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.

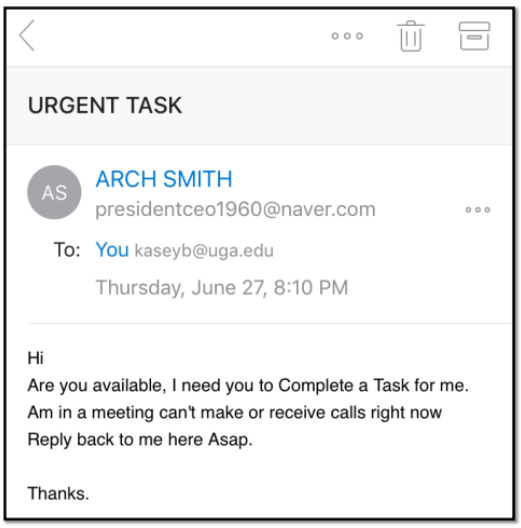
#9	**Nu-mi miroase-a bine!**
Amenințare	Phishing
	Atacurile de phishing implică adesea e-mailuri, mesaje sau site-uri web frauduloase concepute pentru a se da drept organizații legitime, cum ar fi bănci, rețele sociale sau agenții guvernamentale. Aceste forme de înșelătorie recurg la pretexte false, pentru a-i determina pe destinatari să dezvăluie informații confidențiale, cum ar fi datele de autentificare sau numărul de cont bancar. Infractorii cibernetici folosesc informațiile furate pentru a comite furturi de identitate, fraude financiare sau alte activități rău intenționate, ceea ce prezintă riscuri semnificative pentru viața privată a persoanelor (fraude și furt de identitate), finanțele și securitatea online a acestora.
Tipologie	*Exerciții de simulare*
Durată	2x40 minute
Modalitate	*Prezență fizică*
Scop	Această lecție prezintă modul în care escrocii (scammers) pot încerca să obțină informații personale prin phishing. De multe ori, comunicațiile electronice, cum ar fi e-mailurile și mesajele text, pot părea că provin dintr-o sursă demnă de încredere, dar de fapt sunt frauduloase.
Obiective de învățare	▪ Să identifice caracteristicile unei comunicări electronice de încredere ▪ Să explice de ce e important să știi cum să eviți tentativele de phishing ▪ Să diferențieze între mesajele legitime și cele frauduloase, încercările de phishing
Profilul cursantului	13-17 ani
Nr. de participanți	Ideal până la 20 de participanți sau elevi dintr-o singură clasă
Materiale	Pentru această lecție sunt necesare următoarele materiale: ▪ Exemple de phishing (pot fi regăsite în anexă, sau pot fi printate de la această adresă: https://bit.ly/4ebfCdC)
Pregătire	Pregătirea pentru această lecție trebuie să aibă în vedere: ▪ parcurgerea planului de lecție. ▪ imprimarea exemplelor de phishing
Implementare	**Terminologie:** Următorii termeni vor fi discutați pe parcursul lecției: - **Parolă**: o combinație de litere, cifre și alte semne care trebuie introduse pentru a obține acces la multe servicii online (e-mail, conturi de rețele sociale, conturi de cumpărături online etc.) - **Phishing**: încercarea frauduloasă de a obține informații sensibile, cum ar fi numele de utilizator, parole și detalii privind cardurile de credit, prin deghizarea într-o entitate de încredere în cadrul comunicării electronice. **Informații generale:**

