CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Non-formal education practices:

Phishing

R2 CYBER TOOLKIT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

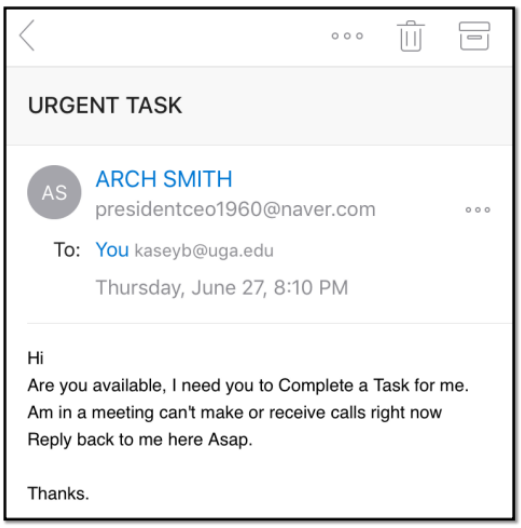
#9	**Niečo je Phishy**
hrozba(y)	Phishing
	Phishingové útoky často zahŕňajú podvodné e-maily, správy alebo webové stránky určené na vydávanie sa za legitímne organizácie, ako sú banky, platformy sociálnych médií alebo vládne agentúry. Tieto klamlivé komunikácie zvyčajne vyzývajú príjemcov, aby pod falošnou zámienkou zverejnili dôverné informácie, ako sú prihlasovacie údaje alebo čísla finančných účtov. Kyberzločinci používajú tieto ukradnuté informácie na spáchanie krádeže identity, finančného podvodu alebo iných škodlivých aktivít, čo predstavuje značné riziko pre súkromie jednotlivcov (Krádež identity a podvody), financie a online bezpečnosť.
Typológia	*Simulačné cvičenia*
Trvanie	Za minúty 2x40
Modalita	*V prítomnosti [prostredie v triede]*
Cieľ	Táto lekcia uvádza, ako sa podvodníci môžu pokúsiť získať osobné informácie prostredníctvom phishingu. Mnohokrát sa elektronická komunikácia, ako sú e-maily a textové správy, môže zdať, že pochádza z dôveryhodného zdroja, no v skutočnosti ide o podvod.
Vzdelávacie ciele	Po účasti na tejto lekcii budú dospelí študenti schopní: • Identifikujte vlastnosti dôveryhodnej elektronickej komunikácie • Vysvetlite, aké je dôležité vedieť, ako sa vyhnúť pokusom o phishing • Rozlišujte medzi legitímnymi a podvodnými správami a pokusmi o phishing
Profil stážistu	13-17 rokov
počet účastníkov	Ideálne do 20 účastníkov, prípadne študentov maximálne jednej triedy.
Materiály	Pre túto lekciu sú potrebné nasledujúce materiály a pomôcky: • Príklady phishingu (pozri v prílohe, alebo si môžete vytlačiť ďalšie príklady tu – zdroj: https://blog.usecure.io/the-most-common-examples-of-a-phishing-email#Email-account-upgrade -podvod)
Príprava	Pri príprave na túto lekciu by facilitátori mali: • Zopakujte si plán hodiny • Tlač príkladov phishingu
Implementácia	**Terminológia:** Počas lekcie sa budú diskutovať o nasledujúcich pojmoch: • **Heslo** : kombinácia písmen klávesnice, číslic a charakteristík, ktoré je potrebné zadať, aby ste získali prístup k mnohým online službám (e-mail, účty sociálnych médií, účty online nakupovania atď.) • **Phishing** : podvodný pokus o získanie citlivých informácií, ako sú používateľské mená, heslá a podrobnosti o kreditných kartách, vydávaním sa za

