Co-funded by the European Union

AKTIVUJÍCÍ SCÉNÁŘ HODINY
vypracovaný v rámci projektu

„INOVACE V ŠKOLNÍM VZDĚLÁVÁNÍ"

TÉMA:

Phishing a falešné stránky

1. Cíle hodiny

Žák:

- rozumí, co je phishing a falešná internetová stránka,
- umí ukázat nejčastější metody kyberzločinců,
- ví, jak jsou falešné zprávy a fake news využívány k podvodům,
- poznává základní zásady bezpečnosti na internetu,
- rozvíjí schopnost analýzy online obsahu a kritického myšlení.

2. Cílová skupina

Žáci základních škol

3. Metody výuky

- Brainstorming
- Mini-přednáška s příklady
- Analýza případů (case study)
- Skupinové cvičení – „Pravá nebo falešná stránka?“
- Řízená diskuse
- Individuální reflexe

Projekt spolufinancovaný Evropskou unií

4. Výukové pomůcky / zdroje

- Počítač, projektor, interaktivní tabule
- Snímky obrazovky fiktivních phishingových e-mailů a falešných stránek
- Karta „10 varovných signálů phishingu“ (pro rozdání žákům)
- Seznam vzdělávacích a fact-checkingových webů:
  - Polsko: https://niebezpiecznik.pl, https://demagog.org.pl
  - Česko: https://manipulatori.cz
  - Slovensko: https://hoax.sk
  - Ukrajina: https://www.stopfake.org/en/news/
  - EU: https://edmo.eu, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

5. Průběh hodiny (45 min)

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

1. Brainstorming – zkušenosti žáků (2–3 min)

- Učitel požádá žáky, aby uvedli příklady situací, kdy:
  - obdrželi podivný e-mail nebo SMS,
  - někdo jim poslal podezřelý odkaz na sociálních sítích,
  - objevila se senzační zpráva o výhře nebo loterii, která vybízela ke kliknutí na odkaz.
- Odpovědi žáků mohou být zapsány na tabuli ve dvou sloupcích: „zdálo se pravdivé“ / „vzbudilo podezření“, aby bylo vidět, že ne všechny zprávy vypadají na první pohled jako podvod.

2. Navádějící otázky (2–3 min)

- Stalo se vám, že jste dostali zprávu slibující výhru, super akci nebo rychlý zisk, ale vypadalo to podezřele?
- Je každá zpráva, kterou dostáváme na internetu, pravdivá a bezpečná?
- Jaká nebezpečí se mohou skrývat za kliknutím na neznámý odkaz?
- Může falešná zpráva vést ke krádeži peněz, hesla do online hry nebo k převzetí účtu na sociálních sítích?
- Proč chtějí kyberzločinci, abychom jednali rychle a bez rozmyšlení?
  (Učitel povzbuzuje žáky ke krátkému sdílení příběhů – bez uvádění soukromých údajů nebo jmen.)

3. Doplňující vysvětlení učitele – rozšířené odborné informace (2 min)

- Phishing je internetový podvod, jehož cílem je vylákat důvěrné informace (hesla, přihlašovací údaje, čísla platebních karet, osobní data).
- Podvodníci využívají:
  - falešné e-maily nebo SMS, vydávají se za banku, kurýrní firmu, nákupní platformu, známého z kontaktů,
  - fake news nebo senzační titulky, které vyvolávají emoce – strach, spěch, naději na výhru,
  - falešné webové stránky, které vypadají téměř totožně jako skutečné stránky bank, obchodů či sociálních sítí.
- Hlavním cílem phishingu je přimět oběť, aby klikla na odkaz, stáhla soubor, zadala přihlašovací údaje nebo potvrdila platbu v domnění, že to dělá na bezpečné stránce.
- Kliknutí na falešný odkaz může vést k:
  - krádeži peněz z bankovního účtu,
  - převzetí účtů ve hrách, aplikacích či na sociálních sítích,
  - šíření virů a spywaru do počítače nebo telefonu.
  (Důležité zdůraznit: oběti phishingu nejsou vinny – vinni jsou podvodníci. Každý se může stát obětí manipulace, pokud není opatrný.)

2. Mini-přednáška: Phishing, falešné stránky a dezinformace (10–12 min)

1. Úvod – hrozby na internetu (1 min)

- Učitel se ptá žáků:
  - „Stalo se vám někdy, že jste dostali zprávu od neznámého člověka s odkazem nebo žádostí o zadání údajů?“
  - „Jak poznáme, jestli je zpráva bezpečná?“
- Uvede téma, zdůrazní, že phishing a falešné stránky jsou nejčastějšími nástroji kyberzločinců, kteří využívají dezinformaci a emoce, aby nás podvedli.

