Co-funded by the European Union

AKTYWIZUJĄCY SCENARIUSZ LEKCJI

opracowany w ramach projektu

„INNOWACJE W EDUKACJI SZKOLNEJ"

Temat lekcji:

Phishing i fałszywe strony

1. Cele lekcji

Uczeń:

- rozumie, czym jest **phishing** i **fałszywa strona internetowa**,
- potrafi wskazać **najczęstsze metody cyberprzestępców**,
- wie, w jaki sposób **fałszywe wiadomości i fake newsy** są wykorzystywane do oszustw,
- poznaje podstawowe **zasady bezpieczeństwa w sieci**,
- rozwija umiejętność **analizy treści online i krytycznego myślenia**.

2. Grupa docelowa

Uczniowie szkół podstawowych

3. Metody nauczania

- Burza mózgów
- Mini-wykład z przykładami
- Analiza przypadków (case study)
- Ćwiczenie w grupach – „Prawdziwa czy fałszywa strona?”
- Dyskusja kierowana
- Refleksja indywidualna

4. Pomoce dydaktyczne / źródła

- Komputer, rzutnik, tablica interaktywna
- Zrzuty ekranów fikcyjnych e-maili phishingowych i fałszywych stron

- Karta „10 sygnałów ostrzegawczych phishingu” (do rozdania uczniom)
- Lista stron edukacyjnych i fact-checkingowych:
  - Polska: https://niebezpiecznik.pl, https://demagog.org.pl
  - Czechy: https://manipulatori.cz
  - Słowacja: https://hoax.sk
  - Ukraina: https://www.stopfake.org/en/news/
  - UE: https://edmo.eu, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

5. Przebieg lekcji (45 min)

1. Wprowadzenie – czy w internecie zawsze jest bezpiecznie? (5–7 min)

1. Burza mózgów – doświadczenia uczniów (2–3 min)

- Nauczyciel prosi uczniów, aby podali przykłady sytuacji, w których:
  - otrzymali dziwną wiadomość e-mail lub SMS,
  - ktoś wysłał im podejrzany link w mediach społecznościowych,
  - pojawiła się sensacyjna informacja o nagrodzie lub loterii, zachęcająca do kliknięcia w link.
- Odpowiedzi uczniów mogą być zapisane na tablicy w dwóch kolumnach: „wydawało się prawdziwe” / „budziło podejrzenia”, aby pokazać, że nie wszystkie wiadomości od razu wyglądają na oszustwo.

2. Pytania naprowadzające (2–3 min)

- Czy zdarzyło się Wam otrzymać wiadomość obiecującą nagrodę, super promocję lub szybki zarobek, ale wyglądało to podejrzanie?
- Czy każda wiadomość, którą dostajemy w internecie, jest prawdziwa i bezpieczna?
- Jakie zagrożenia mogą się kryć za kliknięciem w nieznany link?
- Czy fałszywa wiadomość może doprowadzić do kradzieży pieniędzy, hasła do gry online lub przejęcia konta w mediach społecznościowych?
- Dlaczego cyberprzestępcy chcą, abyśmy działali szybko i bez zastanowienia?

(Nauczyciel zachęca uczniów do krótkiego dzielenia się historiami – bez podawania prywatnych danych ani nazw osób.)

3. Dopowiedzenie nauczyciela – rozszerzone informacje merytoryczne (2 min)

- Phishing to oszustwo internetowe, którego celem jest wyłudzenie poufnych informacji (hasła, loginy, numery kart płatniczych, dane osobowe).
- Oszuści wykorzystują:
    - fałszywe wiadomości e-mail lub SMS, podszywając się pod bank, firmę kurierską, platformę zakupową, znajomego z listy kontaktów,
    - fake newsy lub sensacyjne nagłówki, które wzbudzają emocje – strach, pośpiech, nadzieję na wygraną,
    - fałszywe strony internetowe, które wyglądają prawie tak samo jak prawdziwe witryny banków, sklepów czy portali społecznościowych.
- Głównym celem phishingu jest sprawienie, by ofiara kliknęła w link, pobrała plik, podała dane logowania lub potwierdziła płatność, myśląc, że robi to na bezpiecznej stronie.
- Kliknięcie w fałszywy link może prowadzić do:
    - kradzieży pieniędzy z konta bankowego,
    - przejęcia kont w grach, aplikacjach czy mediach społecznościowych,
    - rozprzestrzenienia wirusów i oprogramowania szpiegującego na komputerze lub telefonie.