	dôveryhodný subjekt v elektronickej komunikácii. **Základné informácie** : Realizácia: (10 minút) Phishing je podvodný pokus o získanie citlivých informácií, ako sú používateľské mená, heslá a údaje o kreditných kartách, vydávaním sa za dôveryhodný subjekt v elektronickej komunikácii. Mnohokrát sa tieto e-maily alebo textové správy objavia, ak pochádzajú z legitímneho zdroja a zvyčajne majú pocit naliehavosti. Odkazy v e-mailoch na neoprávnené získavanie údajov zvyčajne presmerujú používateľa na nedôveryhodnú webovú stránku, kde zadá citlivé informácie. Riziká spojené s pokusmi o phishing zahŕňajú ľudí, ktorí získajú vaše heslá, vydávajú sa za vás, aby získali prístup k vášmu bankovému účtu a iným finančným službám, nakupovali položky online, ľudia, ktorí sa za vás vydávali na stránkach sociálnych médií, a prístup k súkromným informáciám vo vašom počítači. **Aktivita 1: Čo je phishing?** Distribuujte príklady phishingu. Práca v skupinách (20 minút) – rozdeľte študentov do malých skupín po 4 študentoch a poskytnite im príklady phishingu (pozri prílohu). Žiaci majú za úlohu popísať jednotlivé príklady, či ide o podvod alebo nie. Ak áno, prečo? Prezentácia výsledkov študentov - (20 minút) Objasnenie a vysvetlenie - (10 minút) **Aktivita 2: Riešenie pokusov o phishing** Prečo je dôležité vyhýbať sa pokusom o phishing? Napríklad jeden mestský zamestnanec poslal mestu bankové informácie a kyberzločinec dokázal z účtu previesť takmer 800 000 eur, kým si niekto uvedomil chybu. Hoci mesto má poistenie a podvod bol nahlásený úradom, je nepravdepodobné, že sa všetky peniaze podarí získať späť. Hoci tento príklad platí pre mesto, obeťou pokusu o phishing sa môže stať ktokoľvek. Použite flip chart a značky na spoločné brainstormingové akcie, ktoré sa majú vykonať, ak zaznamenáte pokus o phishing. (10 minút) Príklady: • Neklikajte na žiadne odkazy ani nesťahujte žiadne prílohy. Môžu obsahovať vírusy alebo spyware. • Neodpovedajte na e-mail ani textovú správu. • Označiť/zaradiť e-mail ako „nevyžiadanú poštu“ alebo „spam“. • Ak e-mail odkazuje na účet a máte o tento účet obavy, zavolajte do spoločnosti. Nepoužívajte však žiadne kontaktné informácie v e-maile alebo

	texte. Mnohokrát títo zločinci vytvárajú falošné telefónne čísla. Najprv si overte kontaktné informácie spoločnosti inde. • Nahláste phishingový e-mail úradníkom. **Aktivita 3: Odhaľte pokusy o phishing** Kvíz na overenie vedomostí - (10 minút) môžete ho spustiť pre každého, každý študent ho zvládne samostatne a výsledky potom spoločne zdieľame. Zatiaľ čo zámerom aktivity je vybudovať zručnosti v oblasti súkromia a bezpečnosti súvisiace s technológiou, je dôležité, aby facilitátor viedol na konci lekcie krátku diskusiu. Potenciálne otázky z rozboru môžu zahŕňať: • Aké sú niektoré charakteristiky dôveryhodnej elektronickej komunikácie? • Aké sú niektoré charakteristiky podvodnej elektronickej komunikácie? • Prečo je dôležité vedieť, ako sa vyhnúť pokusom o phishing? • Čo by ste mali robiť, ak dostanete e-mail alebo textovú správu, o ktorej si myslíte, že je podvodná?
Tipy a rady	Na konci hodiny odporúčame urobiť so študentmi testy phishingu. Odkaz je tu: https://phishingquiz.withgoogle.com/ . https://phishingquiz.withgoogle.com/?hl=sk https://www.proprofs.com/quiz-school/topic/phishing Je to veľmi dobrá reflexia nadobudnutých vedomostí.
Bezpečnostné opatrenia	-
Vonkajšie referencie a zdroje	• https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams • https://www.commonsense.org/education/digital-citizenship/lesson/dont-feed-the-phish • https://georgia4h.org/wp-content/uploads/Something-is-Phishy.pdf
Partner/ Autor	CPM- Centrum Prevencie Mladeze Slovakia

príloha.

