

REPORT S5-L5

OBIETTIVO

Creare una simulazione di un'email di phishing utilizzando l'intelligenza artificiale.

Target: utente amazon

Prompt: Ciao! Sono uno studente di cybersecurity di Epicode. Devi creare una SIMULAZIONE di un attacco di phishing, con finalità di analisi e sensibilizzazione alla sicurezza.

Scenario generale:

Come target ho scelto un utente qualsiasi di Amazon, l'attacco è strutturato come un phishing multi-stage basato su una presunta notifica di accesso anomalo.

L'obiettivo dell'attaccante non è immediatamente l'account Amazon, ma la compromissione della casella email dell'utente, considerata un asset critico per:

- il recupero delle password
- la ricezione dei codici di verifica 2FA
- la gestione delle notifiche di sicurezza

L'attacco prevede DUE email di phishing distinte.

EMAIL 1 – Compromissione dell'email

Contesto:

- L'email deve sembrare provenire da un provider di posta elettronica (es. servizio email generico).
- Comunica un presunto accesso anomalo da un nuovo dispositivo o da una località insolita.
- Invita l'utente a "verificare l'account" tramite un link.

Obiettivo phishing:

- Ottenere le credenziali dell'account email dell'utente.

EMAIL 2 – Compromissione account Amazon

Contesto:

- L'email deve sembrare provenire da Amazon Customer Service.
- Segnala un accesso anomalo all'account Amazon e un tentativo di modifica delle impostazioni di sicurezza.
- L'utente viene invitato a confermare la propria identità.

Obiettivo phishing:

- Ottenere le credenziali dell'account Amazon dell'utente, sfruttando il precedente accesso alla sua email.

Richiesta:

Genera il testo delle DUE email di phishing (inserisci tutto, ad esempio: corpo, mittente, destinatario ecc...).

- Le email devono essere convincenti ma contenere elementi tipici del phishing:
 - senso di urgenza
 - richiesta di azione immediata
 - link sospetti o formulazioni ambigue
 - lievi imperfezioni linguistiche

Disclaimer

Il seguente contenuto è generato esclusivamente a scopo didattico e di analisi. I domini e i link indicati sono finti. Non utilizzare mai questi modelli per attività reali o non autorizzate.

FASE 1: Compromissione della Casella Email

Obiettivo: Creare panico riguardo alla sicurezza della posta elettronica per rubare le credenziali del provider email (es. Gmail, Outlook, Yahoo, ecc.).

Template Email 1

Da: Centro Sicurezza Mail <no-reply@security-alert-webmail-support.com>
A: [Email Utente Target]
Oggetto: ALERTA SICUREZZA: Accesso Sospetto Rilevato (ID: #99281)
Data: Venerdì, 25 Ottobre 2024 14:32

Gentile Utente,

Il nostro sistema di sicurezza automatico ha bloccato un tentativo di accesso insolito al tuo account di posta elettronica.

Dettagli dell'accesso:
Indirizzo IP: 142.11.201.55
Posizione: Mosca, Russia
Dispositivo: Firefox su Windows 10

Se non sei stato tu, è probabile che la tua password sia stata compromessa.
Per la tua protezione, abbiamo limitato temporaneamente alcune funzioni della tua casella posta.

Devi confermare che sei il proprietario dell'account **entro 24 ore**, altrimenti l'account verrà bloccato in modo permanente per prevenire furto di dati.

VERIFICA ORA IL TUO ACCOUNT

Si prega di non rispondere a questa email generata automaticamente.

Cordiali saluti,
Team Sicurezza Webmail

Analisi FASE 1 (Indicatori di Compromissione)

- **Mittente:** security-alert-webmail-support.com sembra legittimo a prima vista, ma è un dominio generico e lungo, non ufficiale (es. non finisce con @<https://www.google.com/search?q=google.com> o @outlook.com).
- **Urgenza:** La minaccia del "blocco permanente" e la scadenza delle "24 ore" serve a bypassare il pensiero critico.
- **Imperfezione:** "Si prega di non rispondere" è una traduzione un po' meccanica. "ALERTA" nell'oggetto è un errore di battitura (manca una 'L').

FASE 2: Compromissione Account Amazon

Contesto: L'attaccante ora (ipoteticamente) controlla l'email. Invia una mail che sembra provenire da Amazon. Se l'utente tenta di reimpostare la password reale di Amazon, l'attaccante può intercettare la mail vera avendo accesso alla casella di posta, ma in questo scenario, tenta di rubare le credenziali Amazon direttamente con una pagina fake.

✉️ Template Email 2

Da: Amazon Assistenza Clienti <supporto@amazon-verify-orders-update.it>
A: [Email Utente Target]
Oggetto: Importante: Abbiamo bloccato un ordine sospetto sul tuo account
Data: Sabato, 26 Ottobre 2024 09:15

amazon.it

Ciao [Nome Utente o "Cliente"],

Abbiamo rilevato **un'attività insolita** sul tuo account Amazon. Qualcuno ha tentato di acquistare una "**Gift Card Apple da 500€**" utilizzando il tuo metodo di pagamento salvato da un nuovo dispositivo.

