SCENARIUSZ LEKCJI - Phishing

1. Temat lekcji Nie daj się złowić! Jak cyberprzestępcy zastawiają sieci w sieci.

2. Typ szkoły / Wiek uczniów Szkoła podstawowa, klasa 4-6 (uczniowie w wieku 10-13 lat)

3. Liczba godzin 1 godzina lekcyjna (45 minut)

4. Cele lekcji

Główne cele (do osiągnięcia w ciągu jednej lekcji):

- Uczniowie poznają pojęcie phishingu oraz związane z nim zagrożenia.
- Uczniowie nauczą się, jak rozpoznawać fałszywe wiadomości i strony internetowe.

Szczegółowe cele:

a) Zapamiętanie:

- Uczeń wie, czym jest phishing.
- Uczeń zna cechy charakterystyczne podejrzanych wiadomości e-mail i stron internetowych.

b) Zrozumienie:

- Uczeń rozumie, dlaczego nie powinien podawać danych osobowych przez Internet.
- Uczeń rozumie, jak oszuści manipulują wyglądem stron i adresami e-mail.

c) Zastosowanie:

- Uczeń potrafi wskazać sygnały ostrzegawcze w wiadomościach.
- Uczeń potrafi sprawdzić wiarygodność adresu URL i nadawcy wiadomości.

5. Metody i techniki pracy

- Dyskusja kierowana (burza mózgów)
- Analiza przypadków (case study)
- Ćwiczenia praktyczne (identyfikacja phishingu)
- Quiz

6. Środki dydaktyczne

- Komputer z dostępem do Internetu

- Rzutnik multimedialny / tablica interaktywna
- Aplikacja do tworzenia fałszywych wiadomości e-mail (https://emkei.cz/)
- Przykłady phishingowych wiadomości e-mail i fałszywych stron

7. Formy pracy z uczniami

- Praca z całą klasą (dyskusja, prezentacja)
- Praca indywidualna (refleksja, odpowiedzi)

8. Przebieg lekcji

a) Czynności organizacyjne (2 min)

- Sprawdzenie obecności

b) Wprowadzenie (7 min)

Nauczyciel pyta uczniów: *Czy słyszeliście kiedyś o sytuacji, gdy ktoś dostał e-mail od banku lub innej firmy, który okazał się oszustwem? Czy w grach online albo na czatach ktoś kiedyś wysłał wam podejrzany link?* albo *Czy słyszeliście o przypadkach, że ktoś podszył się pod kogoś na komunikatorze?* Pozwala chętnym podzielić się doświadczeniami (np. może któryś uczeń widział taki e-mail u rodziców albo słyszał o oszustwie z wiadomością o wygranej).

Jeśli nikt się nie zgłasza, nauczyciel opisuje krótko wymyśloną sytuację: *Wyobraźcie sobie, że dostajecie e-mail z gry online z informacją o wygraniu super nagrody, ale musicie kliknąć link i zalogować się na stronie. Co byście zrobili?*

Po kilku odpowiedziach nauczyciel informuje, że tematem lekcji jest **phishing**, czyli wyłudzanie danych przez fałszywe wiadomości. Wyjaśnia genezę słowa *phishing* – brzmi podobnie do *fishing* (wędkowanie), bo oszust "zarzuca przynętę" w postaci fałszywej informacji, by złowić ofiarę i wyciągnąć od niej cenne dane. Przedstawia krótko cel zajęć językiem zrozumiałym dla uczniów, np.: *Dziś dowiemy się, co to jest phishing i jak się przed nim chronić – to nasz główny cel.* Podkreśla, że *phisher* (oszust) najczęściej wysyła fałszywe e-maile albo wiadomości SMS, które wyglądają na prawdziwe i próbują nas skłonić do natychmiastowego działania. Nauczyciel może wspomnieć uczniom o realnych dla nich sytuacjach jak gry online.

c) Praca właściwa (35 min)

Kreskówka edukacyjna: (5 min) - załącznik 1.

