Co-funded by the European Union

AKTIVUJÚCI SCENÁR LEKCIE
vypracovaný v rámci projektu

„INOVÁCIE V ŠKOLSKEJ VÝCHOVE"

TÉMA:

Phishing a falošné stránky

1. Ciele hodiny

Žiak:
• rozumie, čo je phishing a falošná internetová stránka,
• dokáže uviesť najčastejšie metódy kyberzločincov,
• vie, akým spôsobom sú falošné správy a fake newsy využívané na podvody,
• pozná základné zásady bezpečnosti na internete,
• rozvíja schopnosť analýzy online obsahu a kritického myslenia.

2. Cieľová skupina

Žiaci základných škôl

3. Metódy vyučovania

• Brainstorming
• Mini-prednáška s príkladmi
• Analýza prípadov (case study)
• Skupinové cvičenie – „Pravá alebo falošná stránka?“
• Riadená diskusia
• Individuálna reflexia

4. Učebné pomôcky / zdroje

• Počítač, projektor, interaktívna tabuľa
• Snímky obrazovky fiktívnych phishingových e-mailov a falošných stránok
• Karta „10 varovných signálov phishingu“ (na rozdanie žiakom)
• Zoznam vzdelávacích a fact-checkingových stránok:
o Poľsko: https://niebezpiecznik.pl, https://demagog.org.pl
o Česko: https://manipulatori.cz
o Slovensko: https://hoax.sk
o Ukrajina: https://www.stopfake.org/en/news/

o EÚ: https://edmo.eu, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

5. Priebeh hodiny (45 min)

1. Úvod – je internet vždy bezpečný? (5–7 min)

1. **Brainstorming – skúsenosti žiakov (2–3 min)**
   • Učiteľ žiakov požiada, aby uviedli príklady situácií, v ktorých:
   o dostali zvláštny e-mail alebo SMS,
   o niekto im poslal podozrivý odkaz na sociálnych sieťach,
   o objavila sa senzačná informácia o výhre alebo lotérii, ktorá nabádala kliknúť na odkaz.
   • Odpovede žiakov možno zapísať na tabuľu v dvoch stĺpcoch: „zdalo sa pravdivé“ / „vzbudzovalo podozrenie“, aby sa ukázalo, že nie všetky správy hneď vyzerajú ako podvod.
2. **Navádzajúce otázky (2–3 min)**
   • Stalo sa vám, že ste dostali správu sľubujúcu odmenu, super akciu alebo rýchly zárobok, ale vyzerala podozrivo?
   • Je každá správa, ktorú dostaneme na internete, pravdivá a bezpečná?
   • Aké hrozby sa môžu skrývať za kliknutím na neznámy odkaz?
   • Môže falošná správa viesť ku krádeži peňazí, hesla do online hry alebo prevzatiu účtu na sociálnych sieťach?
   • Prečo chcú kyberzločinci, aby sme konali rýchlo a bez rozmýšľania?
   (Učiteľ povzbudzuje žiakov, aby sa krátko podelili o svoje príbehy – bez uvádzania súkromných údajov ani mien osôb.)
3. **Doplňujúci výklad učiteľa – rozšírené fakty (2 min)**
   • Phishing je internetový podvod, ktorého cieľom je vylákanie dôverných informácií (heslá, loginy, čísla platobných kariet, osobné údaje).
   • Podvodníci využívajú:
   o falošné e-maily alebo SMS, vydávajúce sa za banku, kuriérsku spoločnosť, nákupnú platformu, známeho z kontaktov,
   o fake news alebo senzačné titulky, ktoré vyvolávajú emócie – strach, náhlenie, nádej na výhru,
   o falošné internetové stránky, ktoré vyzerajú takmer identicky ako skutočné stránky bánk, obchodov či sociálnych sietí.
   • Hlavným cieľom phishingu je prinútiť obeť kliknúť na odkaz, stiahnuť súbor, zadať prihlasovacie údaje alebo potvrdiť platbu v domnení, že ide o bezpečnú stránku.
   • Kliknutie na falošný odkaz môže viesť k:
   o krádeži peňazí z bankového účtu,
   o prevzatiu účtov v hrách, aplikáciách či na sociálnych sieťach,
   o šíreniu vírusov a spywaru na počítači alebo mobile.