2. Definice phishingu (2 min)

- Phishing je internetový podvod, jehož cílem je vylákat osobní údaje nebo peníze, nejčastěji prostřednictvím:
  - e-mailů, SMS, zpráv v komunikátorech,
  - falešných stránek, které se vydávají za banky, obchody, sociální sítě,
  - falešných upozornění v prohlížeči nebo aplikacích („Tvůj telefon je infikován – klikni, abys ho opravil“).
- Cíl kyberzločinců:
  - získat loginy a hesla,
  - ukrást peníze z účtu,
  - převzít účty na sociálních sítích,
  - rozesílat další podvodné zprávy známým oběti.

3. Falešné internetové stránky (2 min)

- Jsou to weby vydávající se za skutečné, které:
  - mají podobnou adresu (např. „paypa1.com“ místo „paypal.com“),
  - kopírují vzhled stránky banky nebo obchodu,
  - žádají o zadání přihlašovacích údajů, čísla karty, osobních dat.
- Kyberzločinci často rozesílají odkazy na tyto stránky v phishingových zprávách, používají zastrašující nebo senzační titulky (např. „Tvůj účet bude smazán, pokud nepotvrdíš údaje“).

4. Techniky používané podvodníky (3 min)

Učitel probírá typické metody manipulace a uvádí příklady:

1. **Šokující zprávy:**
   - „Tvůj účet bude okamžitě zablokován, pokud neklikneš na odkaz!“
   - Využívají strach a spěch, aby oběť jednala impulzivně.
2. **Přísliby výhry nebo supernabídek:**
   - „Vyhrál jsi nový telefon!“, „Získej zdarma kupon – jen dnes!“
   - Vzbuzují naději na zisk nebo výhru.
3. **Vydávání se za instituce:**
   - Zprávy vypadající jako od banky, kurýrní firmy, známého z kontaktů.
   - Často mají padělané logo, podobnou e-mailovou adresu, ale ve skutečnosti pocházejí od podvodníků.
4. **Odkazy vedoucí na falešné stránky:**
   - Vydávají se za přihlašovací panel do banky, sociálních sítí nebo e-shopů.
   - Po zadání údajů mají zločinci plný přístup k účtu.
5. **Dezinformace a fake news:**
   - Falešné zprávy o katastrofách, hrozbách nebo „tajné akci“, které vybízejí ke kliknutí na podezřelý odkaz.
   - Příklad: „Naléhavé! Tvoje město bude evakuováno – podívej se na seznam míst!“ (odkaz vede na stránku vylákávající data).

5. Vztah phishingu k fake news (2 min)

- Fake news mohou být nástrojem kyberpodvodu, když:
  - vytvářejí falešný pocit hrozby nebo senzace, aby přiměly ke kliknutí,
  - vydávají se za zprávy od důvěryhodných institucí nebo informačních portálů,
  - využívají sdílení a virální šíření v síti k masovému rozšíření podvodu.
- Úspěšný phishing často kombinuje prvek lži (fake news) a falešné stránky, čímž vytváří dojem autenticity a časového tlaku.

6. Důsledky pro oběti (1–2 min)

- **Finanční:** krádež prostředků z bankovních účtů, neautorizované platby.
- **Soukromí:** získání osobních údajů, které mohou být využity v dalších podvodech.
- **Sociální:** převzetí účtů na sociálních sítích, rozesílání podvodných zpráv přátelům.
- **Psychologické:** stres, pocit studu nebo viny, snížená důvěra k reálným institucím.

7. Shrnutí mini-přednášky (1 min)

- Phishing je kombinace podvodu, manipulace emocemi a dezinformace.
- Obětí se může stát každý – i opatrní lidé.
- Nejpodstatnější zásady ochrany:
    1. Neklikat na podezřelé odkazy a neotvírat přílohy od neznámých odesílatelů.
    2. Kontrolovat adresy stránek a e-mailů (překlepy, podivné domény).
    3. Nikdy nezadávat důvěrné údaje, pokud máme byť jen stín pochybnosti o zdroji zprávy.

(Učitel ukáže na slajdu příklad fiktivního phishingového e-mailu, aby žáci mohli označit, co je na něm podezřelé.)

