Vermont (USA). Szczególnie zabawne wydawało się im pisanie w Internecie, że jest gejem. Z pewnością chłopak był przeszczęśliwy, kiedy piękna i popularna koleżanka o imieniu Ashley nagle zaczęła prowadzić z nim romantyczne rozmowy w Internecie. On dzielił się z nią swymi przemyśleniami i doświadczeniami, ona przesyłała kolegom najzabawniejsze cytaty - to było celem fałszywego romansu. Korespondencja trwała całe lato. Jesienią Halligan przyszedł do szkoły i dziewczyna powiedziała mu, że jest nieudacznikiem. Na początku października 2003 roku, wczesnym rankiem, podczas gdy jego rodzice spali, chłopiec powiesił się w łazience. Jego ciało zostało znalezione przez starszą siostrę.

Ostatni raz Ryan w Internecie korespondował z byłym kolegą z podstawówki. Napisał mu, że chce skończyć ze sobą. Znajomy odpisał: "Pffff...., dawno już trzeba było to zrobić".

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

WYZWANIE HAKERA NR 4
Grupa 3

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

Znajomy z sieci namówił Amandę do pokazania piersi w trakcie wideoczatu. Zrobił screeny i zaczął rozpowszechniać je w Internecie. Dziewczyna próbowała uciec przed swym prześladowcą, ale on zawsze znajdował jej konta na portalach społecznościowych. Udawał kompletnie inną osobę, starał się, by dodała go do znajomych i znów psuł jej opinię wśród znajomych i nieznajomych. Amanda próbowała walczyć. W październiku 2012 roku nagrała filmik wideo opowiadając swoją historię. Filmik obejrzano 17 milionów razy, ale wsparcie publiczności nie pomogło. Mniej niż miesiąc po publikacji filmiku w sieci dziewczyna powiesiła się. Sprawcę tragedii udało się odnaleźć w Holandii. Okazał się nim 35-letni mężczyzna, który miał niezwykłe hobby - próbował nakłonić obce mu osoby (również chłopaków) z USA, Wielkiej Brytanii i Holandii do rozebrania się na czacie wideo, a następnie nękał je w Internecie.

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

WYZWANIE HAKERA NR 4
Grupa 4

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

14-letnia Megan Meier (USA) była pewna, że jest brzydka, gruba i bezużyteczna. Kilka tygodni przed śmiercią na portalu MySpace dodał ją do przyjaciół pewien chłopak - Josh Evans. Przez pewien czas miło sobie korespondowali, ale wkrótce Josh wyrzucił ją ze znajomych i zaczął pisać jej bardzo przykre rzeczy. Następnie przyłączyli się do zabawy jego inni wirtualni znajomi. Ostatnią wiadomością wysłaną przez Josha, którą Megan odczytała było: "Świat byłby lepszy bez ciebie". Dziewczyna wyłączyła komputer, a 20 minut później powiesiła się w garderobie, gdzie znalazła ją jej matka. Po pewnym czasie rodzice Megan dowiedzieli się, że Josh nigdy nie istniał. Jego profil, dla zabawy, stworzyły trzy kobiety: sąsiadka rodziny Meierów, jej córka oraz podwładna.

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

WYZWANIE HAKERA NR 4
Grupa 5

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

W wieku 18 lat, Amerykanka Jessica Logan wykazała się głupotą - wysłała swoje zdjęcie nago młodemu mężczyźnie poznanemu w sieci. Chłopak rozesłał zdjęcie dziewczyny jej kolegom z klasy. Licealiści z kilku miejscowych szkół zalali Jessicę obraźliwymi wiadomościami na Facebooku i MySpace, a także pisali jej przykre SMS-y. Doszło do tego, że dziewczyna bała się chodzić do szkoły. Jessica wystąpiła w lokalnej telewizji, gdzie opowiedziała o szykanowaniu. Nikt nie czuł wyrzutów sumienia. Dwa miesiące później, kiedy wróciła z pogrzebu znajomego, dziewczyna powiesiła się w swojej sypialni.

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

WYZWANIE HAKERA NR 4
Grupa 6

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

Hope miała tylko 13 lat, kiedy chłopak, który jej się podobał, poprosił ją o przesłanie mu zdjęcia jej piersi. Ma się rozumieć, wkrótce zdjęcie zobaczyły setki ciekawskich dzieci w wieku szkolnym, a na MySpace pojawiła się strona "Ludzie, którzy nienawidzą Hope". Na szkolnych korytarzach przyjaciele bronili Hope przed docinkami, ale nie miała jak uciec od szykan w internecie. Dziewczyna bała się powiedzieć rodzicom o przyczynie mobbingu. Powiesiła się w swoim pokoju. Tuż przedtem napisała w swym dzienniku: "Jestem gotowa. Czuję to w środku. Postaram się powiesić. Mam nadzieję, że się uda"

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

WYZWANIE HAKERA NR 4
Grupa 7

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

17-letniemu Szkotowi, Danielowi Perry'emu, anonimowi użytkownicy wielokrotnie podpowiadali, by się zabił. Może nie doszłoby do tragedii, gdyby Daniel nie dał się namówić na rozmowę na czacie wideo na Skype. "Dziewczyna" z którą rozmawiał, chciała zobaczyć go nago. Spełnił "jej" prośbę. Następnie zaczęto domagać się od Daniela pieniędzy za to, by screeny z rozmowy nie zostały rozpowszechnione w Internecie. Daniel odebrał sobie życie skacząc z mostu.

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

WSKAZÓWKA HAKERA NR 4
Grupa 8

Jestem Hakerem i potrafię wiele zrobić w Internecie, dotrzeć w nim do miejsc dla innych niedostępnych. Zobaczcie jednak, ile złego może się stać, jeśli tzw. „zwykli ludzie" bezmyślnie piszą w sieci o innych, zamieszczają o nich różne materiały, zdjęcia.

Gdyby młoda Chinka wiedziała, co ją czeka, nigdy nie przekroczyłaby progu małego sklepu z odzieżą. Kilka dni później okazało się, że właściciele sklepu napisali o niej na swoim blogu, nazywając ją złodziejką. Wkleili jej zdjęcie z kamery i poprosili internautów, by zebrali informacje o dziewczynie. Było wielu chętnych. Wkrótce wszystkim znane były jej dane włącznie z adresem. Kiedy pogłoski o kradzieży dotarły do szkoły, dziewczyna zwolniła się z zajęć, poszła w stronę rzeki i skoczyła z mostu.

To przykład tragicznie zakończonej cyberprzemocy. Wejdź na stronę ukrytą w kodzie QR i spróbuj określić jaki typ cyberprzemocy został zastosowany w danym przypadku:

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

WYZWANIE HAKERA NR 5

Nie mogę przekazywać informacji oficjalnie, więc są zakodowane. Teraz czas na wycieczkę w nowym wydaniu, bo wirtualną. Szybko możecie zdobyć niezwykłe wiadomości. Udajcie się do miejsca, które wskaże wam język Internetu za pomocą kodów QR

Przeczytajcie treści ukryte na stronach oznaczonych ikonkami. Wykorzystacie je do uzupełnienia zdań oraz quizu:

Osoby, które tworzą w sieci nienawistne, obraźliwe wpisy, nazywamy .....

W adresie swojej poczty elektronicznej nie używaj .....

Jeśli publikujesz w ....., zadbaj, by widzieli je tylko Twoi znajomi.

Pamiętaj, że ..... z kim rozmawiasz w Internecie.

Zasady jak zachowywać się w Internecie to .....

Odpowiedzi dla prowadzącego zajęcia:

1. Osoby, które tworzą w sieci nienawistne, obraźliwe wpisy, nazywamy hejterami.
2. W adresie swojej poczty elektronicznej nie używaj własnego imienia i nazwiska (imie.nazwisko@sieciaki.pl).
3. Jeśli publikujesz w sieci swoje zdjęcia, zadbaj, by widzieli je tylko Twoi znajomi.
4. Pamiętaj, że nigdy nie możesz mieć pewności, z kim rozmawiasz w Internecie. Ktoś, kto podaje się za Twojego rówieśnika, w rzeczywistości może być dużo starszy i mieć wobec Ciebie złe zamiary.
5. Zasady jak zachowywać się w Internecie to Netykieta.

ZAŁĄCZNIK NR 1

SCREENY QUIZU

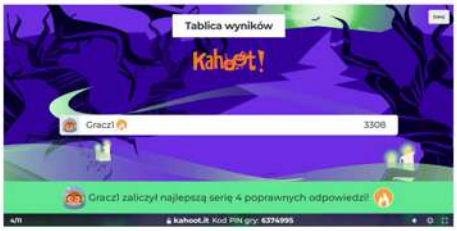
1. Uruchom grę tak, żeby była widoczna na dużym ekranie, np. tablicy multimedialnej, telewizorze poprzez link:

https://create.kahoot.it/creator/4fc90560-83d3-4f72-8397-f63004fe681b

Zaznacz na ekranie, że chcesz grę kontynuować jako gość, w wersji klasycznej. Otrzymasz kod PIN wygenerowany dla danej gry. Daj uczniom PIN i poproś ich o wpisanie go na swoich urządzeniach w aplikacji Kahoot. Uczniowie muszą podać także swoje pseudonimy. Kliknij „początek", wtedy rozpocznie się gra. Gra polega na szybkim wybraniu właściwej odpowiedzi spośród zaproponowanych. Uczniowie w aplikacjach na swoich urządzeniach klikają dany kolor. Mają 30 sekund na podanie każdej odpowiedzi. Po każdym pytaniu pojawia się ranking, punktowany jest czas i poprawność odpowiedzi. Po przejściu przez wszystkie pytania pojawia się lista zwycięzców.


Zasady jak zachowywać się w Internecie to:
17
Etykieta
Netykieta
Savoir-vivre
Kulturokieta
kahoot.it Kod PIN gry: 6374995

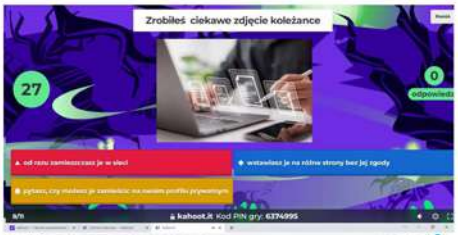

Zasady jak zachowywać się w Internecie to:
Etykieta
Netykieta
Kulturokieta
kahoot.it Kod PIN gry: 6374995


Tablica wyników
Kahoot!
Gracz1
3308
Gracz1 zaliczył najlepszą serię 4 poprawnych odpowiedzi!
kahoot.it Kod PIN gry: 6374995


Cyberprzemocą nie jest:
28
wykluczanie ofiary w mediach
sexting
cyberstalking
mobbing
kahoot.it Kod PIN gry: 6374995


Bezpieczne hasło w Internecie powinno składać się
25
co najmniej 7 różnych znaków
najwyżej z 8 znaków
samych cyfr
kahoot.it Kod PIN gry: 6374995

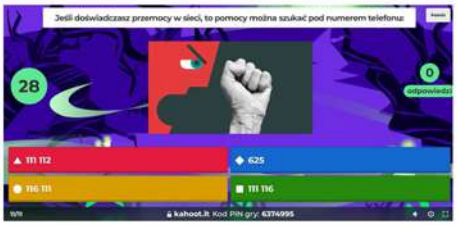

Które z tych haseł jest najbezpieczniejsze
23
kotek4
Kotek!!111
kotek123!
koTek!!791
kahoot.it Kod PIN gry: 6374995


Zrobiłeś ciekawe zdjęcie koleżance
27
kahoot.it Kod PIN gry: 6374995


Zrobiłeś ciekawe zdjęcie koleżance
27
kahoot.it Kod PIN gry: 6374995

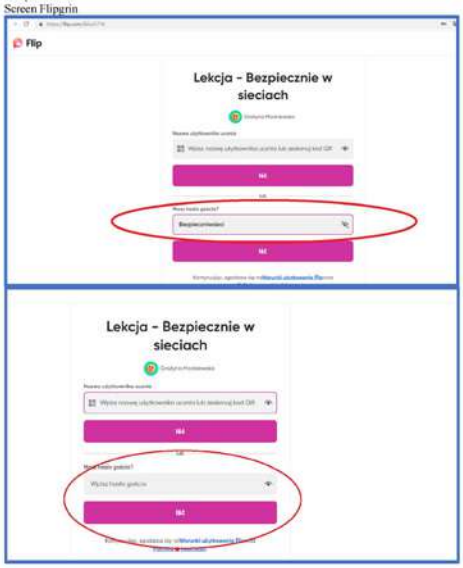

Cyberprzemoc jest przestępstwem.
16
Prawda
Fałsz
kahoot.it Kod PIN gry: 6374995


Cyberprzemoc nie odbywa się za pośrednictwem
mediów społecznościowych
poczty elektronicznej
listu na kartce papieru
kahoot.it Kod PIN gry: 6374995


Jeśli doświadczasz przemocy w sieci, to pomocy można szukać pod numerem telefonu:
28
111 112
625
116 111
111 116
kahoot.it Kod PIN gry: 6374995


Bezpieczeństwo w sieci
Gracz1
kahoot.it Kod PIN gry: 6374995

Załącznik nr 2
Screen Flipgrin



WSKAŹNIKI KWASOWO – ZASADOWE W SOCIAL MEDIACH

autorka: Magdalena Ankiewicz - Kopicka

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Proponowany scenariusz dotyka treści z zakresu cyberzagrożeń wynikających z korzystania z social mediów. Mózg lubi niespodzianki, dlatego nieoczywiste połączenie lekcji chemii z lekcją informatyki może spowodować większe zainteresowanie poruszaną podczas zajęć tematyką i skłonić młodzież do głębszej refleksji.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Cele kształcenia – wymagania ogólne z podstawy programowej przedmiotu chemia
uczeń:
- pozyskuje i przetwarza informacje z różnorodnych źródeł z wykorzystaniem technologii informacyjno – komunikacyjnych;
- stosuje poprawną terminologię.
Treści nauczania – wymagania szczegółowe z podstawy programowej

IV Roztwory i reakcje w roztworach wodnych - uczeń:
7) klasyfikuje substancje jako kwasy lub zasady zgodnie z teorią Brønsteda-Lowry'ego; wskazuje sprzężone pary kwas – zasada;
8) uzasadnia przyczynę kwasowego odczynu wodnych roztworów kwasów, zasadowego odczynu wodnych roztworów niektórych wodorotlenków (zasad) i amoniaku oraz odczynu niektórych wodnych roztworów soli zgodnie z teorią Brønsteda-Lowry'ego; pisze odpowiednie równania reakcji.
Cele ogólne powiązane z podstawą programową Informatyka

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. Uczeń:
4) bezpiecznie buduje swój wizerunek w przestrzeni medialnej;

V. Przestrzeganie prawa i zasad bezpieczeństwa. Uczeń:
1) postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

chemia / informatyka

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Adresaci lekcji (wiek, klasa)

1 lub 2 klasa liceum ogólnokształcącego (14,15,16 lat)

Cel ogólny lekcji i cele szczegółowe

Charakterystyka wskaźników zasadowo – kwasowych połączona z popularyzacją wiedzy z zakresu bezpieczeństwa w cyberprzestrzeni.
Uczeń:

- podaje przykłady wskaźników pH i omawia ich zastosowanie;
- definiuje pojęcie kwasu, zasady i soli wg teorii Arrheniusa;
- zapisuje równania reakcji dysocjacji kwasów, zasad i soli;
- dokonuje klasyfikacji substancji na elektrolity i nieelektrolity,
- posługuje się językiem i terminami chemicznymi;
- definiuje pojęcie „cyberprzemocy";
- zna formy cyberprzemocy i jej konsekwencje;
- wie, czym jest cyfrowy ślad;
- zna sposoby zapobiegania zagrożeniom internetowym;
- wykorzystuje technologie informacyjno-komunikacyjne w wyszukiwaniu i selekcji informacji;
- aktywnie uczestniczy w dyskusji.

CYBER BEZPIECZNI

Metody pracy

- pogadanka;
- ćwiczenia interaktywne;
- moderacja wizualna.

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

- projektor / tablica interaktywna;
- link do kartki z zadaniem do wykonania przed lekcją: http://iwishyouto.com/view/32f305179afc5cc7;
- ćwiczenie wisielec: https://learningapps.org/watch?v=p3moe115k21;
- ćwiczenie – wykreślanka: https://learningapps.org/watch?v=pwnsgeno321;
- prezentacja np. PowerPoint;
- tablety szkolne lub smartfony uczniów (opcjonalnie szary papier i markery dla grup);
- karteczki z nazwami wskaźników do losowania;
- karty charakterystyk wybranych wskaźników zasadowo – kwasowych;
- ćwiczenie wykreślanka: https://learningapps.org/watch?v=ppdsqnyo322.

0110
1010
0101

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

Przed zajęciami:
Nauczyciel wysyła kartkę (np. przy użyciu dziennika elektronicznego) z zadaniem do wykonania przed kolejną lekcją: http://iwishyouto.com/view/32f305179afc5cc79 (slajd nr 1). Uczniowie mają przygotować sobie herbatę, a następnie dodać do niej cytrynę, zapisać obserwacje i sformułować wnioski.

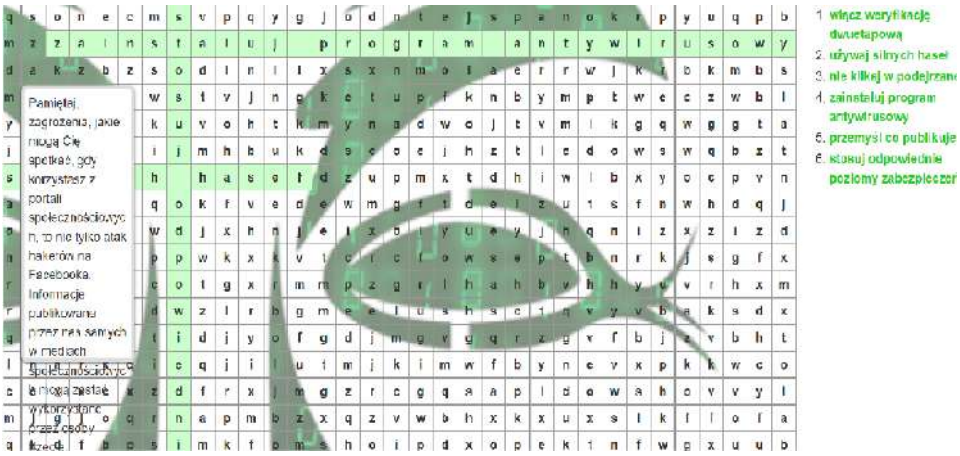
Wprowadzenie (5 minut)
Na początku lekcji prowadzący wraz z młodzieżą określa jaką funkcję może pełnić esencja herbaciana. Następnie uczniowie odgadują inną nazwę wskaźników kwasowo – zasadowych rozwiązując ćwiczenie „wisielec ''- https://learningapps.org/watch?v=p3moe115k21.

Realizacja (35 minut)
Nauczyciel podaje temat lekcji oraz określa NaCoBezu i wyjaśnia działanie wskaźników (slajd nr 4). Później młodzież odszukuje przy wykorzystaniu tablicy interaktywnej lub tabletów/smartfonów ukryte przez prowadzącego w wykreślance nazwy przykładowych wskaźników - https://learningapps.org/watch?v=pwnsgeno321 (slajd nr 5).

W kolejnym etapie lekcji nauczyciel łączy uczniów w zespoły i poleca stworzenie profilu wylosowanego wskaźnika na Fakebooku przy wykorzystaniu strony internetowej https://www.classtools.net/FB/home-page.* Młodzież najpierw zbiera informacje na temat swojego bohatera przy wykorzystaniu dostarczonych przez prowadzącego kart charakterystyk i/lub wiadomości znalezionych w internecie, a następnie tworzy jego profil (slajd nr 6). Po upływie wyznaczonego czasu liderzy grup prezentują efekty prac zespołów.
* Opcjonalnie młodzież może przedstawić wskaźnik na arkuszach szarego papieru.

Podsumowując ćwiczenie nauczyciel inicjuje rozmowę na temat social mediów zadając pytania: Czy łatwo jest założyć fikcyjne konto na facebooku? Jaki może być cel takiego działania? Moderując dyskusję prowadzący omawia wybrane zagrożenia internetowe, definiuje pojęcia m.in. cybermobbing, cyberbullying, trolling, podkreśla rolę wizerunku w internecie, zwracając jednocześnie uwagę na cyfrowy ślad.

Zakończenie (5 minut):
Zamykając dyskusję nauczyciel zaprasza do wykonania ćwiczenia- https://learningapps.org/watch?v=ppdsqnyo3229 (slajd nr 7), które zawiera proste wskazówki pozwalające na minimalizację zagrożeń w cyberprzestrzeni. Zadaniem młodzieży jest odnalezienie sześciu podstawowych zasad, które przypomną, jak zwiększyć bezpieczeństwo swoich danych w sieci. Uczniowie pracują wykorzystując własne smartfony / tablet szkolne lub wspólnie wykonują ćwiczenie na tablicy interaktywnej.



zrzut z ekranu

Kończąc zajęcia prowadzący zachęca młodzież do przygotowania krótkiego quizu na temat zagadnień z zakresu cyberbezpieczeństawa poruszanych na lekcji, dla rówieśników – gra zostanie przeprowadzona podczas godzin wychowawczych w innych klasach.

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

https://www.gov.pl/web/baza-wiedzy/cyberedukacja [online, dostęp z dn. 01.11.2022].

Lista dodatkowych plików, będących integralną częścią scenariusza

Załącznik nr 1 – link do prezentacji https://docs.google.com/presentation/d/1sj14bSNx_SZX07v7DLje1MI4Rffyocnv/edit?usp=sharing&ouid=111010848078344227112&rtpof=true&sd=true
Załącznik nr 1- Screeny quizu w Kahoot
Załącznik nr 2- Screen filmu we Flipgrip


Jaką funkcję może
pełnić w chemii
esencja herbaciana?


