Phishing

Vytvorené s finančou podporou Fondu SK-NIC
www.divadlonahojdacke.sk

Teoreticko-odborné podklady

Phishing je forma online podvodu, pri ktorej sa útočník vydáva za dôveryhodnú osobu alebo organizáciu, aby získal citlivé údaje (heslá, čísla kariet, osobné informácie) alebo prinútil používateľa vykonať neželanú akciu (kliknúť, zaplatiť, stiahnuť súbor).

Podstata phishingu:

- Útočník vytvára falošné správy, e-maily, webové stránky alebo profily, ktoré vyzerajú oficiálne.
- Hrá sa na autoritu alebo známy subjekt (banka, kuriér, sociálna sieť, učiteľ, kamarát).
- Útočník využíva psychologické triky – strach, naliehavosť, odmenu, zvedavosť.

Najčastejšie formy:

- E-mailový phishing – falošné e-maily s výzvou na kliknutie, vyplnenie údajov alebo otvorenie prílohy.
- Spear-phishing – cielené útoky na konkrétnu osobu, s použitím jej mena či informácií.
- Smishing – podvodné SMS správy.
- Vishing – telefonické podvody, kde sa volajúci vydáva za inštitúciu.
- Fake login stránky – imitácie prihlasovacích portálov (napr. do e-mailu či banky).

Typické znaky phishingu:

- Emocionálny tlak: „Urob to hneď!“, „Hrozí zablokovanie účtu!“
- Neštandardný jazyk, gramatické chyby.
- Neznámy alebo podozrivý odosielateľ

Príklady známych phishingových kampaní:

„Nigérijský princ“ – starý typ podvodu, kde niekto tvrdil, že je bohatý princ a potrebuje len získať vaše údaje, aby vám poslal peniaze.

Falošné balíky – správy, že si musíte zaplatiť „doplatenie poštovného“, aby vám doručili balík.

Falošné banky a PayPal – e-maily, ktoré vyzerajú ako od banky, ale pýtajú si vaše heslá alebo číslo karty.

Herné podvody – správy, že môžete získať herné mince, skin alebo konzolu, ak zadáte prihlasovacie údaje.

Vzdelávacie ciele

- Deti vedia, čo je phishing / podvodná správa.
- Rozpoznajú základné znaky podvodnej správy.
- Naučia sa jednoduché pravidlá: nezdieľať osobné údaje, nekliknúť na podozrivé odkazy, poradiť sa s dospelým.
- Vedia, aké kroky vykonať, ak narazia na podozrivú správu (blokovať, urobiť snímku, povedať dospelému).

Pomôcky a materiály

- Vytlačené ukážky e-mailov/správ (pravé vs. falošné)
- Kartičky so situáciami pre role-play
- Tabuľa, fixky, karty „KLIKNI / NEKLIKNI“
- Komiks

Phishing

Vytvorené s finančou podporou Fondu SK-NIC
FOND SK NIC
DIVADLO NA HOJDAČKE
www.divadlonahojdacke.sk

Práca so žiakmi

1. Úvod (5–8 min.)

Otvorenie témy otázkami:

- Dostal už niekto z vás e-mail alebo správu, ktorá sľubovala výhru?
- Pýtal sa vás niekto cez internet na heslo alebo číslo karty rodiča?

Jednoduché vysvetlenie:

- Phishing je spôsob, ako sa ľudia snažia získať tvoje údaje alebo peniaze podvodom — často posielajú falošné správy, ktoré vyzerajú pravdivo.
- Takéto správy cielia na zvedavosť a emócie (sociálny inžiniering). Link často vedie na falošnú prihlasovaciu stránku (kradne prihlasovacie údaje), na stiahnutie škodlivého súboru (malvér), alebo na reklamnú/prevádzkovú stránku, ktorá infikuje zariadenie.

Ukážka komiksu:
prečítajte a rozanalyzujte komiks

2. Hlavná časť – rozpoznanie podvodnej správy (10 min.)

Vysvetliť jednoduché znaky phishingu (5 min.)

- Správa žiada o osobné údaje (heslo, číslo karty rodiča, adresa).
- Správa tlačí na rýchle konanie („klikni teraz“, „iba dnes“).
- Odkaz v správe nevyzerá ako oficiálna stránka (podivné slová v adrese už dnes podvodníci nahrádzajú stále sofistikovanejšími a vizuálne vernými kópiami originálnych webov).
- Správa obsahuje chyby v pravopise alebo divné frázy (umelá inteligencia a internetové predkladače zahraničných podvodníkov majú čoraz lepšie jazykové modely, chyby v pravopise podvodných správ už bývajú málokedy).
- Odosielateľ je neznámy alebo sa tvári, že je niekto iný.