3. Skupinové cvičení – „Pravá nebo falešná stránka?“ (15–20 min)

Cíl cvičení

- Rozvoj schopnosti rozpoznávat pokusy o phishing.
- Naučit žáky analyzovat podezřelé zprávy a webové stránky.
- Uvědomění si, jak kyberzločinci manipulují emocemi (strach, spěch, výhra), aby přiměli k zadání údajů nebo kliknutí na odkaz.
- Vytvoření vlastních zásad bezpečného chování na internetu.

1. Rozdělení do skupin (1 min)

- Třída se rozdělí do týmů po 3–4 žácích.
- Každá skupina dostane 3 vytištěné nebo promítnuté příklady:
    1. **Pravá stránka banky nebo obchodu** (např. oficiální přihlašovací panel).
    2. **Falešná phishingová stránka**, která je velmi podobná té skutečné.

3. **Phishingová zpráva** (SMS/e-mail od „kurýrní firmy“ nebo „banky“) s žádostí o kliknutí na odkaz nebo zadání údajů.

1. Pravá stránka banky/obchodu

(Oficiální přihlašovací panel – příklad)

Nadpis: „Bank Polska Online – Přihlášení“
Adresa stránky (URL): https://secure.bankpolska.pl

Vzhled:

- Logo banky vlevo nahoře.
- Vpravo – volba změny jazyka (PL / EN).
- Přihlašovací pole: „Identifikátor“ + „Heslo“.
- Ikona zámku v liště prohlížeče (zelená nebo šedá).
- Patička s právní informací a odkazy: „Podmínky“, „Ochrana osobních údajů“.

Prvky autenticity:

- Adresa v doméně banky.
- SSL certifikát (https:// + zámek).
- Žádné překlepy, správný jazyk.

2. Falešná phishingová stránka

(Velmi podobná té skutečné)

Nadpis: „Bank Polska – Přihlášení“
Adresa stránky (URL): https://bankpolska-login.secure-info.net

Vzhled:

- Podobné logo banky (lehce rozmazané, horší kvalita).
- Rozvržení stránky téměř stejné, ale chybí možnost změny jazyka.
- Přihlašovací pole totožná, ale tlačítko „Přihlásit“ má jinou barvu.
- Chybí SSL certifikát nebo je zámek přeškrtnutý/červený.
- Patička bez odkazů na podmínky a ochranu osobních údajů.

Znaky falešnosti:

- Doména jiná než oficiální (např. přidaná slova, netypická koncovka).
- Často skrytý překlep v názvu domény (např. „banlkpolska.pl“).
- Někdy vyskakovací okno žádající o „aktualizaci údajů“.

3. Phishingová zpráva

(SMS nebo e-mail od „kurýrní firmy“ nebo „banky“)

Příklad SMS:
„Tvůj balík čeká na doručení. Doplať 1,99 PLN, abys ho obdržel: https://inpost-paczka-secure.net“

Příklad e-mailu od „banky“:
Předmět: „Naléhavé! Tvůj účet byl zablokován“
Text:
„Vážený kliente,
zaznamenali jsme neobvyklou aktivitu na tvém účtu. Pro odblokování přístupu klikni na odkaz níže a přihlas se:

Přihlásit se nyní

Pokud nepotvrdíš údaje do 24 hodin, účet bude trvale zablokován.“

Znaky podezřelosti:

- Časový tlak („do 24 hodin“).
- Odkaz vedoucí na jinou doménu.
- Jazykové chyby nebo podivné formulace.
- Nečekané žádosti o zadání údajů.

2. Pomůcka – „Karta 10 varovných signálů phishingu“ (2 min)

Každá skupina dostane kartu se seznamem nejčastějších varovných znaků:

Nr	Varovný signál
1	Překlepy, podivná adresa stránky (např. „paypa1.com“ místo „paypal.com“).
2	Chybí „https://“ a zámek v adresním řádku.
3	E-mailová adresa odesílatele vypadá podezřele (např. náhodný sled znaků).
4	Zpráva obsahuje jazykové chyby, netypické písmo nebo zvláštní rozvržení textu.
5	Výhrůžky nebo časový tlak („Pokud neklikneš, účet bude zablokován!“).

Co-funded by the European Union

Nr	Varovný signál
6	Příslib výhry, dárku nebo superakce bez důvodu.
7	Odkazy vedoucí na neznámé domény nebo stránky bez kontaktu.
8	Žádost o zadání hesel, čísla karty nebo osobních údajů.
9	Přílohy v neznámém formátu, zejména .exe, .zip.
10	Netypické logo nebo grafika, jiný vzhled stránky než obvykle.