(Ważne, by podkreślić: ofiary phishingu nie są winne – winni są oszuści. Każdy może paść ofiarą manipulacji, jeśli nie zachowa ostrożności.

2. Mini-wykład: Phishing, fałszywe strony i dezinformacja (10–12 min)

1. Wprowadzenie – zagrożenia w sieci (1 min)

- Nauczyciel pyta uczniów:
    - *„Czy zdarzyło Wam się dostać wiadomość od nieznanej osoby, z linkiem lub prośbą o podanie danych?”*
    - *„Jak rozpoznajemy, czy wiadomość jest bezpieczna?”*
- Wprowadza temat, podkreślając, że phishing i fałszywe strony to najczęstsze narzędzia cyberprzestępców, którzy wykorzystują dezinformację i emocje, by nas oszukać.

2. Definicja phishingu (2 min)

- Phishing to oszustwo internetowe, którego celem jest wyłudzenie danych osobowych lub pieniędzy, najczęściej poprzez:
    - e-maile, SMS-y, wiadomości w komunikatorach,

- fałszywe strony podszywające się pod banki, sklepy, portale społecznościowe,
- fałszywe powiadomienia w przeglądarce lub aplikacjach („Twój telefon jest zainfekowany – kliknij, aby go naprawić").

- Cel cyberprzestępców:
  - zdobycie loginów i haseł,
  - kradzież pieniędzy z konta,
  - przejęcie kont w mediach społecznościowych,
  - rozsyłanie kolejnych oszukańczych wiadomości do znajomych ofiary.

3. Fałszywe strony internetowe (2 min)

- To witryny udające prawdziwe, które:
  - mają podobny adres (np. „paypa1.com" zamiast „paypal.com"),
  - kopiują wygląd strony banku lub sklepu,
  - proszą o wpisanie danych logowania, numeru karty, danych osobowych.
- Cyberprzestępcy często rozsyłają linki do takich stron w wiadomościach phishingowych, używając zastraszających lub sensacyjnych nagłówków (np. „Twoje konto zostanie usunięte, jeśli nie potwierdzisz danych").

4. Techniki stosowane przez oszustów (3 min)

Nauczyciel omawia typowe metody manipulacji, podając przykłady:

1. Szokujące wiadomości:
   - „Twoje konto zostanie zablokowane natychmiast, jeśli nie klikniesz w link!"
   - Wykorzystują strach i pośpiech, aby ofiara działała impulsywnie.
2. Obietnice nagrody lub superoferty:
   - „Wygrałeś nowy telefon!", „Odbierz darmowy kupon – tylko dziś!"
   - Wzbudzają nadzieję na zysk lub wygraną.
3. Podszywanie się pod instytucje:
   - Wiadomości wyglądające jak od banku, firmy kurierskiej, znajomego z listy kontaktów.
   - Często mają podrobione logo, podobny adres e-mail, ale w rzeczywistości pochodzą od oszustów.

4. Linki prowadzące do fałszywych stron:
    - Udają panel logowania do banku, serwisów społecznościowych lub sklepów internetowych.
    - Po wpisaniu danych przestępcy mają pełen dostęp do konta.
5. Dezinformacja i fake newsy:
    - Fałszywe wiadomości o katastrofach, zagrożeniach lub „tajnych promocjach", które zachęcają do kliknięcia w podejrzany link.
    - Przykład: *„Pilne! Twoje miasto zostanie objęte ewakuacją – zobacz listę miejsc!"* (link prowadzi do strony wyłudzającej dane).

5. Związek phishingu z fake newsami (2 min)

- Fake newsy mogą być narzędziem cyberprzestępstwa, gdy:
    - tworzą fałszywe poczucie zagrożenia lub sensacji, by nakłonić do kliknięcia,
    - udają wiadomości od zaufanych instytucji lub portali informacyjnych,
    - wykorzystują udostępnienia i wirusowy zasięg w sieci do masowego rozprzestrzeniania oszustw.
- Skuteczny phishing często łączy element kłamstwa (fake news) i fałszywe strony, tworząc wrażenie autentyczności i presji czasu.