(Dôležité zdôrazniť: obeť phishingu nie je vinná – vinní sú podvodníci. Každý sa môže stať obeťou manipulácie, ak nebude opatrný.)

2. Mini-prednáška: Phishing, falošné stránky a dezinformácia (10–12 min)

1. **Úvod – hrozby na internete (1 min)**
   • Učiteľ sa pýta žiakov:
   o „Stalo sa vám, že ste dostali správu od neznámej osoby s odkazom alebo prosbou o zadanie údajov?“
   o „Ako spoznáme, či je správa bezpečná?“
   • Uvádza tému s dôrazom na to, že phishing a falošné stránky sú najčastejšie nástroje kyberzločincov, ktorí využívajú dezinformáciu a emócie, aby nás podviedli.
2. **Definícia phishingu (2 min)**
   • Phishing je internetový podvod, ktorého cieľom je vylákanie osobných údajov alebo peňazí, najčastejšie prostredníctvom:
   o e-mailov, SMS, správ v komunikátoroch,
   o falošných stránok vydávajúcich sa za banky, obchody, sociálne siete,
   o falošných upozornení v prehliadači alebo aplikáciách („Tvoj telefón je infikovaný – klikni, aby si ho opravil“).
   • Cieľom kyberzločincov je:
   o získanie loginov a hesiel,
   o krádež peňazí z účtu,
   o prevzatie účtov na sociálnych sieťach,
   o ďalšie rozposielanie podvodných správ známym obete.
3. **Falošné internetové stránky (2 min)**
   • Sú to weby predstierajúce, že sú skutočné, ktoré:
   o majú podobnú adresu (napr. „paypa1.com“ namiesto „paypal.com“),
   o kopírujú vzhľad stránky banky alebo obchodu,
   o žiadajú o zadanie prihlasovacích údajov, čísla karty, osobných údajov.
   • Kyberzločinci často rozposielajú odkazy na takéto stránky v phishingových správach, používajúc zastrašujúce alebo senzačné titulky (napr. „Tvoj účet bude zmazaný, ak nepotvrdíš údaje“).
4. **Techniky používané podvodníkmi (3 min)**
   Učiteľ rozoberá typické manipulačné metódy, uvádza príklady:
5. **Šokujúce správy:**
   o „Tvoj účet bude okamžite zablokovaný, ak neklikneš na odkaz!“
   o Využívajú strach a náhlenie, aby obeť konala impulzívne.
6. **Sľuby odmeny alebo superponuky:**
   o „Vyhral si nový telefón!“, „Získaj darčekový kupón – len dnes!“
   o Vyvolávajú nádej na zisk alebo výhru.
7. **Vydávanie sa za inštitúcie:**
   o Správy vyzerajúce ako od banky, kuriérskej spoločnosti, známeho z kontaktov.

o Často majú napodobnené logo, podobnú e-mailovú adresu, ale v skutočnosti pochádzajú od podvodníkov.