WSKAŹNIKI
Słabe kwasy (H-ind) lub zasady (ind-OH)
organiczne, które pod wpływem kationów H_3O^+ /
anionów OH^- zmieniają barwę.
Ich forma zdysocjowana i niezdysocjowana różnią się
zabarwieniem.
Zmiany pH wpływają na wzajemny stosunek stężeń obu
postaci wskaźnika, a w konsekwencji na przyjmowane przez
niego zabarwienie.
Każdy ze wskaźników ma charakterystyczny zakres pH, w
którym następuje zmiana jego koloru.


Polecenie
Odgadnij inną nazwę wskaźników
OK
A B C D E F G H I J K L M N O P
Q R S T U V W X Y Z Ä Ö Ü
https://learningapps.org/watch?v=p3moe115k21

Na tropie wskaźników

- https://learningapps.org/watch?v=pwnsgeno321

Praca w zespołach

- Stwórzcie profil wskaźnika oznaczonego
- https://www.classtools.net/FB/home-page

Najpierw zbierzcie informację na temat Waszego bohatera, a następnie zbudujcie jego profil.

Na zakończenie

https://learningapps.org/watch?v=ppdsgnyo322

W SIECI CYBERPAJĄCZKA

autorka: Katarzyna Jaworska

CYBER BEZPIECZNI

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Spontaniczna zabawa, która towarzyszy dzieciom w młodszym wieku szkolnym, to cenna wartość. To właśnie dzięki niej dziecko prawidłowo rozwija się we wszystkich sferach. Co prawda jej formy różnią się w zależności od wieku dziecka, ale jej rola pozostaje nadal niezmienna. Tworząc scenariusz kierowałam się więc jedną zasadą. To zabawa ma prowadzić do nauki, a nauka ma stać się zabawą, dlatego scenariusz lekcji „W sieci" został przeze mnie tak napisany, aby właśnie poprzez zabawę wprowadzić dzieci w cyberświat, gdzie znajomość podstawowych zasad cyberbezpieczeństwa jest niezwykle ważne.

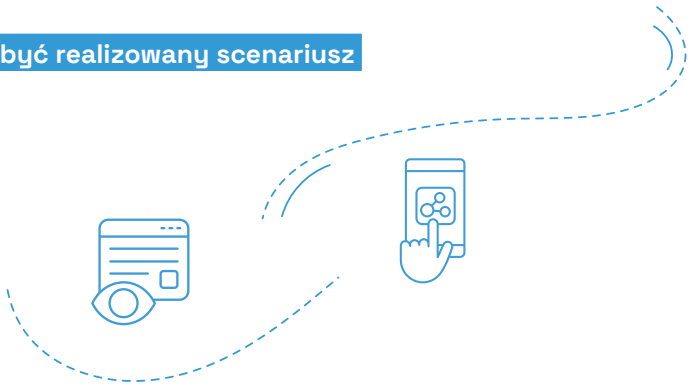
Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

III. Edukacja społeczna.
1. Osiągnięcia w zakresie rozumienia środowiska społecznego. Uczeń:
1) identyfikuje się z grupą społeczną, do której należy: rodzina, klasa w szkole, drużyna sportowa, społeczność lokalna, naród; respektuje normy i reguły postępowania w tych grupach;
3) przyjmuje konsekwencje swojego uczestnictwa w grupie i własnego w niej postępowania w odniesieniu do przyjętych norm i zasad;
10) wykorzystuje pracę zespołową w procesie uczenia się, w tym przyjmując rolę lidera zespołu i komunikuje się za pomocą nowych technologii.

VII. Edukacja informatyczna.
5. Osiągnięcia w zakresie przestrzegania prawa i zasad bezpieczeństwa. Uczeń:
1) posługuje się udostępnioną mu technologią zgodnie z ustalonymi zasadami;
2) rozróżnia pożądane i niepożądane zachowania innych osób (również uczniów) korzystających z technologii, zwłaszcza w sieci internet;
3) przestrzega zasad dotyczących korzystania z efektów pracy innych osób i związanych z bezpieczeństwem w internecie.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

edukacja informatyczna/edukacja społeczna



Adresaci lekcji (wiek, klasa)

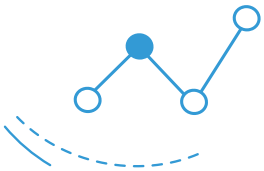
9 lat, uczniowie kl. III

Cel ogólny lekcji i cele szczegółowe

Cel główny: Poznanie zasad cyberbezpieczeństwa i sposobów radzenia sobie w sytuacji zagrożenia w internecie.

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Cele szczegółowe. Uczeń:
- poznaje podstawowe zagrożenia, które może napotkać w sieci;
- poznaje zasady cyberbezpieczeństwa;
- przeciwdziała sytuacjom niebezpiecznym online;
- zapoznaje się ze sposobami radzenia sobie w sytuacji zagrożenia w internecie;
- podaje numer telefonu, na który może zadzwonić w przypadku, gdy poczuje się niekomfortowo korzystając z internetu;
- wzbogaca słownik czynny o słownictwo związane z tematem;
- doskonali spostrzegawczość wzrokową;
- czyta i słucha ze zrozumieniem;
- współpracuje w grupie;
- szanuje przyjęte normy.



CYBER BEZPIECZNI

Metody pracy

- gra dydaktyczna (gra)
- pogadanka (pogadanka przedstawiająca nowe wiadomości)

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

- link do prezentacji i gry https://view.genial.ly/635e4e82cc462300129bd1e7
- tablica multimedialna i 2 laptopy dla każdej z drużyn z dostępem do internetu,
- karty do wycięcia i wydrukowania „Regulamin cyberbezpieczeństwa"– załącznik nr 1
- dyplom – załącznik nr2
- kartka A1, klej

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

Przebieg zajęć

PRZED ZAJĘCIAMI NAUCZYCIEL:

1. Drukuje z gry „W sieci cyberpajączka" karty „Regulamin cyberbezpieczeństwa" (karty dostępne są w zasadach gry lub w załączniku nr 1 do scenariusza).
2. Drukuje dla każdego dziecka dyplom- załącznik nr 2

FAZA ORGANIZACYJNA – 5min

• Wchodząc do klasy każde dziecko losuje z koszyka jedną kredkę. Połowę kredek stanowią kredki zielone, a drugą kredki czerwone. W tym momencie następuje podział uczniów na 2 grupy. Grupa zielonych i grupa czerwonych. Należy pamiętać, aby łączna ilość kredek odpowiadała dokładnie ilości uczniów w klasie.

• Powitanie i sprawdzenie obecności.

• Nauczyciel nie podaje celów lekcji, ponieważ będą one przedstawione uczniom na początku rozgrywania gry.

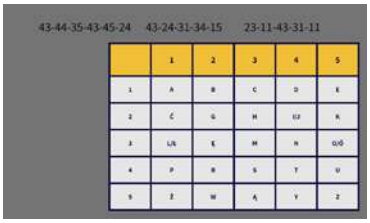
FAZA REALIZACYJNA – 35 min.

- Udostępnienie prezentacji na laptopach każdej z drużyn link tutaj https://view.genial.ly/635e4e82cc462300129bd1e7

• **slajd nr 1 *„Szyfr hakera - Stosuj silne hasła!"***

Nauczyciel prosi uczniów, aby dobrali się w grupy, które zostały ustalone na początku zajęć, a nas-

tępnie rozszyfrowali hasło, które będzie potrzebne do uruchomienia prezentacji, a co za tym idzie do rozpoczęcia lekcji. Ta grupa, która jako pierwsza rozszyfruje hasło rozpocznie grę „W sieci cyberpajączka".



Po rozszyfrowaniu hasła przez jedną z drużyn nauczyciel zbiera tablety i wyświetla tę samą prezentację, ale już na tablicy multimedialnej, gdzie prezentuje poprawne odszyfrowanie hasła wszystkim uczniom. Po odszyfrowaniu hasła następuje krótka pogadanka na temat tego, kim jest haker, po co i w jakim celu tworzymy hasła oraz co to znaczy, że hasło jest silne. Następnie nauczyciel informuje uczniów, że w podczas rozgrywania gry poznają m.in. zasady tworzenia silnych haseł.

• **slajd nr 2, 3 i 4** nauczyciel wyświetla na tablicy multimedialnej

• **slajd nr 5 – *„W sieci"*** - gra właściwa w grupach, rozgrywana na tablicy multimedialnej. Zaletą gry jest to, że można rozegrać ją w grupach, parach lub nawet samemu.

- Gra kończy się wygraną dla tej grupy, która jako pierwsza dojdzie do pola oznaczonego nr 54.
- Po skończonej grze wszyscy wspólnie tworzą „Regulamin cyberbezpieczeństwa",

przyklejając na kartkę A1 wylosowane w trakcie gry karty.

- Rozdanie dyplomów dla każdego ucznia.

FAZA PODSUMOWUJĄCA I UWZGLĘDNIAJĄCA EWALUACJĘ – 5 min.

Podsumowując lekcję, nauczyciel prosi, aby każdy uczeń na dyplomie, w miejscu chmurki namalował jedną z trzech buziek (obojętną, zadowoloną lub smutną), co będzie odpowiadać stopniowi zadowolenia z zajęć.

ZADANIE DOMOWE

Wykonaj piktogram do jednej z 15 zasad bezpiecznego korzystania z internetu, które poznałeś na dzisiejszych zajęciach. Gotowe piktogramy przykleimy do „Regulaminu cyberbezpieczeństwa".

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

https://bezpiecznyinternet.edu.pl/co-to-jest-program-antywirusowy-i-jak-dziala/#jak-dzialaja-programy-antywirusowe
https://trybawaryjny.pl/linki-https/

https://wklasie.uniwersytetdzieci.pl/dashboard
https://pixabay.com/pl/photos/protok%c3%b3%c5%82-ssl-https-bezpiecze%c5%84stwo-2890762/
https://www.benchmark.pl/testy_i_recenzje/dobre-haslo-jak-tworzyc-bezpieczne-hasla.html

Lista dodatkowych plików, będących integralną częścią scenariusza

Załącznik nr 1 karty do wydrukowania i wycięcia „Zasady bezpiecznego korzystania z internetu" – wydrukuj w 2 egzemplarzach

Nie ufaj osobom poznanym w sieci! Nigdy nie masz pewności, jaka osoba siedzi za ekranem komputera, bo przecież jej nie widzisz.	**Stosuj różne hasła!** Stosuj różne hasła do różnych kont i często je zmieniaj.	**Nie ukrywaj złych informacji!** Mów zawsze, gdy coś cię przestraszy i zaniepokoi.	**Korzystaj z internetu z umiarem!** Od internetu możesz się uzależnić podobnie, jak ludzie uzależniają się od narkotyków, papierosów i alkoholu.	**Używaj programów antywirusowych!** Programy te chronią komputer przed złośliwymi wirusami.
Nie włączaj komputera podczas nieobecności rodziców w domu! Rodzice są po to, aby w porę zareagować i kontrolują czas spędzany przed ekranem komputera.	**Nie karm trolla!** Ignoruj zaczepki, nie wdawaj się z nim w dyskusję, ignoruj go. Troll po pewnym czasie ustąpi, bo przestaniesz go interesować.	**Nie loguj się na portalach internetowych!** Zgodnie z prawem musisz mieć ukończone 13 lat, żeby zostać członkiem takiej społeczności.	**Stosuj silne hasła do każdego konta!** Silne hasła to takie, które trudno odgadnąć.	**Chroń swoją prywatność!** Nigdy nie podawaj swojego imienia, nazwiska, adresu, numeru telefonu.
Nie klikaj w podejrzane linki! Klikając w podejrzane linki możesz ściągnąć groźnego wirusa.	**Anonimowość nie oznacza bezkarności!** Masz prawo posługiwać się pseudonimem w sieci, ale nie oznacza to wcale, że nie ponosisz odpowiedzialności za swoje słowa.	**Nie hejtuj!** Szanuj innych w sieci i nikogo nie obrażaj. Traktuj innych się tak, jakbyś sam chciał być traktowany.	**Nie wierz we wszystko, co przeczytasz w sieci!** Nie wszystkie informacje w sieci są prawdziwe.	**Dzwoń na numer 116 111, gdy coś cię zaniepokoi, a wstydzisz się o tym powiedzieć rodzicom!**

43-44-35-43-45-24 43-24-31-34-15 23-11-43-31-11

	1	2	3	4	5
1	A	B	C	D	E
2	Ć	G	H	I/J	K
3	L/Ł	Ę	M	N	O/Ó
4	P	R	S	T	U
5	Ż	W	Ą	Y	Z

S-44-35-43-45-24 43-24-31-34-15 23-11-43-31-11

	1	2	3	4	5
1	A	B	C	D	E
2	Ć	G	H	I/J	K
3	L/Ł	Ę	M	N	O/Ó
4	P	R	S	T	U
5	Ż	W	Ą	Y	Z

S-T-35-43-45-24 43-24-31-34-15 23-11-43-31-11

	1	2	3	4	5
1	A	B	C	D	E
2	Ć	G	H	I/J	K
3	L/Ł	Ę	M	N	O/Ó
4	P	R	S	T	U
5	Ż	W	Ą	Y	Z

S-T-O-43-45-24 43-24-31-34-15 23-11-43-31-11

	1	2	3	4	5
1	A	B	C	D	E
2	Ć	G	H	I/J	K
3	L/Ł	Ę	M	N	O/Ó
4	P	R	S	T	U
5	Ż	W	Ą	Y	Z

MECZ O BEZPIECZNĄ SIEĆ

autorka: Magdalena Honkowicz

CYBER BEZPIECZNI

Nawiązania do problematyki związanej z cyberbezpieczeństwem

Scenariusz lekcji wprost nawiązuje do problematyki cyberbezpieczeństwa. Uczniowie zaznajamiani są z terminologią związaną z niebezpieczeństwami w Internecie, zasadami bezpiecznego korzystania z Internetu, jak również z działaniami profilaktycznymi, mającymi na celu ochronić ich przed niebezpieczeństwami w sieci oraz z działaniami, które należy podjąć już po wystąpieniu niebezpieczeństwa.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

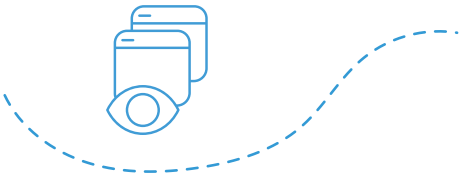
IV. Rozwijanie kompetencji społecznych. Uczeń: 1. uczestniczy w zespołowym rozwiązaniu problemu posługując się technologią taką jak: poczta elektroniczna, forum, wirtualne środowisko kształcenia, dedykowany portal edukacyjny; 2. identyfikuje i docenia korzyści płynące ze współpracy nad wspólnym rozwiązywaniem problemów. **V. Przestrzeganie prawa i zasad bezpieczeństwa.** Uczeń: 1. posługuje się technologią zgodnie z przyjętymi zasadami i prawem; przestrzega zasad bezpieczeństwa i higieny pracy; 2. uznaje i respektuje prawo do prywatności danych i informacji oraz prawo do własności intelektualnej; 3. wymienia zagrożenia związane z powszechnym dostępem do technologii oraz do informacji i opisuje metody wystrzegania się ich.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

informatyka, warsztaty z cyberbezpieczeństwa

Adresaci lekcji (wiek, klasa)

uczniowie, ok. 9 – 12 lat, klasa IV – VI szkoły podstawowej



Cel ogólny lekcji i cele szczegółowe

Cel ogólny lekcji: przestrzeganie prawa i zasad bezpieczeństwa, zasad bezpiecznego korzystania z Internetu.

Cele szczegółowe**:** Uczeń: 1. zna zasady bezpiecznego korzystania z Internetu, 2. potrafi chronić siebie i innych w Internecie, 3. zna i potrafi nazwać zagrożenia/niebezpieczeństwa w Internecie, 4. wykorzystuje technologie informacyjno-komunikacyjne w nabywaniu wiedzy.

Metody pracy

rozmowa / dyskusja, praca na wirtualnej/interaktywnej tablicy, mapy myśli, praca z kamerką, metoda problemowa, praca z komputerem

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

białe, czyste kartki A4, przypory do pisania, komputer/laptop, tablica Jamboard, dostęp do Internetu, aplikacja do prowadzenia zajęć online: np. MS Teams

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

FORMA: zajęcia online, np. przy wykorzystaniu MS Teams

LISTA TO-DO NAUCZYCIELA przed zajęciami:

- zapoznać się z funkcjonowaniem interaktywnej tablicy Jamboard (przykładowe instrukcje podane w źródłach),
- przygotować tablicę Jamboard według wzoru (wzór dostępny w załączonych materiałach, wzór można wykorzystać jako prezentację, jeżeli korzystanie z tablicy nie jest możliwe – wtedy uczniowie jedynie wypowiadają się),
- poprosić uczniów, aby na zajęcia przygotowali czystą, białą kartkę A4 i przybory do pisania,
- poprosić uczniów o sprawdzenie stanu technicznego swojego sprzętu, aby każdy mógł bez przeszkód korzystać z kamerki, komputera i Internetu (uwaga: tablica Jamboard wymaga zainstalowania aplikacji na telefonie czy tablecie, dlatego najlepiej poprosić uczniów o to, aby korzystali na zajęciach z komputera lub laptopa).

PRZYWITANIE, ZAPREZENTOWANIE UCZNIOM FORMY ZAJĘĆ, ROZGRZEWKA – 7 MIN

Nauczyciel wita się z uczniami, a następnie uświadamia uczniom, że podczas tych zajęć wszyscy odbędą trening, dzięki któremu będą gotowi rozgrywać mecze o bezpieczną sieć, czyli będą przygotowani do bezpiecznego korzystania z Internetu. Podczas zajęć/treningu potrzebna będzie czysta, biała kartka A4 i przybory do pisania. Nauczyciel upewnia się, czy uczniowie mają przy sobie potrzebne materiały. Uczniom, którzy nie przygotowali materiałów, nauczyciel daje chwilę na ich przygotowanie/zorganizowanie. Nauczyciel wyjaśnia na czym polegają role uczniów i jego samego podczas lekcji. Uczniowie będą odbywali trening, a nauczyciel będzie trenerem, który przeprowadzi ich przez wszystkie etapy treningu. Nauczyciel tłumaczy, że zajęcia „MECZ O BEZPIECZNĄ SIEĆ" będą składały się z 3 etapów:

1. Rozgrzewka,
2. Odprawa przedmeczowa,
3. Trening przedmeczowy.

UWAGA! Na tym etapie zajęć istotna jest postawa prowadzącego (modulacja głosu, mowa ciała przedkamerką). Wyjaśniając uczniom kontekst i formę zajęć (trening przygotowujący do meczu o bezpieczną sieć) nauczyciel przyjmuje odpowiednią postawę, aby wzbudzić w uczniach **ciekawość.**

ROZGRZEWKA

Nauczyciel prosi wszystkich uczniów o wyłączenie kamerek. Wyjaśnia uczniom, że przeczyta im kilka stwierdzeń. Osoby, które zgadzają się z danym stwierdzeniem, **włączają** swoją kamerkę. Osoby, które nie zgadzają się z danym stwierdzeniem, pozostawiają kamerkę **wyłączoną**.
Prowadzący odczytuje następujące stwierdzenia:

- *Nie wyobrażam sobie już świata bez Internetu.*
- *Internet daje wiele możliwości.*
- *Uważam, że w sieci jest wiele zagrożeń.*
- *Uważam, że potrafię bezpiecznie korzystać z Internetu.*

Nauczyciel gratuluje uczniom ukończenia Rozgrzewki i zapowiada kolejny etap treningu.

ODPRAWA PRZEDMECZOWA – 15 min

Nauczyciel wyświetla uczniom utworzoną przez siebie tablicę Jamboard i krótko tłumaczy jak korzystać z tablicy, a następnie udostępnia uczniom link do tablicy w komentarzu spotkania. Każdy z uczniów powinien mieć możliwość edytowania tablicy i poruszania się po niej. Jeżeli nie jest to możliwe lub znacznie utrudnione (np. jeden z uczniów usuwa elementy tablicy bez pozwolenia), nauczyciel jedynie wyświetla tablicę na ekranie spotkania i sam operuje elementami tablicy.

Nauczyciel uświadamia uczniom, że wiele osób przed nimi doświadczyło zagrożeń i niebezpieczeństw w Internecie. Jako uczestnicy treningu uczniowie muszą zapoznać się z przebiegiem innych meczówo bezpieczną sieć – tj. z doświadczeniami innych osób korzystających z Internetu.

Nauczyciel wyjaśnia, że zadanie polega na dopasowaniu nazwy danego niebezpieczeństwa do historii, w której dane niebezpieczeństwo wystąpiło. Nauczyciel prosi jednego z chętnych uczniów o odczytanie na głos historii. Po jej odczytaniu uczniowie zgłaszają się (np. podnoszą rękę w górę w aplikacji), jeżeli chcą udzielić odpowiedzi na pytanie: *Jak nazywa się tego typu niebezpieczeństwo w Internecie?* Uczeń, który udzieli prawidłowej odpowiedzi, proszony jest o to, aby przyporządkował kartę z nazwą niebezpieczeństwa do danej historii, a nauczyciel usuwa pozostałe nazwy.

Po prawidłowym dopasowaniu nazwy niebezpieczeństwa do historii nauczyciel zadaje uczniom pytania: *Gdybyś miał możliwość podróżowania w czasie, co poradziłbyś bohaterowi/bohaterce zaprezentowanej historii, aby go/ją uchronić?* (szukanie rozwiązań profilaktycznych, zapobiegających niebezpieczeństwu, np. rozmowa z rodzicem lub inną zaufaną osobą dorosłą, weryfikowanie osób, które obserwujemy w Internecie, konsultowanie wyzwań internetowych z rodzicami i wzięcie udziału w wyzwaniach, które mają pozytywny, charytatywny charakter).

