CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Pratiche di educazione non formale:

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.

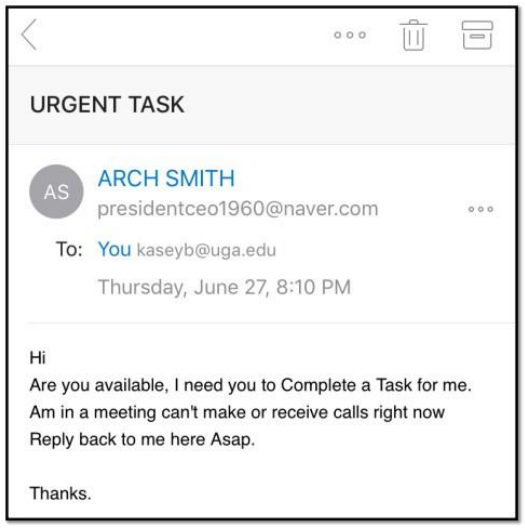
#9	**Qualcosa è fetido**
Minaccia/e	**Phishing**
	Gli attacchi di phishing spesso coinvolgono e-mail, messaggi o siti web fraudolenti progettati per impersonare organizzazioni legittime, come banche, piattaforme di social media o agenzie governative. Queste comunicazioni ingannevoli in genere spingono i destinatari a rivelare informazioni riservate, come credenziali di accesso o numeri di conti finanziari, con un falso pretesto. I criminali informatici utilizzano queste informazioni rubate per commettere furti d'identità, frodi finanziarie o altre attività dannose, con rischi significativi per la privacy (furto d'identità e frode), le finanze e la sicurezza online delle persone.
Tipologia	*Esercizi di simulazione*
Durata	In minuti 2x40
Modalità	*In presenza [in aula]*
Obiettivo	Questa lezione illustra come i truffatori possono tentare di ottenere informazioni personali attraverso il phishing. Molte volte le comunicazioni elettroniche, come e-mail e messaggi di testo, possono sembrare provenire da una fonte affidabile, ma in realtà sono fraudolente.
Obiettivi di apprendimento	Dopo aver partecipato a questa lezione, i discenti adulti saranno in grado di: - Identificare le caratteristiche di una comunicazione elettronica affidabile. - Spiegare l'importanza di sapere come evitare i tentativi di phishing. - Distinguere i messaggi legittimi da quelli fraudolenti e i tentativi di phishing.
Profilo del tirocinante	13-17 anni
n° partecipanti	Idealmente fino a 20 partecipanti, o studenti di una classe al massimo.
I materiali	Per questa lezione sono necessari i seguenti materiali e forniture: - Esempi di phishing (vedi allegato, oppure puoi stampare i prossimi esempi qui - fonte: https://blog.usecure.io/the-most-common-examples-of-a-phishing-email#Email-account-upgrade-scam)
Preparazione	Per preparare questa lezione, i facilitatori devono: - Rivedere il piano di lezione - Stampa di esempi di phishing
Attuazione	**Terminologia:** Durante la lezione verranno discussi i seguenti termini: **- Password**: una combinazione di lettere, numeri e caratteristiche della tastiera che deve essere inserita per accedere a molti servizi online (e-mail, account di social media, account per acquisti online, ecc.) **- Phishing**: tentativo fraudolento di ottenere informazioni sensibili come nomi utente, password e dati di carte di credito, camuffandosi da entità affidabile in una comunicazione elettronica.

	Informazioni di base: Attuazione: (10 minuti) Il phishing è un tentativo fraudolento di ottenere informazioni sensibili come nomi utente, password e dati di carte di credito, camuffandosi da entità affidabile in una comunicazione elettronica. Spesso queste e-mail o messaggi di testo sembrano provenire da una fonte legittima e di solito hanno un senso di urgenza. I link presenti nelle e-mail di phishing portano l'utente a un sito web non attendibile dove inserire informazioni sensibili. I rischi associati ai tentativi di phishing includono l'ottenimento delle password, l'impersonificazione dell'utente per accedere al suo conto bancario e ad altri servizi finanziari, l'acquisto di articoli online, l'impersonificazione dell'utente nei siti di social network e l'accesso a informazioni private sul suo computer. **Attività 1: Cos'è il phishing?** Distribuire esempi di phishing. Lavoro di gruppo (20 minuti) - dividete gli studenti in piccoli gruppi di 4 studenti e date loro degli esempi di phishing (vedi allegato). Gli studenti hanno il compito di descrivere i singoli esempi, se si tratta di una frode o meno. Se sì, perché? Presentazione dei risultati degli studenti - (20 minuti) Chiarimenti e spiegazioni - (10 minuti) **Attività 2: Gestire i tentativi di phishing** Perché è importante evitare i tentativi di phishing? Ad esempio, un dipendente comunale ha inviato le informazioni bancarie della città e il criminale informatico è riuscito a trasferire quasi 800.000 euro dal conto prima che qualcuno si accorgesse dell'errore. Sebbene il Comune abbia un'assicurazione e la truffa sia stata denunciata alle autorità, è improbabile che tutto il denaro possa essere recuperato. Sebbene questo esempio si riferisca a una città, chiunque può essere vittima di un tentativo di phishing. Utilizzate la lavagna a fogli mobili e i pennarelli per fare un brainstorming collettivo sulle azioni da intraprendere in caso di tentativo di phishing. (10 minuti) Gli esempi includono: - Non fare clic su alcun link o scaricare alcun allegato. Potrebbero contenere virus o spyware. - Non rispondete all'e-mail o al messaggio di testo. - Contrassegnare/categorizzare l'e-mail come "spazzatura" o "spam".