8. **Odkazy vedúce na falošné stránky:**
   o Tvária sa ako prihlasovací panel do banky, sociálnych sietí alebo e-shopov.
   o Po zadaní údajov získajú páchatelia plný prístup k účtu.
9. **Dezinformácia a fake news:**
   o Falošné správy o katastrofách, hrozbách alebo „tajných akciách“, ktoré nabádajú kliknúť na podozrivý odkaz.
   o Príklad: „Urgentné! Tvoje mesto bude evakuované – pozri zoznam miest!“ (odkaz vedie na stránku vylákavajúcu údaje).
10. **Súvislosť phishingu s fake news (2 min)**
    • Fake news môžu byť nástrojom kyberzločinu, keď:
    o vytvárajú falošný pocit ohrozenia alebo senzácie, aby prinútili kliknúť,
    o napodobňujú správy od dôveryhodných inštitúcií alebo médií,
    o využívajú zdieľania a virálny dosah na internete na masové šírenie podvodu.
    • Úspešný phishing často spája klamstvo (fake news) a falošné stránky, čím vytvára dojem autenticity a časového tlaku.
11. **Dôsledky pre obete (1–2 min)**
    • Finančné: krádež prostriedkov z bankových účtov, neautorizované platby.
    • Súkromia: prevzatie osobných údajov, ktoré môžu byť využité v ďalších podvodoch.
    • Sociálne: prevzatie účtov na sociálnych sieťach, rozosielanie podvodných správ známym.
    • Psychologické: stres, pocit hanby alebo viny, oslabená dôvera k skutočným inštitúciám.
12. **Zhrnutie mini-prednášky (1 min)**
    • Phishing je kombinácia podvodu, manipulácie emóciami a dezinformácie.
    • Obeťou sa môže stať každý – aj opatrní ľudia.
    • Najdôležitejšie zásady ochrany:
13. Neklikať na podozrivé odkazy a neotvárať prílohy od neznámych odosielateľov.
14. Kontrolovať adresy stránok a e-mailov (preklepy, zvláštne domény).
15. Nikdy nezadávať dôverné údaje, ak máme čo i len malú pochybnosť o zdroji správy.
    (Učiteľ ukazuje príklad fiktívneho phishingového e-mailu na slajde, aby žiaci mohli označiť, čo v ňom je podozrivé.)

3. Skupinové cvičenie – „Pravá alebo falošná stránka?” (15–20 min)

Cieľ cvičenia

• Rozvíjať schopnosť rozpoznávať pokusy o phishing.
• Naučiť žiakov analyzovať podozrivé správy a internetové stránky.
• Uvedomiť si, ako kyberzločinci manipulujú emóciami (strach, náhlenie, odmena), aby prinútili zadať údaje alebo kliknúť na odkaz.
• Vytvoriť vlastné zásady bezpečnosti na internete.

Co-funded by the European Union

1. Rozdelenie do skupín (1 min)

• Trieda sa rozdelí na 3–4 členné tímy.
• Každá skupina dostane 3 vytlačené alebo premietnuté príklady:

1. Skutočná stránka banky alebo obchodu (napr. oficiálny prihlasovací panel).
2. Falošná phishingová stránka, ktorá sa nápadne podobá na pravú.
3. Phishingová správa (SMS/e-mail od „kuriérskej firmy“ alebo „banky“) s výzvou na kliknutie na odkaz alebo zadanie údajov.

1. Skutočná stránka banky/obchodu

(Oficiálny prihlasovací panel – príklad)
Nadpis: „Bank Polska Online – Prihlás sa”
Adresa stránky (URL): https://secure.bankpolska.pl
Vzhľad:
• Logo banky v ľavom hornom rohu.
• Vpravo – možnosť zmeny jazyka (PL / EN).
• Prihlasovacie polia: „Identifikátor” + „Heslo”.
• Ikona zámku v lište prehliadača (zelená alebo sivá).
• Päta so právnymi informáciami a odkazmi: „Podmienky”, „Ochrana súkromia”.

Prvky autenticity:
• Adresa v doméne banky.
• Certifikát SSL (https:// + zámok).
• Žiadne preklepy, správny jazyk.

2. Falošná phishingová stránka

(Nápadne podobná pravej)
Nadpis: „Bank Polska – Prihlásenie”
Adresa stránky (URL): https://bankpolska-login.secure-info.net
Vzhľad:
• Podobné logo banky (mierne rozmazané, horšia kvalita).
• Usporiadanie stránky takmer identické, ale chýba možnosť zmeny jazyka.
• Prihlasovacie polia rovnaké, ale tlačidlo „Prihlásiť sa” je v inej farbe.
• Chýba certifikát SSL alebo zámok je preškrtnutý/červený.
• Pätička bez odkazov na podmienky a ochranu súkromia.

Znaky falošnosti:
• Iná doména ako oficiálna (napr. ďalšie slová, netypická koncovka).
• Skrytý preklep v názve domény (napr. „banlkpolska.pl”).
• Niekedy vyskakovacie okno so žiadosťou o „aktualizáciu údajov”.