Aby uczniowie lepiej zrozumieli sytuacje phishingowe, nauczyciel uruchamia krótki film animowany z serii **"Owce w Sieci"**, odcinek "Papla" – który pokazuje w przystępny sposób, jak łatwo można wyłudzić czyjeś dane osobowe i hasła w Internecie. Po projekcji nauczyciel zadaje pytania: *Jakie błędy popełniła postać z filmu? Co zrobił*

oszust? Jak można było tego uniknąć?" Uczniowie krótko omawiają, co zrozumieli z filmiku: że nie wolno zbyt łatwo ufać nieznajomym w sieci i zdradzać o sobie zbyt wiele informacji.

Ćwiczenie 1: Analiza fałszywego e-maila (7 min) – załącznik 2 (instrukcja do aplikacji oraz treść wiadomości).

Nauczyciel prezentuje na tablicy **przykładową wiadomość e-mail** stworzoną przy użyciu aplikacji https://emkei.cz/, rzekomo od dyrektora szkoły. Razem z nauczycielem uczniowie szukają **jak najwięcej podejrzanych elementów** w tej wiadomości. Nauczyciel podpowiada, na co zwracać uwagę:

- nietypowy adres nadawcy (np. dziwna domena e-mail),
- brak polskich znaków lub liczne błędy,
- zwroty typu "Pilne!", "Natychmiast" itp.,
- prośba o podanie danych
- prośba o kliknięcie linku.

Podkreśla, że phisherzy często **tworzą fałszywe strony internetowe do złudzenia przypominające prawdziwe** strony banków czy sklepów. Czasem wysyłają wiadomość, która **wygląda jak oficjalna**, ale np. cała jest grafiką z linkiem.

Ćwiczenie 2: Fałszywa strona internetowa (7 min) – załącznik 3.

Nauczyciel pyta uczniów, czy wiedzą, jak wygląda strona logowania do Facebooka. Po odpowiedziach nauczyciel otwiera fałszywą stronę: **plik lokalny z załącznika 3** i pyta uczniów, czy to ta? Uczniowie odpowiadają.

Jeśli jakiś uczeń stwierdzi, że nie, to nauczyciel prosi go o wyjaśnienie, czym w takim razie się różni? Po krótkiej rozmowie nauczyciel wyjaśnia, że należy uważać na wszystkie linki w mailach i wiadomościach czy na stronach internetowych, ponieważ ta strona jest fałszywa.

Nauczyciel prezentuje i krótko omawia kilka przykładów oszust phishingowych na podstawie prezentacji + krótko przypomina definicję phishingu. **Załącznik 4**

d) Podsumowanie pracy uczniów (3 min)

Nauczyciel wspólnie z klasą podsumowuje lekcję. Prosi chętnych uczniów, by wymienili po **jednym najważniejszym wniosku** z dzisiejszych zajęć – co zapamiętali lub co ich najbardziej zaskoczyło.

e) Ocena (10 min)

- Pytania sprawdzające zrozumienie tematu (Quiz)

Uczniowie na tablicy interaktywnej po kolei, wywołani przez nauczyciela przeciągają elementy podejrzane oraz bezpieczne do odpowiednich grup.

- Szybka autoocena uczniowska: Co już wiem? Czego się nauczyłem?

9. Ewaluacja

- Nauczyciel obserwuje zaangażowanie uczniów w dyskusję i ćwiczenia
- Krótka ankieta ustna: Czy temat był dla Was interesujący? Czy wiecie, jak się chronić przed phishingiem? *Kto czuje, że teraz umiałby rozpoznać podejrzanego maila? Ręka do góry*.
- Nauczyciel zapowiada, że na następnej lekcji porozmawiamy sobie o vishingu – czyli o phisingu głosowym. Forma oszustwa nie za pomocą wiadomości, a rozmów telefonicznych.

Załączniki:

1. **Link do filmu edukacyjnego:** https://www.youtube.com/watch?v=e4WTiDx5mlA
2. Instrukcja – jak stworzyć fałszywy mail w aplikacji emkei.