	- Se l'e-mail fa riferimento a un conto e siete preoccupati per quel conto, chiamate la società. Tuttavia, non utilizzate le informazioni di contatto contenute nell'e-mail o nel testo. Spesso questi criminali creano numeri di telefono falsi. Verificate prima le informazioni di contatto dell'azienda altrove. - Segnalate l'e-mail di phishing ai funzionari. **Attività 3: Individuare i tentativi di phishing** Quiz per verificare le conoscenze - (10 minuti) si può fare per tutti, ogni studente può farlo individualmente e poi si condividono i risultati insieme. Sebbene l'intento dell'attività sia quello di sviluppare le competenze in materia di privacy e sicurezza legate alla tecnologia, è importante che il facilitatore conduca una discussione di debrief alla fine della lezione. Tra le possibili domande di debriefing si possono citare: - Quali sono le caratteristiche di una comunicazione elettronica affidabile? - Quali sono le caratteristiche delle comunicazioni elettroniche fraudolente? - Perché è importante sapere come evitare i tentativi di phishing? - Cosa fare se si riceve un'e-mail o un testo che si ritiene fraudolento?
Suggerimenti e consigli	Si consiglia di fare dei test di phishing con gli studenti alla fine della lezione. Il link è qui: https://phishingquiz.withgoogle.com/. https://phishingquiz.withgoogle.com/?hl=en https://www.proprofs.com/quiz-school/topic/phishing È un'ottima riflessione sulle conoscenze acquisite.
Misure di sicurezza	-
Esterno riferimenti e risorse	- 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/ Autore	CPM- Centrum Prevencie Mladeze Slovacchia

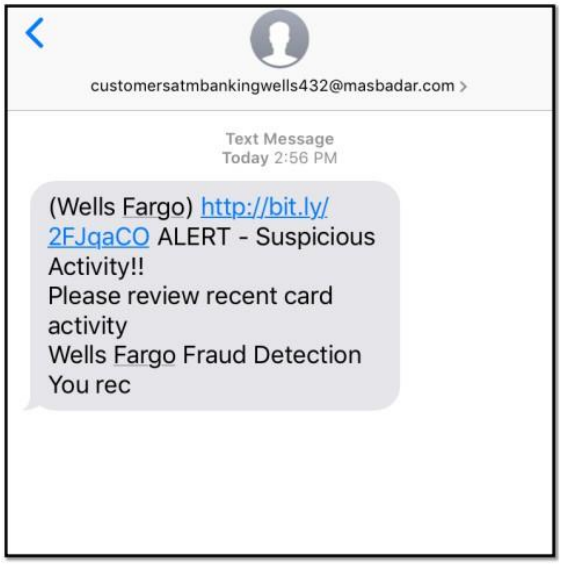
Allegato.

Distribuite esempi di e-mail e testi di phishing.



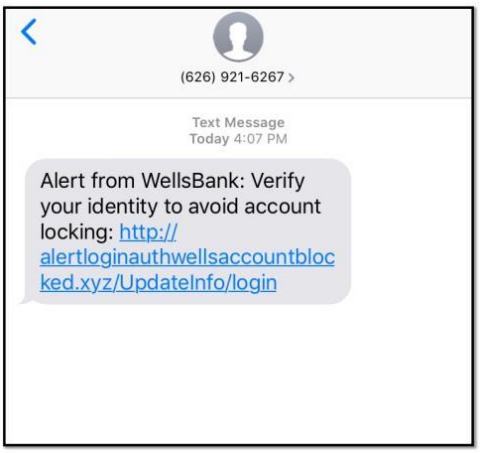
Spiegate quanto segue per il messaggio di posta elettronica:

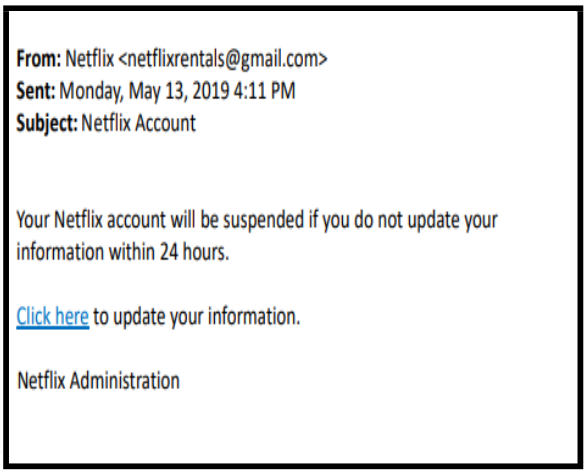
La dipendente (che lavora per l'Università della Georgia) ha ricevuto questo messaggio di posta elettronica. Il suo supervisore è Arch Smith, quindi riceve regolarmente e-mail da lui. Tuttavia, dopo ulteriori indagini, il messaggio presenta alcuni aspetti sospetti:
- Sebbene l'e-mail provenga da "Arch Smith", l'indirizzo e-mail inviato non indica che sia stato Arch a inviare il messaggio. Poiché la corrispondenza è legata al lavoro, è anche sospetto che non provenga da un account e-mail associato all'Università della Georgia.
- L'ortografia, la grammatica e la meccanica dell'e-mail destano preoccupazione. Vengono messe in maiuscolo parole che non dovrebbero esserlo. La punteggiatura e la grammatica non sono corrette in alcuni casi.
- L'e-mail non è firmata da Arch Smith. La maggior parte delle e-mail termina con una sorta di chiusura e firma.
- L'e-mail sembra molto urgente e non cita specificamente il motivo dell'urgenza. Inoltre, il mittente non è in grado di rispondere alle telefonate (cosa che sarebbe considerata una pratica "normale" in una situazione di emergenza).



Spiegare quanto segue per il messaggio di testo:

La persona ha una banca con Wells Fargo e a volte riceve aggiornamenti via e-mail dalla banca. Tuttavia, dopo ulteriori indagini, questo messaggio presenta alcuni aspetti sospetti:
- Il mittente di questo messaggio utilizza l'indirizzo e-mail customersatmbankingwells432@masbadar.com. Non sembra essere un indirizzo e-mail legittimo associato a Wells Fargo.
- Il link incorporato nel messaggio è un url di Bigly. Bigly è un servizio che accorcia gli URL, senza mostrare l'URL completo del sito web. Sebbene molti gruppi utilizzino questi servizi, dovreste cliccare sull'url accorciato solo se conoscete il mittente.
- L'ortografia, la grammatica e la meccanica del testo destano preoccupazione. Il messaggio non è completo.





Un tipico caso di ottenimento dei vostri dati bancari online - Il phishing è un tentativo fraudolento di ottenere informazioni sensibili come nomi utente, password e dati di carte di credito, camuffandosi da entità affidabile in una comunicazione elettronica. Molte volte, a chi risponde a questo tipo di e-mail viene chiesto di fare qualcosa che non garantisce la sicurezza online. Può anche capitare che venga chiesto loro di cliccare su un link e di condividere informazioni. Ad esempio, può essere chiesto di condividere la propria password, informazioni finanziarie, codici pin o di inviare denaro o acquistare articoli (come carte

regalo). Spesso il momento è urgente perché "è stata rilevata un'attività sospetta" o "il vostro conto è bloccato" fino a nuove azioni.

Alcune caratteristiche di un'e-mail di phishing sono:

- Necessità di verificare le informazioni del conto (ad esempio, conto e-mail, conto bancario, conto di trasferimento di denaro, ecc.) Spesso l'e-mail dice che le informazioni personali sono scadute o devono essere verificate.
- Link nell'e-mail/testo o nell'allegato. Di solito il link non fornisce l'URL, quindi è difficile stabilire a quale sito web vi reindirizzerà. In ogni caso, fate clic solo su link provenienti da mittenti affidabili.
- Senso di urgenza. Molte volte le e-mail di phishing vi danno un tempo limitato (ad esempio 24 ore) per risolvere un "problema" che non esiste.
- Troppo bello per essere vero. Le e-mail di phishing possono promettere una sorta di "ritorno", come contanti o carte regalo, se prima si compie un'azione (di solito fornendo informazioni personali/sensibili).
- Errori ortografici, grammaticali e/o meccanici. Un errore di battitura occasionale può capitare in un'e-mail legittima, ma una quantità eccessiva di errori indica un'e-mail di phishing.
- Lunghezza. Alcune e-mail di phishing possono essere brevi. Altre possono essere molto lunghe e spiegare una circostanza (ad esempio, perché questa persona non può fare qualcosa e ha bisogno del vostro aiuto).
- Saluto generico. Molte e-mail di phishing non hanno un saluto o iniziano semplicemente con "ciao".

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.