Distribuujte príklady phishingového e-mailu a phishingového textu.



Vysvetlite pre e-mailovú správu nasledovné:

Zamestnanec (ktorý pracuje pre University of Georgia) dostal túto e-mailovú správu. Jej nadriadeným je Arch Smith, takže od neho pravidelne dostáva e-maily. Po ďalšom vyšetrovaní však táto správa obsahuje niekoľko podozrivých vecí:

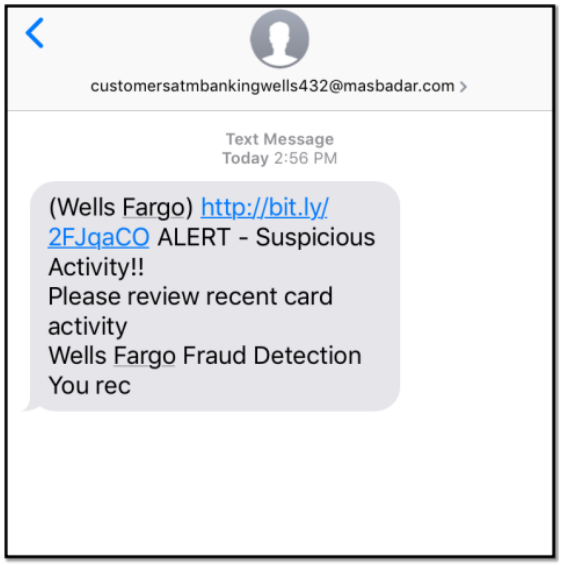
• Aj keď je e-mail od „Arch Smith“, odoslaná e-mailová adresa neznamená, že správu odoslal Arch. Keďže korešpondencia súvisí s prácou, je tiež podozrivé, že nepochádza z e-mailového účtu spojeného s University of Georgia.

• Pravopis, gramatika a mechanika e-mailu vyvolávajú obavy. Slová sú písané veľkými písmenami, ktoré by nemali byť. Interpunkcia a gramatika sú v niektorých prípadoch nesprávne.

• E-mail v skutočnosti nie je podpísaný od Arch Smith. Väčšina e-mailov končí nejakou uzávierkou a podpisom.

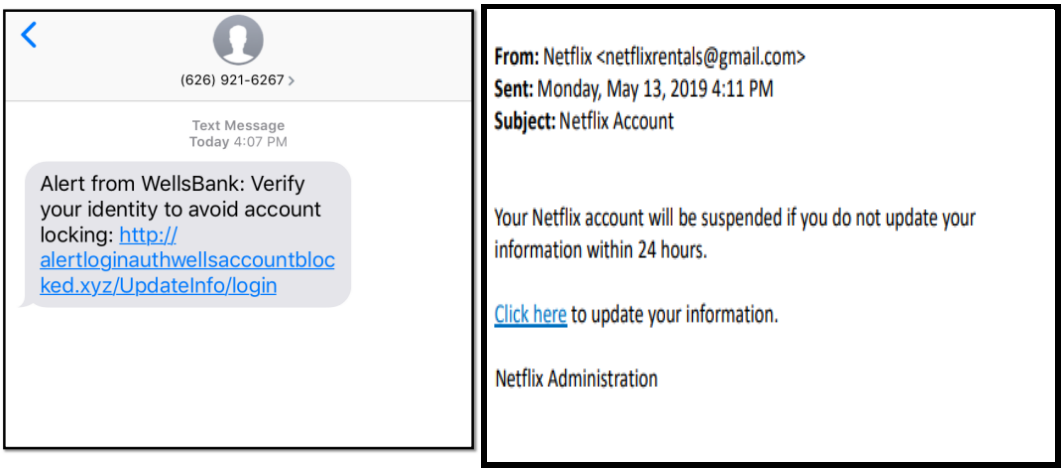
• E-mail sa zdá byť veľmi naliehavý a konkrétne neuvádza, prečo sú veci naliehavé. Odosielateľ tiež nemôže prijímať telefónne hovory (čo by sa v núdzovej situácii považovalo za „bežnú“ prax).