6. Konsekwencje dla ofiar (1–2 min)

- Finansowe: kradzież środków z kont bankowych, nieautoryzowane płatności.
- Prywatności: przejęcie danych osobowych, które mogą być wykorzystane w innych oszustwach.
- Społeczne: przejęcie kont w mediach społecznościowych, wysyłanie oszukańczych wiadomości do znajomych.
- Psychologiczne: stres, poczucie wstydu lub winy, obniżone zaufanie do prawdziwych instytucji.

7. Podsumowanie mini-wykładu (1 min)

- Phishing to połączenie oszustwa, manipulacji emocjami i dezinformacji.
- Każdy może paść jego ofiarą – nawet osoby ostrożne.
- Najważniejsze zasady ochrony:
    1. Nie klikać w podejrzane linki i nie otwierać załączników od nieznanych nadawców.

2. Sprawdzać adresy stron i e-maili (literówki, dziwne domeny).
3. Nigdy nie podawać poufnych danych, jeśli mamy choć cień wątpliwości co do źródła wiadomości.

(Nauczyciel pokazuje przykładowy fikcyjny e-mail phishingowy na slajdzie, by uczniowie mogli wskazać, co w nim jest podejrzane.)

3. Ćwiczenie grupowe – „Prawdziwa czy fałszywa strona?" (15–20 min)

Cel ćwiczenia

- Rozwijanie umiejętności rozpoznawania prób phishingu.
- Nauczenie uczniów analizowania podejrzanych wiadomości i stron internetowych.
- Uświadomienie, jak cyberprzestępcy manipulują emocjami (strach, pośpiech, nagroda), aby skłonić do podania danych lub kliknięcia w link.
- Stworzenie własnych zasad bezpieczeństwa w sieci.

1. Podział na grupy (1 min)

- Klasa dzieli się na zespoły 3–4 osobowe.
- Każda grupa otrzymuje 3 wydrukowane lub wyświetlone przykłady:
    1. Prawdziwa strona banku lub sklepu (np. oficjalny panel logowania).
    2. Fałszywa strona phishingowa, łudząco podobna do prawdziwej.
    3. Wiadomość phishingowa (SMS/e-mail od „firmy kurierskiej" lub „banku"), z prośbą o kliknięcie linku lub podanie danych.

1. Prawdziwa strona banku/sklepu

(Oficjalny panel logowania – przykład)

Nagłówek: „Bank Polska Online – Zaloguj się"
Adres strony (URL): https://secure.bankpolska.pl
Wygląd:

- Logo banku w górnym lewym rogu.
- Po prawej – opcja zmiany języka (PL / EN).
- Pola logowania: „Identyfikator" + „Hasło".
- Ikona kłódki w pasku przeglądarki (zielona lub szara).
- Stopka z informacją prawną i linkami: „Regulamin", „Polityka prywatności".

Elementy autentyczności:

- Adres w domenie banku.
- Certyfikat SSL (https:// + kłódka).
- Brak literówek, poprawny język.

2. Fałszywa strona phishingowa

(Łudząco podobna do prawdziwej)

Nagłówek: „Bank Polska – Logowanie”
Adres strony (URL): https://bankpolska-login.secure-info.net
Wygląd:

- Podobne logo banku (lekko rozmyte, gorsza jakość).
- Układ strony prawie identyczny, ale brak opcji zmiany języka.
- Pola logowania takie same, ale przycisk „Zaloguj” jest w innym kolorze.
- Brak certyfikatu SSL lub kłódka jest przekreślona/czerwona.
- Stopka bez linków do regulaminu i polityki prywatności.

Cechy fałszywości:

- Domena inna niż oficjalna (np. dodatkowe słowa, nietypowe rozszerzenie).
- Często ukryta literówka w nazwie domeny (np. „banlkpolska.pl”).
- Czasem wyskakujące okno proszące o „aktualizację danych”.

3. Wiadomość phishingowa

(SMS lub e-mail od „firmy kurierskiej” lub „banku”)

Treść przykładowego SMS:

„Twoja paczka czeka na odbiór. Dopłać 1,99 zł, aby ją otrzymać: https://inpost-paczka-secure.net”

Treść przykładowego e-maila od „banku”:

Temat: *„Pilne! Zablokowano Twoje konto”*
Treść:
„Szanowny Kliencie,
wykryliśmy nietypową aktywność na Twoim koncie. Aby odblokować dostęp, kliknij poniższy link i zaloguj się:
Zaloguj się teraz
Jeśli nie potwierdzisz danych w ciągu 24 godzin, konto zostanie trwale zablokowane.”

