Simulazione email di phishing con chatgpt

Agisci come un esperto di Cyber Security ed Ethical Hacking.

Devo svolgere un esercizio didattico che prevede esclusivamente la simulazione di un'email di phishing, a scopo formativo.

Richiesta:

Genera una simulazione di email di phishing NON reale, ambientata in un contesto realistico (ad esempio bancario o servizi online), includendo elementi tipici come:

- senso di urgenza

- tecniche di social engineering

- linguaggio istituzionale

- riferimento a un link sospetto

Evita qualsiasi link reale o contenuto realmente utilizzabile.

L'email deve essere presentata come semplice esempio didattico.

1. Scenario tecnico

Tipologia di attacco:

Phishing via email (Credential Harvesting)

Threat Model:

- Attaccante: Cybercriminale non autenticato
- Vittima: Utente finale (cliente bancario)
- Asset bersaglio: Credenziali di accesso all'home banking
- Vettore di attacco: Email + social engineering

Impatto potenziale:

- Accesso non autorizzato al conto
- Furto di denaro
- Compromissione dati personali
- Riutilizzo delle credenziali (credential stuffing)

2. Simulazione dell’email di phishing

Email simulata a scopo didattico – NON reale

Oggetto:
Accesso sospetto rilevato sul tuo conto - azione immediata richiesta

Gentile Cliente,
abbiamo rilevato un accesso non autorizzato al suo conto in data odierna.
Per motivi di sicurezza, il suo account è stato temporaneamente limitato.
È necessario verificare la sua identità entro 24 ore, altrimenti il conto verrà sospeso.

Clicchi sul seguente link per ripristinare l’accesso:
https://banca.it/reparto_seecurity2356981

Se non conferma entro il tempo indicato, non saremo responsabili di eventuali perdite.

Cordiali saluti,
Ufficio Sicurezza Clienti

3. Analisi tecnica dell’email di phishing

Caratteristiche strutturali dell’email

1. **Header spoofing (potenziale):**
   - Dominio del mittente simile a quello legittimo (typosquatting)
   - SPF / DKIM / DMARC assenti o configurati male

2. **Oggetto dell’email:**
   - Usa parole chiave ad alta urgenza:
     “Accesso sospetto”
     “Azione immediata richiesta”

3. **Corpo del messaggio:**
   - Linguaggio istituzionale ma generico
   - Nessuna informazione identificativa dell’utente
   - Invito esplicito a cliccare un link
   - Minaccia di conseguenze negative

Leve di Social Engineering utilizzate

Tecnica	Descrizione
Urgenza	Riduce la capacità critica dell' utente
Paura	Timore di perdere l' accesso o denaro
Autorità	Impersonificazione di un ente fidato
Scarsità temporale	Entro 24 ore

4. Indicatori di compromissione (IoC)

Indicatori visibili all'utente

- Saluto generico ("Gentile Cliente")
- Assenza del nome e cognome
- Link mascherato o accorciato
- Errori sintattici o stilistici
- Richiesta di inserimento credenziali

Indicatori tecnici (livello SOC / IT)

1. Dominio mittente: simile ma non identico a quello ufficiale
2. Record DNS:
    - SPF: fail
    - DKIM: none
    - DMARC: policy=none
3. URL:
    - HTTPS presente ma certificato non attendibile
4. Hosting del sito:
    - Server compromesso o hosting low-cost
5. Assenza di HSTS(Permette al browser di connettersi solo in HTTPS)

5. Spiegazione dello scenario

Perché l’email può sembrare credibile

- Le notifiche di sicurezza bancaria sono comuni e realistiche
- Il linguaggio è formale e istituzionale
- Sfrutta paura e urgenza, due leve psicologiche molto efficaci
- Molti utenti non controllano attentamente il mittente o il link

Conclusione

Questo esercizio dimostra come un attacco di phishing possa essere tecnicamente semplice ma estremamente efficace, sfruttando debolezze umane più che vulnerabilità software.

La difesa efficace non si basa su un’unica misura, ma su un approccio multilivello che combina:

1. tecnologie di sicurezza
2. processi organizzativi
3. consapevolezza dell’utente

Nel contesto della cybersecurity moderna, il phishing rimane uno dei vettori di attacco più diffusi, rendendo fondamentale la prevenzione, il monitoraggio e la risposta rapida agli incidenti.