	Implementare: (10 minute) Phishing-ul este o încercare frauduloasă de a obține informații sensibile, cum ar fi numele de utilizator, parole și detalii ale cardurilor de credit, prin deghizarea ca entitate de încredere într-o comunicare electronică. De multe ori, aceste e-mailuri sau mesaje text par să provină dintr-o sursă legitimă și, de obicei, au un caracter urgent. Link-urile din e-mailurile de phishing duc de obicei utilizatorul pe un site web deținut de escroci, unde se cere introducerea unor informații sensibile. Riscurile asociate încercărilor de phishing includ compromiterea parolelor, furtul de identitate în vederea accesării contului bancar și a altor servicii financiare, achiziționarea de articole online, furtul de identitate pe rețele sociale și accesarea informațiilor private de pe calculatorul utilizatorului înșelat. **Activitatea 1: Ce este phishing-ul?** Distribuiți exemple de phishing. Lucrul în grupuri (20 de minute) - împărțiți elevii în grupuri mici de câte 4 elevi și dați-le exemple de phishing (a se vedea anexa). Elevii au sarcina de a descrie exemplele individuale, dacă este o fraudă sau nu. Dacă da, de ce? Prezentarea rezultatelor elevilor - (20 de minute) Clarificări și explicații - (10 minute) **Activitatea 2: Gestionarea tentativelor de phishing** De ce este important să evitați tentativele de phishing? De exemplu, un angajat de la o primărie a trimis informațiile bancare ale instituției, iar infractorul cibernetic a reușit să transfere aproape 800.000 Euro din cont, înainte ca cineva să-și dea seama de greșeală. Deși municipalitatea are asigurare și escrocheria a fost raportată autorităților, este puțin probabil ca toți banii să poată fi recuperați. Deși acest exemplu se aplică unui oraș, oricine poate fi victima unei tentative de phishing. Folosiți flipchart-ul și markerele pentru a face un brainstorming colectiv cu privire la măsurile pe care trebuie să le luați în cazul în care vă confruntați cu o tentativă de phishing. (10 minute) Exemplele includ: ▪ Să nu faceți clic pe niciun link și să nu descărcați niciun atașament. Acestea ar putea conține viruși sau spyware. ▪ Nu răspundeți la un e-mail sau la un mesaj text asupra căruia aveți dubii. ▪ Marcați/categorizați e-mailul ca „junk” sau „spam”. ▪ Dacă e-mailul face referire la un cont și sunteți îngrijorat cu privire la acel cont, sunați compania. Cu toate acestea, nu folosiți nicio informație de contact din e-mail sau mesaj. De multe ori, acești

	infractori creează numere de telefon false. Verificați mai întâi informațiile de contact ale companiei în altă parte. ▪ Raportați oficialilor e-mailul de phishing. **Activitatea 3: Identificarea tentativelor de phishing** Test de verificare a cunoștințelor - (10 minute) fiecare elev îl poate face individual, apoi rezultatele sunt împărtășite clasei. Deși intenția este ca activitatea să consolideze competențele în materie de confidențialitate și securitate în utilizarea tehnologiei, este important ca facilitatorul să conducă o discuție de bilanț la sfârșitul lecției. Câteva întrebări care pot fi folosite în scop de clarificare: ▪ Care caracteristicile comunicațiilor electronice demne de încredere? ▪ Care caracteristicile comunicațiilor electronice frauduloase? ▪ De ce este important să știți cum să evitați tentativele de phishing? ▪ Ce ar trebui să faceți dacă primiți un e-mail sau un text pe care îl considerați fraudulos?
Sugestii și recomandări	Vă recomandăm să aplicați testele de phishing elevilor la sfârșitul lecției, testele se află la următoarele adrese: https://phishingquiz.withgoogle.com/. https://phishingquiz.withgoogle.com/?hl=en https://www.proprofs.com/quiz-school/topic/phishing Rezultatele testelor vor fi un bun indicator al cunoștințelor dobândite
Precauții	-
Referințe externe și resurse	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/ Author	CPM- Centrum Prevencie Mladeze Slovakia

Anexe.

Distribuiți exemple ale unui email tip phishing și ale unui mesaj de același tip.

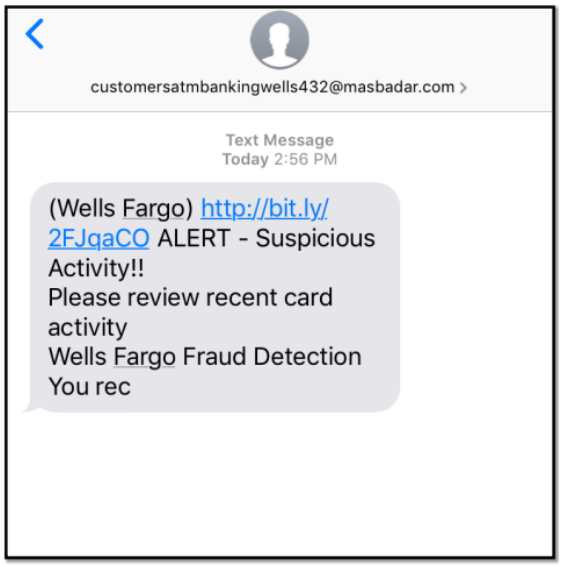


Explicați următoarele pentru mesajul e-mail:

Angajata (care lucrează pentru Universitatea din Georgia) a primit acest email. Supervizorul ei este Arch Smith, așa că primește în mod regulat e-mailuri de la el. Cu toate acestea, la o analiză mai atentă, există unele lucruri suspecte în legătură cu acest mesaj:

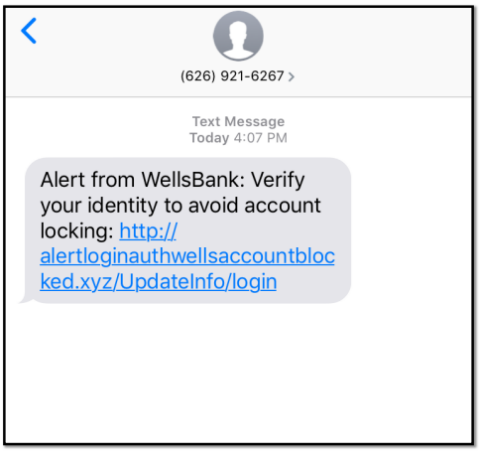
- Deși e-mailul provine de la „Arch Smith", adresa de e-mail a expeditorului nu indică faptul că Arch a trimis mesajul. Deoarece corespondența este legată de muncă, este de asemenea suspect faptul că nu provine de la un cont de email asociat cu Universitatea din Georgia.
- Ortografia, gramatica și modul de adresare ridică semne de întrebare. Sunt scrise cu majuscule cuvinte care nu ar trebui să fie scrise astfel. Punctuația și gramatica sunt incorecte în unele cazuri.
- E-mailul nu este semnat de Arch Smith. Majoritatea e-mailurilor se încheie cu o încheiere și semnătură.
- E-mailul pare foarte urgent și nu precizează natura urgenței. De asemenea, expeditorul nu poate răspunde la apeluri telefonice (ceea ce ar fi un lucru normal pentru o situație de urgență).

Explică următorul mesaj text:



Persoana este clientul băncii Wells Fargo și uneori primește actualizări prin e-mail de la bancă. Cu toate acestea, la o privire mai atentă, există unele lucruri suspecte în legătură cu acest mesaj:

- Expeditorul acestui mesaj utilizează adresa de e-mail customersatmbankingwells432@masbadar.com. Aceasta nu pare a fi o adresă de e-mail legitimă asociată cu Wells Fargo.
- Linkul încorporat în mesaj este o adresă URL bitly. Bitly este un serviciu care abreviază adresele URL - fără a afișa adresa URL completă a site-ului. În timp ce multe grupuri folosesc aceste servicii, ar trebui să faceți clic pe URL-ul scurtat numai dacă cunoașteți expeditorul.
- Ortografia, gramatica și modul de formulare al textului ridică probleme. Mesajul nu este complet.



From: Netflix <netflixrentals@gmail.com>
Sent: Monday, May 13, 2019 4:11 PM
Subject: Netflix Account

Your Netflix account will be suspended if you do not update your information within 24 hours.

Click here to update your information.

Netflix Administration

Phishing-ul este o încercare frauduloasă de a obține informații sensibile, cum ar fi numele de utilizator, parole și detalii ale cardurilor de credit; infractorul aflat în spatele tentativei de fraude pretinde că este o entitate de încredere într-o comunicare electronică. Este folosit cel mai frecvent pentru obținerea datelor bancare. De multe ori, persoanele care răspund la aceste tipuri de emailuri sunt rugate să facă ceva care le periclitează siguranța online, să facă clic pe un link și să împărtășească informații. De exemplu, li se poate cere să își dezvăluie parola, informații bancare, coduri PIN sau să trimită bani, să cumpere articole (cum ar fi carduri cadou). Este simulată o falsă urgență, care pune presiune, prin formulări de tipul „a fost detectată o activitate suspectă” sau „contul dvs. este blocat până la acțiuni ulterioare”.

Caracteristici ale unui email de phishing:

- Solicitarea de a actualiza informațiile asociate contului (cont de email, bancar, cont pentru transfer de bani etc.). De multe ori, emailul spune că informațiile dvs. personale au expirat sau trebuie să fie verificate.
- Link în e-mail/text sau atașament. De obicei, link-ul nu vă furnizează adresa URL, astfel încât este greu să determinați către ce site vă va redirecționa. În orice caz, faceți clic numai pe linkuri de la expeditori de încredere.

- Starea de urgență. De multe ori, emailurile de phishing vă oferă un timp limitat (ex. 24 de ore) pentru a rezolva o „problemă” care nu există.
- Prea frumos pentru a fi adevărat. Emailurile de phishing ar putea promite un fel de „recompensă”, cum ar fi bani sau carduri cadou, dacă faceți ceva mai întâi (transmiterea de informații personale/sensibile).
- Greșeli de ortografie, gramatică și/sau formularea mesajului. O greșeală de tipar ocazională apare ocazional într-un email legitim, dar un email de phishing conține un număr excesiv de erori.
- Lungime. Unele emailuri de phishing pot fi scurte, altele pot fi foarte lungi, explicații ale unor circumstanțe excepționale (ex. o persoană care nu poate face ceva și are nevoie de ajutorul dvs.).
- Salutul generic. Multe emailuri de phishing nu au un salut sau încep pur și simplu cu „Bună ziua”.

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.