Cechy podejrzane:

- Presja czasu („w ciągu 24 godzin”).
- Link prowadzący do innej domeny.
- Błędy językowe lub dziwne sformułowania.
- Nieoczekiwane prośby o podanie danych.

2. Narzędzie pomocnicze – „Karta 10 sygnałów ostrzegawczych phishingu” (2 min)

Każda grupa otrzymuje kartę z listą najczęstszych znaków ostrzegawczych:

Nr	Sygnał ostrzegawczy
1	**Literówki, dziwny adres strony (np. „paypa1.com” zamiast „paypal.com”).**
2	**Brak „https://” i kłódki w pasku adresu.**
3	**Adres e-mail nadawcy wygląda podejrzanie (np. ciąg losowych znaków).**
4	**Wiadomość zawiera błędy językowe, nietypową czcionkę lub dziwny układ tekstu.**
5	**Groźby lub presja czasu („Jeśli nie klikniesz, konto zostanie zablokowane!”).**
6	**Obietnica nagrody, prezentu lub superpromocji bez powodu.**
7	**Linki prowadzące do nieznanych domen lub stron bez kontaktu.**
8	**Prośba o podanie haseł, numeru karty lub danych osobowych.**
9	**Załączniki w nieznanym formacie, szczególnie .exe, .zip.**
10	**Nietypowe logo lub grafika, inny wygląd strony niż zwykle.**

3. Zadanie dla grup (8–10 min)

Każda grupa analizuje trzy przykłady i:

1. Oznacza, które treści są prawdziwe, a które phishingowe.
2. Zaznacza na wydruku lub w tabeli sygnały ostrzegawcze z listy 10 punktów.
3. Wskazuje emocje, które próbuje wywołać oszust (strach, pośpiech, nagroda, poczucie obowiązku).
4. Formułuje zasadę ochrony, która pozwoliłaby uniknąć tego oszustwa (np. „zawsze sprawdzam adres strony”, „nie klikam w linki z SMS-ów”).

Co-funded by the European Union

Tabela do wypełnienia:

Przykład wiadomości/strony	Prawdziwa czy fałszywa?	Sygnały ostrzegawcze (nr z karty)	Jak się chronić?

4. Prezentacja wyników (4–5 min)

- Każda grupa omawia jeden przykład, który uznała za najciekawszy lub najtrudniejszy do rozpoznania.
- Nauczyciel zapisuje na tablicy najczęściej wymieniane sygnały ostrzegawcze, tworząc wspólną „listę zasad bezpieczeństwa online".

5. Podsumowanie ćwiczenia (1–2 min)

- Phishing często wygląda profesjonalnie i wiarygodnie, dlatego tak łatwo dać się oszukać.
- Kluczowe zasady ochrony:
    1. Nigdy nie podaję haseł ani numerów kart po kliknięciu w link z wiadomości.
    2. Sprawdzam adres strony i nadawcę wiadomości.
    3. Nie działam pod presją czasu – zawsze mogę sprawdzić sprawę w inny sposób (np. dzwoniąc do banku).
    4. Jeśli coś wygląda podejrzanie – lepiej nie klikać.

4. Dyskusja: Jak bronić się przed phishingiem i oszustwami w sieci? (8–10 min)

1. Cel dyskusji

- Uświadomienie uczniom, dlaczego nawet ostrożne osoby mogą paść ofiarą phishingu.
- Zrozumienie, jak emocje, pośpiech i brak weryfikacji informacji ułatwiają działanie cyberprzestępcom.

- Wypracowanie praktycznych zasad bezpiecznego korzystania z linków, wiadomości i stron internetowych.

2. Pytania do uczniów (bazowe)

- Dlaczego wiele osób klika w fałszywe wiadomości, mimo że wydają się podejrzane?
- Jakie emocje najczęściej wykorzystują cyberprzestępcy (strach, ciekawość, pośpiech, chęć wygranej)?
- Czy wszystkie linki od „znajomych" są bezpieczne? Dlaczego czasem nawet konta znajomych mogą wysyłać fałszywe treści?
- Jak można sprawdzić, czy strona jest prawdziwa (np. https, certyfikat, literówki w adresie, oficjalna domena)?
- Czy fake newsy mogą być pierwszym krokiem do oszustwa (np. fałszywe informacje o katastrofach, loteriach, promocjach)? Jak działa taki mechanizm?