Ukážte príklady — učiteľ premietne alebo napíše na tabuľu:

„Vyhrali ste nový tablet! Klikni sem a zadaj číslo karty!“ → PODVOD

„Ahoj, som tvoja triedna, klikni a napíš heslo“ (no učiteľ by nikdy nežiadal heslo) → PODVOD

„Tvoja kniha je pripravená v knižnici“ (správa z knižnice bez mena) → skontroluj u dospelého/knižnice.

3. Aktivita „Lovci phishingu“ (10–12 min.)

Pomôcky: vytlačené ukážky správ (5–6), niektoré reálne, niektoré podvodné (ale zjednodušené).

Priebeh: deti v skupinách (3–4) dostanú sadu správ. Úloha: určiť, ktorá správa je podvodná a zakrúžkovať ZNAKY podozrivosti (žiadosť o heslo, divný link, naliehavosť).

Výstup: každá skupina povie, prečo je/nie je správa podvodná.

4. Aktivita „Čo urobíš?“ (role-play, 5–10 min.)

Rozdeľte situácie na kartičky, každá skupina 1–2 minútovú krátku scénku:

- Dostaneš správu: „Vyhral si!“ žiada o číslo karty rodiča.
- Dostaneš správu od „kamaráta“, ktorý ťa žiada o tvoje heslo.
- Dostaneš e-mail: „Banka potrebuje potvrdenie“ s podozrivým linkom – aplikovateľné pre dospelých.
- Dostaneš správu od známeho „nie si na tejto fotke náhodou ty?“ s pripojeným neznámym linkom na prekliknutie.

Vytvorené s finančou podporou Fondu SK-NIC
FOND SK NIC
DIVADLO NA HOJDAČKE
www.divadlonahojdacke.sk

5. Záverečné zhrnutie a pravidlá (5–7 min.)
Spoločne zhrňte jednoduché zásady (napíšte na tabuľu):

- Nezadávaj osobné údaje cez odkazy v správach.
- Nikomu nepíš svoje heslo (ani kamarátovi).
- Neklikaj na cudzie odkazy, najprv sa spýtaj dospelého.
- Ak si nie istý/á, pýtaj sa dospelého (rodiča, učiteľa).
- Urob snímku obrazovky a ulož dôkaz, ak je to podozrivé.
- Nahlás a zablokuj podozrivý účet.
- Ak ide o správu od známeho, over si to s danou osobou iným kanálom (SMS, telefonát, alebo iný messenger). Nepoužívaj možnosť „odpovedať“ v tom istom chate, lebo účet môže byť hacknutý.

Doplnkové aktivity / rozšírenie

- Domáca úloha pre deti: Spýtaj sa doma – „Dostal(a) niekto z rodiny podozrivú správu? Čo urobili?“ (krátka poznámka pre triedu)
- Workshop pre rodičov: krátke info (10–15 min.) po rodičovskom združení — ukážte typické phishingové správy a vysvetlite pravidlá.
- „Phishingová anketa“: počas týždňa zbierajte anonymné ukážky podozrivých správ, ktoré žiaci dostali, a na nasledujúcej hodine ich analyzujte (bez zverejnenia citlivých údajov).

Postup, ak dieťa narazí na podvodnú správu (návod pre učiteľa/školu)

1. Dieťa urobí snímku obrazovky (ak môžu) a pošle/ukáže ju učiteľovi/rodičovi.
2. Učiteľ/dospelý nahlási účet/platformu (report) a zablokuje odosielateľa.
3. Ak ide o finančné požiadavky, informujte rodičov a prípadne políciu (ak došlo k finančnej škode).
4. Učiteľ zaznamená prípad do triednej dokumentácie (bez zverejnenia menom), ak treba, konzultuje vec so školským psychológom.

Rady učiteľovi (praktické tipy)

- Pri práci s reálnymi príkladmi nikdy nezdieľajte skutočné citlivé údaje žiakov. Upraviť texty tak, aby boli bezpečné na zobrazenie.
- Používajte jednoduchý jazyk, konkrétne príklady a krátke role-play aktivity.
- Dôraz na to, že nie je hanba priznať, že si urobil chybu (napr. klikol si) — dôležité je okamžite to povedať dospelému.
- Zapojte rodičov: krátky info-list s pravidlami „Čo robiť, keď dieťa dostane podozrivú správu“.