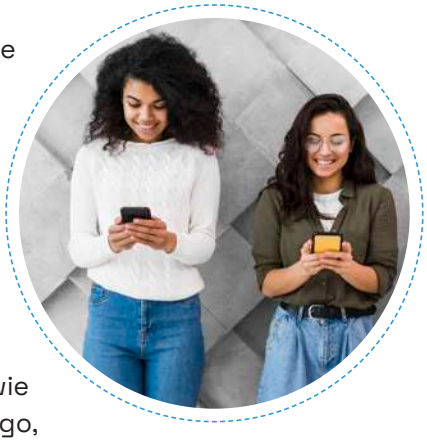
Jak można pomóc bohaterowi tej historii? (szukanie rozwiązań już po wystąpieniu niebezpieczeństwa/skutków danego niebezpieczeństwa, np. zgłoszenie sprawy w szkole, rozmowa z rodzicami). Nauczyciel i uczniowie analizują udzielone odpowiedzi i wypisują

pomysły na karteczkach na interaktywnej tablicy. Nauczyciel gratuluje uczniom ukończenia tego etapu treningu i zapowiada kolejny etap zajęć.

UWAGA: HISTORIE POTRZEBNE DO TEGO ZADANIA W ZAŁĄCZNIKACH!

TRENING PRZEDMECZOWY – 15 min

Nauczyciel przechodzi na kolejną kartę stworzonej tablicy Jamboard. Tak jak w poprzednim zadaniu – jeżeli korzystanie z wirtualnej tablicy przez wszystkich uczestników lekcji jest niemożliwe lub znacznie utrudnione, nauczyciel sam operuje elementami tablicy.



Nauczyciel prosi uczniów o przygotowanie czystej, białej kartki A4. Następnie prosi uczniów, aby ułożyli ją przed sobą poziomo, a na jej środku napisali hasło: **BEZPIECZNA SIEĆ.** Na tym etapie treningu wyzwaniem dla uczniów jest skompletowanie podstawowych narzędzi, które będą im potrzebne podczas każdego meczu o bezpieczną sieć – tj. zasad bezpiecznego korzystania z Internetu. Nauczyciel wyświetla uczniom różne wskazówki i zasady na tablicy. Pośród tych wskazówek znajdują się również wskazówki fałszywe – pułapki. Nauczyciel razem z uczniami analizuje wyświetlane propozycje pod kątem tego, czy dana wskazówka/zachowanie/zasada jest odpowiednia dla osoby korzystającej z Internetu czy nie – jeżeli uczniowie po konsultacji z nauczycielem uznają, że konkretna wskazówka jest warta tego, aby „wykorzystać" ją (zapamiętać) podczas meczu o bezpieczną sieć (każdorazowe korzystanie z Internetu) uczniowie zapisują taką wskazówkę na kartce wokół hasła umieszczonego w centrum. Natomiast w odniesieniu do zasad-pułapek zadanie uczniów polega na przeformułowaniu ich w taki sposób, aby stały się właściwymi wskazówkami. Przeformułowane wskazówki również zapisują na kartce dookoła hasła.

Jeżeli uczniowie chcą podzielić się jeszcze innymi, własnymi zasadami bezpiecznego korzystania z Internetu (również tymi, które padły jako rady w poprzednim zadaniu) **nauczyciel pozwala im na swobodne podzielenie się swoimi pomysłami** i na przeanalizowanie danej propozycji na forum. Jeżeli propozycja zostanie uznana przez uczniów i nauczyciela za wartą dodania do karty pracy – uczniowieumieszczają ją na swoich mapach myśli.

Po przeanalizowaniu wszystkich wskazówek uczniowie łączą strzałkami hasło umieszczone w centrum z konkretnymi zasadami/wskazówkami. Nauczyciel zachęca uczniów, aby stworzoną mapę myśli umieścili w swoim pokoju czy miejscu, gdzie zazwyczaj korzystają z Internetu, aby za każdym razem przypominała im o zasadach bezpiecznego korzystania z Internetu.

Wskazówki/zasady (na zielono prawidłowe propozycje, na czerwono pułapki)

Bez zastanowienia podaję swoje dane (imię, nazwisko, numer telefonu, adres zamieszkania) w Internecie

Gdy coś mnie w Internecie zaniepokoi, opowiadam o tym rodzicom lub innej zaufanej osobie dorosłej

Obrażam innych w mediach społecznościowych

Kontroluję to, ile czasu spędzam w sieci

Klikam w podejrzane linki

Korzystam z oprogramowań chroniących moje urządzenia (np. program antywirusowy)
Korzystam tylko ze stron internetowych, które są zabezpieczone – mają kłódkę w pasku przeglądarki
Komentuję wpisy/posty innych w sposób złośliwy
Podszywam się pod inne osoby w Internecie
Chętnie nawiązuję kontakty z nieznajomymi w sieci
Uważam na to, kogo obserwuję w Internecie
Uważam na to, co i gdzie publikuję w sieci
Pytam rodziców lub inne zaufane osoby dorosłe, jeżeli nie wiem jak korzystać z danej strony internetowej czy aplikacji
Pozostaję zalogowany/zalogowana na różnych komputerach i urządzeniach
Podaję swoje loginy oraz hasła koleżankom i kolegom
Tworzę różne hasła, które trudno odgadnąć
Odmawiam, jeżeli ktoś namawia mnie do publikowania zdjęć czy postów, których wcale nie chcę publikować
Publikuję zdjęcia i filmiki z wizerunkiem innych osób bez ich zgody
Nie publikuję cudzych prac w Internecie pod swoim imieniem i nazwiskiem
Ufam wszystkim osobom w Internecie
Nie wierzę we wszystkie informacje, o których przeczytam w Internecie – weryfikuję treści, które czytam
Pobieram pliki z niepewnych źródeł

PODSUMOWANIE ZAJĘĆ, GRATULACJE, ZAKOŃCZENIE ZAJĘĆ – 7 min

Nauczyciel prosi, aby każdy z uczniów na interaktywnej tablicy odpowiedział na pytanie:
Co szczególnie zapamiętałeś z dzisiejszych zajęć?

Następnie nauczyciel umożliwia uczniom zapoznanie się ze wszystkimi odpowiedziami.
Czy coś się powtórzyło? Czy odpowiedzi są podobne, czy bardzo się różnią?

Dodatkowo nauczyciel pyta uczniów o ich wrażenia po zajęciach.
Czy podobały Wam się dzisiejsze zajęcia? Dlaczego tak/nie?
Co Was zaskoczyło na dzisiejszych zajęciach?

Nauczyciel gratuluje uczniom ukończenia treningu, dzięki któremu będą mogli na co dzień bezpiecznie rozgrywać mecze o bezpieczną sieć – bezpiecznie korzystać z Internetu. Nauczyciel dziękuje uczniom za udział w treningu i żegna się z uczniami.

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

Bochenek M., Polak Z., Silicki K., Wrońska A., *Jak zapewnić dzieciom bezpieczeństwo w Internecie, Poradnik dla nauczycieli*, https://akademia.nask.pl/pliki/1-jak-zapewnic-uczniom-bezpieczenstwo-w-internecie-poradnik-dla-nauczycieli.pdf
Grzemny D., *W innym trybie. Edukacja praw człowieka online*, Warszawa 2021, https://amnesty.org.pl/wp-content/uploads/2021/03/W-innym-trybie-edukacja-praw-czlowieka-online.pdf

red. Lizut J., Wrońska A., *Standard bezpieczeństwa online placówek oświatowych*, Warszawa 2018, https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf
red. Rywczyńska A., Wójcik S., *Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów*, Warszawa 2018, https://www.saferinternet.pl/pliki/publikacje/kompendium2019.pdf

Bezpieczeństwo twojego dziecka – Zagrożenia, https://www.gov.pl/web/baza-wiedzy/bezpieczenstwo-twojego-dziecka---zagrozenia
Dzieci w wirtualnej sieci. Poradnik dla rodziców, https://ko.poznan.pl/wp-content/uploads/2022/03/broszura-dzieci-w-wirtualnej-sieci_wydanie-iii_17.02.2022.pdf
Klikam z głową. Poradnik dla rodziców i nauczycieli, https://cik.uke.gov.pl/news/poradnik-dla-nauczycieli-i-rodzicow,228.html
https://avigon.pl/blog/bezpieczenstwo-dziecka-w-sieci-wskazowki-dla-rodzicow-i-dzieci
https://dziecisawazne.pl/dziecko-bezpieczne-w-sieci/
https://edukacja.fdds.pl/course/index.php?categoryid=33
https://nordvpn.com/pl/blog/bezpieczenstwo-w-sieci-dla-dzieci/
https://sieciaki.pl/warto-wiedziec/zasady-bezpieczenstwa
https://www.giganciprogramowania.edu.pl/blog/bezpieczenstwo-dziecka-w-sieci-wskazowki-dla-rodzicow-i-dzieci
https://www.netcomplex.pl/blog/jak-byc-bezpiecznym-w-sieci-zasady-cyberbezpieczenstwa

Jamboard
http://konferencje.frse.org.pl/img/default/Mfile/file/3754/jamboard.pdf
https://sensonauka.pl/praca-grupowa-z-tablica-jamboard-na-lekcjach-zdalnych/

Lista dodatkowych plików, będących integralną częścią scenariusza

1. wzór tablicy Jamboard
2. historie do zadania 2

ROZGRZEWKA

ODPRAWA PRZEDMECZOWA

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Kamil i Adam grali w jednej drużynie piłkarskiej i oboje byli środkowymi napastnikami. Kamil nie przykładał się do ćwiczeń na treningach, często je opuszczał i kłócił się z kolegami z drużyny, a nawet z trenerem. Natomiast Adam brał aktywnie udział we wszystkich treningach oraz przykładał się do powierzonych mu zadań na boisku. Od pewnego czasu to Adam wychodził w pierwszej jedenastce, z kolei Kamil, decyzją trenera, przesiadywał całe mecze na ławce rezerwowych. Kamil zaczął wysyłać do Adama obraźliwe wiadomości za pomocą komunikatora internetowego. Początkowo raz dziennie, później coraz częściej. Z czasem wysyłał do Adama również obraźliwe maile, groźby. Dodatkowo przerabiał jego zdjęcia w edytorze zdjęć i wysyłał mu je o różnych porach dnia z obraźliwymi komentarzami. Adam zaczął się bać treningów i spotkań z Kamilem. Nie chciał również chodzić do szkoły. Pozostali członkowie drużyny zaczęli obawiać się, że Kamil również będzie wysyłał im podobne wiadomości, więc zaczęli opuszczać treningi. Po tych wydarzeniach drużyna nie wygrała ani jednego meczu.

PRO-ANA

TROLL PARENTING

CYBERSTALKING

INTERNET CHALLANGE

Kasia wybrała się z rodzicami na wakacje. Podczas wyjazdu do Torunia oblała się wodą. Plama była widoczna szczególnie na spodniach dziewczynki. Rodzice zatrzymali się na parkingu, aby Kasia mogła się przebrać. W pewnym momencie mama Kasi wyjęła z torebki telefon i zrobiła dziewczynce zdjęcie, a następnie opublikowała to zdjęcie w Internecie na jednym z portali społecznościowych z dopiskiem „mój mały bejbik". Mama Kasi często publikowała w Internecie podobne zdjęcia dziewczynki w różnych „śmiesznych" sytuacjach z równie „zabawnymi" komentarzami. Kasi nie podobało się to, że mama publikowała takie zdjęcia bez jej zgody.

CYBERSTALKING

PRO-ANA

TROLL PARENTING

INTERNET CHALLANGE

Maciek wrócił ze szkoły i zaczął przeglądać jeden ze swoich ulubionych portali społecznościowych. Zauważył, że kilku jego internetowych idoli opublikowało filmiki, w których rywalizowali o to, kto połknie najwięcej małych kolorowych cukierków. Maciek zdał sobie sprawę, że żaden uczeń z jego szkoły jeszcze nie „odważył się" na wstawienie takiego filmiku. Poza nim nikogo nie było w domu, więc uznał, że to najlepszy czas na podjęcie się takiego zadania. Zdał sobie jednak sprawę, że nie ma w domu żadnych kolorowych cukierków. Pobiegł do kuchni, gdzie mama trzymała tabletki – kolorowe i okrągłe. Maciek uznał, że będą idealnie nadawały się do filmiku. Przygotował telefon, włączył kamerkę, przedstawił się i zaczął połykać kolorowe tabletki mamy. Maciek stracił przytomność. Gdy rodzice Maćka wrócili do domu, nie mogli go obudzić. Maciek trafił do szpitala.

INTERNET CHALLANGE

CYBERSTALKING

TROLL PARENTING

PRO-ANA

Julka to szczupła i niska dziewczynka. Niestety koleżanki z klasy Julki wyzywają ją, najczęściej używając określenia „gruba". Pewnego dnia Julka wróciła zapłakana do domu. Chciała żeby koleżanki z klasy ją lubiły, więc postanowiła poszukać w Internecie informacji o tym, jak szybko schudnąć. Natrafiła na pewien blog, w którym jedna ze starszych dziewczyn opisywała zasady, które mają pomóc uzyskać „idealną" figurę. Na blogu widniał tytuł: „Jeśli nie jesteś szczupła, to znaczy, że nie jesteś fajna". Julka zaczęła stosować się do wskazanych na blogu zasad. Znalazła również inne podobne blogi. Jednocześnie zaczęła bardzo ograniczać jedzenie. W szkole wyrzucała do kosza przygotowane przez mamę drugie śniadania, w domu wmawiała rodzicom, że już jadła, albo że nie jest głodna. Pomimo tego, że stosowała się do zasad i głodziła się, wcale nie czuła się lepiej i dalej była obrażana przez koleżanki z klasy. Często też nie miała siły, jednak panicznie bała się jeść.

PRO-ANA

CYBERSTALKING

INTERNET CHALLANGE

TROLL PARENTING

TRENING PRZEDMECZOWY

Bez zastanowienia podaję swoje dane (imię, nazwisko, numer telefonu, adres zamieszkania) w Internecie

Pobieram pliki z niepewnych źródeł

Obrażam innych w mediach społecznościowych

Gdy coś mnie w Internecie zaniepokoi, opowiadam o tym rodzicom lub innej zaufanej osobie dorosłej

Korzystam tylko ze stron internetowych, które są zabezpieczone – mają kłódkę w pasku przeglądarki

Kontroluję to, ile czasu spędzam w sieci

Ufam wszystkim osobom w Internecie

Korzystam z oprogramowań chroniących moje urządzenia (np. program antywirusowy)

Publikuję zdjęcia i filmiki z wizerunkiem innych osób bez ich zgody

Komentuję wpisy/posty innych w sposób złośliwy

Klikam w podejrzane linki

Nie wierzę we wszystkie informacje, o których przeczytam w Internecie – weryfikuję treści, które czytam

Podszywam się pod inne osoby w Internecie

Chętnie nawiązuję kontakty z nieznajomymi w sieci

Nie publikuję cudzych prac w Internecie pod swoim imieniem i nazwiskiem

Podaję swoje loginy oraz hasła koleżankom i kolegom

Uważam na to, kogo obserwuję w Internecie

Pytam rodziców lub inne zaufane osoby dorosłe, jeżeli nie wiem jak korzystać z danej strony internetowej czy aplikacji

Odmawiam, jeżeli ktoś namawia mnie do publikowania zdjęć czy postów, których wcale nie chcę publikować

Pozostaję zalogowany/zalogowana na różnych komputerach i urządzeniach

Uważam na to, co i gdzie publikuję w sieci

Tworzę różne hasła, które trudno odgadnąć

CO SZCZEGÓLNIE ZAPAMIĘTAŁEŚ Z DZISIEJSZYCH ZAJĘĆ?

GRATULACJE!!!

Historia nr 1

CYBERSTALKING

Notatka dla nauczyciela: Zjawisko natrętnego i złośliwego dręczenia pojedynczej osoby, grupy osób lub całej organizacji przy użyciu technologii informacyjnej, w szczególności Internetu. Prześladowca określany jest często jako stalker.

Kamil i Adam grali w jednej drużynie piłkarskiej i oboje byli środkowymi napastnikami. Kamil nie przykładał się do ćwiczeń na treningach, często je opuszczał i kłócił się z kolegami z drużyny, a nawet z trenerem. Natomiast Adam brał aktywnie udział we wszystkich treningach oraz przykładał się do powierzonych mu zadań na boisku. Od pewnego czasu to Adam wychodził w pierwszej jedenastce, z kolei Kamil, decyzją trenera, przesiadywał całe mecze na ławce rezerwowych. Kamil zaczął wysyłać do Adama obraźliwe wiadomości za pomocą komunikatora internetowego. Początkowo raz dziennie, później coraz częściej. Z czasem wysyłał do Adama również obraźliwe maile, groźby. Dodatkowo przerabiał jego zdjęcia w edytorze zdjęć i wysyłał mu je o różnych porach dnia z obraźliwymi komentarzami. Adam zaczął się bać treningów i spotkań z Kamilem. Nie chciał również chodzić do szkoły. Pozostali członkowie drużyny zaczęli obawiać się, że Kamil również będzie wysyłał im podobne wiadomości, więc zaczęli opuszczać treningi. Po tych wydarzeniach drużyna nie wygrała ani jednego meczu.

Historia nr 2

TROLL PARENTING

Notatka dla nauczyciela: Publikowanie przez rodziców i opiekunów wizerunku dziecka w Internecie w ośmieszającym czy wręcz kompromitującym kontekście. Kasia wybrała się z rodzicami na wakacje. Podczas wyjazdu do Torunia oblała się wodą. Plama była widoczna szczególnie na spodniach dziewczynki. Rodzice zatrzymali się na parkingu, aby Kasia mogła się przebrać. W pewnym momencie mama Kasi wyjęła z torebki telefon i zrobiła dziewczynce zdjęcie, a następnie opublikowała to zdjęcie w Internecie na jednym z portali społecznościowych z dopiskiem „mój mały bejbik". Mama Kasi często publikowała w Internecie podobne zdjęcia dziewczynki w różnych „śmiesznych" sytuacjach z równie „zabawnymi" komentarzami. Kasi nie podobało się to, że mama publikowała takie zdjęcia bez jej zgody.

Historia nr 3

INTERNET CHALLANGE

Notatka dla nauczyciela: Idea internetowych wyzwań polega na wrzucaniu do sieci filmików przedstawiających osoby, które usiłują sprostać najdziwniejszym zadaniom – w teorii zabawnym, często jednak groźnym. Istotą tej mody jest pokazanie swoich dokonań możliwie jak najszerszemu gronu odbiorców. Maciek wrócił ze szkoły i zaczął przeglądać jeden ze swoich ulubionych portali społecznościowych. Zauważył, że kilku jego internetowych idoli opublikowało filmiki, w których rywalizowali o to, kto połknie najwięcej małych kolorowych cukierków. Maciek zdał sobie sprawę, że żaden uczeń z jego szkoły jeszcze nie „odważył się" na wstawienie takiego filmiku. Poza nim nikogo nie

było w domu, więc uznał, że to najlepszy czas na podjęcie się takiego zadania. Zdał sobie jednak sprawę, że nie ma w domu żadnych kolorowych cukierków. Pobiegł do kuchni, gdzie mama trzymała tabletki – kolorowe i okrągłe. Maciek uznał, że będą idealnie nadawały się do filmiku. Przygotował telefon, włączył kamerkę, przedstawił się i zaczął połykać kolorowe tabletki mamy. Maciek stracił przytomność. Gdy rodzice Maćka wrócili do domu, nie mogli go obudzić. Maciek trafił do szpitala.

Historia nr 4

PRO-ANA

Notatka dla nauczyciela: Styl życia polegający na dążeniu do doskonałości, za jaką uważa się wychudzoną figurę. Ana pochodzi od słowa anoreksja, czyli zaburzenia odżywiania polegającego na patologicznym głodzeniu się. Pro-ana promuje anoreksję i jest bardzo aktywny w Internecie, popularny szczególnie wśród dziewcząt, które odchudzając się zakładają blogi. Znakiem rozpoznawczym jest dekalog pro-ana, który rozpoczyna się hasłem: „Jeśli nie jesteś szczupła, to znaczy, że nie jesteś atrakcyjna", promotorzy pro-ana często posługują się symbolami motyli. Julka to szczupła i niska dziewczynka. Niestety koleżanki z klasy Julki wyzywają ją, najczęściej używając określenia „gruba". Pewnego dnia Julka wróciła zapłakana do domu. Chciała żeby koleżanki z klasy ją lubiły, więc postanowiła poszukać w Internecie informacji o tym, jak szybko schudnąć. Natrafiła na pewien blog, w którym jedna ze starszych dziewczyn opisywała zasady, które mają pomóc uzyskać „idealną" figurę. Na blogu widniał tytuł: „Jeśli nie jesteś szczupła, to znaczy, że nie jesteś fajna". Julka blogu zasad. Znalazła również inne podobne blogi. Jednocześnie zaczęła bardzo ograniczać jedzenie. W szkole wyrzucała do kosza przygotowane przez mamę drugie śniadania, w domu wmawiała rodzicom, że już jadła, albo że nie jest głodna. Pomimo tego, że stosowała się do zasad i głodziła się, wcale nie czuła się lepiej i dalej była obrażana przez koleżanki z klasy. Często też nie miała siły, jednak panicznie bała się jeść.

AUTORZY I BOHATEROWIE NASZYCH LEKTUR W SIECI!

autorka: Karolina Strógarek,
Maja Cieślak-Strzelec

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Na lekcji zaprezentowana zostanie gra ”W sieci”.