3. Pytania pogłębiające dyskusję

- Czy kliknięcie w link jest zawsze bezpieczne, jeśli wiadomość pochodzi od kogoś znajomego? (np. przejęte konto wysyła zainfekowane wiadomości).
- Dlaczego cyberprzestępcy często dodają „pilne ostrzeżenia" lub „czasową ofertę", abyśmy kliknęli szybko i bez zastanowienia?
- Czy każda nagroda w internecie jest prawdziwa? Jakie „czerwone flagi" wskazują, że to oszustwo?
- Jak odróżnić prawdziwy komunikat od banku czy firmy kurierskiej od fałszywego?
- Co zrobić, jeśli przez przypadek klikniemy w link lub podamy dane oszustom? Kto może pomóc w takiej sytuacji?

4. Mini-analiza – krótkie przykłady do omówienia

Nauczyciel może zaprezentować 2–3 fikcyjne wiadomości (wydruki lub slajdy):

1. *„Pilne! Twoje konto zostanie zablokowane w ciągu 24h, kliknij tutaj i potwierdź swoje dane!"*
2. *„Hej, zobacz ten filmik – czy to ty? 😂 [link]" (wiadomość z konta znajomego)*
3. *„Wygrałeś smartfon! Odbierz nagrodę, klikając w link poniżej."*

Pytania:

- Jakie emocje wzbudza ta wiadomość?
- Co w niej wygląda podejrzanie?

- Jak powinniśmy zareagować w takiej sytuacji?

5. Wnioski z dyskusji – „Złote zasady bezpieczeństwa”

Na podstawie odpowiedzi uczniów i analizy przykładów nauczyciel tworzy listę zasad (na tablicy lub flipcharcie), np.:

1. Zawsze sprawdzam nadawcę – nawet jeśli wiadomość jest od znajomego.
2. Nie klikam w linki z nieznanych źródeł ani w podejrzane załączniki.
3. Sprawdzam adres strony – prawdziwe serwisy mają poprawną nazwę domeny i kłódkę „https://”.
4. Nie ufam „nagłym promocjom” i „wygranym bez powodu” – nic nie przychodzi za darmo.
5. Nie działam w pośpiechu – oszuści chcą, żebyśmy klikali bez myślenia.
6. W razie wątpliwości pytam dorosłego, bank, specjalistę lub sprawdzam komunikat na oficjalnej stronie.

6. Podsumowanie nauczyciela (1–2 min)

- Cyberprzestępcy wykorzystują emocje i zaufanie, aby nas oszukać – phishing działa nie dlatego, że ktoś jest „nieuważny”, ale dlatego, że jest sprytnie zaplanowany.
- Każdy może stać się ofiarą, ale dzięki ostrożności, weryfikacji informacji i nieklikaniu w przypadkowe linki możemy skutecznie się chronić.
- Fake newsy są często pierwszym krokiem do oszustwa, bo tworzą sensację, która zachęca do kliknięcia i prowadzi do fałszywych stron phishingowych.

5. Podsumowanie i refleksja (7–10 min)

1. Refleksja indywidualna – dokończ zdania (3–4 min)

Każdy uczeń otrzymuje kartkę lub korzysta z zeszytu i kończy zdania:

- „Zrozumiałem/am, że phishing…”
- „Najbardziej podejrzane w fałszywych wiadomościach jest…”
- „Zanim kliknę w link, sprawdzę…”
- „Aby chronić swoje konto, będę…”
- *(opcjonalnie)* „Gdybym przypadkiem kliknął w podejrzany link, powinienem…”

Nauczyciel podkreśla, że nie ma złych odpowiedzi – to ćwiczenie służy przełożeniu wiedzy na praktyczne nawyki.

2. Krótka wymiana doświadczeń (2–3 min)

- Chętni uczniowie odczytują swoje odpowiedzi (lub nauczyciel zbiera anonimowo karteczki i czyta wybrane przykłady).
- Dyskusja kierowana pytaniami:
    - Czy Wasze odpowiedzi się powtarzały?
    - Która zasada ochrony przed phishingiem pojawiała się najczęściej?
    - Czy pojawiły się nowe pomysły, które warto zapamiętać?

