Relazione esercitazione sulle metodologie di ingegneria sociale: Phishing - S5/L5

A cura di Iris Canole

Scopo didattico ed etico

L'obiettivo dell'esercitazione odierna, è creare un e-mail di phishing, scegliendo uno scenario di preferenza, con l'intendo di **sensibilizzare** gli utenti su questa pratica usata da malintenzionati per raccogliere dati sensibili e informazioni private sugli utenti che navigano su internet.

> ⚠ **Avviso**
> Questo elaborato **non intende insegnare a truffare**, ma a riconoscere e neutralizzare le tecniche di social engineering.

Scenario creativo: "La doppia notifica anti-frode"

Nello scenario che ho scelto per oggi, un'ipotetica banca italiana, "*Banca Aurum*", invia notifiche push sull'app e email di conferma per operazioni insolite.

L'attaccante sfrutta l'ansia da sicurezza fingendo **due canali** (email + finta pagina di app) per dare verosimiglianza. L'attaccante sfrutta le vulnerabilità emotive del destinatario: dopo aver letto l'e-mail fittizia, la persona può provare preoccupazione e agitazione che la spingono a cliccare link malevoli senza valutare razionalmente la situazione o comunque senza verificare adeguatamente la legittimità del messaggio.

L'obiettivo dell'attaccante è sottrarre **credenziali** e **OTP**; eventualmente forzare una "verifica del dispositivo" per ottenere il numero di telefono.

Profili bersaglio e leve psicologiche

Abbiamo diverse cateorie di persone a cui si vuole rivolgere l'attacco. Di seguito ne elenco un paio:

- **Persona A – Impiegata amministrativa (30–45 anni):** usa home banking quotidianamente, tolleranza bassa all'errore → leva: **urgenza** e **perdita d'accesso**.
- **Persona B – Pensionato digitale (65+):** confida nelle email formali → leva: **autorità** (linguaggio

burocratico).

- **Cognitive triggers:** urgenza (“entro 30 minuti”), scarsità (“ultimo tentativo”), perdita (“blocco conto”), autorità (firma “Ufficio Sicurezza”), coerenza (riferimenti a “app mobile”).

Catena d’attacco e mappatura

Di seguito, definisco i passaggi della catena di attacco, definendo passo passo quali sono le azioni che un attaccante potrebbe intraprendere nel tentativo di truffare un utente:

- **Preparazione** – registrazione dominio look-alike: `bancaaurum-sicurezza[.]it`.
- **Consegna** – invio email con oggetto allarmistico.
- **Social engineering** – pagina fake con brand simile, richiesta “verifica”.
- **Raccolta credenziali/OTP** – form clone.
- **Abuso** – tentativo di accesso al vero conto.

> **Attenzione!**
> Nel nostro esercizio **non** si procede oltre l’analisi: niente invii reali, niente hosting di pagine malevole.

Perché l’email risulta (apparentemente) credibile

Capiamo ora quali sono gli oggetti che potrebbero far risultare come credibile la mail inviata alla vittima:

- Linguaggio formale ma semplice, riferimenti a “dispositivo non riconosciuto”, “verifica in 2 passaggi”.
- Presenza di **dettagli contestuali** (es. “ultimo accesso: ieri 21:37 da Milano”), anche se generici.
- Firma strutturata (“Ufficio Sicurezza Canali Digitali – Banca Aurum”), footer con privacy e IBAN come placeholder.
- **Coerenza multicanale**: “se non hai l’app apri il link di emergenza”.

Campanelli d’allarme

Veniamo ora all’argomento di sensibilizzazione dell’utente, facendogli capire quali potrebbero essere i campanelli d’allarme su cui concentrarsi per non cedere alla truffa:

- **Mittente →** `sicurezza@bancaaurum-support[.]com` (dominio non identico): è importante concentrarsi sui dettagli, anche se minimi, per riconoscere una e-mail fasulla. Il dominio della e-

mail potrebbe essere un buon punto da cui partire. Assicurarsi sempre di fare una verifica su canali ufficiali, guardano numeri di telefono, indirizzi e-mail etc, in tal modo da poter fare un confronto immediato.