Naszym zdaniem ta gra świetnie wpisuje się w kierunki polityki oświatowej państwa na rok szkolny 2022/2023, ponieważ kształtuje postawy ukierunkowane na odpowiedzialność. Uczeń zauważa dalekowzroczność działań, w których bierze udział. Uczy się krytycznego podejścia do treści publikowanych w internecie i mediach społecznościowych. Sam podejmuje decyzję, które postępowanie jest prawidłowe, mądre i niezagrażające bezpośredniemu bezpieczeństwu, co chroni zarówno jego, jak sprzęt, z którego korzysta.

Uczniowie podczas rozgrywki mogą sprawdzić, jaką mają wiedzę na temat cyberbezpieczeństwa i netykiety.

Uczniowie refleksyjnie patrzą na technologie, którymi posługuje się na co dzień i na jej wpływ na relacje międzyludzkie.

Dodatkowym atutem scenariusza jest połączenie i utrwalenie wiadomości z zakresu literatury obowiązkowej i informacji związanych z życiorysem autorów tychże lektur, sprawdzenie wiedzy i umiejętności ucznia z zakresu cyberbezpieczeństwa, i najważniejsze – udowodnienie, że każdy ma wpływ na to, jak wygląda codzienność, jak może wyglądać świat. To poczucie sprawczości jest elementem, który ma wzbudzić w uczniu poczucie, że stawianie czoła wyzwaniom ma sens, że oni sami mogą kontrolować siebie, że mają wpływ na działania, których się podejmują.

Podsumowaniem lekcji będą słowa-klucze, które zapisują na kartkach uczestnicy zajęć i przymocują do tablicy.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Język polski:
Kształcenie literackie i kulturowe:
Uczeń:
- zna wybrane utwory z literatury polskiej i światowej (I 2),
- rozwija zdolności dostrzegania wartości: prawdy, dobra, piękna, szacunku dla człowieka i kierowania się tymi wartościami (I 4),
- poznaje wybrane dzieła wielkich pisarzy polskich w kontekście podstawowych informacji o epokach, w których tworzyli (I 6).

Tworzenie wypowiedzi:
- dokonuje selekcji informacji (III 1.4).

Samokształcenie:
- rozwija szacunek dla wiedzy, wyrabianie pasji poznawania świata i zachęcanie do praktycznego

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI”.

zastosowania zdobytych wiadomości (IV 1),
- rozwija umiejętności samodzielnego docierania do informacji, dokonywania ich selekcji, syntezy oraz wartościowania(IV 2).

Informatyka:
Rozwijanie kompetencji społecznych:
- ocenia krytycznie informacje i ich źródła, w szczególności w sieci, pod względem rzetelności i wiarygodności w odniesieniu do rzeczywistych sytuacji, docenia znaczenie otwartych zasobów w sieci i korzysta z nich (IV 2).

Przestrzeganie prawa i zasad bezpieczeństwa:
- opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją (V 1),
- postępuje etycznie w pracy z informacjami (V 2),
- rozróżnia typy licencji na oprogramowanie oraz na zasoby w sieci (V 3).

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

język polski, informatyka, lekcja wychowawcza

Adresaci lekcji (wiek, klasa)

8 klasa

Cel ogólny lekcji i cele szczegółowe

Zadaniem nauczyciela jest pokazanie uczniowi sensowności zdobywanej na lekcjach wiedzy i umiejętności jej wykorzystania w różnych wariantach zadaniowych. Zaciekawienie uczniów bohaterami literackimi i życiorysami autorów nie jest łatwe, dlatego trzeba szukać nowych metod, które pozwolą zapamiętać uczniowi jak najwięcej, a jeżeli jest to forma zabawy-zagadki, to naszym zdaniem tylko rozbudza to w uczniu zapotrzebowanie na samodzielne pogłębianie wiedzy i zapamiętanie nieszablonowych informacji. Kluczowa jest oczywiście znajomość języka ojczystego i sprawne posługiwanie się nim, ponieważ to ułatwia przyswajanie wiedzy z innych dziedzin i jest dla każdego ucznia podstawą sukcesu szkolnego.

Cel ogólny:
- uświadomienie uczniom, że cyberbezpieczeństwo jest priorytetem we współczesnym świecie,
- zwiększenie świadomości dotyczących cyberzagrożeń.

Cele szczegółowe:
- utrwalenie wiedzy na temat cyberprzemocy i cyberzagrożeń,
- utrwalenie wiadomości dotyczących autorów lektur obowiązkowych i bohaterów z lektur obowiązkowych,
- kształtowanie postawy krytycznego myślenia,

- szacowanie ryzyka,
- wzbudzenia w uczniach ciekawości poznawczej, by skłonić ich do refleksji dotyczącej rozważań na temat świata i człowieka.

Metody pracy

eksponujące, problemowe, aktywizujące, praca grupowa i indywidualna

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

- wydrukowana plansza wraz z kartami,
- pionki,
- kostka do gry,
- instrukcja gry,
- kolorowe kartki papieru na słowa-klucze,
- markery,
- puzzle.

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

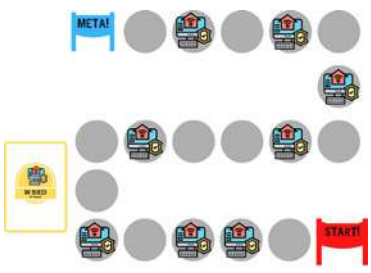
- Faza wstępna lekcji (5 min.)

Nauczyciel chce wzbudzić zainteresowanie uczniów, dlatego prosi o ułożenie puzzli.
https://www.jigsawplanet.com/?rc=play&pid=1ed22e318248
lub załącznik 1
Rutyna: widzę – myślę – zastanawiam się.

Wykorzystuje tę rutynę do wprowadzenia tematu o bezpieczeństwie w sieci. Następnie pyta, co widzą, co myślą i nad czym jeszcze się zastanawiają w związku z tą ilustracją. Można przewidzieć, że uczniowie będą zaskoczeni tym, że Adam Mickiewicz korzysta z sieci. Usłyszymy tu swobodne wypowiedzi uczniów. Może pojawić się refleksja - jak autorzy i bohaterowie lektur poradziliby sobie w czasach internetu? Nauczyciel zapisuje temat na tablicy: Autorzy i bohaterowie naszych lektur w sieci! Nauczyciel określa cele lekcji.

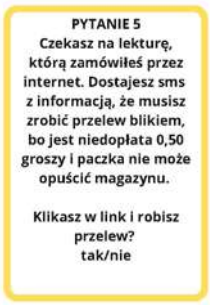
- Faza główna (łącznie 30 min.)

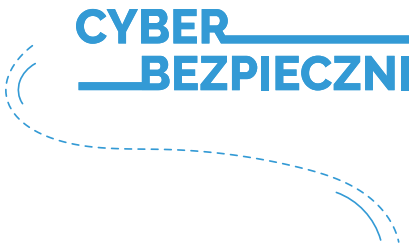
Nauczyciel dzieli uczniów na drużyny oraz tłumaczy zasady gry ”W sieci”.



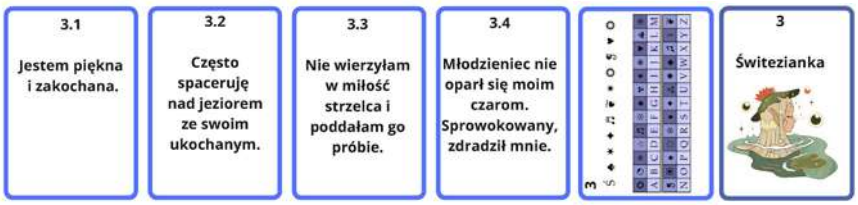
PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI”.

- Następnie uczniowie rozpoczynają grę. Podczas odpowiedzi na pytania związane z bezpieczeństwem w sieci uczniowie rozwiązują problemy typowe dla użytkowników sieci. Przykładowe pytanie i odpowiedź.





Następnie dzięki informacjom zdobytym po ukończeniu kolejnych 4 etapów gry odgadują, kim jest opisywany bohater lub autor lektur.
Przykład 4 informacji.



- Faza końcowa (6 min.)

Pojawia się pytanie: Jak myślisz, czy wylosowany i wskazany przez Ciebie bohater lub autor lektury szkolnej poradziłby sobie z niebezpieczeństwami czyhającymi w sieci? Uczniowie najprawdopodobniej zastanawiają się, jaki współcześnie mają na nas wpływ nowe technologie i jak bezpiecznie z nich korzystać? Snują refleksje na temat nowinek technologicznych i ich roli w życiu? Wymieniają się spostrzeżeniami na forum klasy. Podsumowaniem lekcji będą słowa-klucze, które zapiszą na kartkach uczestnicy zajęć i przymocują do tablicy. Pojawią się słowa: bezpieczeństwo, sieć, cyberprzemoc, hejt, prawa autorskie, ochrona danych osobowych.

- Zakończenie lekcji (2 min.)

Nauczyciel prosi, aby chętni uczniowie przygotowali za pomocą generatora
Darmowy Generator Memów z własnymi ustawieniami - Generator Memów (mem-generator.pl)
mem z przesłaniem bohatera lub autora lektury dotyczący bezpieczeństwa w sieci i cyberprzemocy. Kończy lekcję słowami: Bądź jak bohater kart, tajemniczy! nauczyciel prosi uczniów o ewaluację zajęć poprzez zaznaczenie cyfr od 1 do 10 na tarczy strzelniczej umieszczonej na drzwiach wyjściowych z sali.

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

Barbara Kaczmarzyk, Piotr Szczepański, Marlena Dąbrowska, Wybrane zagadnienia Cyberbezpieczeństwa: https://cejsh.icm.edu.pl

Juliusz Kleiner, Włodzimierz Maciąg, *Zarys dziejów literatury polskiej*, Wrocław, Zakład Narodowy im. Ossolińskich, 1985, ISBN 03-04-01406-8

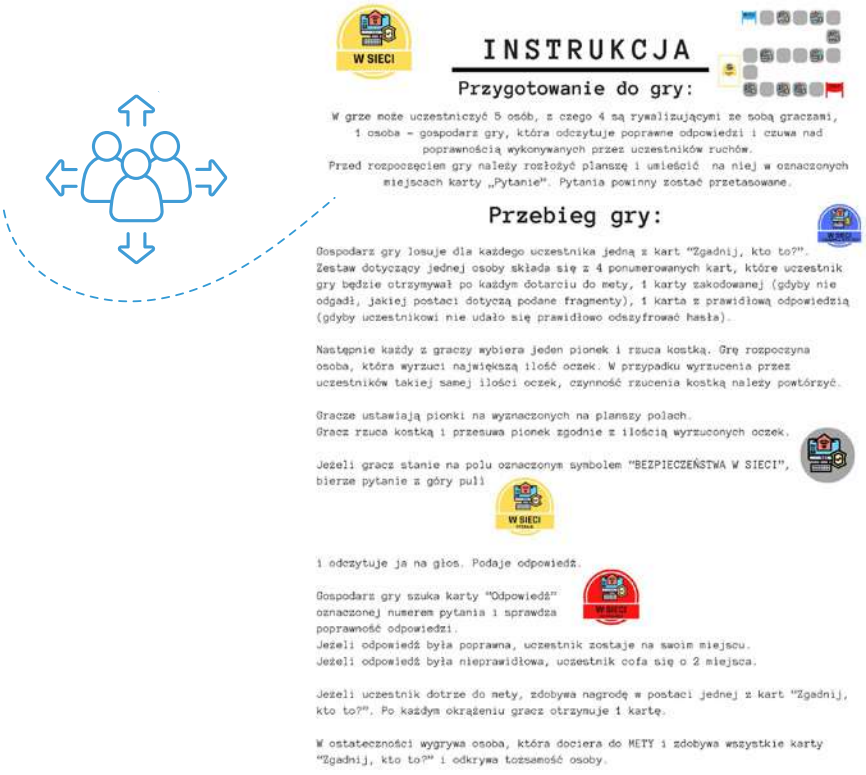
Jarosław Marek Rymkiewicz, Dorota Siwicka, Alina Witkowska, Marta Zielińska, *Mickiewicz - encyklopedia*, Warszawa 2001, ISBN 83-7311-012-7

Sławomir Koper, *Nobliści skandaliści*, Warszawa 2019, ISBN 9788366252790

Encyklopedia humanisty, Warszawa-Bielsko-Biała, Wydawnictwo Szkolne PWN, ISBN 978-83-2621-199-7

Lista dodatkowych plików, będących integralną częścią scenariusza

załącznik 1 - Instrukcja gry “W sieci”,
załącznik 2 - Plansza gry , puzzle, pytania , odpowiedzi, karty postaci do gry “W sieci”.



INSTRUKCJA

Przygotowanie do gry:

W grze może uczestniczyć 5 osób, z czego 4 są rywalizującymi ze sobą graczami, 1 osoba – gospodarz gry, która odczytuje poprawne odpowiedzi i czuwa nad poprawnością wykonywanych przez uczestników ruchów.
Przed rozpoczęciem gry należy rozłożyć planszę i umieścić na niej w oznaczonych miejscach karty „Pytanie". Pytania powinny zostać przetasowane.

Przebieg gry:

Gospodarz gry losuje dla każdego uczestnika jedną z kart "Zgadnij, kto to?". Zestaw dotyczący jednej osoby składa się z 4 ponumerowanych kart, które uczestnik gry będzie otrzymywał po każdym dotarciu do mety, 1 karty zakodowanej (gdyby nie odgadł, jakiej postaci dotyczą podane fragmenty), 1 karta z prawidłową odpowiedzią (gdyby uczestnikowi nie udało się prawidłowo odszyfrować hasła).

Następnie każdy z graczy wybiera jeden pionek i rzuca kostką. Grę rozpoczyna osoba, która wyrzuci największą ilość oczek. W przypadku wyrzucenia przez uczestników takiej samej ilości oczek, czynność rzucenia kostką należy powtórzyć.

Gracze ustawiają pionki na wyznaczonych na planszy polach.
Gracz rzuca kostką i przesuwa pionek zgodnie z ilością wyrzuconych oczek.

Jeżeli gracz stanie na polu oznaczonym symbolem "BEZPIECZEŃSTWA W SIECI", bierze pytanie z góry puli

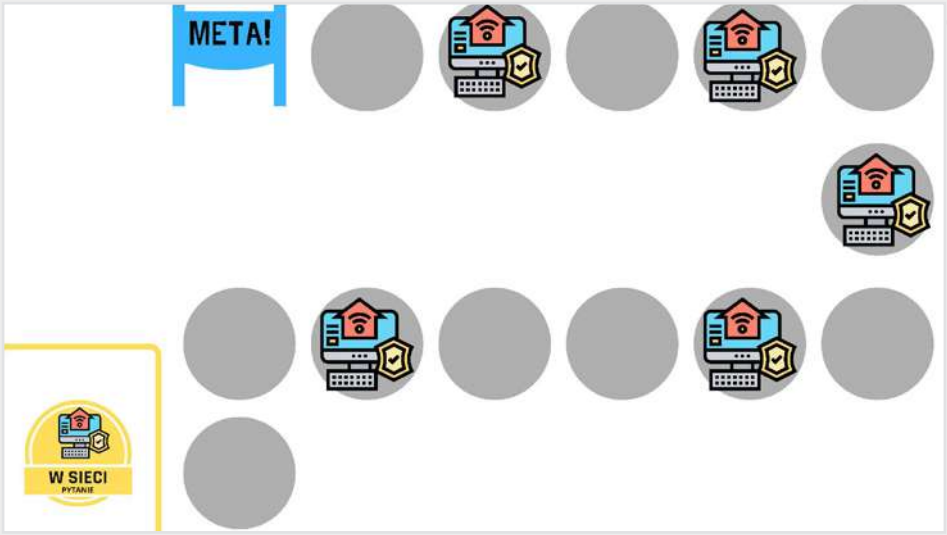
i odczytuje ja na głos. Podaje odpowiedź.

Gospodarz gry szuka karty "Odpowiedź" oznaczonej numerem pytania i sprawdza poprawność odpowiedzi.
Jeżeli odpowiedź była poprawna, uczestnik zostaje na swoim miejscu.
Jeżeli odpowiedź była nieprawidłowa, uczestnik cofa się o 2 miejsca.

Jeżeli uczestnik dotrze do mety, zdobywa nagrodę w postaci jednej z kart "Zgadnij, kto to?". Po każdym okrążeniu gracz otrzymuje 1 kartę.

W ostateczności wygrywa osoba, która dociera do METY i zdobywa wszystkie karty "Zgadnij, kto to?" i odkrywa tożsamość osoby.

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI”.



PYTANIE 1
Dostałeś maila z informacją, że wygrałeś darmowy pobyt w parku rozrywki. Możesz zabrać ze sobą dwie osoby towarzyszące. Musisz tylko kliknąć w link i wskazać datę, kiedy odwiedzisz miejsce, o którym od dawna marzyłeś.

Jak się zachowasz? Klikasz w link?
tak/nie

PYTANIE 2
Korzystasz z komputera w szkolnej bibliotece. Sprawdzasz swoją pocztę internetową. Aby następnym razem przyspieszyć proces logowania zapisujesz swoje hasło w pamięci komputera.

Takie zachowanie jest rozsądne?
tak/nie

PYTANIE 3
Zakładałeś nową pocztę i zastosowałeś w haśle co najmniej 15 znaków, które są kombinacją wielkich i małych liter oraz znaków specjalnych. Nie ma w nim żadnych informacji osobistych, takich jak: imię, nazwisko, data urodzenia.

Czy Twoje hasło jest bezpieczne?
tak/ nie

PYTANIE 4
Twoja koleżanka nie może wysłać maila ze swojego konta. Prosi Ciebie o dostęp do Twojej poczty. Wystarczy tylko, że podasz jej hasło.

Podajesz jej hasło?
tak/nie

PYTANIE 5
Czekasz na lekturę, którą zamówiłeś przez internet. Dostajesz sms z informacją, że musisz zrobić przelew blikiem, bo jest niedopłata 0,50 groszy i paczka nie może opuścić magazynu.

Klikasz w link i robisz przelew?
tak/nie

PYTANIE 6
Masz 2 godziny zajęć z informatyki. Siedzisz przed swoim stanowiskiem. Zadzwonił dzwonek i wychodzisz na przerwę. Wiesz, że sala podczas przerwy jest otwarta i może tam wejść ktokolwiek.

Wylogowujesz się z platformy, na której tworzysz projekt?
tak/nie

PYTANIE 7
Masz notesik, w którym zapisujesz hasła do wszystkich swoich kont. Notes zawsze masz przy sobie. Nigdy nie zostawiasz go na na stole. Zapobiegasz, by nie dostał się w niepowołane ręce.

Zachowujesz zasady ochrony swoich danych?
tak/nie

PYTANIE 8
Na stronie internetowej, której nie znasz, znalazłeś film. Chcesz go obejrzeć, bo to nowość kinowa i w dodatku możesz ją obejrzeć za darmo. Musisz tylko podać swoje imię i nazwisko oraz pesel jednego z rodziców.

Podajesz dane, o które Cię proszą i oglądasz film?
tak/nie

PYTANIE 9
Twoja koleżanka dostała swoją pierwszą kartę bankomatową. Pin do karty ma zapisany na małej karteczce, którą przykleiła z tyłu karty.

Zachowanie Twojej koleżanki jest zgodne z zasadami bezpieczeństwa ochrony swoich danych?
tak/ nie

PYTANIE 10
Chcesz uczyć się języka angielskiego online. Znalazłeś szkołę, w której miesięczny kurs kosztuje 120 zł. Sprawdziłeś opinie. Są pozytywne. Znalazłeś stronę, na której taki sam kurs kosztuje 50 zł. Nie ma jednak żadnych opinii, ani informacji, kto tam prowadzi zajęcia. Wybierasz sprawdzoną stronę?
tak/nie

PYTANIE 11
Znalazłeś na stronie, której nie znasz, informację o koncercie Twojego ulubionego zespołu muzycznego. Możesz okazyjnie kupić bilet, jeśli prześlesz podany w mailu link 5 osobom.

Przesyłasz wiadomość dalej i korzystasz z promocji?
tak/nie

PYTANIE 12
Twoja młodsza siostra dostała swój pierwszy komputer. Na każdym z kont, które założyła, ma jedno, to samo hasło. Przyjaciółka poinformowała Twoją siostrę, że postępuje niewłaściwie.

Przyjaciółka siostry ma rację?
tak/nie

PYTANIE 13
Twojej mamie wyświetliła się reklama butów, które ostatnio oglądała. Weszła na stronę i już miała dokonać zakupu, gdy zauważyła, że jedna z literek podanej strony różni się od strony, z której korzystała do tej pory. Mama wstrzymała transakcję.

Czy mama postąpiła słusznie?
tak/nie

PYTANIE 14
Od kilku miesięcy grasz w swoją ulubioną grę online. Masz już sporo punktów, ale nie możesz przejść do następnego levelu. Nieznajomy z sieci proponuje Ci, że przekaże Tobie swoje punkty, bo mu się gra znudziła i nie będzie już w nią grał. Musisz tylko podać mu swój login i hasło, by Ci je udostępnił.

Dziękujesz, ale nie korzystasz z propozycji nieznajomego.
tak/nie

PYTANIE 15
Twoja mama otrzymała w prezencie nowy komputer, który nie miał programu antywirusowego. Mama poprosiła tatę, aby go zakupił i zainstalował. Tata twierdził, że nie ma takiej potrzeby.

Czy mama miała rację?
tak/nie

PYTANIE16
Twój kolega często korzysta z komputera w szkolnej bibliotece. Ma nawyk wylogowywania się i usuwania historii przeglądania.

Ten nawyk jest nieprawidłowy.
tak/nie

PYTANIE 17
Od jakiegoś czasu czatujesz z nieznajomym w sieci. To dla Ciebie wyjątkowa osoba, rozumie Cię, doradza, komplementuje. Nieznajomy zaproponował Tobie, że spędzi z Tobą czas, ale tylko podczas nieobecności rodziców. Prosi o podanie adresu, by przyjechać.