3. Wspólna lista – „5 (lub więcej) zasad bezpiecznego korzystania z linków i stron" (3 min)

Na tablicy lub flipcharcie powstaje wspólna lista zasad bezpieczeństwa. Przykładowe propozycje:

1. Nigdy nie podaję haseł ani numerów kart w podejrzanych linkach lub po kliknięciu w wiadomość e-mail/SMS.
2. Sprawdzam dokładny adres strony (literówki, prawidłowa domena, „https://" i symbol kłódki).
3. Nie klikam w nagłe oferty nagrody, loterii, „pilnych ostrzeżeń" – najpierw sprawdzam je w oficjalnych źródłach (np. loguję się do banku ręcznie, dzwonię do firmy kurierskiej).
4. Nie działam w pośpiechu – oszuści chcą, byśmy klikali impulsywnie.
5. Konsultuję podejrzane wiadomości z rodzicami, nauczycielem lub specjalistą.
6. *(opcjonalnie)* Używam oprogramowania antywirusowego, aktualizuję system i hasła – to dodatkowa ochrona przed atakami.

(Lista może zostać sfotografowana lub zapisana w zeszytach jako „Zasady bezpiecznego korzystania z linków i stron").

4. Podsumowanie nauczyciela – przekaz końcowy (1–2 min)

- Phishing to oszustwo oparte na emocjach i zaufaniu – nawet osoby dorosłe, znające się na technologii, dają się czasem nabrać.
- Najważniejsza zasada: jeśli coś wygląda podejrzanie lub zbyt pięknie, aby było prawdziwe – nie klikaj, nie podawaj danych, sprawdź źródło.

- Bezpieczeństwo w sieci zależy od czujności każdego z nas – lepiej zapytać, sprawdzić lub poczekać, niż stracić dane czy pieniądze.

(Można zakończyć lekcję krótkim quizem ustnym lub pytaniem: „Jaką jedną zasadę zapamiętasz na przyszłość?" – uczniowie odpowiadają pojedynczymi hasłami.)

6. Słownik pojęć

Pojęcie	**Definicja**
Phishing	Próba wyłudzenia danych (loginy, hasła, dane bankowe) poprzez fałszywe wiadomości, podszywanie się pod zaufane instytucje.
Fałszywa strona	Witryna udająca oficjalną stronę banku, sklepu, serwisu, której celem jest kradzież danych lub pieniędzy.
Dezinformacja w phishingu	Wykorzystanie fałszywych wiadomości lub fake newsów, by nakłonić ofiarę do kliknięcia w link lub pobrania pliku.
Cyberprzestępca	Osoba lub grupa stosująca metody oszustwa w internecie, by zdobyć dane lub pieniądze.
Bezpieczne linki	Strony i adresy zaczynające się od „https", z poprawną nazwą domeny, pochodzące ze sprawdzonych źródeł.

---

7. Przewodnik metodyczny dla nauczyciela

1. Przygotowanie materiałów

- **Przykłady:**
  - Korzystaj wyłącznie z **fikcyjnych wiadomości i stron phishingowych**, stworzonych na potrzeby zajęć, aby uniknąć zagrożenia kliknięcia w prawdziwe linki czy ujawnienia danych.
  - Możesz wzorować się na prawdziwych atakach phishingowych, ale **zmień nazwy, logotypy, adresy URL** tak, aby były neutralne i edukacyjne.
  - Nie pokazuj **realnych danych użytkowników**, nawet jako przykład – zachowaj pełną anonimowość.
- **Różnorodność materiałów:**
  - Przygotuj **zrzuty ekranu** stron logowania, powiadomień e-mailowych, SMS-ów, reklam w mediach społecznościowych.

- Możesz wprowadzić **element scenki** – odegranie sytuacji, w której ktoś dostaje podejrzaną wiadomość, a inni próbują jej prawidłowo zareagować.
- Pokaż **różne formy phishingu**: klasyczny e-mail, fałszywe promocje, linki od „znajomych", posty w social mediach, fałszywe aplikacje.

