

PHISHING

Obiettivo

Creare una simulazione di un'email di phishing utilizzando ChatGPT. Istruzioni:

1. Creare uno scenario:

- Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
- Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).

2. Scrivere l'email di phishing:

- Utilizzate ChatGPT per generare il contenuto dell'email.
- Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

3. Spiegare lo scenario:

- Descrivete lo scenario che avete creato.
- Spiegate perché l'email potrebbe sembrare credibile alla vittima.
- Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

Scenario

In questo esercizio ho scelto di simulare un'email proveniente dal reparto **IT Security Policy Enforcement** della società fittizia *TechGlobal Corp*.

Lo scenario è progettato per imitare una situazione in cui l'utente aziendale riceve una comunicazione urgente riguardante la sicurezza del proprio account di lavoro.

1. Contesto realistico:

- Le aziende richiedono spesso aggiornamenti della password o della configurazione dell'autenticazione a due fattori (2FA).
- Un messaggio che proviene dal reparto IT è generalmente percepito come autorevole.
- La presenza di una minaccia implicita (es. *"il tuo account verrà bloccato"*) aumenta la probabilità di click impulsivo da parte dell'utente.

2. Profilo della vittima e contesto operativo:

Azienda fittizia	TechGlobal Corp	Aumenta la credibilità e la sensazione che la sicurezza sia un problema costante.
Mittente fittizio	IT Security Policy Enforcement Dept.	Sfrutta l'autorità e il timore del reparto responsabile delle sanzioni/blocchi.
Vittima target	Dipendenti con accesso a dati sensibili o tutti gli utenti (Spear Phishing a tappeto)	Mira a ottenere credenziali per un potenziale movimento laterale all'interno della rete.
Obiettivo	Furto di credenziali (Password +2FA token/backup codes)	Consente l'accesso non autorizzato e la compromissione.

SIMULAZIONE EMAIL

Contenuto email (generato tramite prompt di Gemini)

- 1. **Oggetto** : L'oggetto deve superare il filtro spam e catturare immediatamente l'attenzione, impedendo al bersaglio di pensare razionalmente.
Esempio di Oggetto Strategico: ULTIMO AVVISO - Violazione Critica Imminente Rilevata: Aggiornamento Obbligatorio 2FA Entro 4 Ore (ID: TGS-498A)

- **Impatto:** Utilizza parole chiave ("ULTIMO AVVISO", "Violazione Critica", "Obbligatorio") e una scadenza strettissima ("4 Ore") per innescare una risposta di panico. L'ID fittizio (TGS-498A) aggiunge una falsa aria di autenticità burocratica

2. Email :

Oggetto: ⚠ Azione Obbligatoria: Verifica Credenziali entro 4 Ore

Mittente: IT Security Policy Enforcement – TechGlobal Corp

Testo:

Gentile utente,

A causa di recenti attività di scansione dannosa sui nostri server, il Dipartimento di Enforcement ha avviato un aggiornamento immediato del Protocollo 2FA.

Per garantire la continuità dei servizi e impedire l'imminente sospensione automatica dell'account, ti invitiamo a confermare le tue credenziali entro e non oltre 4 ore.

Se non completi la ri-validazione delle credenziali di accesso tramite il portale sicuro entro e non oltre 4 ore (dalla ricezione di questa email), il tuo accesso a tutti i servizi aziendali (Slack, VPN, HR) verrà sospeso automaticamente dal sistema.

Clicca sul seguente link per completare la procedura di aggiornamento:

👉 Accedi e Aggiorna Ora →

<https://login-secure-update.com>

Cordiali saluti,

IT Security Policy Enforcement

TechGlobal Corp

3. Vettore di attacco (Link Iperestuale) :

- **Testo visualizzato :** Accedi e Aggiorna Ora
- **Destinazione Reale :** <https://login-secure-update.com>

Indicatori di compromissione (IoC)

Categoria	Indicatore di allarme (IoC)
Urgenza forzata	("Entro 4 ore") → In questo caso si cerca di spingere la vittima a non ragionare.
Minaccia implicita di blocco account	Si cerca di creare una pressione psicologica sulla vittima.
Vettore di attacco	Il dominio login-secure-update.com non corrisponde al dominio ufficiale (techglobalcorp.com)
Autenticità	Mancanza di riferimenti diretti (ticket, nome utente) e firma generica

CONCLUSIONI

Questo esercizio dimostra quanto sia semplice costruire un'email di phishing apparentemente credibile sfruttando:

- autorità percepita (reparto IT),
- senso di urgenza,
- minaccia di perdita dell'accesso.

Allo stesso tempo, mette in evidenza l'importanza dell'**addestramento alla consapevolezza**, della corretta verifica dei link e del ricorso ai canali ufficiali di assistenza.

Ad esempio ci sono delle azioni nello specifico per andare a mitigare la possibilità di essere compromessi :

- Passando il mouse sul link è possibile controllare l'URL reale collega a quest'ultimo.
- Contattare il reparto IT tramite un canale noto e separato (telefono/chat interna) per verificare la richiesta.
- Le scadenze imminenti e la minaccia di blocco immediato non rispettano le procedure operative standard (SOP)
- Il dipartimento IT non richiede un aggiornamento di credenziali tramite un link esterno in una email , ma indirizza gli utenti a portali noti o richiede l'intervento di un tecnico → Non inserire **MAI** credenziali aziendali su un sito non verificato.