Podajesz adres?
tak/nie

PYTANIE 18
Twoja przyjaciółka informuje Cię, że otrzymała od Ciebie maila z dziwną wiadomością. Ty jednak nie wysyłałeś jej nic w ostatnim tygodniu.

Ignorujesz tę informację i dalej korzystasz ze swojego konta?
tak/nie

PYTANIE 19
Jedna koleżanka z Twojej klasy nie lubi zajęć na basenie, bo nie umie pływać. Kolega z klasy z ukrycia nagrywa filmik, na którym widać jak nie radzi sobie podczas zajęć. Rozsyła filmik do znajomych.

Informujesz kolegę, że ma usunąć filmik?
tak/nie

PYTANIE 20
Twój kolega usunął filmik, który ośmieszał i szkalował jedną z koleżanek z klasy.

Kolega może czuć się bezpiecznie i bezkarnie?
tak/nie

PYTANIE 21
Twój kolega twierdzi, że jest różnica pomiędzy krytykowaniem a hejtowaniem.

Twój kolega ma rację?
tak/nie

PYTANIE 22
Uczniowie biorą udział w konkursie na najlepszego bloga kulinarnego. Jedna koleżanka sama przygotowuje potrawy i fotografuje dania, by potem wrzucić je na swojego bloga. Druga nie ma dobrego aparatu, dlatego wrzuca na bloga zdjęcia ściągnięte z internetu, które nie są na wolnej licencji. Tylko pierwsza osoba postępuje prawidłowa?
tak/nie


ODPOWIEDŹ 1
NIE, nie wolno Ci kliknąć w podejrzany link. Usuwasz wiadomość.
ODPOWIEDŹ 2
NIE, nie jest rozsądne, ponieważ z tego komputera korzysta wiele osób i ktoś może włamać się na Twoje konto.
ODPOWIEDŹ 3
TAK, Twoje hasło spełnia wymogi bezpieczeństwa.
ODPOWIEDŹ 4
NIE, nie wolno podawać swojego hasła osobom postronnym. Ta wiedza jest tajemnicą, która nie powinna trafić do innych osób.
ODPOWIEDŹ 5
NIE, nie wolno Tobie klikać w podejrzane linki. Możesz stracić wszystkie swoje oszczędności.
ODPOWIEDŹ 6
TAK, wylogowujesz się, aby nikt nie miał dostępu do tego projektu i w ramach psikusa nie wprowadził Tobie zmian albo nie skopiował Twojego pomysłu.
ODPOWIEDŹ 7
TAK, w ten sposób chronisz dostęp do swoich kont.
ODPOWIEDŹ 8
NIE, nie podajesz takich danych. Ktoś chce najprawdopodobniej wyłudzić cudze dane. Może wykorzystać to i sfałszować dowód osobisty.


ODPOWIEDŹ 9
NIE, jej zachowanie było nieodpowiedzialne. W przypadku zgubienia lub kradzieży kart, ktoś może jej użyć i wypłacić pieniądze z bankomatu lub dokonać transakcji w sklepie.
ODPOWIEDŹ 10
TAK, aby nie stracić pieniędzy, zawsze należy sprawdzić opinie dotyczące danego produktu czy usługi i wybierać bezpieczne zakupy w internecie.
ODPOWIEDŹ 11
NIE, nie przesyłasz wiadomości dalej. To może być wirus niebezpieczny dla Twojego urządzenia.
ODPOWIEDŹ 12
TAK, używanie jednego hasła do wielu kont stwarza niebezpieczeństwo, że jeżeli ktoś złamie hasło jednej strony, to bez problemu wykorzysta je do przejęcia pozostałych kont.
ODPOWIEDŹ 13
TAK, mama postąpiła słusznie. Najprawdopodobniej trafiła na stronę, która niemal w idealny sposób "udawała" stronę, na której zawsze robiła zakupy. Fałszywa strona chciała wyłudzić login i hasło, to tzw. phishing.
ODPOWIEDŹ 14
TAK, postąpiłeś prawidłowo. Nie udostępniasz swoich danych. Możesz trafić przecież na oszusta, który okradnie Twoje konto.
ODPOWIEDŹ 15
TAK, mama miała rację. Zainstalowanie sprawdzonego i aktualnego programu antywirusowego może uchronić nasz sprzęt przed złośliwym oprogramowaniem.
ODPOWIEDŹ 16
NIE, Twój kolega postępuje słusznie. Zawsze należy się wylogować i usunąć historię przeglądania. Dzięki temu zachowujesz prywatność.

ODPOWIEDŹ 17

NIE, nigdy nie podajesz takich danych osobie, której nie znasz. To byłoby nierozważne i niebezpieczne. Informujesz rodziców o tej sytuacji. Oni podejmą decyzję czy o sprawie należy poinformować policję.

ODPOWIEDŹ 18

NIE, nie możesz tego zignorować. Najprawdopodobniej ktoś włamał się na Twoje konto. Natychmiast zmieniasz hasło. Informujesz koleżankę, by usunęła wiadomość, która nie pochodzi od Ciebie.

ODPOWIEDŹ 19

TAK, informujesz kolegę, że ma usunąć filmik. Wszelkie treści, które ośmieszają lub poniżają osobę są cyberprzemocą! Hejt jest karalny! To przestępstwo!

ODPOWIEDŹ 20

NIE, kolega nie może czuć się bezkarnie. To, że on usunął filmik ze swojego konta nie znaczy, że filmik dalej nie krąży w sieci i dalej nie narusza dóbr osobistych osoby poszkodowanej. Hejter nigdy nie pozostanie w ukryciu. Poniesie odpowiedzialność prawną za swoje czyny!

ODPOWIEDŹ 21

TAK, Twój kolega ma rację. Pamiętać należy, że granica pomiędzy krytyką a hejtem może być trudna do uchwycenia. Jeżeli krytykujesz, rób to w sposób kulturalny, używaj słów, które nie są nacechowane negatywnie. Nie obrażaj, nie poniżaj! Tego typu zachowania mają znamiona hejtu!

ODPOWIEDŹ 22

TAK, tylko pierwsza osoba postępuje prawidłowo. Druga kradnie cudzą własność. Jest mnóstwo stron, które pozwalają za darmo pobrać zdjęcia. Pamiętaj, aby podawać źródło zasobów, z których korzystasz. Unikniesz wtedy niepotrzebnych pytań dotyczących praw autorskich.

1.1

Jestem kobietą. Lubię mundur.

1.2

Kocham swój kraj.

1.3

Żegnali mnie w głuchej puszczy, w chacie leśnika.

1.4

Pisał o mnie sam Adam.

2.1

Jestem mężczyzną.

2.2

Uwielbiam uczty.

2.3

Często nie potrafię dochować tajemnic, które powierzają mi bogowie.

2.4

W języku polskim funkcjonuje frazeologizm, który w swojej treści ma moje imię.

3.1 Jestem piękna i zakochana.	3.2 Często spaceruję nad jeziorem ze swoim ukochanym.	3.3 Nie wierzyłam w miłość strzelca i poddałam go próbie.	3.4 Młodzieniec nie oparł się moim czarom. Sprowokowany, zdradził mnie.
4.1 Jestem mężczyzną. Imię otrzymałem na cześć pewnego sławnego wodza.	4.2 Wróciłem po studiach do rodzinnej posiadłości.	4.3 Zauroczyła mnie pewna kobieta, ale zakochałem się w cudownej i rozsądnej dziewczynie.	4.4 Wstępuję do Legionów Polskich. Jestem dzielnym żołnierzem.

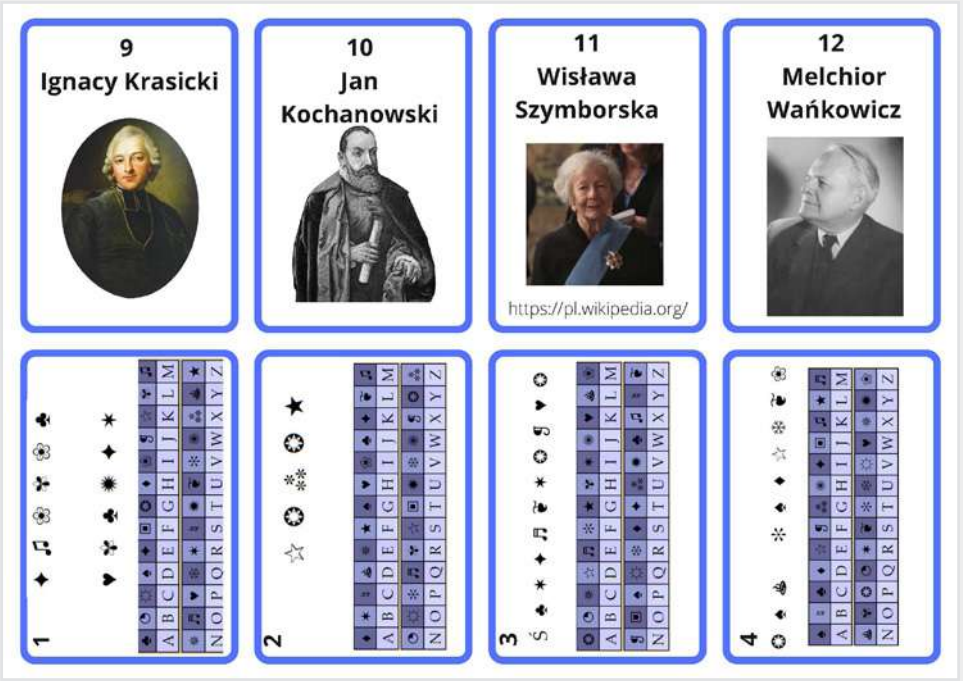
5.1 Jestem piękna. Mówią, że jestem dumna i wyniosła.	5.2 Zdarza mi się kłamać i manipulować pewnym chłopcem.	5.3 Bywam egoistyczna.	5.4 Jestem symbolem kobiecości, miłości i kruchości.
6.1 Jestem mężczyzną. Dużo w życiu widziałem.	6.2 Zamieszkałem na małej wyspie.	6.3 Po latach ciężkiej pracy i walki na różnych polach w obronie niepodległości, pragnąłem spokoju.	6.4 Pewnego dnia otrzymałem paczkę, która odmieniła moje życie.

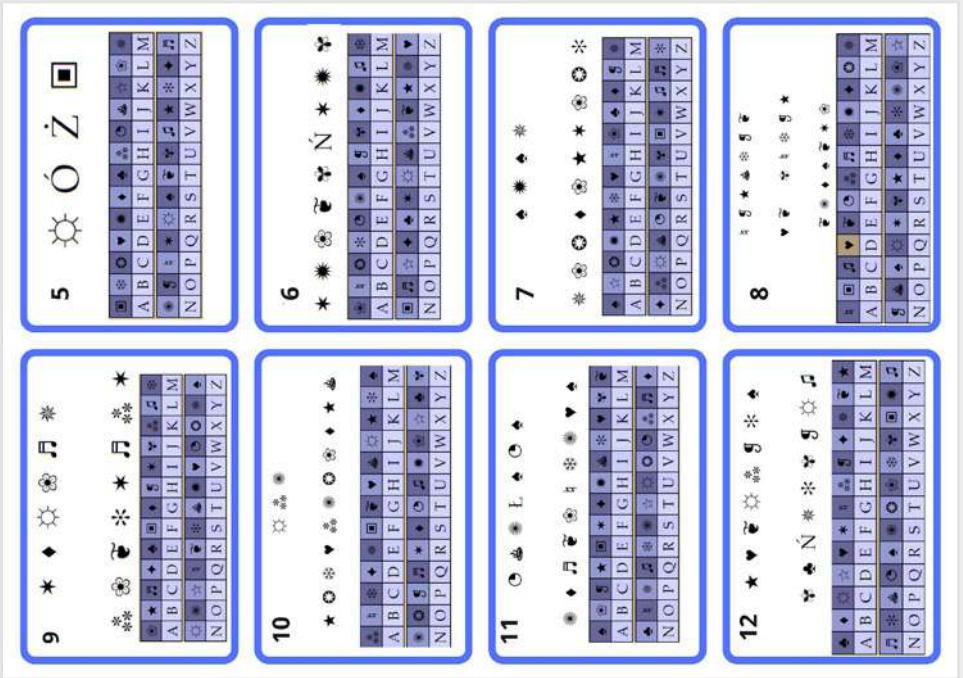

7.1
Byłem najpiękniejszym prezentem bożonarodzeniowym dla moich rodziców.
7.2
Urodziny i imieniny mam tego samego dnia.
7.3
Jestem poetą romantycznym. Piszę o miłości.
7.4
Moje utwory są wzniosłe i patetyczne. Dominują w nich idee narodowo-wyzwoleńcze.
8.1
Studiowałem architekturę. Lubiłem rysować.
8.2
Od zawsze interesowało mnie lotnictwo.
8.3
Służyłem w lotnictwie wojskowym. Miałem wypadek i przeniesiono mnie do rezerwy.
8.4
Moja książka ukazała się w XX wieku i szybko zyskała popularność.


9.1
Nazywają mnie "księciem poetów polskich".
9.2
Jestem biskupem warmińskim. Lubię czekoladę i kocham ogrody.
9.3
Biorę udział w obiadach czwartkowych. Współpracuję z królem Stanisławem Augustem.
9.4
Tworzę w oświeceniu. Napisałem pierwszą nowożytną powieść.
10.1
Jestem uważany za ojca poezji polskiej.
10.2
Studiowałem w Krakowie, Padwie. Lubiłem podróżować.
10.3
Moim ukochanym miejsce stał się Czarnolas.
10.4
Gatunki, w których tworzę: tren, pieśń, fraszki.

11.1 Jestem kobietą. Urodziłam się w Wielkopolsce. Lubię podróże.	11.2 Oprócz poważnych wierszy, tworzę także limeryki.	11.3 Ponoć jestem mistrzynią ironii. Lubię dostawać od znajomych tandetne gadżety.	11.4 W 1996 roku otrzymałam Nagrodę Nobla.
12.1 Mówią o mnie, że jestem wybitnym polskim reporterem.	12.2 Mam dwie córki: Krysię i Martę. Kocham z nimi podróżować.	12.3 Wymyśliłem najsłynniejsze hasło przedwojennej Polski: "Cukier krzepi". Otrzymałem za nie olbrzymie honorarium.	12.4 Moja córka Marta odziedziczyła po mnie dziennikarskiego bakcyla. Pracuje dla polskich i anglojęzycznych czasopism.

1 Emilia Plater 	2 Syzyf 	3 Świtezianka 	4 Pan Tadeusz 
5 Róża 	6 Skawiński 	7 Adam Mickiewicz 	8 Antoine de Saint-Exupéry 


9
Ignacy Krasicki
10
Jan
Kochanowski
11
Wisława
Szymborska
https://pl.wikipedia.org/
12
Melchior
Wańkowicz



JAK BUDOWAĆ I CHRONIĆ SWÓJ WIZERUNEK W SIECI?

autorka: Agnieszka Łazarek

Nawiązania do problemtyki związanej z cyberbezpieczeństwem

Kreowanie wizerunku młodego człowieka w Internecie.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Informatyka
III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi. Uczeń:
2. rozwija umiejętności korzystania z różnych urządzeń do tworzenia elektronicznych wersji tekstów, obrazów, dźwięków, filmów i animacji;
IV. Rozwijanie kompetencji społecznych. Uczeń:
2. ocenia krytycznie informacje i ich źródła, w szczególności w sieci, pod względem rzetelności i wiarygodności w odniesieniu do rzeczywistych sytuacji, docenia znaczenie otwartych zasobów w sieci i korzysta z nich;
V. Przestrzeganie prawa i zasad bezpieczeństwa. Uczeń:
1. opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją;
Wiedza o społeczeństwie
I. Społeczna natura człowieka. Uczeń:
2. przedstawia zasady komunikowania się; wyjaśnia zasady skutecznej autoprezentacji – kształtowania swojego wizerunku;
X. Środki masowego przekazu. Uczeń:
3. przedstawia funkcje reklamy i krytycznie analizuje wybrany przekaz reklamowy.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

Godzina wychowawcza, informatyka, wiedza o społeczeństwie

Adresaci lekcji (wiek, klasa)

13-14 lat; VII-VIII klasa

Cel ogólny lekcji i cele szczegółowe

Cel ogólny: Uczeń: wie, jak tworzyć i chronić swój wizerunek w sieci.

Cele szczegółowe: Uczeń:
- rozumie pojęcia cyfrowego śladu i reputacji online;
- zna korzyści i konsekwencje publikowania materiałów w sieci;
- aktywnie uczestniczy w dyskusji;

- wie, w jaki sposób dbać o reputację online w sieci;
- tworzy model wzorcowego profilu społecznościowego.

Metody pracy

- opis;
- zabawa dydaktyczna;
- dyskusja;
- metoda problemowa;
- quiz;
- praca twórcza.

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

- tablica interaktywna
- https://edpuzzle.com/media/63694642a85b6e413a469ed2
- karta pracy „Co składa się na Twój wizerunek w sieci?”
- plik jamboard
- karteczki samoprzylepne
- karta pracy „Wzorcowy profil społecznościowy”
- https://quizizz.com/admin/quiz/63695d6a6b225a001ea40d2c?source=quiz_share
- tablety lub telefony komórkowe do przeprowadzenia quizu

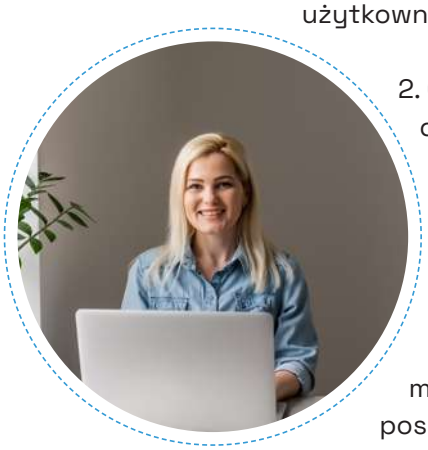
Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

Wprowadzenie

Nauczyciel rozdaje trojgu uczniów uczniom w klasie kartę pracy „Dodaj komentarz...”. Dzieci dopisują komentarze i przekazują sobie nawzajem kartę. Po zakończonej pracy zawartość kart zostaje odczytana. (5 minut)

Część główna

1. Na podstawie ćwiczenia wstępnego prowadzący nauczyciel odczytuje udzielone przez uczniów odpowiedzi. Wyjaśnia, że każdy wpis, zdjęcie lub inna czynność, która pozostawia ślad obecności użytkownika, nazywa się cyfrowym śladem. (2 minuty)



2. Cyfrowe ślady w internecie – burza mózgów. Nauczyciel zachęca uczniów do podawania przykładów aktywności internetowej, która pozostawia tzw. cyfrowy ślad. W wersji stacjonarnej uczniowie zapisują odpowiedzi na karteczkach samoprzylepnych, zaś w wersji on-line odpowiedzi udzielane zostaną za pośrednictwem platformy jamboard.google.com (7 minut)

3. Nauczyciel prezentuje uczniom film „Bekanie” z cyklu „Owce w sieci” umieszczony w aplikacji Edpuzzle. Uczniowie zapisują odpowiedzi za pomocą wyżej wymienionej aplikacji (wersja on-line i stacjonarna w przypadku posiadania odpowiedniego sprzętu). Następnie uczestnicy zajęć dzielą się wnioskami na temat obejrzanych treści. (10 minut)

Link do filmu z pytaniami:
https://edpuzzle.com/media/63694642a85b6e413a469ed2
4. Nauczyciel pokazuje i omawia infografikę „Co składa się na Twój wizerunek w sieci?" (Załącznik nr 1). Uczniowie podają propozycje innych elementów wizerunku internetowego. (5 minut)

5. Oryginalność w sieci. Nauczyciel rozpoczyna dyskusję na temat dzielenia się swoimi pasjami w internecie. Przypomina, że należy pamiętać o kilku zasadach: w jakiej formie chcemy pokazać nasze zainteresowania, każdy film lub zdjęcie zostają w internecie (cyfrowy ślad), film też wpływa na naszą reputację online. Następnie wypełnia kartę pracy „Wzorcowy profil społecznościowy" (Załącznik nr 2) (w wersji papierowej – w przypadku zajęć on-line uczniowie otrzymują link do edycji w programie Canva). Po wykonaniu pracy chętni uczniowie prezentują jej efekty. (10 minut)

Podsumowanie
Uczniowie w programie quizziz wykonują test sprawdzający wiedzę związaną z tematyką zajęć.
Link do quizu:
https://quizizz.com/admin/quiz/63695d6a6b225a001ea40d2c?source=quiz_share
Po wykonaniu nauczyciel krótko podsumowuje test. (6 minut)

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

1. Borkowska A., Witkowska M., (2020), *Sharenting i wizerunek dziecka w sieci. Poradnik dla rodziców*,
2. Warszawa: NASK – Państwowy Instytut Badawczy [online, dostęp z dn. 22.12.2021].
3. 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].