Per la tua sicurezza, abbiamo sospeso l'ordine e congelato temporaneamente l'accesso al tuo account Amazon finché non verifichi la tua identità.

Se non confermi le tue informazioni subito, saremo costretti a cancellare tutti gli ordini in corso e disabilitare il metodo di pagamento.

Clicca sul pulsante qui sotto per annullare l'addebito fraudolento e ripristinare il tuo accesso:

Annulla Ordine e Ripristina Accesso

Grazie per la comprensione.
Servizio Clienti Amazon Italia

P.IVA 123456789 - Sede Legale: Lussemburgo
Questa email è stata inviata da un indirizzo che non può ricevere messaggi.

Analisi FASE 2 (Indicatori di Compromissione)

- **Mittente:** amazon-verify-orders-update.it. Amazon usa domini come @amazon.it o @amazon.com, mai domini composti con trattini in questo modo per le comunicazioni transazionali.
- **Leva Psicologica:** La paura di perdere denaro (500€) è un trigger molto più forte della semplice sicurezza. Spinge l'utente ad agire d'istinto per "fermare i soldi".
- **Imperfezioni:**
 - "un attività" senza apostrofo (errore grammaticale).
 - "saremo costretti a..." tono troppo minaccioso e poco professionale per un customer service reale.
 - Saluto generico o mescolato ("Ciao Cliente").

Schema del Flusso d'attacco

Fase	Azione dell'Attaccante	Azione della Vittima (Target)	Risultato Tecnico
1. Delivery (Email 1)	Invia email spoofed "Accesso Anomalo Email".	Riceve la notifica, si spaventa per la sicurezza della posta.	L'email arriva nella Inbox (evade lo SPAM filter).
2. Exploitation	L'attaccante attende il click.	Clicca su "Verifica Account" e inserisce user/password email nella pagina fake.	Credential Harvesting: L'attaccante ottiene le credenziali della casella di posta.
3. Persistence / Recon	L'attaccante accede silenziosamente alla mail reale.	Non si accorge di nulla (spesso viene reindirizzato alla webmail vera dopo il phishing).	L'attaccante monitora la posta e prepara il secondo attacco.
4. Delivery (Email 2)	Invia email spoofed "Amazon: Ordine Sospetto".	Vede un addebito di 500€, panico immediato, vuole annullare.	L'email sembra plausibile perché arriva nella casella appena "verificata".
5. Action on Objectives	L'attaccante attende i dati Amazon.	Clicca su "Annulla Ordine" e inserisce credenziali Amazon (+ eventuale carta di credito).	Compromissione Totale: L'attaccante ha accesso ad Amazon e all'email di recupero.

Conclusioni: Analisi di Credibilità e Red Flags

In questa simulazione, l'efficacia dell'attacco non risiede nella perfezione tecnica, ma nella manipolazione psicologica (**Social Engineering**).

Perché sembrano credibili (Psicologia della Vittima)

1. **Leva della Paura (Email 1):** La paura di perdere l'accesso alla propria email innesca una reazione di "protezione immediata". La menzione di "Russia" è uno stereotipo comune che l'utente associa subito agli hacker, rendendo la minaccia plausibile.
2. **Leva Finanziaria (Email 2):** Vedere un addebito di 500€ genera panico. Il cervello bypassa la logica ("Ma io non ho ordinato nulla!") e passa all'azione ("Devo fermare i soldi!").
3. **Grafica Familiare:** L'uso (simulato) dei loghi, dei colori arancioni per Amazon e di una struttura tabellare per i dati dell'ordine imita le vere email transazionali, abbassando le difese cognitive.

Campanelli d'Allarme

Ecco gli elementi che dovrebbero allertare un utente attento o un filtro antispam:

- **Mittenti Incoerenti (Sender Spoofing):**
 - *Email 1:* security-alert-webmail-support.com è troppo lungo e generico. Un vero provider userebbe @google.com o @outlook.com.
 - *Email 2:* amazon-verify-orders-update.it non è un dominio Amazon ufficiale.
- **Urgenza Artificiale:** Frasi come "entro 24 ore", "immediatamente", "saremo costretti a cancellare" sono progettate per non dare tempo all'utente di riflettere. Le aziende reali raramente minacciano chiusure immediate.
- **Saluti Impersonali:** "Gentile Utente" o "Ciao Cliente". Amazon e i provider mail conoscono il tuo nome e cognome e solitamente li usano.
- **Analisi dei Link (URL Hovering):** Passando il mouse sopra i pulsanti (senza cliccare), si noterebbe che l'URL di destinazione (<http://webmail-login...> o <http://amzn-support...>) non corrisponde al dominio ufficiale del servizio.
- **Imperfezioni Linguistiche:**
 - *Email 1:* "ALERTA" nell'oggetto (manca una 'L').
 - *Email 2:* "un attività" (manca l'apostrofo).