3. Phishingová správa

(SMS alebo e-mail od „kuriérskej firmy“ alebo „banky“)

Text ukážkového SMS:
„Tvoja zásielka čaká na doručenie. Doplať 1,99 zł, aby si ju dostal: https://inpost-paczka-secure.net”

Text ukážkového e-mailu od „banky“:
Predmet: „Urgentné! Tvoj účet bol zablokovaný”
Obsah:
„Vážený klient,
zaznamenali sme neobvyklú aktivitu na tvojom účte. Aby sme obnovili prístup, klikni na odkaz nižšie a prihlás sa:

Prihlás sa teraz

Ak nepotvrdíš údaje do 24 hodín, účet bude natrvalo zablokovaný.”

Znaky podozrivosti:
• Tlak na čas („do 24 hodín”).
• Odkaz vedúci na inú doménu.
• Jazykové chyby alebo zvláštne formulácie.
• Neočakávané žiadosti o zadanie údajov.

2. Pomocný nástroj – „Karta 10 varovných signálov phishingu” (2 min)

Každá skupina dostane kartu s najčastejšími varovnými znakmi:

Nr	Varovný signál
1	Preklepy, zvláštna adresa stránky (napr. „paypa1.com“ namiesto „paypal.com“).
2	Chýba „https://” a zámok v lište adresy.
3	E-mailová adresa odosielateľa vyzerá podozrivo (napr. sled znakov).
4	Správa obsahuje jazykové chyby, netypické písmo alebo zvláštne rozloženie textu.

Co-funded by the European Union

Nr	Varovný signál
5	Hrozby alebo časový tlak („Ak neklikneš, účet bude zablokovaný!”).
6	Sľub odmeny, darčeka alebo superakcie bez dôvodu.
7	Odkazy vedúce na neznáme domény alebo stránky bez kontaktu.
8	Žiadosť o zadanie hesiel, čísla karty alebo osobných údajov.
9	Prílohy v neznámom formáte, najmä .exe, .zip.
10	Netypické logo alebo grafika, iný vzhľad stránky než obvykle.

3. Úloha pre skupiny (8–10 min)

Každá skupina analyzuje tri príklady a:

1. Označí, ktoré obsahy sú pravé a ktoré phishingové.
2. Zakrúžkuje na výtlačku alebo v tabuľke varovné signály zo zoznamu 10 bodov.
3. Uvedie emócie, ktoré sa podvodník snaží vyvolať (strach, náhlenie, odmena, pocit povinnosti).
4. Formuluje zásadu ochrany, ktorá by umožnila tomuto podvodu predísť (napr. „vždy kontrolujem adresu stránky“, „neklikám na odkazy z SMS“).

Tabuľka na vyplnenie:

Príklad správy/stránky	Pravá alebo falošná?	Varovné signály (číslo z karty)	Ako sa chrániť?

Co-funded by the European Union

Príklad správy/stránky	Pravá alebo falošná?	Varovné signály (číslo z karty)	Ako sa chrániť?

4. Prezentácia výsledkov (4–5 min)

• Každá skupina predstaví jeden príklad, ktorý považovala za najzaujímavejší alebo najťažší na rozpoznanie.
• Učiteľ zapisuje na tabuľu najčastejšie uvádzané varovné signály a vytvára spoločný zoznam „zásad online bezpečnosti“.

5. Zhrnutie cvičenia (1–2 min)

• Phishing často vyzerá profesionálne a dôveryhodne, preto je ľahké sa nechať oklamať.
• Kľúčové zásady ochrany:

1. Nikdy nezadávam heslá ani čísla kariet po kliknutí na odkaz zo správy.
2. Kontrolujem adresu stránky a odosielateľa správy.
3. Nekonám pod časovým tlakom – vždy môžem vec preveriť inak (napr. zavolať do banky).
4. Ak niečo vyzerá podozrivo – radšej neklikám.

4. Diskusia: Ako sa brániť pred phishingom a podvodmi na internete? (8–10 min)

1. Cieľ diskusie

• Upozorniť žiakov, prečo sa aj opatrní ľudia môžu stať obeťou phishingu.
• Pochopiť, ako emócie, náhlenie a nedostatočná kontrola informácií uľahčujú činnosť kyberzločincom.
• Vypracovať praktické zásady bezpečného používania odkazov, správ a internetových stránok.