Lista dodatkowych plików, będących integralną częścią scenariusza

Załącznik nr 1 „Co składa się na Twój wizerunek w sieci?"
Załącznik nr 2 „Wzorcowy profil społecznościowy"

CYBER BEZPIECZNI

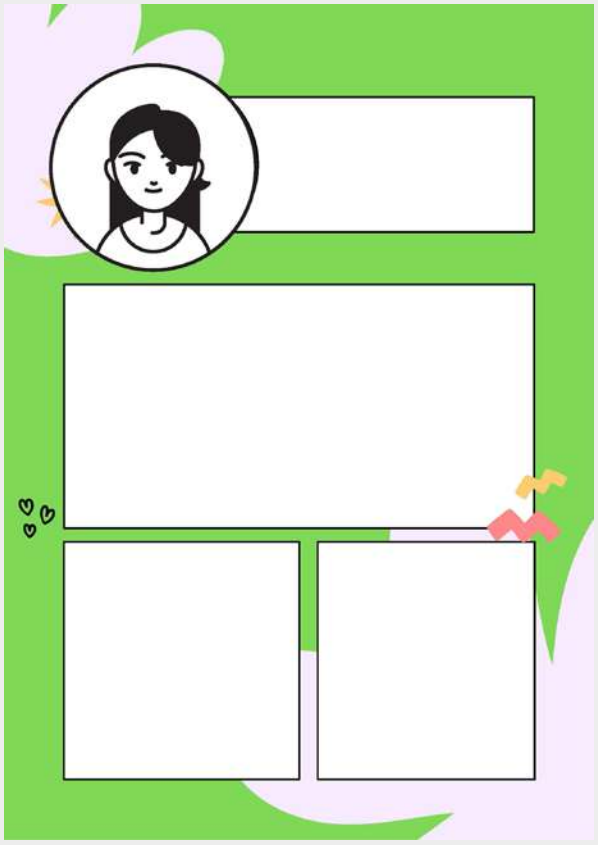
Co składa się na Twój wizerunek w sieci?

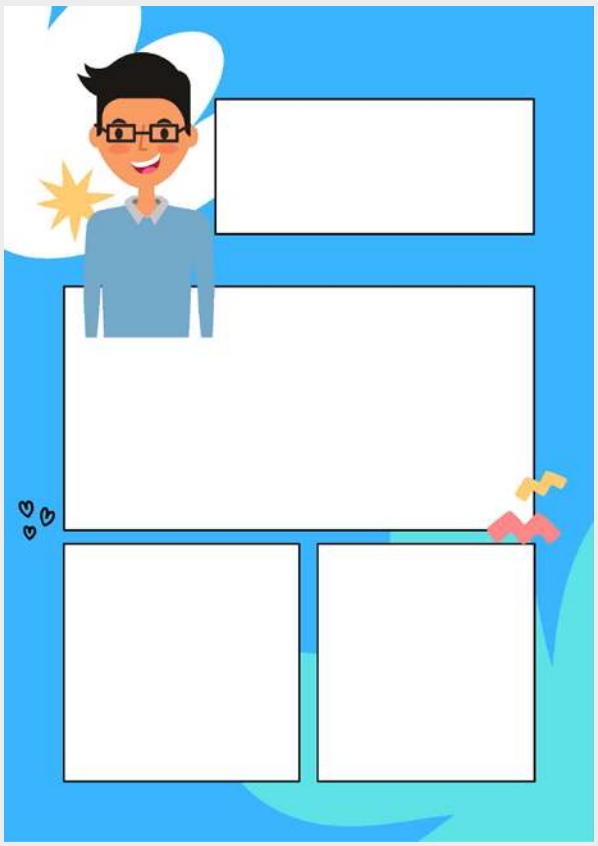
- zdjęcia, filmy i inne materiały z Twoim udziałem, publikowane przez Ciebie lub inne osoby;
- sposób wyrażania się i komunikowania, czyli co i w jaki sposób piszesz.

- przynależność do różnych grup i społeczności na poszczególnych portalach;

- wyszukiwane informacje, serwisy, z jakich korzystasz, pobierane i udostępniane materiały
- oznaczenia przez znajomych lub inne osoby;

- każdy ślad, jaki po sobie zostawiasz w sieci (posty, komentarze, wypowiedzi, lajki);





NIE DAJ SIĘ ZŁOWIĆ W SIECI

autorka: Iwona Cugier

CYBER BEZPIECZNI

Wskazanie nawiązania do problemtyki związanej z cyberbezpieczeństwem

Pojęcia: phishing, bezpieczeństwo hasła, poszanowanie wizerunku, hejt, nieznajomi w sieci, szkodliwe oprogramowanie.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Język polski
uczestniczy w rozmowie na zadany temat; rozróżnia argumenty odnoszące się do faktów i logiki oraz odwołujące się do emocji; dokonuje selekcji informacji; rozróżnia współczesne formy komunikatów (np. e-mail, SMS); korzysta z informacji zawartych w różnych źródłach, gromadzi wiadomości, selekcjonuje informacje; rozwija umiejętność krytycznej oceny pozyskanych informacji; rozwija umiejętności efektywnego posługiwania się technologią informacyjną oraz zasobami internetowymi i wykorzystuje te umiejętności do prezentowania własnych zainteresowań.

Informatyka
opisuje kwestie związane z wykorzystaniem komputerów i sieci komputerowych, takie jak bezpieczeństwo; posługuje się technologią zgodnie z przyjętymi zasadami i prawem; przestrzega zasad bezpieczeństwa i higieny pracy; wymienia zagrożenia związane z powszechnym dostępem do technologii oraz do informacji i opisuje metody wystrzegania się ich; stosuje profilaktykę antywirusową i potrafi zabezpieczyć przed zagrożeniem komputer wraz z zawartymi w nim informacjami; projektuje, tworzy i zapisuje w wizualnym języku programowania pomysły historyjek.

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

informatyka, plastyka

Adresaci lekcji (wiek, klasa)

12-13 lat, klasa 6

Cel ogólny lekcji i cele szczegółowe

Cel ogólny: Przestrzeganie zasad bezpieczeństwa, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Cele szczegółowe:
- Poznaje zasady bezpiecznego surfowania po sieci
- Wie, jak zabezpieczyć swoje dane osobowe i sprzęt
- Wie, do kogo może się zwrócić w sytuacji poczucia zagrożenia

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

• Wykonuje plakat „Kodeks uważności w internecie”
• Rozmawia z rodzicami na temat bezpieczeństwa w internecie i potrafi podać przykłady phishingu
• Wykonuje z rodzicami test na temat phishingu

Metody pracy

Metoda odwróconej klasy.
Metody aktywizujące: burza mózgów, studium przypadku, dyskusja, metoda projektowa, plakat
Metody oparte na praktycznej działalności uczniów z wykorzystaniem aplikacji Google

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

Komputer nauczyciela z dostępem do internetu, aplikacje Google, komputery uczniowskie

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

1. Powitanie, zapoznanie z celem lekcji - nawiązanie do materiału z obejrzanego w domu filmu - Konferencja Asów Internetu fragment na temat UWAŻNOSCI w sieci. (2 min.)

2. Zebranie odpowiedzi na pytanie „Z czym kojarzy ci się phishing?” z wykorzystaniem strony/aplikacji mentimeter (5 min.)Informacja dla uczniów:
Przypomnijcie sobie film obejrzany w domu. Proszę o odpowiedź na pytanie, które znajdziecie po wejściu na stronę menti.com i wpisaniu kodu. Możecie też użyć skanera kodów qr (oba kody – i liczbowy i qr – zapisane na slajdzie wyświetlonej prezentacji). Metimeter to również aplikacja, którą można pobrać ze sklepu Google Play lub App Store.

3. Wyszukiwanie definicji phishingu w internecie, podsumowanie (4 min.)
Phishing – 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.

4. Rozmowa nt. doświadczeń związanych z phishingiem – „Czy zdarzyło się wam spotkać z próbą oszukania was lub waszych bliskich?” „Jaki rodzaj komunikacji chciał wykorzystać oszust?” (SMS, mail, rozmowa telefoniczna) – praca zbiorowa lub w grupach 2 - osobowych (w zależności od grupy/poziomu kompetencji) (2 razy po 2 min.)
Grupy losujemy np. za pomocą narzędzia https://www.randomlists.com/list-randomizer

5. Zmiana przydziału w grupach – np. połączenie dwóch 2-osobowy w jedną 4-osobową.
Rozróżnianie – phishing czy nie, co na to wskazuje? (link, adres mailowy, adres strony, nazwa medium, załączniki...) (10 min.)
UWAGA: Przykłady z różnych kanałów – SMS, mail, komunikatory) praca w grupach 4-osobowych.
Z racji wieku uczniów nie dajemy przykładów związanych z fałszywą stroną banku. W podsumowaniu zadań możemy jednak pokazać taki przykład i rozszerzyć temat o oszustwo np. na blik.

W zależności od rodzaju sprzętu grupy korzystają z udostępnionego linku - https://tiny.pl/ww4bw lub z kodu qr (w załączniku).
Informacja dla uczniów:
Wasza praca będzie miała charakter grupowy – dobierzecie się w zespoły (objaśnienie sposobu doboru). Korzystając z linku/kodu qr otwórzcie stronę z prezentacją. Zapoznajcie się z umieszczoną tam instrukcją i wykonajcie zadanie. Macie na to 10 min.
UWAGA: Przestrzeń w klasie przygotowana jest do pracy grupowej – odpowiednie ustawienie stolików. Nauczyciel rozdaje kartki z linkiem/kodem qr, które posłużą również do zapisywania odpowiedzi. Podczas pracy dyskretnie kontroluje postęp pracy. W razie potrzeby wydłuża czas pracy (nie za dużo – około 5 min.)

6. Podsumowanie pracy zespołów – zbiorowe.
Nauczyciel zaznacza proponowaną opcję w tabelce, narysowanej na tablicy, za pomocą krzyżyka (5 min.)

Nr zadania	Nr grupy			
	1	2	3	4
1				
2				
3				
4				
5				

7. Podsumowanie zajęć w formie przygotowania przez grupy plakatu „Kodeks uważności w internecie". Plakat (format A1) zawierający zasady poznane na zajęciach będzie uzupełniany podczas kolejnych zajęć, gdy uczniowie wzbogacą swoją wiedzę o nowe elementy (bezpieczeństwo hasła, poszanowanie wizerunku, hejt, nieznajomi w sieci, szkodliwe oprogramowanie) (10 min.)
Ozdabiać będziecie na lekcji plastyki, realizując temat ornamentu i sztuki użytkowej. Zadanie pracy domowej – obejrzenie kolejnego fragmentu Konferencji na temat silnego hasła, weryfikacji dwuetapowej i zabezpieczenia telefonu (od 1.39 do 1.57 SIŁA) (5 min.) Rozmowa z rodzicami/opiekunami na temat prób oszustwa i wykonanie quizu - https://phishingquiz.withgoogle.com/

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

Konferencja Asów Internetu 11 lutego 2021 r. (fragmenty – od 59.45 do 1.19)
Konferencja Asów Internetu 11 lutego 2021 r. (fragmenty – od 1.39 do 1.57)
https://www.randomlists.com/team-generator
https://www.menti.com/alcobzjw6qrs (ankieta w mentimeter)
https://phishingquiz.withgoogle.com/

Lista dodatkowych plików, będących integralną częścią scenariusza

Prezentacja nt. phishingu

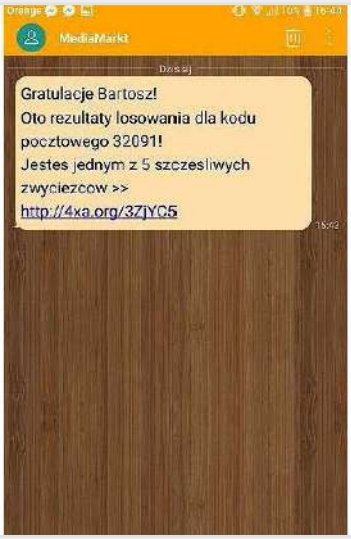
Phishing czy nie?

Ustalcie w grupie, czy jest to przykład oszustwa. Jeśli uważacie, że tak - napiszcie, dlaczego tak sądzicie? Macie na to 10 min.

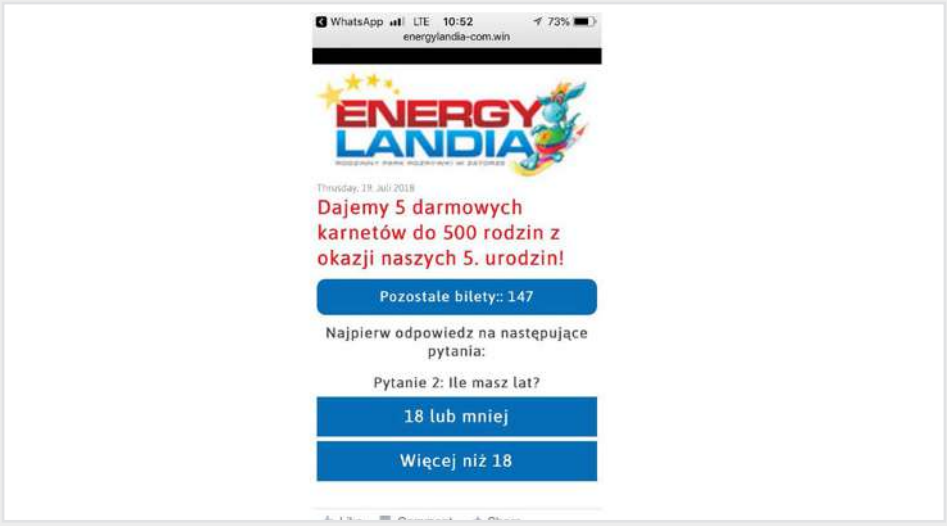
Odpowiedzi napiszcie na kartkach według wzoru:

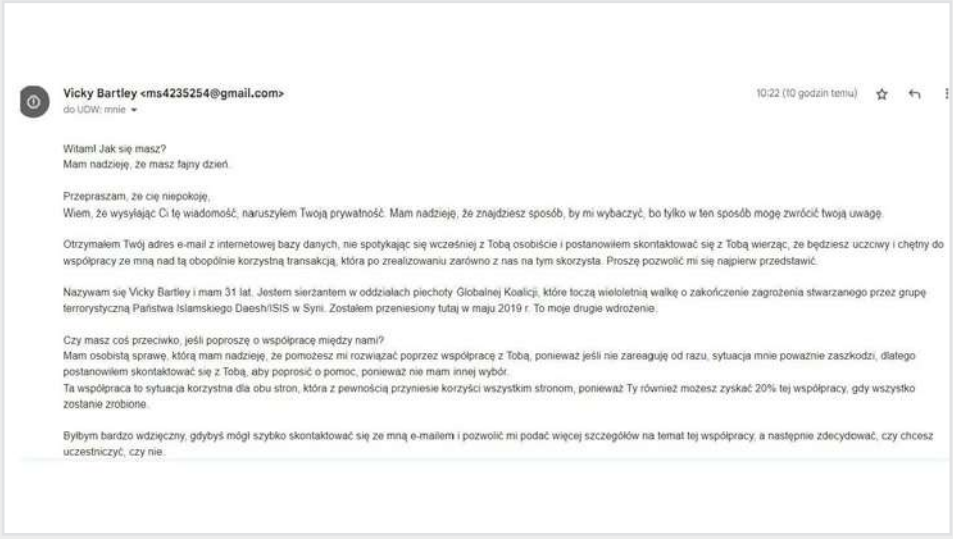
1 - phishing/nie phishing - *wyjaśnienie*

2 - .....




dotpay
Potwierdzenie platnosci
Numer transakcji:
M7295-1680
Kwota:
620,47 PLN
Status:
wykonana
Drogi Uzytkowniku! (Adresatem tej wiadomosci jest
Odnotowalismy próbe platnosci w kwocie 620,47 PLN
Opis zamówienia:
Wplata Online
Data i czas:
20 listopada 2017 23:42:59
Jezeli wplata zostala dokonana przelewem, odbiorca przelewu na wyciagu bedzie Dotpay SA Wielicka 72, 30-552 Krakow.
Informacja o wykonaniu platnosci zostala przekazana do sprzedawcy, a nalezne mu srodki udostepnione w Serwisie Dotpay.
Ewentualne pytania dotyczace realizacji zamówienia prosimy kierowac do sprzedawcy
Ta wiadomosc zostala wygenerowana automatycznie. Prosimy na nia nie odpowiadac.
Copyright © 2000-2017 Dotpay S.A. Wszystkie prawa zastrzezone.
Dotpay S.A.
ul. Wielicka 72, 30-552 Krakow, Polska, KRS 0000256796, NIP 634-26-61-860, REGON 240770255,
kapital zakladowy 4.000.000,00 PLN oplacono gotówka.
1 załącznik: Platnosc_w_systemie_Dotpay_M7295-1680_PDF.exe
Zapisz


WhatsApp LTE 10:52 73%
energylandia-com.win
ENERGY LANDIA
Thursday, 19 July 2018
Dajemy 5 darmowych karnetów do 500 rodzin z okazji naszych 5. urodzin!
Pozostale bilety:: 147
Najpierw odpowiedz na następujące pytania:
Pytanie 2: Ile masz lat?
18 lub mniej
Więcej niż 18


Vicky Bartley <ms4235254@gmail.com>
do UDW: mnie
10:22 (10 godzin temu)
Witam! Jak się masz?
Mam nadzieję, że masz fajny dzień.
Przepraszam, że cię niepokoję.
Wiem, że wysyłając Ci tę wiadomość, naruszyłem Twoją prywatność. Mam nadzieję, że znajdziesz sposób, by mi wybaczyć, bo tylko w ten sposób mogę zwrócić twoją uwagę.
Otrzymałem Twój adres e-mail z internetowej bazy danych, nie spotykając się wcześniej z Tobą osobiście i postanowiłem skontaktować się z Tobą wierząc, że będziesz uczciwy i chętny do współpracy ze mną nad tą obopólnie korzystną transakcją, która po zrealizowaniu zarówno z nas na tym skorzysta. Proszę pozwolić mi się najpierw przedstawić.
Nazywam się Vicky Bartley i mam 31 lat. Jestem sierżantem w oddziałach piechoty Globalnej Koalicji, które toczą wieloletnią walkę o zakończenie zagrożenia stwarzanego przez grupę terrorystyczną Państwa Islamskiego Daesh/ISIS w Syrii. Zostałem przeniesiony tutaj w maju 2019 r. To moje drugie wdrożenie.
Czy masz coś przeciwko, jeśli poproszę o współpracę między nami?
Mam osobistą sprawę, którą mam nadzieję, że pomożesz mi rozwiązać poprzez współpracę z Tobą, ponieważ jeśli nie zareaguję od razu, sytuacja mnie poważnie zaszkodzi, dlatego postanowiłem skontaktować się z Tobą, aby poprosić o pomoc, ponieważ nie mam innej wyboru.
Ta współpraca to sytuacja korzystna dla obu stron, która z pewnością przyniesie korzyści wszystkim stronom, ponieważ Ty również możesz zyskać 20% tej współpracy, gdy wszystko zostanie zrobione.
Byłbym bardzo wdzięczny, gdybyś mógł szybko skontaktować się ze mną e-mailem i pozwolić mi podać więcej szczegółów na temat tej współpracy, a następnie zdecydować, czy chcesz uczestniczyć, czy nie.

Przygotujcie plakat

Tytuł plakatu: Kodeks uważności w internecie.

Format: A1

Uwaga: Kodeks możecie uzupełniać również podczas zajęć plastyki.

Wasz kodeks zostanie zaprezentowany podczas obchodów Dnia Bezpiecznego Internetu. Później ozdobi korytarz szkoły.

SAFER THINGS

autorka: Agnieszka Pierwocha

CYBER BEZPIECZNI

Wskazanie nawiązania do problemtyki związanej z cyberbezpieczeństwem

Rodzaje przestępstw popełnianych w siedzi. Sposoby zapobiegania staniu się ofiarom przestępstwa.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

Podstawa programowa – wariant III.1.R
Język obcy nowożytny nauczany jako pierwszy (kontynuacja 1. języka obcego nowożytnego ze szkoły podstawowej – kształcenie w zakresie rozszerzonym)
I. 12: Uczeń posługuje się dość bogatym zasobem środków językowych (leksykalnych, gramatycznych, ortograficznych oraz fonetycznych), umożliwiającym realizację pozostałych wymagań ogólnych w zakresie następujących tematów: nauka i technika (korzystanie z podstawowych urządzeń technicznych i technologii informacyjno-komunikacyjnych oraz szanse i zagrożenia z tym związane);
II. Uczeń rozumie różnorodne złożone wypowiedzi ustne wypowiadane w naturalnym tempie:
II. 1: Uczeń reaguje na polecenia
II. 5: Uczeń znajduje w wypowiedzi określone informacje
II. 7: Uczeń wyciąga wnioski wynikające z informacji zawartych w wypowiedzi
III. Uczeń rozumie różnorodne złożone wypowiedzi pisemne:
III. 4: Uczeń znajduje w tekście określone informacje
III. 7: Uczeń wyciąga wnioski wynikające z informacji zawartych w tekście
IV. Uczeń tworzy w miarę złożone, spójne i logiczne, płynne wypowiedzi ustne:
IV. 2: Uczeń ustnie opowiada o czynnościach, doświadczeniach i wydarzeniach z przeszłości i teraźniejszości;
IV. 6: Uczeń ustnie wyraża i uzasadnia swoje opinie i poglądy, przedstawia i ustosunkowuje się do opinii i poglądów inn ych osób;
IV. 8: Uczeń ustnie przedstawia zalety i wady różnych rozwiązań;
IV.10: Uczeń ustnie przedstawia sposób postępowania (np. udziela instrukcji, wskazówek, określa zasady);
VI. Uczeń reaguje ustnie w różnorodnych, również złożonych i nietypowych sytuacjach:
VI. 3: uzyskuje i przekazuje informacje i wyjaśnienia;
VI.4: wyraża swoje opinie i uzasadnia je, pyta o opinie, zgadza się lub nie zgadza się z opiniami innych osób, komentuje wypowiedzi uczestników dyskusji, wyraża wątpliwość;
VIII.5: Uczeń przetwarza tekst ustnie lub pisemnie: streszcza w języku obcym przeczytany tekst;
X. Uczeń dokonuje samooceny i wykorzystuje techniki samodzielnej pracy nad językiem (np. korzystanie ze słownika, poprawianie błędów, prowadzenie notatek, stosowanie mnemotechnik, korzystanie z tekstów kultury w języku obcym nowożytnym).
XI. Uczeń współdziała w grupie (np. w lekcyjnych i pozalekcyjnych językowych pracach projektowych).
XII. Uczeń korzysta ze źródeł informacji w języku obcym nowożytnym (np. z encyklopedii, mediów, instrukcji obsługi), również za pomocą technologii informacyjno - komunikacyjnych.