3. Úkol pro skupiny (8–10 min)

Každá skupina analyzuje tři příklady a:

1. Určí, které obsahy jsou pravé a které phishingové.
2. Označí na výtisku nebo v tabulce varovné signály ze seznamu 10 bodů.
3. Uvede, jaké emoce se snaží podvodník vyvolat (strach, spěch, výhra, pocit povinnosti).
4. Formuluje zásadu ochrany, která by pomohla tomuto podvodu předejít (např. „vždy kontroluji adresu stránky“, „nekliku na odkazy z SMS“).

Tabulka k vyplnění:

Příklad zprávy/stránky	Pravá nebo falešná?	Varovné signály (č. z karty)	Jak se chránit?

Projekt spolufinancovaný Evropskou unií

Co-funded by the European Union

Příklad zprávy/stránky Pravá nebo falešná? Varovné signály (č. z karty) Jak se chránit?

4. Prezentace výsledků (4–5 min)

- Každá skupina představí jeden příklad, který považovala za nejzajímavější nebo nejobtížnější k rozpoznání.
- Učitel zapisuje na tabuli nejčastěji zmiňované varovné signály a vytváří společný „seznam zásad online bezpečnosti“.

5. Shrnutí cvičení (1–2 min)

- Phishing často vypadá profesionálně a věrohodně, proto je snadné se nechat oklamat.
- Klíčové zásady ochrany:
    1. Nikdy nezadávám hesla ani čísla karet po kliknutí na odkaz ze zprávy.
    2. Kontroluji adresu stránky a odesílatele zprávy.
    3. Nejednám pod časovým tlakem – vždy si mohu věc ověřit jinak (např. zavoláním do banky).
    4. Pokud něco vypadá podezřele – raději neklikám.

4. Diskuse: Jak se bránit phishingu a podvodům na internetu? (8–10 min)

1. Cíl diskuse

- Uvědomit žákům, proč se obětí phishingu mohou stát i opatrní lidé.
- Pochopit, jak emoce, spěch a absence ověřování informací usnadňují činnost kyberzločincům.
- Vypracovat praktické zásady bezpečného používání odkazů, zpráv a webových stránek.

2. Otázky pro žáky (základní)

- Proč mnoho lidí kliká na falešné zprávy, i když vypadají podezřele?

- Jaké emoce nejčastěji využívají kyberzločinci (strach, zvědavost, spěch, touha po výhře)?
- Jsou všechny odkazy od „přátel“ bezpečné? Proč někdy i účty přátel mohou posílat falešný obsah?
- Jak lze ověřit, zda je stránka pravá (např. https, certifikát, překlepy v adrese, oficiální doména)?
- Mohou fake news být prvním krokem k podvodu (např. falešné zprávy o katastrofách, loteriích, akcích)? Jak tento mechanismus funguje?

3. Prohlubující otázky do diskuse

- Je kliknutí na odkaz vždy bezpečné, pokud zpráva pochází od někoho známého? *(např. převzatý účet posílá infikované zprávy)*
- Proč kyberzločinci často přidávají „naléhavá varování“ nebo „časově omezenou nabídku“, aby nás přiměli kliknout rychle a bez přemýšlení?
- Je každá výhra na internetu skutečná? Jaké „červené vlajky“ naznačují, že jde o podvod?
- Jak rozeznat skutečné sdělení od banky či kurýrní firmy od falešného?
- Co udělat, když omylem klikneme na odkaz nebo zadáme údaje podvodníkům? Kdo může pomoci v takové situaci?

4. Mini-analýza – krátké příklady k rozboru

Učitel může ukázat 2–3 fiktivní zprávy (výtisky nebo slajdy):

1. „Naléhavé! Tvůj účet bude zablokován do 24h, klikni zde a potvrď své údaje!“
2. „Hej, podívej se na tohle video – jsi to ty? 😂 [odkaz]“ *(zpráva z účtu přítele)*
3. „Vyhrál jsi smartphone! Získej výhru kliknutím na odkaz níže.“

Otázky:

- Jaké emoce tato zpráva vyvolává?
- Co v ní vypadá podezřele?
- Jak bychom měli v takové situaci reagovat?