2. Otázky pre žiakov (základné)

• Prečo veľa ľudí kliká na falošné správy, hoci sa zdajú podozrivé?
• Aké emócie najčastejšie využívajú kyberzločinci (strach, zvedavosť, náhlenie, túžba vyhrať)?
• Sú všetky odkazy od „známych“ bezpečné? Prečo môžu aj účty známych posielať falošný obsah?
• Ako možno overiť, či je stránka pravá (napr. https, certifikát, preklepy v adrese, oficiálna doména)?
• Môžu byť fake news prvým krokom k podvodu (napr. falošné správy o katastrofách, lotériách, akciách)? Ako taký mechanizmus funguje?

3. Prehlbujúce otázky do diskusie

• Je vždy bezpečné kliknúť na odkaz, ak správa pochádza od niekoho známeho? (napr. prevzatý účet posiela infikované správy).
• Prečo kyberzločinci často pridávajú „urgentné varovania“ alebo „časovo obmedzené ponuky“, aby sme klikli rýchlo a bez premýšľania?
• Je každá odmena na internete skutočná? Aké „červené vlajky“ naznačujú, že ide o podvod?
• Ako odlíšiť pravé oznámenie od banky či kuriérskej firmy od falošného?
• Čo urobiť, ak omylom klikneme na odkaz alebo zadáme údaje podvodníkom? Kto nám môže v takej situácii pomôcť?

4. Mini-analýza – krátke ukážky na diskusiu

Učiteľ môže ukázať 2–3 fiktívne správy (vytlačené alebo na slajdoch):

1. „Urgentné! Tvoj účet bude zablokovaný do 24h, klikni tu a potvrď svoje údaje!“
2. „Hej, pozri si toto video – si to ty? 😂 [odkaz]” (správa z účtu známeho)
3. „Vyhral si smartfón! Prevezmi si výhru kliknutím na odkaz nižšie.”

Otázky:
• Aké emócie vyvoláva táto správa?
• Čo v nej vyzerá podozrivo?
• Ako by sme mali reagovať v takej situácii?

5. Závery z diskusie – „Zlaté zásady bezpečnosti”

Na základe odpovedí žiakov a analýzy príkladov učiteľ vytvorí zoznam zásad (na tabuli alebo flipcharte), napr.:

1. Vždy si overujem odosielateľa – aj keď správa je od známeho.
2. Neklikám na odkazy z neznámych zdrojov ani na podozrivé prílohy.
3. Kontrolujem adresu stránky – pravé služby majú správnu doménu a zámok „https://“.
4. Neverím „náhlym akciám“ a „výhram bez dôvodu“ – nič nie je zadarmo.

5. Nekonám v náhlení – podvodníci chcú, aby sme klikli bez rozmýšľania.
6. V prípade pochybností sa pýtam dospelého, banky, odborníka alebo overujem správu na oficiálnej stránke.

6. Zhrnutie učiteľa (1–2 min)

• Kyberzločinci využívajú emócie a dôveru, aby nás podviedli – phishing funguje nie preto, že je niekto „nepozorný“, ale preto, že je šikovne naplánovaný.
• Každý sa môže stať obeťou, ale vďaka opatrnosti, overovaniu informácií a neklikaním na náhodné odkazy sa môžeme účinne chrániť.
• Fake news sú často prvým krokom k podvodu, pretože vytvárajú senzáciu, ktorá láka kliknúť a vedie na falošné phishingové stránky.

5. Zhrnutie a reflexia (7–10 min)

1. Individuálna reflexia – dokonči vety (3–4 min)

Každý žiak dostane papier alebo použije zošit a dokončí vety:
• „Pochopil/a som, že phishing…”
• „Najpodozrivejšie na falošných správach je…”
• „Skôr než kliknem na odkaz, overím…”
• „Aby som chránil/a svoj účet, budem…”
• (voliteľne) „Keby som náhodou klikol/a na podozrivý odkaz, mal/a by som…”

Učiteľ zdôrazní, že neexistujú zlé odpovede – toto cvičenie slúži na prenesenie vedomostí do praktických návykov.