XIII. Uczeń stosuje strategie komunikacyjne (np. domyślanie się znaczenia wyrazów z kontekstu, identyfikowanie słów kluczy lub internacjonalizmów) i strategie kompensacyjne, w przypadku gdy nie zna lub nie pamięta wyrazu (np. upraszczanie formy wypowiedzi, zastępowanie innym wyrazem, opis, wykorzystywanie środków niewerbalnych).

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

język angielski

Adresaci lekcji (wiek, klasa)

17-19 lat, poziom zaawansowania B2/B2+

Cel ogólny lekcji i cele szczegółowe

Cel ogólny:
• Utrwalenie i poszerzenie znajomości słownictwa związanego z korzystaniem z podstawowych urządzeń technicznych i technologii informacyjno-komunikacyjnych, ze szczególnym uwzględnieniem tematyki cyberbezpieczeństwa

Cele szczegółowe - Uczniowie:
• potrafią nazwać różne rodzaje cyberprzestępstw
• rozmawiają o szansach i zagrożeniach związanych z korzystaniem z technologii informacyjno-komunikacyjnych
• proponują możliwe sposoby zapobiegania staniu się ofiarą cyberprzstępczości

Metody pracy

Burza mózgów
Gra dydaktyczna – mini escape room stworzony w Genially
Praca w grupach
Metoda ewaluacyjna – mini ankieta w Classroomscreen.com
Prezentacja

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

Komputer z dostępem do Internetu
Projektor/Monitor interaktywny
Telefony komórkowe uczniów/Tablety lub komputery dostępne dla uczniów
Aplikacje:
• Classroomscreen.com
• Jigsawplanet.com
• Microsoft TEAMS
• Mentimeter.com
• Genially
• Quizlet (zadanie domowe/zadanie dodatkowe dla uczniów, którzy pracują szybciej)
• Wakelet (kolekcja dodatkowych materiałów dla uczniów)

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

czas	element lekcji
0-2	Przywitanie z uczniami oraz sprawdzenie obecności na lekcji. Nauczyciel wyświetla na ekranie tablicę Classroomscreen.com, na której uporządkowane są wszystkie czekające uczniów zadania.https://classroomscreen.com/app/screen/w/9eae51f9-13fc-45c1-ad86-d7750e74d-1d0/g/0c7d4f11-18ae-44ea-9f26-dc41f5ac8969---v1---default-screen-group/s/b5b7ef23-0f71-4915-be22-df02e2dba953
3-6	Rozgrzewka językowa i wprowadzenie tematu zajęć Uczniowie skanują kod QR z tablicy i układają puzzle by odkryć temat zajęć. https://www.jigsawplanet.com/?rc=play&pid=0126bf970e64 Następnie uczniowie wysyłają do nauczyciela wiadomość prywatną w aplikacji Teams, w której krótko wyrażają swoją opinię/ustosunkowują się do tematu zajęć jakim jest cyberbezpieczeństwo.
7-17	Cyberbezpieczeństwo i przestępstwa popełniane w sieci - prezentacja utworzona na mentimeter.com https://www.mentimeter.com/app/presentation/f36bc8ee770fb-1f255032502a070674a Slajd 1 (tytułowy) - uczniowie mogą dodawać komentarze oraz reakcje pokazujące ich stosunek do tematu. Slajd 2 – uczniowie oceniają czy czują się bezpiecznie surfując po sieci. Uśredniony wynik prezentowany jest na slajdzie. (metoda ewaluacyjna) Slajd 3 – uczniowie wpisują po 5 słówek/wyrażeń, które kojarzą im się z cyberprzestępczością (burza mózgów) Slajdy 4-7 – mini quiz dotyczący cyberprzestępczości mający na celu dodatkowe zmotywowanie uczniów do aktywnego udziału w zajęciach poprzez odrobinkę rywalizacji. Slajd 8 – Uczniowie dzielą się swoimi pomysłami na temat zapobiegania przestępstwom w sieci. (burza mózgów) Dzięki zastosowaniu prezentacji utworzonej w Mentimeter uczniowie mogą zabierać głos w dyskusji na forum grupy, jak również wpisywać komentarze w prezentacji. Dzięki temu rozwiązaniu również uczniowie nieśmiali lub niepewni siebie biorą aktywny udział w zajęciach.
18-19	Rozgrzewka językowa i wprowadzenie tematu zajęć Uczniowie skanują kod QR z tablicy i układają puzzle by odkryć temat zajęć. https://www.jigsawplanet.com/?rc=play&pid=0126bf970e64 Następnie uczniowie wysyłają do nauczyciela wiadomość prywatną w aplikacji Teams, w której krótko wyrażają swoją opinię/ustosunkowują się do tematu zajęć jakim jest cyberbezpieczeństwo.
20-29	Rozgrzewka językowa i wprowadzenie tematu zajęć Uczniowie skanują kod QR z tablicy i układają puzzle by odkryć temat zajęć. https://www.jigsawplanet.com/?rc=play&pid=0126bf970e64 Następnie uczniowie wysyłają do nauczyciela wiadomość prywatną w aplikacji Teams, w której krótko wyrażają swoją opinię/ustosunkowują się do tematu zajęć jakim jest cyberbezpieczeństwo.
30-39	Rozgrzewka językowa i wprowadzenie tematu zajęć Uczniowie skanują kod QR z tablicy i układają puzzle by odkryć temat zajęć. https://www.jigsawplanet.com/?rc=play&pid=0126bf970e64 Następnie uczniowie wysyłają do nauczyciela wiadomość prywatną w aplikacji Teams, w której krótko wyrażają swoją opinię/ustosunkowują się do tematu zajęć jakim jest cyberbezpieczeństwo.
40-45	Rozgrzewka językowa i wprowadzenie tematu zajęć Uczniowie skanują kod QR z tablicy i układają puzzle by odkryć temat zajęć. https://www.jigsawplanet.com/?rc=play&pid=0126bf970e64 Następnie uczniowie wysyłają do nauczyciela wiadomość prywatną w aplikacji Teams, w której krótko wyrażają swoją opinię/ustosunkowują się do tematu zajęć jakim jest cyberbezpieczeństwo.

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime
https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams- and-crimes/ransomware

https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams- and-crimes/spoofing-and-phishing

Lista dodatkowych plików, będących integralną częścią scenariusza

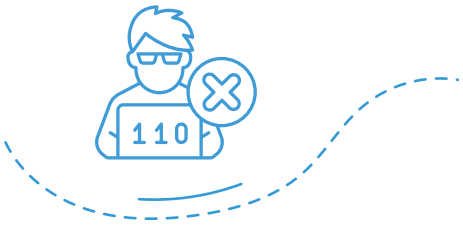
Tablica classroomscreen: https://classroomscreen.com/app/screen/w/9e-ae51f9-13fc-45c1-ad86-

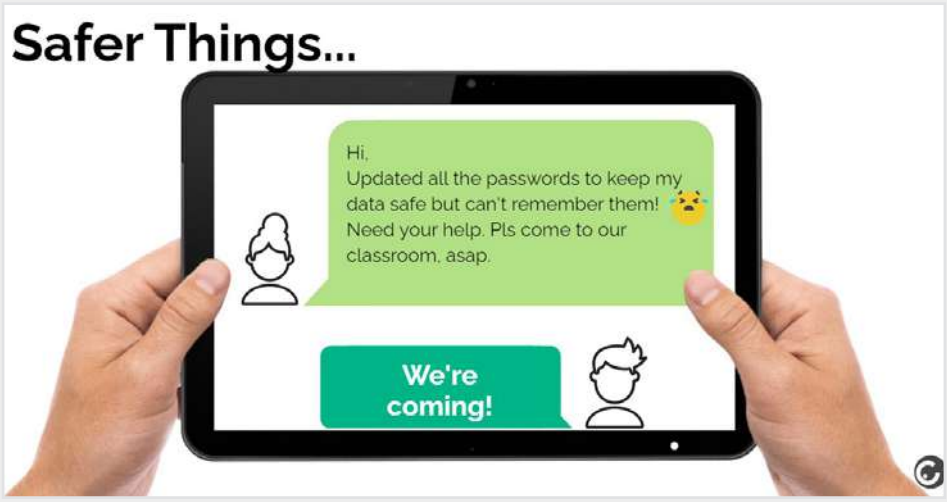
d7750e74d1d0/g/0c7d4f11-18ae-44ea-9f26-dc41f5ac8969---v1---default-screen- group/s/b5b7ef23-0f71-4915-be22-df02e2dba953

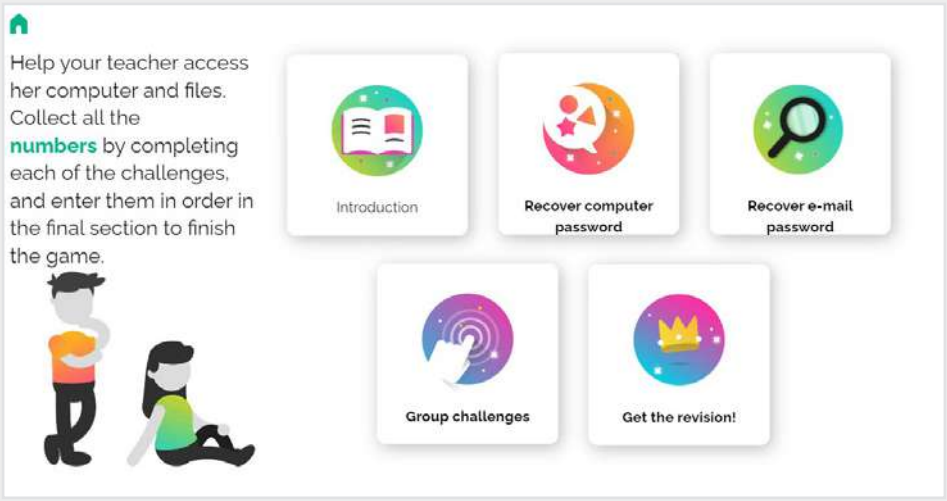
Rozgrzewka – puzzle: https://www.jigsawplanet.com/?rc=play&pid=0126bf970e64
Prezentacja wprowadzająca mentimeter:
https://www.mentimeter.com/app/presentation/f36bc8ee770fb1f255032502a070674a

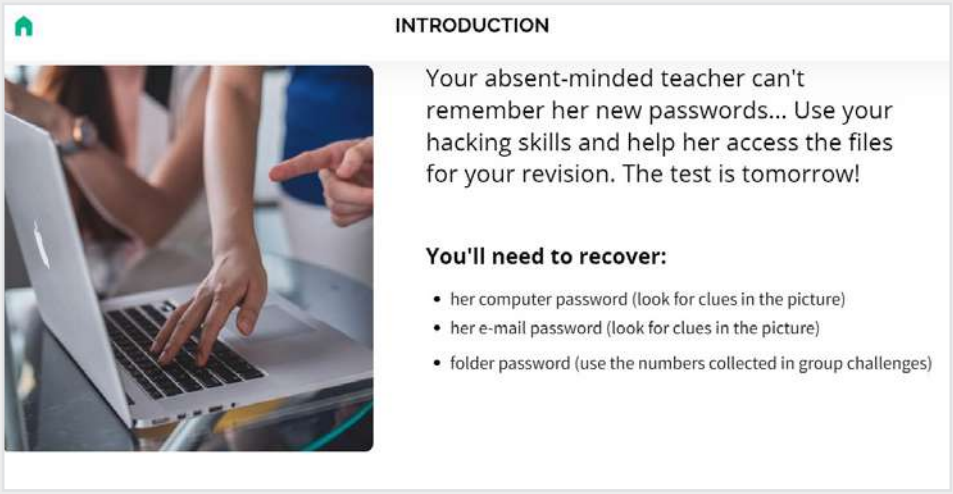
Presentacja- escape room: https://view.genial.ly/636855519803b10015dd12d2/interactive- content-vibrant-breakout

Materiały dla uczniów (zadanie domowe i powtórki do kartkówki)
https://wakelet.com/wake/W7uUrbygGSjf8bWG5r_KI
https://drive.google.com/file/d/1dUgzp3fb-RD4P596GXNtxAJGU1YWs-an/view?usp=sharing




Safer Things...
Hi,
Updated all the passwords to keep my data safe but can't remember them! Need your help. Pls come to our classroom, asap.
We're coming!


Help your teacher access her computer and files. Collect all the numbers by completing each of the challenges, and enter them in order in the final section to finish the game.
Introduction
Recover computer password
Recover e-mail password
Group challenges
Get the revision!


INTRODUCTION
Your absent-minded teacher can't remember her new passwords... Use your hacking skills and help her access the files for your revision. The test is tomorrow!
You'll need to recover:
• her computer password (look for clues in the picture)
• her e-mail password (look for clues in the picture)
• folder password (use the numbers collected in group challenges)

The State of Security

NEWS. TRENDS. INSIGHTS. Tripwire, Inc.

FEATURED ARTICLES TOPICS PODCAST VERT RESOURCES EXPLORE TRIPWIRE

5 Ways Your Organization Can Ensure Improved Data Security

DAVID BISSON

JAN 28, 2020

Each year on January 28, the United States, Canada, Israel and 47 European countries observe Data Privacy Day. The purpose of Data Privacy Day is to inspire dialogue on the importance of online privacy. **1.**_____

In observance of Data Privacy Day this year, here are five ***recommendations*** through which organizations can ***bolster*** their data security efforts.

Train Your Workforce

Organizations can use a security ***awareness*** training program to educate their employees about the importance of data security. Curricula CEO Nick Santora recommends that organizations begin by creating a team to create a strategic plan for the security awareness training program. Buy-in from the top is critical to this type of program, so the team should include executive management as well as initiative leaders.

2._____

This training should consist of digital security best practices and ***phishing*** testing. Digital security writer Anastasios Arampatzis also recommends that the program address drivers of malicious behavior to ***mitigate*** the risk of insider threats.

Embrace a Data-Centric Security Strategy

Mobile, the Internet of Things (IoT) and the cloud have dissolved the traditional ***boundaries*** of the network. As such, organizations need to now ***approach*** network security from a more holistic and strategic viewpoint. **3.**_____

Once they have an idea of what data they have, organizations should protect their data by doing ***encryption*** the right way. They should also look to the Center for Internet Security's Control 10 – Data Recovery Capabilities. As part of their implementation of this Control, organizations should develop a ***robust*** data backup strategy and test that strategy and their backups often.

Implement Multi-Factor Authentication (MFA)

Many of us are quick to change our login ***credentials*** following the public disclosure of a data breach. But by then, it could be too late. **4.**_____

_____ That gives attackers plenty of time to compromise those exposed accounts before anyone knows what happened.

Acknowledging that threat, organizations should take additional steps to shore up their users' business accounts against compromise. They can do so by following the ***requirements*** of the Center for Internet Security's Control 4 – Controlled Use of Administrative Privileges and using multi-factor authentication (MFA) for all administrative account access. They should also encourage users to implement MFA across their personal web accounts.

Set Strict Permissions for the Cloud

As they increasingly migrate their workloads to the cloud, organizations need to lock down their cloud-based data. Human error has already been responsible for the ***exposure*** of numerous AWS S3 buckets. In many of those incidents, a misconfiguration was responsible for exposing the personal information of millions of customers.

To prevent another AWS S3 breach, organizations should strategically use ACLs to grant read/write permissions to certain AWS accounts and/or predefined S3 groups. Security personnel should ***subsequently*** audit those accounts and their levels of access to ensure the principle of least privilege. They should not necessarily apply default permissions to their cloud-based data; in fact, they could choose to grant read-only access to a few system manager-specific s3 buckets

Exercise ***Vigilance*** for Patch Management

Finally, organizations can strengthen the security of their data by patching vulnerabilities through which malicious actors could gain access to their network assets. **5.**_____

_____ No test can cover every possible system configuration, so organizations should follow Tripwire VERT Senior Security Researcher Lane Thames' guidance and conduct their patch testing on a best-effort basis.

Organizations' **engagement** with a security fix doesn't end after they've ***implemented*** it. Indeed, they need to follow up a patch's ***deployment*** by scanning their system to confirm that the vulnerability is no longer present. This step will reveal if the patch has addressed the vulnerable components and if organizations need to take additional measures to remediate the ***vulnerability***.

Just the Beginning of Data Security

Security awareness training, a data-centric security strategy, MFA, strict cloud permissions and a robust patch management strategy are all efforts by which organizations can advance their data security. Even so, organizations can implement additional measures to prepare their systems in time for Data Privacy Day and beyond. They can learn more about these security controls here.

Read the text carefully and fill in the gaps with the sentences below. Theres one extra sentence you don't need.

A. *As Tripwire Principal Security Researcher Travis Smith noted in another blog post for The State of Security, many victimized businesses don't detect a data breach (if at all) until hundreds of days later.*
B. *At that point, the team can begin developing programs to educate the organization's workforce, including the C-Suite.*
C. *Information security expert Jeff Man urges organizations to specifically embrace a data-centric approach through which they develop a strategic understanding of what data they have and how valuable that data is to their business operations.*
D. *These discussions also seek to inspire individuals and businesses to take action in an effort to respect privacy, safeguard data and enable trust.*
E. *They can do this by formulating a patch management program through which they test patches before they deploy them on their production systems.*
F. *Failure to comply with this regulation can result in fines of up to 4% of gross revenue.*

How can you enhance your data security? Why is it so important? *(Write 120-150 words, use minimum 5 words from the text – the ones in bold)*

NHWWIPS2022@, CZYLI NAJBEZPIECZNIEJSZE HASŁO WE WSZECHŚWIECIE I „POD SŁOŃCEM”

autorka: Karolina Bąk

Wskazanie nawiązania do problemtyki związanej z cyberbezpieczeństwem

Nadawanie bezpiecznego hasła do poczty elektronicznej, ale także zabezpieczanie hasłem ważnej korespondencji służbowej stanowi istotny element pracy w każdym zawodzie, w której wykorzystujemy cyberprzestrzeń do przekazywania sobie informacji. Od silnego hasła oraz wprowadzenia weryfikacji dwuetapowej często zależy bezpieczeństwo danych całej organizacji.

Treści z podstawy programowej Ministerstwa Edukacji Narodowej realizowane w scenariuszu

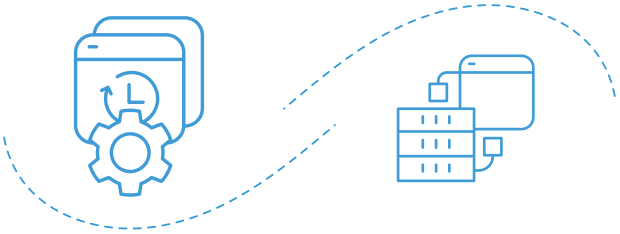
Podstawowa programowa Technik spedytor 333108 – SPL.05.2. Podstawy spedycji – efekt kształcenia: 2) sporządza korespondencję służbową oraz SPL.05.9. Kompetencje personalne i społeczne – efekt kształcenia: 2) przestrzega tajemnicy związanej z wykonywanym zawodem i miejscem pracy

Przedmiot/y nauczania, w ramach którego/ych ma być realizowany scenariusz

Pracownia techniki biurowej

Adresaci lekcji (wiek, klasa)

Klasa 3 i 4 technikum – wiek 17-19 lat



Cel ogólny lekcji i cele szczegółowe

Cel ogólny: Zapoznanie z zasadami tworzenia silnych haseł używanych w korespondencji służbowej do zabezpieczenia poczty elektronicznej, dokumentów oraz innych platform używanych w pracy biurowej.
Cele szczegółowe:
Uczeń zna zasady tworzenia bezpiecznych haseł.
Uczeń rozumie w jakim celu stosuje się silne hasła i gdzie je wykorzystać w pracy biurowej.
Uczeń potrafi utworzyć swoje oryginalne hasło i zaszyfrować dokument wysyłany za pomocą poczty elektronicznej.
Uczeń wskazuje związek tworzenia silnych haseł w pracy biurowej z życiem codziennym np. w bankowości elektronicznej.

Metody pracy

burza mózgów,
wykład,
case study,
praca indywidualna,
dyskusja.

Spis pomocy dydaktycznych, które mają być wykorzystane do przeprowadzenia lekcji

komputer,
prezentacja multimedialna PowerPoint,
Google Classroom,
studium przypadku – własny zaszyfrowany dokument Word,
„Stop klatki" wspomagające koncentrację uczniów,
gra edukacyjna „Milionerzy" – learningapps.org

Przebieg lekcji ze wskazaniem czasu na poszczególne jej elementy

Przywitanie uczniów, czynności organizacyjne (3 min).
Sformułowanie celu lekcji (2 min).
Wspólne sformułowanie celu i zasad tworzenia silnych, bezpiecznych haseł (10 min).
Omówienie obszarów w jakich stosuje się silne hasła w pracy biurowej, a także powiązanie z zastosowaniem w codziennym życiu – bankowość elektroniczna (10 min).
Praca indywidualna – kreowanie własnych bezpiecznych haseł oraz szyfrowanie nimi dokumentów – Word (15 min).
Podsumowanie tematu zajęć – gra „Milionerzy" (5 min).