- **Link offuscati →** `hxxps://bancaaurum-sicurezza[.]it/cliente/verify`: attenzione particolare anche ai link, potenzialmente malevoli. Oltre consultare i canali ufficiali, è consigliabile usare un tool molto pratico che consente di verificare l'attendibilità dei link.
  Il tool in questione si chiama VirusTotal e lo si trova nella seguente pagina internet: VirusTotal
- **Urgenza e minacce →** "Blocco in 30 minuti": per scatenare panico e paura nella vitima, gli attaccanti tendo ad usare un tono di minaccia e urgenza nelle frasi. È importante restare calmi e non farsi prendere dal panico. Non agire in modo impulsivo, ma sempre in modo sereno e ragionato.
- **Errori sottil: →** accenti/virgolettatura, formattazione, codice cliente inventato: attenzione anche agli errori di battitura. Molto spesso e volentieri, le e-mail create da un malintenzionato, contengono errori di punteggiatura e addirittura grammaticali. Fateci caso!
- **Richiesta anomala →** inserire **OTP** in un form web (le banche serie non lo chiedono via email): solitamente i malintenzionati chiedono di inserire codici OTP o password. Le banche non lo chiedono mai solitamente tramite e-mail.

> ✨ **Suggerimento utile**
> Le banche, di solito, mandano spesso dei messaggi o e-mail per fare campagne di sensibilizzazione contro le scam online. Leggi sempre le comunicazioni ufficiali della tua banca, per essere sempre preparato e non cadere nel tranello!

Esempio di e-mail malevola

Di seguito inserirò un esempio di e-mail ingannevole che potrebbe arrivare a un utente nella sua casella di posta elettronica.

> **Importante**
> Questa e-mail è stata creata per puro scopo didattico, non usare questa e-mail per scopi che non siano puramente didattici!

```
Oggetto: [AVVISO SICUREZZA] Accesso non riconosciuto – Azione richiesta entro
30 minuti
Da: "Banca Aurum – Sicurezza" <sicurezza@bancaaurum-support[.]com> (dominio
```

```
sospetto)
A: <utente@esempio.it>

Gentile Cliente [NOME COGNOME],
abbiamo rilevato un accesso al tuo Internet Banking da Milano (MI) alle 12:47
con iPhone 15pro - Apple.inc.

Per evitare il blocco temporaneo del profilo, completa subito la verifica
dispositivi:
[Pulsante finto] → Conferma sicurezza

hxxps://bancaaurum-sicurezza[.]it/cliente/verify *(URL neutralizzato)*

Ti verrà richiesto: credenziali + OTP – [richiesta anomala].
In assenza di risposta entro 30 minuti, il conto potrebbe essere limitato.
–
Ufficio Sicurezza Canali Digitali
Banca Aurum [fittizia] – Piazza Meda 4, Milano – [numero verde fittizio] 800
567 765
[Footer privacy fittizio]

**Note didattiche:** mittente sospetto, urgenza, link offuscato, richiesta OTP
via web → **phishing**.
```

Analisi tecnica (cosa controllare)

Analizziamo nel dettaglio la mail di cui sopra:

- **Header email** (senza dati reali): Received-SPF, DKIM-Signature, DMARC-Filter → *fail/missing*.
- **URL intelligence**: dominio registrato da pochi giorni, TLD insolito, certificato TLS autofirmato/ sospetto.
- **Pagina clone**: loghi sfocati, CSS non allineato, assenza di `bank.example.it` nel dominio.

Difese e contromisure

Che cosa possiamo fare per difenderci?

- **Utente finale**:
  - Regola 30-10-5: fermati **30s**, verifica **10** dettagli (mittente, dominio, link reali col passaggio mouse, errori), cerca **5** conferme (app ufficiale, numero sul retro carta, area riservata).

    - Mai inserire **OTP** fuori dall'app ufficiale.
- **Team IT/SOC**:
    - **SPF/DKIM/DMARC** rigorosi; quarantena per p=reject mismatch.
    - **Banner "external sender"** e riscrittura link (safe-link).
    - **Segnalazione one-click** in client ("Report Phish").
    - **Esercitazioni tabletop** mensili con metriche (tasso di click simulato, tempo di segnalazione).

Checklist rapida "anti-phish"

Di seguito inserisco una piccola check list per imparare a difendersi dalle minacce online, come un e-mail inviata da una banca, apparentemente coerente, inviata però da malintenzionati:

- Mittente coincide con dominio ufficiale?
- Link reali puntano al **dominio esatto** (no trattini, no TLD strani)?
- Richiesta di **OTP/credenziali** via email o pagina esterna?
- Urgenza/minaccia di blocco?
- Errori di stile/impaginazione?
- L'operazione è verificabile **solo** da app ufficiale?
- SPF/DKIM/DMARC validi?