2. Krátka výmena skúseností (2–3 min)

• Dobrovoľní žiaci prečítajú svoje odpovede (alebo učiteľ anonymne vyberie a prečíta kartičky).
• Riadená diskusia otázkami:
o Opakovali sa vaše odpovede?
o Ktoré zásady ochrany pred phishingom sa objavovali najčastejšie?
o Objavili sa nové nápady, ktoré sa oplatí zapamätať?

3. Spoločný zoznam – „5 (alebo viac) zásad bezpečného používania odkazov a stránok” (3 min)

Na tabuľu alebo flipchart vznikne spoločný zoznam zásad bezpečnosti. Ukážkové návrhy:

1. Nikdy nezadávam heslá ani čísla kariet v podozrivých odkazoch alebo po kliknutí na e-mail/SMS.
2. Kontrolujem presnú adresu stránky (preklepy, správna doména, „https://" a symbol zámku).
3. Neklikám na náhle ponuky odmien, lotérií, „urgentné varovania" – najprv ich overím v oficiálnych zdrojoch (napr. prihlásením do banky ručne, telefonátom kuriérskej firme).
4. Nekonám v náhlení – podvodníci chcú, aby sme klikali impulzívne.
5. Konzultujem podozrivé správy s rodičmi, učiteľom alebo odborníkom.
6. (voliteľne) Používam antivírus, aktualizujem systém a heslá – je to dodatočná ochrana pred útokmi.

4. Zhrnutie učiteľa – záverečné posolstvo (1–2 min)

• Phishing je podvod založený na emóciách a dôvere – aj dospelí, ktorí sa vyznajú v technológiách, sa niekedy nechajú nachytať.
• Najdôležitejšia zásada: ak niečo vyzerá podozrivo alebo príliš dobre, aby to bola pravda – neklikaj, nezadávaj údaje, over zdroj.
• Bezpečnosť na internete závisí od pozornosti každého z nás – lepšie je sa opýtať, overiť alebo počkať, než prísť o údaje či peniaze.

(Lekciu možno ukončiť krátkym ústnym kvízom alebo otázkou: „Akú jednu zásadu si zapamätáš do budúcna?" – žiaci odpovedajú jedným slovom alebo heslom.)

6. Slovník pojmov

Pojem	Definícia
Phishing	Pokus o vylákanie údajov (loginy, heslá, bankové údaje) prostredníctvom falošných správ, vydávanie sa za dôveryhodné inštitúcie.
Falošná stránka	Webová stránka predstierajúca, že je oficiálnou stránkou banky, obchodu, portálu, ktorej cieľom je krádež údajov alebo peňazí.
Dezinformácia vo phishingu	Využívanie falošných správ alebo fake news na prinútenie obete kliknúť na odkaz alebo stiahnuť súbor.
Kyberzločinec	Osoba alebo skupina používajúca podvodné metódy na internete, aby získala údaje alebo peniaze.
Bezpečné odkazy	Stránky a adresy začínajúce na „https", so správnym názvom domény, pochádzajúce z overených zdrojov.

7. Metodický sprievodca pre učiteľa

Co-funded by the European Union

1. Príprava materiálov

• **Príklady:**
o Používaj výlučne fiktívne správy a phishingové stránky vytvorené pre účely vyučovania, aby sa predišlo riziku kliknutia na skutočné odkazy alebo zverejneniu údajov.
o Môžeš sa inšpirovať skutočnými phishingovými útokmi, ale zmeň názvy, logá, URL adresy tak, aby boli neutrálne a vzdelávacie.
o Neprezentuj reálne používateľské údaje ani ako príklad – zachovaj úplnú anonymitu.

• **Rôznorodosť materiálov:**
o Priprav snímky obrazovky prihlasovacích stránok, e-mailových upozornení, SMS, reklám na sociálnych sieťach.
o Môžeš zaradiť aj scénku – hranie situácie, kde niekto dostane podozrivú správu a ostatní reagujú správnym spôsobom.
o Ukáž rôzne formy phishingu: klasický e-mail, falošné akcie, odkazy od „známych“, príspevky na sociálnych sieťach, falošné aplikácie.