Vysvetlite pre textovú správu nasledovné:



Vysvetlite pre textovú správu nasledovné:

Táto osoba bankuje s Wells Fargo a niekedy dostáva e-mailové aktualizácie z banky. Po ďalšom vyšetrovaní však táto správa obsahuje niekoľko podozrivých vecí:
• Odosielateľ tejto správy používa e-mailovú adresu customersatmbankingwells432@masbadar.com. Zdá sa, že nejde o legitímnu e-mailovú adresu spojenú s Wells Fargo.
• Odkaz vložený do správy je z veľkej časti url. Bigly je služba, ktorá skracuje adresy URL – nezobrazuje celú adresu URL webových stránok. Zatiaľ čo mnohé skupiny využívajú tieto služby, mali by ste kliknúť na skrátenú adresu URL iba vtedy, keď poznáte odosielateľa.
• Pravopis, gramatika a mechanika textu vyvolávajú obavy. Správa nie je úplná.



Typické prípady získania údajov o vašom internetovom bankovníctve – Phishing je podvodný pokus o získanie citlivých informácií, ako sú používateľské mená, heslá a údaje o kreditných kartách, a to prezlečením sa za dôveryhodný subjekt v elektronickej komunikácii. Ľudia, ktorí odpovedajú na tieto typy e-mailov, sú mnohokrát požiadaní, aby urobili niečo, čo ich nezabezpečí online. Môžu byť tiež požiadaní, aby klikli na odkaz a zdieľali informácie. Môžu byť napríklad požiadaní, aby zdieľali svoje heslo, finančné informácie, PIN kódy, alebo aby poslali peniaze alebo si kúpili položky (napríklad darčekové karty). Mnohokrát je načasovanie naliehavé, pretože „bola zistená podozrivá aktivita“ alebo „váš účet je zablokovaný“ až do ďalších krokov.

Niektoré funkcie phishingového e-mailu zahŕňajú:

• Potreba overiť informácie o účte (napr. e-mailový účet, bankový účet, účet na prevod peňazí atď.). Mnohokrát sa v e-maile uvádza, že platnosť vašich osobných údajov vypršala alebo je potrebné ich overiť.
• Odkaz v e-maile/texte alebo prílohe. Odkaz vám zvyčajne neposkytuje adresu URL, takže je ťažké určiť, na ktorú webovú stránku vás presmeruje. Bez ohľadu na to klikajte iba na odkazy od dôveryhodných odosielateľov.
• Pocit naliehavosti. Mnohokrát vám phishingové e-maily poskytujú obmedzený čas (napr. 24 hodín) na vyriešenie „problému“, ktorý neexistuje.
• Príliš dobré na to, aby to bola pravda. Phishingové e-maily by mohli sľúbiť nejaký druh „návratu“, ako napríklad hotovosť alebo darčekové karty, ak najprv niečo urobíte (zvyčajne im poskytnete osobné/citlivé informácie).
• Pravopisné, gramatické a/alebo mechanické chyby. Občas sa vyskytne preklep v legitímnom e-maile, ale nadmerné množstvo chýb zahŕňa phishingový e-mail.
• Dĺžka. Niektoré phishingové e-maily môžu byť krátke. Iné môžu byť veľmi dlhé a vysvetľujú okolnosť (napr. prečo táto osoba nemôže niečo urobiť a prečo potrebuje vašu pomoc).

• Všeobecný pozdrav. Mnoho phishingových e-mailov neobsahuje pozdrav alebo jednoducho začína výrazom „ahoj“.

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.