Bibliografia i źródła wykorzystane do przygotowania scenariusza lekcji

Materiały NBP – Fundacja Młodzieży Przedsiębiorczości – Bezpieczne finanse
https://blog.avast.com/pl/10-rad-jak-wybra%C4%87-silne-has%C5%82o
https://support.microsoft.com/pl-pl/windows/tworzenie-i-u%C5%BCywanie-silnych-hase%C5%82-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
https://bezpiecznyinternet.edu.pl/jak-stworzyc-bezpieczne-haslo/

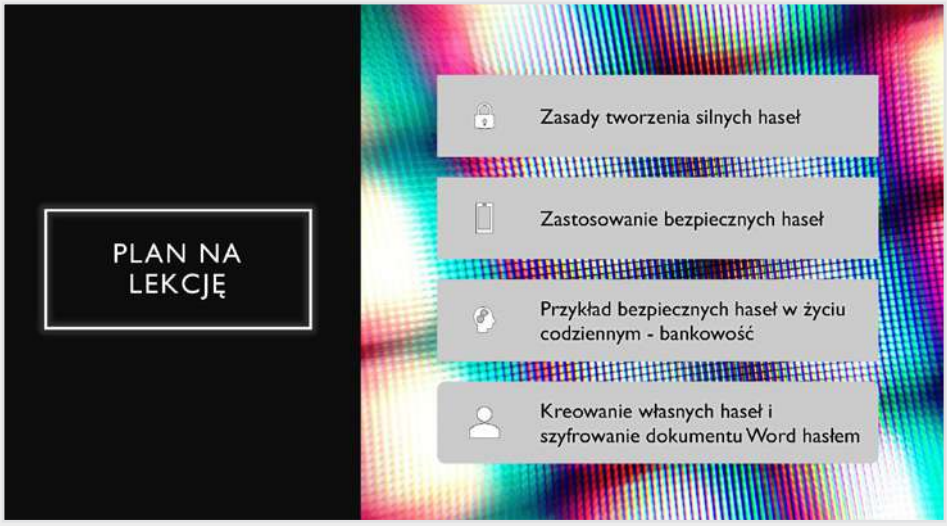
Lista dodatkowych plików, będących integralną częścią scenariusza

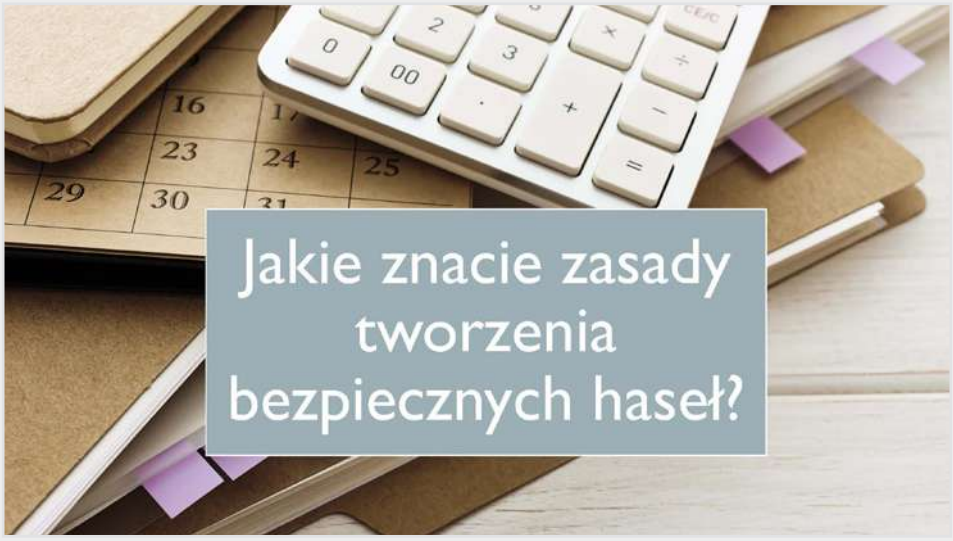
Prezentacja Power Point
Link do gry edukacyjnej podsumowującej lekcję
https://learningapps.org/watch?v=p2om280nv22

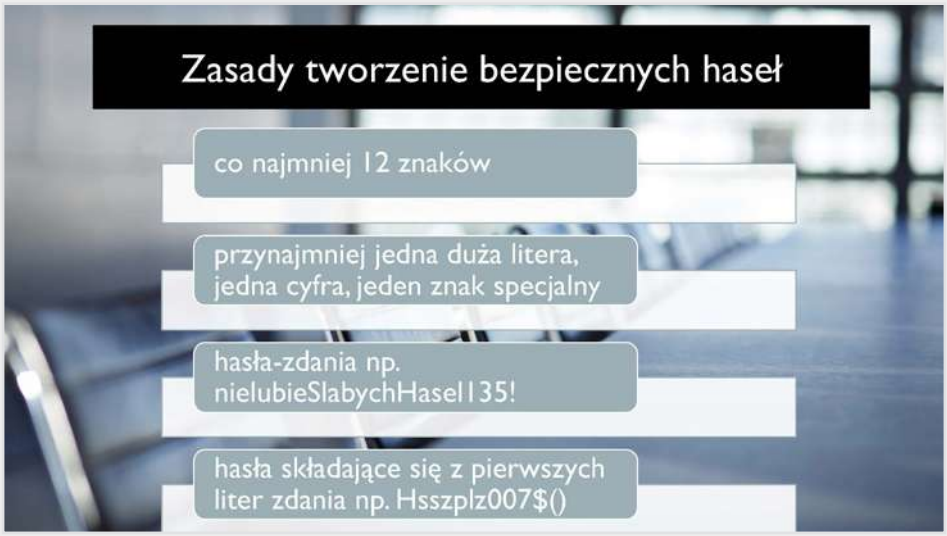
CYBER BEZPIECZNI

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".


NHWWIPS2022@, CZYLI NAJBEZPIECZNIEJSZE HASŁO WE WSZECHŚWIECIE I „POD SŁOŃCEM”
Karolina Bąk


PLAN NA LEKCJĘ
Zasady tworzenia silnych haseł
Zastosowanie bezpiecznych haseł
Przykład bezpiecznych haseł w życiu codziennym - bankowość
Kreowanie własnych haseł i szyfrowanie dokumentu Word hasłem

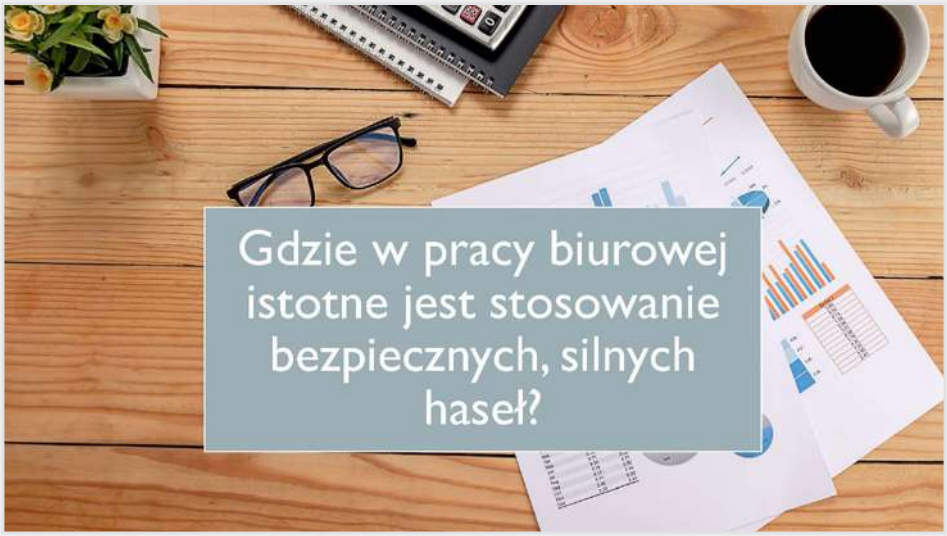

Jakie znacie zasady tworzenia bezpiecznych haseł?



STOP KLATKA!

Jakie znasz zasady tworzenia oryginalnych, silnych haseł?

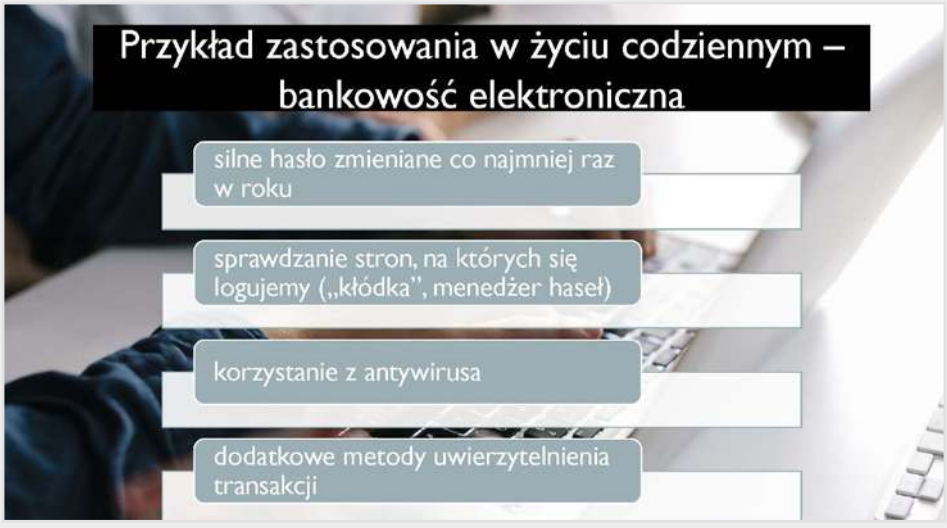
PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".


Gdzie w pracy biurowej istotne jest stosowanie bezpiecznych, silnych haseł?


ZASTOSOWANIE W PRACY BIUROWEJ SILNYCH HASEŁ
poczta służbowa
dostęp do służbowych urządzeń elektronicznych
dostęp do wewnętrznych serwerów firmowych
szyfrowanie przesyłanych dokumentów np. Word, PDF


STOP KLATKA!
PRODUCTION
DIRECTOR
SCENE
TAKE
ROLL
DATE
Jakie są 4 podstawowe obszary stosowania bezpiecznych haseł w pracy biurowej?


Jakie znamy inne zastosowanie silnych haseł w życiu codziennym?


Przykład zastosowania w życiu codziennym – bankowość elektroniczna
silne hasło zmieniane co najmniej raz w roku
sprawdzanie stron, na których się logujemy („kłódka", menedżer haseł)
korzystanie z antywirusa
dodatkowe metody uwierzytelnienia transakcji

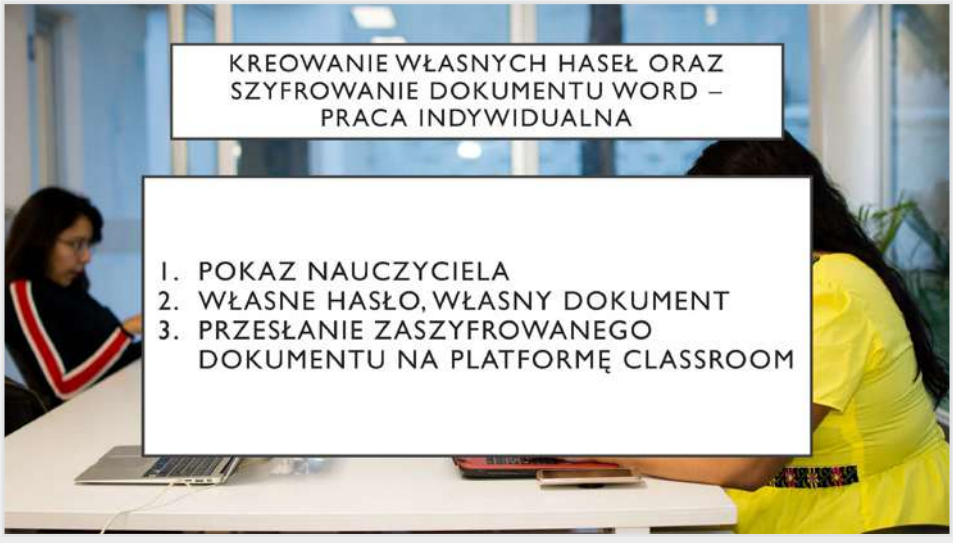

Przykład zastosowania w życiu codziennym – bankowość elektroniczna
sprawdzenie podejrzanych wiadomości email i smsów
limity transakcyjne i powiadomienia o przelewach
korzystanie z własnego sprzętu/internetu do logowania
dokładne czytanie wiadomości z banku

STOP KLATKA!

Wymień inne przykłady zastosowania bezpiecznego hasła w życiu codziennym?

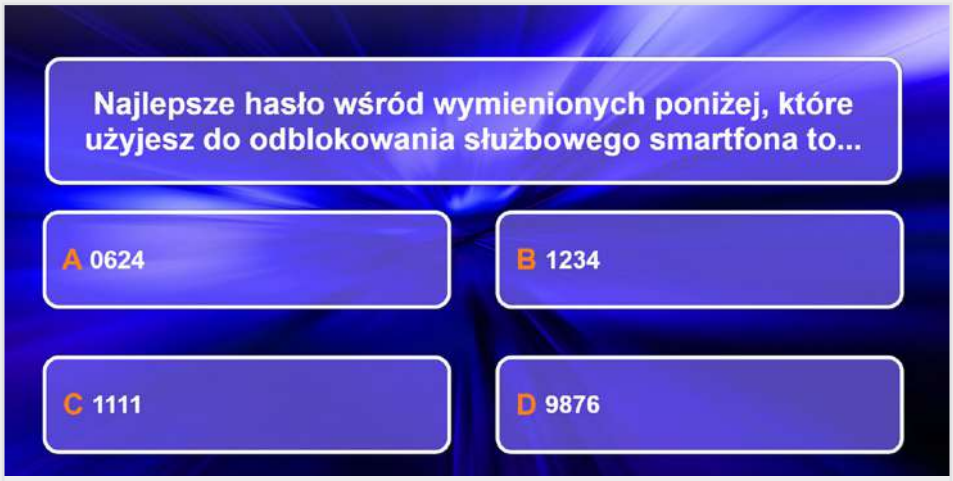
STOP KLATKA!

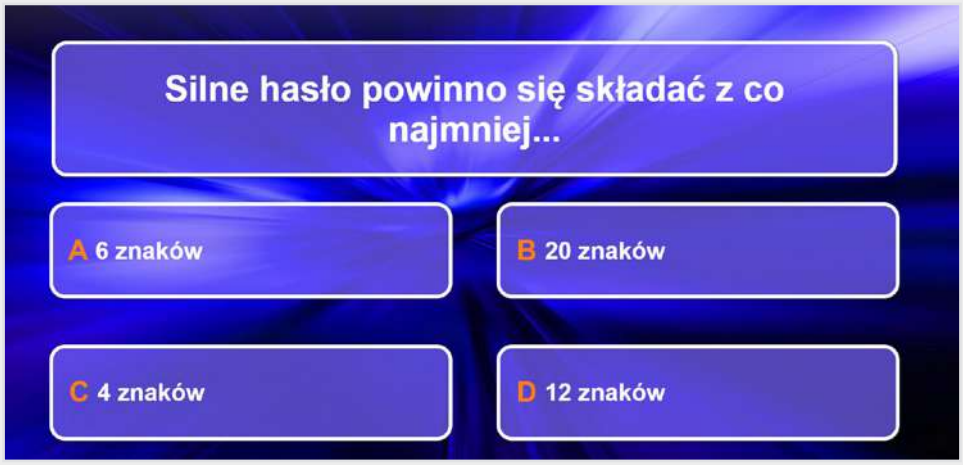
Jakie są zasady bezpiecznego korzystania z bankowości elektronicznej?



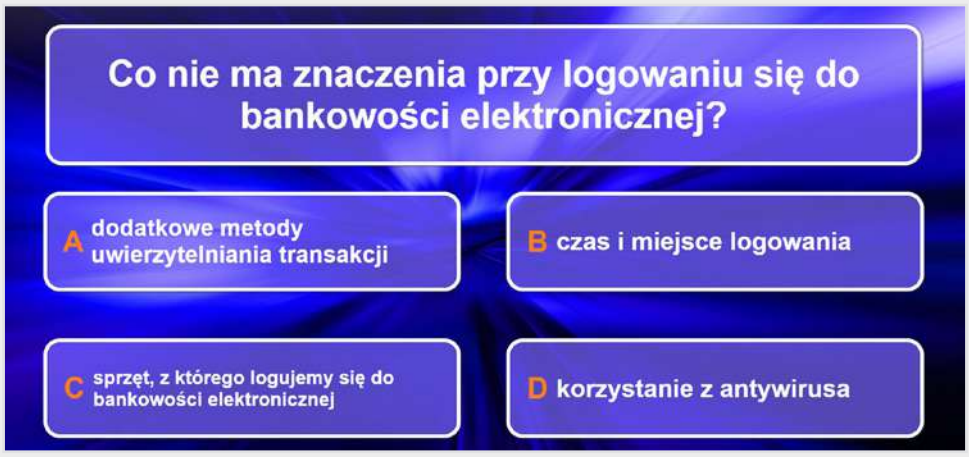

PODSUMOWANIE – „MILIONERZY”
HTTPS://LEARNINGAPPS.ORG/WATCH?V=P2OM280NV22

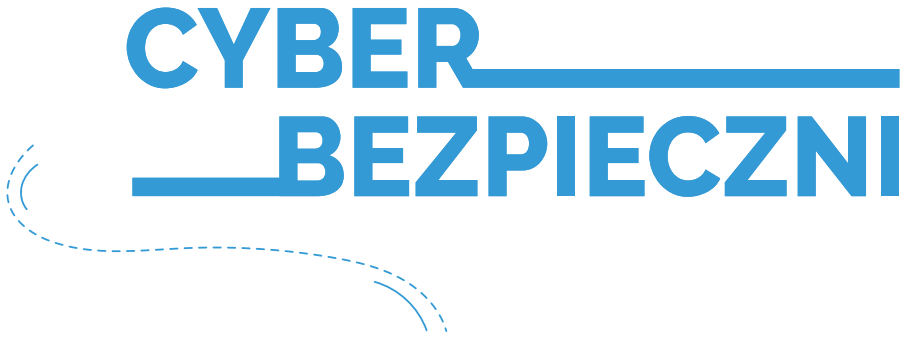

DZIĘKUJĘ ZA UWAGĘ
ALBO RACZEJ DZU ;)


Najlepsze hasło wśród wymienionych poniżej, które użyjesz do odblokowania służbowego smartfona to...
A 0624
B 1234
C 1111
D 9876


Silne hasło powinno się składać z co najmniej...
A 6 znaków
B 20 znaków
C 4 znaków
D 12 znaków


Aby dodatkowo zabezpieczyć pracowniczą pocztę elektroniczną należy...
A zapisać hasło na kartce przy komputerze
B stosować weryfikację dwuetapową
C korzystać z tego samego hasła do kilku serwisów
D nigdy nie zmieniać hasła


Co nie ma znaczenia przy logowaniu się do bankowości elektronicznej?
A dodatkowe metody uwierzytelniania transakcji
B czas i miejsce logowania
C sprzęt, z którego logujemy się do bankowości elektronicznej
D korzystanie z antywirusa


CYBER
BEZPIECZNI

FUNDACJA POLSKIEGO FUNDUSZU ROZWOJU

Fundacja Polskiego Funduszu Rozwoju to organizacja non-profit utworzona w 2018 roku przez Polski Fundusz Rozwoju. Fundacja realizuje swoje zadania statutowe poprzez działania i projekty z zakresu edukacji – poprzez własne projekty, wspieranie inicjatyw społecznych (granty i darowizny) i wolontariat pracowniczy. Główny cel tych projektów to przeciwdziałanie wykluczeniu cyfrowemu, wyrównywanie szans edukacyjnych, wyrównywanie szans na rynku pracy różnych grup społecznych – w tym dzieci zamieszkujących tereny Polski wschodniej, dzieci-wychowanków ośrodków wychowawczych i pieczy zastępczej oraz seniorów – poprzez programy edukacyjne bazujące na nowych technologiach.

Fundacja realizuje szereg inicjatyw edukacyjnych, a największą z nich jest Centralny Dom Technologii, czyli unikatowy w skali kraju projekt, łączący świat nauki, technologii i biznesu. Centralny Dom Technologii tworzy zespół edukatorów i ekspertów nowoczesnej edukacji opartej na metodologii STEAM. W Centralnym Domu Technologii, mieszczącym się w Warszawie, organizowane są wydarzenia, projekty partnerskie, ale głównym i najważniejszym obszarem działalności są zajęcia warsztatowe stacjonarne i online dla dzieci, młodzieży i dorosłych, w tym także dla osób starszych.

Dodatkowe obszary działalności Fundacji to wspieranie innowacyjności, przedsiębiorczości, motywowanie do zwiększania kompetencji przez całe życie, budowanie postaw prospołecznych i aktywizacja zawodowa. Podstawowe grupy odbiorców działań realizowanych przez Fundację to dzieci, młodzież oraz osoby starsze, jednakże naszym celem jest stworzenie całego ekosystemu dobrych praktyk i zaangażowanych instytucji, tak aby realizowane projekty miały realny wpływ na życie beneficjentów Fundacji. W ramach realizacji swoich celów statutowych Fundacja PFR tworzy własne autorskie projekty, ale także przystępuje do Partnerstw, dzięki którym ma możliwość realizacji projektów społecznych, edukacyjnych i kulturalnych.

Więcej informacji na temat Fundacji znajduje się na stronie: **www.fundacjapfr.pl**

PFR Fundacja

PROJEKT JEST FINANSOWANY ZE ŚRODKÓW KANCELARII PREZESA RADY MINISTRÓW W RAMACH OGÓLNOPOLSKIEGO PROGRAMU ROZWOJU KOMPETENCJI UCZNIÓW I NAUCZYCIELI „CYBERBEZPIECZNI".

Centralny Dom Technologii

Partner ścieżki edukacyjnej
Cyfrowa przedsiębiorczość

allegro

Patron medialny

pap
POLSKA AGENCJA PRASOWA

Edukacja Jutra

CYBER BEZPIECZNI

Projekt jest dofinansowany ze środków Kancelarii Prezesa Rady Ministrów w ramach ogólnopolskiego programu rozwoju kompetencji uczniów i nauczycieli „Cyberbezpieczni".