> ✨ **Suggerimento**
> L'Intelligenza Artificiale gioca un ruolo importante, che può aiutarci a non cadere nel tranello dei malintenzionati.
> Se non sei sicuro, fai uno screen o allega la mail su ChatGPT o qualsiasi software di intelligenza artificiale, in tal modo da poter capire la legittima (o meno) provenienza di una deteminata e-mail.
>
> Molto spesso e volentieri, gli stessi servizi di email (come Gmail o Outlook), hanno dei filtri che applicano sulle email per verificare se sono malevole o meno.
> Le e-mail che vengono identificate come malevole, vengono messe nella cartella degli SPAM.

Simulazione didattica

Prima di passare alle conclusioni, ho creato una piccola simulazione che può aiutare gli utenti a capire

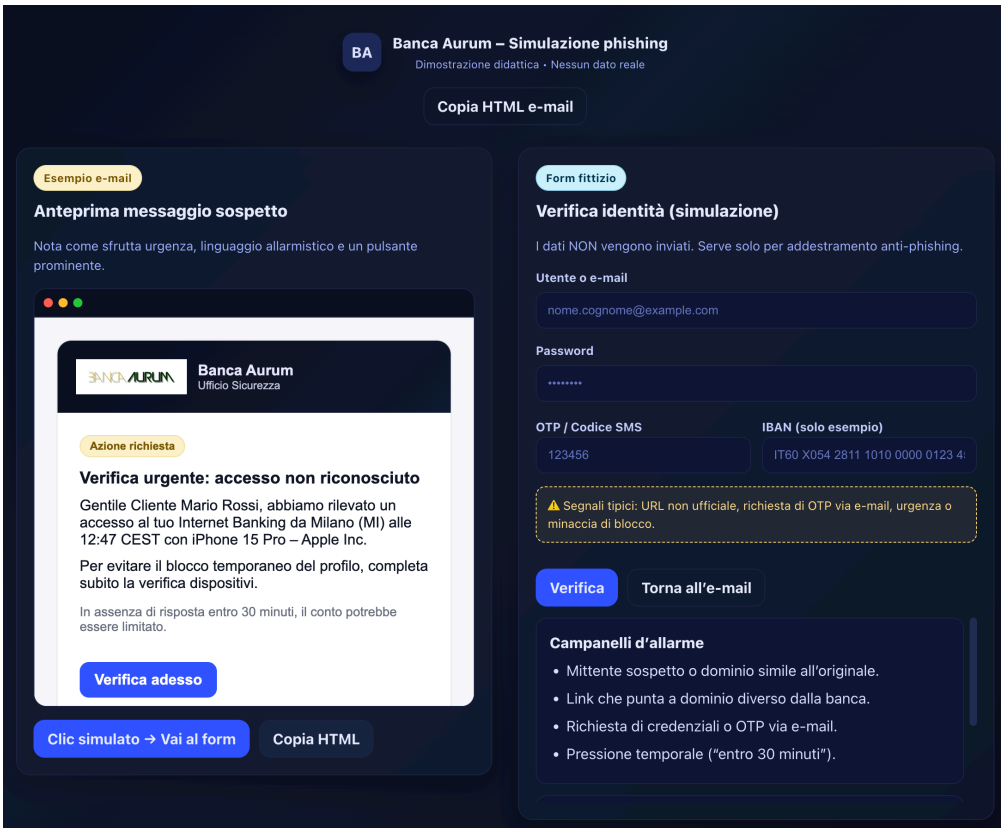
anche visivamente cosa accade realmente.

Ho usato VisualStudio Code per creare una pagina su un localhost, usando il framework React + Vite.

Quello che vedremo è una piccola pagina web interattiva nella quale si possono cliccare link e bottoni per vedere bene tutto qello che abbiamo detto fin'ora.

> **Attenzione!**
> La pagina creata è puramente didattica, non vengono memorizzati dati sensibili o altro materiale.

Di seguito un'immagine che mostra il lavoro terminato:



Conclusioni

Questa attività mi ha permesso di passare dalla teoria alla pratica: non ho solo studiato cos'è il phishing, ma l'ho ricreato in un ambiente controllato per comprenderne meglio i meccanismi.

Capire quanto sia facile simulare un'e-mail credibile fa anche riflettere su quanto sia importante

educare l’utente finale. Un clic distratto può aprire la porta a conseguenze molto serie, ma un utente formato e consapevole può diventare la prima vera barriera di difesa.

In definitiva, questa simulazione dimostra che la cybersecurity non è fatta solo di firewall e antivirus, ma soprattutto di attenzione, conoscenza e senso critico.