Krok 1: Wejdź na stronę

Przejdź do: https://emkei.cz/

Krok 2: Wypełnij formularz

1. **From name** – wpisz nazwę nadawcy (np. Anna Nowak, `Dyrektor Szkoły`).
2. **From e-mail** – wpisz fałszywy adres, np.annanowak.dyrektor@wp.pl *(Może wyglądać realistycznie, ale nie musi istnieć naprawdę)*.
3. **To** – wpisz swój własny adres e-mail (lub zostaw pusty, jeśli nie będziesz wysyłać wiadomości).
4. **Subject** – wpisz temat wiadomości (np. `Ważne! Aktualizacja legitymacji szkolnych`).
5. **Attachments** – pozostaw puste (niepotrzebne do demonstracji).
6. **Text** – wpisz treść wiadomości. Możesz skorzystać z przykładowego tekstu phishingowego (Treść poniżej.

Krok 3: (Opcjonalnie) kliknij przycisk „Send”

7. Tylko jeśli chcesz przetestować wysyłkę – najlepiej na swój **własny adres e-mail** w celach demonstracyjnych.
   Nie wysyłaj do uczniów ani innych osób!
   Alternatywa: zrób **zrzut ekranu** wiadomości lub pokaż formularz wypełniony na tablicy interaktywnej.

Przykładowa fałszywego maila do analizy

Temat: Ważne! Aktualizacja legitymacji szkolnych.

Treść: Drodzy Uczniowie,

Zgodnie z nowymi przepisami wprowadzonymi przez Kuratorium Oświaty, szkoła musi zaktualizować Wasze legitymacje uczniowskie. Jest to konieczne, aby mogły one dalej obowiązywać i dawały Wam prawo do różnych zniżek – na przykład przy wejściu do kina, muzeum, zoo czy parku rozrywki. 🎵 🦁 🎡

Aby przygotować zaktualizowaną legitymację, prosimy, abyście przesłali w odpowiedzi na tę wiadomość następujące dane:

- imię i nazwisko,
- numer PESEL,
- adres zamieszkania,
- numer telefonu do Waszego rodzica lub opiekuna.

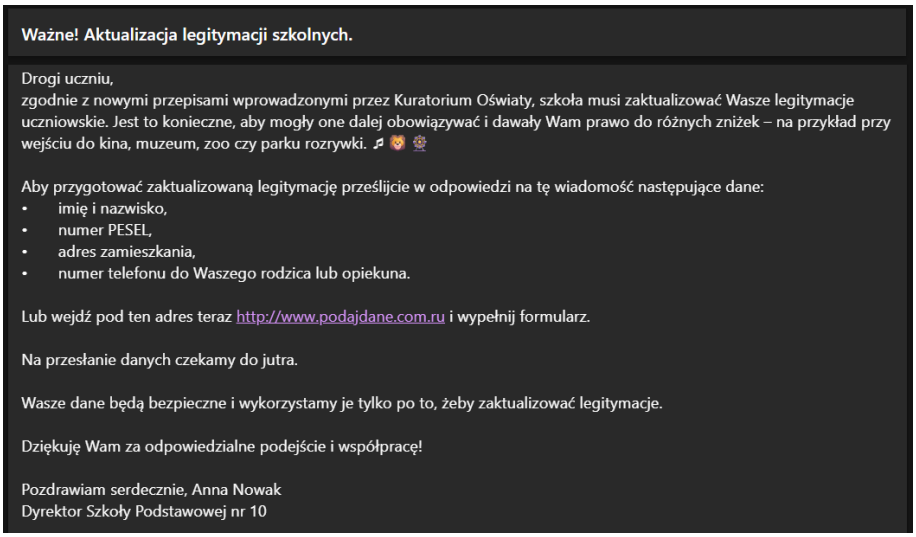
Lub weszli pod ten adres http://www.podajdane.com.ru i wypełnili formularz.

Na przesłanie danych czekamy do jutra.

Wasze dane będą bezpieczne i wykorzystamy je tylko po to, żeby zaktualizować legitymacje.

Dziękuję Wam za odpowiedzialne podejście i współpracę!

Pozdrawiam serdecznie, Anna Nowak
Dyrektor Szkoły Podstawowej nr 10



3. **Fałszywa strona facebooka:** Plik lokalny fałszywej strony facebooka. **POBIERZ**

4. **Przykłady phishingu:** **https://prezi.com/view/7atLIlkU9WjUmSzHrOt3/**

5. **Pytania sprawdzające:**

Quiz, w którym uczniowie wskazują bezpieczne i niebezpieczne sygnały w komunikatach,na platformie learning apps:

https://learningapps.org/view40927263