5. Závěry z diskuse – „Zlaté zásady bezpečnosti“

Na základě odpovědí žáků a analýzy příkladů učitel vytvoří seznam zásad (na tabuli nebo flipchartu), např.:

1. Vždy ověřuji odesílatele – i když je zpráva od známého.
2. Neklikám na odkazy z neznámých zdrojů ani na podezřelé přílohy.
3. Kontroluji adresu stránky – pravé servery mají správnou doménu a zámek „https://“.
4. Nedůvěřuji „náhlým akcím“ a „výhrám bez důvodu“ – nic není zadarmo.
5. Nejednám ve spěchu – podvodníci chtějí, abychom klikali bezmyšlenkovitě.
6. V případě pochybností se ptám dospělého, banky, specialisty nebo ověřuji sdělení na oficiální stránce.

6. Shrnutí učitele (1–2 min)

- Kyberzločinci využívají emoce a důvěru, aby nás podvedli – phishing funguje ne proto, že je někdo „nepozorný“, ale proto, že je chytře naplánovaný.
- Obětí se může stát každý, ale díky opatrnosti, ověřování informací a neklikání na náhodné odkazy se můžeme účinně chránit.
- Fake news jsou často prvním krokem k podvodu, protože vytvářejí senzaci, která vybízí ke kliknutí a vede na falešné phishingové stránky.

5. Shrnutí a reflexe (7–10 min)

1. Individuální reflexe – dokonči věty (3–4 min)

Každý žák dostane papír nebo použije sešit a dokončí věty:

- „Pochopil/a jsem, že phishing…“
- „Nejpodezřelejší na falešných zprávách je…“
- „Než kliknu na odkaz, zkontroluji…“
- „Abych chránil/a svůj účet, budu…“
- *(volitelně)* „Kdybych omylem klikl/a na podezřelý odkaz, měl/a bych…“

Učitel zdůrazní, že neexistují špatné odpovědi – cvičení slouží k přenesení znalostí do praktických návyků.

2. Krátká výměna zkušeností (2–3 min)

- Dobrovolní žáci přečtou své odpovědi (nebo učitel anonymně sebere lístky a přečte vybrané příklady).
- Diskuse vedená otázkami:
  - Opakovaly se vaše odpovědi?
  - Která zásada ochrany před phishingem se objevovala nejčastěji?

- Objevily se nové nápady, které stojí za to si zapamatovat?

3. Společný seznam – „5 (nebo více) zásad bezpečného používání odkazů a stránek“ (3 min)

Na tabuli nebo flipchartu vzniká společný seznam bezpečnostních zásad. Příklady:

1. Nikdy nezadávám hesla ani čísla karet do podezřelých odkazů nebo po kliknutí na e-mail/SMS.
2. Kontroluji přesnou adresu stránky (překlepy, správná doména, „https://“ a symbol zámku).
3. Neklikám na náhlé nabídky výhry, loterie, „naléhavá varování“ – nejdřív je ověřuji v oficiálních zdrojích (např. ručně se přihlásím do banky, zavolám kurýrní firmě).
4. Nejednám ve spěchu – podvodníci chtějí, abychom klikali impulzivně.
5. Konzultuji podezřelé zprávy s rodiči, učitelem nebo odborníkem.
6. *(volitelně)* Používám antivirový software, aktualizuji systém a hesla – to je další ochrana před útoky.

(Seznam může být vyfocen nebo zapsán do sešitů jako „Zásady bezpečného používání odkazů a stránek“.)

4. Shrnutí učitele – závěrečné poselství (1–2 min)

- Phishing je podvod založený na emocích a důvěře – i dospělí, kteří rozumí technologiím, se někdy nechají nachytat.
- Nejpodstatnější zásada: pokud něco vypadá podezřele nebo příliš krásně, než aby to byla pravda – neklikej, nezadávej údaje, ověř si zdroj.
- Bezpečnost na internetu závisí na bdělosti každého z nás – lepší je zeptat se, ověřit nebo počkat, než přijít o údaje či peníze.

(Lekci je možné ukončit krátkým ústním kvízem nebo otázkou: „Jakou jednu zásadu si zapamatuješ do budoucna?“ – žáci odpovídají jednoslovně či krátkou frází.)

6. Slovník pojmů

Pojem	Definice
Phishing	Pokus o vylákání údajů (loginy, hesla, bankovní data) prostřednictvím falešných zpráv, vydávání se za důvěryhodné instituce.

Pojem	Definice
Falešná stránka	Webová stránka vydávající se za oficiální web banky, obchodu nebo služby, jejímž cílem je krádež údajů nebo peněz.
Dezinformace ve phishingu	Využití falešných zpráv nebo fake news k přimění oběti kliknout na odkaz nebo stáhnout soubor.
Kyberzločinec	Osoba nebo skupina používající podvodné metody na internetu s cílem získat data nebo peníze.
Bezpečné odkazy	Stránky a adresy začínající „https“, se správnou doménou, pocházející z ověřených zdrojů.