2. Sposób prowadzenia zajęć

- **Punkt wyjścia:**
  - Zacznij lekcję od **pytania otwierającego**, np.: „Czy ktoś z Was kiedykolwiek dostał wiadomość, która wyglądała podejrzanie? Co w niej zwróciło Waszą uwagę?".
  - Upewnij się, że rozmowa **nie prowadzi do ośmieszania uczniów** – phishing może dotknąć każdego.
- **Mini-wykład:**
  - Prezentuj krótkie informacje (max 2–3 min bloki) przeplatane pytaniami do uczniów, aby utrzymać ich uwagę.
  - Posługuj się prostymi przykładami i zrozumiałym językiem – unikaj nadmiaru terminologii technicznej.
- **Ćwiczenia praktyczne:**
  - Analiza fałszywych stron i wiadomości powinna być **bezpieczna** (bez aktywnych linków).
  - Uczniowie powinni mieć możliwość **zaznaczania sygnałów ostrzegawczych** (np. markerem na wydrukach lub na tablicy interaktywnej).
  - Daj czas na **wspólną wymianę wniosków**, by uczniowie mogli porównać obserwacje.

3. Moderowanie dyskusji

- Zachęcaj uczniów do podawania przykładów z własnego życia lub historii zasłyszanych od rodziny i znajomych.
- Podkreślaj, że **nikt nie jest odporny na oszustwa internetowe** – ofiarą phishingu padają również specjaliści od bezpieczeństwa IT.
- Zasada: **„Nie wyśmiewamy, tylko analizujemy"** – reaguj, jeśli w klasie pojawiają się komentarze wyśmiewające sytuacje innych.
- Możesz użyć techniki **„Pytanie do klasy"**: zamiast oceniać odpowiedź, pytaj „Czy ktoś myśli inaczej?", „Czy ktoś ma inny pomysł na rozwiązanie?".

Co-funded by the European Union

4. Zapewnienie bezpiecznej atmosfery

- Podkreślaj, że **phishing to przestępstwo**, a nie wina osoby, która dała się nabrać.
- Jeśli ktoś podzieli się doświadczeniem bycia ofiarą oszustwa, **okaż wsparcie i uznanie za odwagę w podzieleniu się historią**.
- Wyjaśnij uczniom, że **najlepszą obroną jest wiedza, a nie wstyd** – im więcej wiemy o oszustwach, tym lepiej potrafimy się chronić.

5. Cel wychowawczy lekcji

- Kształtowanie:
  - **Świadomości zagrożeń cyfrowych** związanych z phishingiem i fałszywymi stronami.
  - **Nawyków sprawdzania linków i nadawców wiadomości**, zanim klikniemy lub podamy dane.
  - **Odporności na manipulację emocjami** (strach, pośpiech, nagłe nagrody).
  - **Postawy odpowiedzialnego użytkownika internetu**, który dba nie tylko o swoje bezpieczeństwo, ale także ostrzega innych przed oszustwami.

6. Dodatkowe propozycje rozszerzenia lekcji

- **Zadanie domowe:** Uczniowie zbierają 3 przykłady fałszywych wiadomości (z internetu lub tworzą własne fikcyjne) i na następnej lekcji analizują je w grupach.
- **Mini-projekt klasowy:** Stworzenie plakatu „10 sygnałów ostrzegawczych phishingu” lub „Jak sprawdzić, czy strona jest bezpieczna?”, który można powiesić w szkole.
- **Symulacja ataku phishingowego (bezpieczna):** Nauczyciel przygotowuje krótką „fałszywą wiadomość” i uczniowie mają za zadanie wskazać wszystkie sygnały, że to oszustwo.

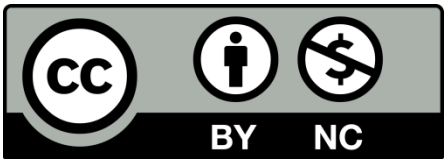
8. Źródła edukacyjne i fact-checkingowe

- **EDMO – European Digital Media Observatory**
  https://edmo.eu
- **Europol – Cybercrime**
  https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
- **EUvsDisinfo**
  https://euvsdisinfo.eu

Projekt dofinansowany przez Unię Europejską

Co-funded by the European Union

- **Niebezpiecznik.pl (PL)**
  https://niebezpiecznik.pl
- **Demagog.org.pl (PL)**
  https://demagog.org.pl
- **Manipulátoři.cz (CZ)**
  https://manipulatori.cz
- **Hoax.sk (SK)**
  https://hoax.sk
- **StopFake.org (UA)**
  https://www.stopfake.org/en/news/



Projekt dofinansowany przez Unię Europejską