2. Spôsob vedenia hodiny

• **Východiskový bod:**
o Začni hodinu otvárajúcou otázkou, napr.: „Dostal niekto z vás niekedy správu, ktorá vyzerala podozrivo? Čo vás na nej zaujalo?“
o Uisti sa, že diskusia nebude viesť k zosmiešňovaniu žiakov – phishing sa môže dotknúť každého.

• **Mini-prednáška:**
o Podávaj krátke informácie (max. 2–3 min bloky) prekladané otázkami pre žiakov, aby si udržal ich pozornosť.
o Používaj jednoduché príklady a zrozumiteľný jazyk – vyhýbaj sa nadmernému množstvu technickej terminológie.

• **Praktické cvičenia:**
o Analýza falošných stránok a správ musí byť bezpečná (bez aktívnych odkazov).
o Žiaci by mali mať možnosť označovať varovné signály (napr. fixkou na výtlačkoch alebo na interaktívnej tabuli).
o Daj priestor na spoločné zdieľanie záverov, aby si žiaci mohli porovnať svoje pozorovania.

3. Moderovanie diskusie

• Povzbudzuj žiakov, aby uvádzali príklady zo svojho života alebo príbehy počuté od rodiny a známych.

• Zdôrazňuj, že nikto nie je imúnny voči internetovým podvodom – obeťou phishingu sa stávajú aj IT bezpečnostní špecialisti.
• Zásada: „Nevysmievame sa, iba analyzujeme“ – reaguj, ak sa v triede objavia posmešné komentáre.
• Môžeš použiť techniku „Otázka pre triedu“: namiesto hodnotenia odpovede sa pýtaj „Myslí si niekto inak?“, „Má niekto iný nápad na riešenie?“

4. Zabezpečenie bezpečnej atmosféry

• Zdôrazni, že phishing je trestný čin, a nie vina osoby, ktorá sa nechala oklamať.
• Ak sa niekto podelí o skúsenosť s tým, že bol obeťou podvodu, prejav podporu a uznanie za odvahu zdieľať svoj príbeh.
• Vysvetli žiakom, že najlepšou obranou je vedomosť, nie hanba – čím viac vieme o podvodoch, tým lepšie sa vieme chrániť.

5. Výchovný cieľ hodiny

• Formovanie:
o Povedomia o digitálnych hrozbách spojených s phishingom a falošnými stránkami.
o Návykov kontrolovať odkazy a odosielateľov správ pred kliknutím alebo zadaním údajov.
o Odolnosti voči manipulácii emóciami (strach, náhlenie, náhle odmeny).
o Postoja zodpovedného používateľa internetu, ktorý sa stará nielen o vlastnú bezpečnosť, ale tiež varuje ostatných pred podvodmi.

6. Doplnkové návrhy na rozšírenie hodiny

• **Domáca úloha:** Žiaci nazbierajú 3 príklady falošných správ (z internetu alebo vytvoria vlastné fiktívne) a na ďalšej hodine ich analyzujú v skupinách.
• **Mini-projekt triedy:** Vytvorenie plagátu „10 varovných signálov phishingu“ alebo „Ako overiť, či je stránka bezpečná?“, ktorý sa môže vyvesiť v škole.
• **Simulácia phishingového útoku (bezpečná):** Učiteľ pripraví krátku „falošnú správu“ a žiaci majú za úlohu označiť všetky znaky, že ide o podvod.

8. Vzdelávacie a fact-checkingové zdroje

• **EDMO – European Digital Media Observatory**
https://edmo.eu

Co-funded by the European Union

• **Europol – Kyberkriminalita**
https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

• **EUvsDisinfo**
https://euvsdisinfo.eu

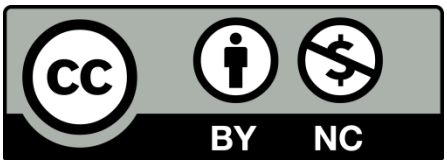
• **Niebezpiecznik.pl (PL)**
https://niebezpiecznik.pl

• **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 spolufinancovaný Európskou úniou