7. Metodický průvodce pro učitele

1. Příprava materiálů

- **Příklady:**
  - Používej výhradně fiktivní phishingové zprávy a stránky vytvořené pro účely výuky, aby nedošlo k riziku kliknutí na skutečné odkazy nebo odhalení dat.
  - Můžeš se inspirovat reálnými phishingovými útoky, ale změň názvy, loga, adresy URL tak, aby byly neutrální a vzdělávací.
  - Nepředváděj reálná uživatelská data ani jako příklad – vždy zachovej plnou anonymitu.
- **Rozmanitost materiálů:**
  - Připrav snímky obrazovky přihlašovacích stránek, e-mailových upozornění, SMS, reklam na sociálních sítích.
  - Můžeš zařadit scénku – sehrání situace, kdy někdo dostane podezřelou zprávu a ostatní mají správně zareagovat.
  - Ukaž různé formy phishingu: klasický e-mail, falešné akce, odkazy od „známých“, příspěvky na sociálních sítích, falešné aplikace.

2. Způsob vedení hodiny

- **Výchozí bod:**
  - Začni hodinu otevírací otázkou, např.: „Dostal někdo z vás někdy zprávu, která vypadala podezřele? Co vás na ní zaujalo?“
  - Ujisti se, že diskuse nevede k zesměšňování žáků – phishing se může týkat každého.
- **Mini-přednáška:**
  - Přednášej krátké bloky informací (max. 2–3 min) prokládané otázkami na žáky, aby zůstali soustředění.

    - Používej jednoduché příklady a srozumitelný jazyk – vyhýbej se přemíře odborné terminologie.
- **Praktická cvičení:**
    - Analýza falešných stránek a zpráv musí být bezpečná (bez aktivních odkazů).
    - Žáci by měli mít možnost označovat varovné signály (např. fixem na výtiscích nebo na interaktivní tabuli).
    - Dej prostor pro společné sdílení závěrů, aby žáci mohli porovnat své postřehy.

3. Moderování diskuse

- Povzbuzuj žáky, aby uváděli příklady ze svého života nebo příběhy od rodiny a známých.
- Zdůrazňuj, že nikdo není imunní vůči internetovým podvodům – obětí phishingu se stávají i IT specialisté.
- Zásada: **„Nesmějeme se, jen analyzujeme“** – zasáhni, pokud se ve třídě objeví posměšné komentáře.
- Můžeš použít techniku „Otázka pro třídu“: místo hodnocení odpovědi se ptej „Myslí si někdo něco jiného?“, „Má někdo jiný nápad na řešení?“

4. Zajištění bezpečné atmosféry

- Zdůrazňuj, že phishing je trestný čin, a ne vina osoby, která se nechala nachytat.
- Pokud se někdo podělí o zkušenost, že se stal obětí podvodu, ukaž podporu a uznání za odvahu k sdílení.
- Vysvětli žákům, že nejlepší obranou je znalost, ne stud – čím víc víme o podvodech, tím lépe se umíme chránit.

5. Výchovný cíl hodiny

- Formování:
    - **Povědomí** o digitálních hrozbách souvisejících s phishingem a falešnými stránkami.
    - **Návyky** kontroly odkazů a odesílatelů zpráv před kliknutím nebo zadáním údajů.
    - **Odolnosti** vůči manipulaci emocemi (strach, spěch, náhlé výhry).
    - **Postoje** odpovědného uživatele internetu, který dbá nejen o své bezpečí, ale také varuje ostatní před podvody.

Co-funded by the European Union

6. Další návrhy rozšíření hodiny

- **Domácí úkol:** Žáci shromáždí 3 příklady falešných zpráv (z internetu nebo vytvoří vlastní fiktivní) a na příští hodině je analyzují ve skupinách.
- **Mini-projekt třídy:** Vytvoření plakátu „10 varovných signálů phishingu“ nebo „Jak ověřit, zda je stránka bezpečná?“, který lze vyvěsit ve škole.
- **Simulace phishingového útoku (bezpečná):** Učitel připraví krátkou „falešnou zprávu“ a žáci mají označit všechny znaky, že jde o podvod.

8. Vzdělávací a fact-checkingové zdroje

- **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
- **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 Evropskou unií