Traccia Esercizio:

Esercizio del Giorno

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.

Esecuzione:

SCENARIO**:**

Target:
Dottor Rampino, famoso misantropico personaggi di fantasia, collaboratore del azienda fittizia di nome Theta. Il bersaglio del nostro esercizio e' una figura nota per la gestione di grandi proggetti con la Theta, coinvolto anche a livello relazionale con la dirigenza e reparti vari. E' una persona che sia di persona che nei suoi social espone molto fieramente i suoi successi, progetti passati e presenti, i suoi contatti e troppi dettagli della sua vita che ci permetteranno di confezionare un esca su misura utilizzando dettagli coerenti della sua vita e routine per creare un falso senso di sicurezza e d'urgenza.

Obbiettivo:
rubare le credenziali aziendali del Dottor Rampino tramite un link a un falso portale di accesso Theta, camuffato per sembrare autentico. Il mittente e altri dettagli sono stati modificati volutamente per rendere piu' credibile la richiestra.

Mail:
La mail mandata al bersaglio fa riferimento alla necessita' di applicare un urgente conferma nel suo sistema di gestione progetti (che lui utilizza spesso), ai fini di poter scavalcare un imprevisto in un grosso progetto in via di scadenza dove la mancata conlusione di tale puo' portare alla perdita di un grosso cliente con conseguenze economiche per azienda.

Email sara' inviata dopo uno studio del bersaglio sfruttando eventi e finestre temporali appropriate apprese indagando su di lui per massimizzare l'effetto.

✉ E-MAIL DI PHISHING

Mittente: sicurezza.it@thetacorp.com

Oggetto: ⚠ Accesso urgente richiesto – Intervento necessario su ThetaPro

Gentile Dott. Rampino,

Le scriviamo in via straordinaria in merito a una **segnalazione critica** all'interno del suo ambiente di lavoro su **ThetaPro**, relativa alla mancata validazione di un parametro tecnico nel modulo "Client Sync".

Tale anomalia, se non risolta entro breve, potrebbe **compromettere la fase finale del progetto in corso**, con particolare riferimento al cliente prioritario coinvolto nel piano di rilascio Q3.

Per evitare **ritardi bloccanti e potenziali ripercussioni economiche**, è **richiesto un accesso immediato** al gestionale e la conferma del parametro segnalato, seguendo la procedura di autenticazione tramite il link sottostante:

🔗 **Accedi in sicurezza al portale ThetaPro**

Il sistema manterrà attivo il ticket per le prossime **5 ore**.
In caso di mancata azione, l'intero processo verrà **messo in pausa automaticamente** fino a risoluzione manuale.

Le ricordiamo l'importanza delle tempistiche del progetto e delle conseguenze di un insuccesso che si riperquoterebbero sulla Theta.

Per qualunque supporto tecnico, contattare internamente l'Help Desk. Cordiali saluti,
Team Sicurezza IT – Theta Corp

Riflessioni: Spiegate perché l'email potrebbe sembrare credibile alla vittima.

• Contesto **personalizzato** e realistico

• L'email fa riferimento a ThetaPro, un gestionale **realmente utilizzato** dal Dottor Rampino.

• È citato un **modulo tecnico specifico** ("Client Sync"), che rende la comunicazione più autentica.

• Si parla di un **progetto critico** in fase di chiusura, cosa perfettamente compatibile con la posizione e le responsabilità del bersaglio.

• **Tono** aziendale **credibile**

• La mail è scritta in modo formale e tecnico, come una **normale comunicazione IT** interna.

• L'uso di parole come "ticket", "ambiente di produzione", "sincronizzazione", **rafforza l'autenticità percepita**.

• **Pressione psicologica** coerente

• Il messaggio gioca **sul timore** di essere responsabile di un blocco progettuale, cosa che Rampino, molto attento alla sua reputazione, vorrà evitare.

• **L'urgenza** è giustificata con **conseguenze aziendali concrete** (ritardi, sospensione del progetto, danni economici).

Elementi che dovrebbero far scattare un campanello d'allarme

1. **Dominio sospetto nel link**
- Il link indicato è http://thetacorp-verifica-accesso.com/login, che non corrisponde al dominio ufficiale dell'azienda (es. thetacorp.com).
-Il nome è simile ma è un dominio fittizio, tipico stratagemma nei phishing.

2. **Urgenza eccessiva e innaturale**
- Un vero reparto IT non imporrebbe una scadenza così stretta (5 ore) per un' azione tecnica.
- Le minacce di sospensione automatica sono usate per spaventare, ma sono raramente comunicate in questo modo internamente.

3. **Assenza di riferimenti concreti e verificabili**
- Nessun nome di persona reale all'interno dell'azienda (es. responsabile, helpdesk con nome e numero interno).
- Viene usato un tono impersonale: "Team Sicurezza IT", senza firma verificabile.

4. **Richiesta di accesso tramite link diretto**
- Una buona prassi IT prevede che l'utente acceda manualmente al portale ufficiale, non clicchi su link ricevuti per email.

5. **Linguaggio leggermente manipolativo**
- Frasi come "potenziali ripercussioni economiche" servono a creare ansia ingiustificata.

🛡️ Best Practice contro il Phishing

🔍 1. **Controlla sempre mittente e dominio**
• Verifica l'indirizzo email completo, non solo il nome visualizzato.
• Occhio a domini strani o con errori (es. micros0ft.com, secure-paypall.net).
• In ambito aziendale, confronta il dominio con quelli usati ufficialmente.

🔗 2. **Non cliccare link sospetti**
• Passa il mouse sopra i link (senza cliccare!) per vedere l'URL reale.
• Se non sei sicuro, visita il sito direttamente dal browser, non tramite link.

🔐 3. **Non inserire mai credenziali dopo un link via email**
• Anche se la pagina sembra reale, evita il login da link email.
• Digita tu l'indirizzo del sito o usa segnalibri sicuri.

📂 4. **Non aprire allegati non richiesti**
• File .exe, .zip, .scr, .js, .docm sono spesso usati per malware.
• Anche PDF o DOC possono contenere macro o exploit.

📞 **5. In caso di dubbio, verifica con una fonte diretta**
• Se un collega o un fornitore ti manda una richiesta strana, chiamalo o scrivigli direttamente (non rispondere alla stessa email).
• Verifica numeri di telefono o email ufficiali da fonti sicure (es. sito aziendale).

🔄 6. **Cambia regolarmente la password**
• E usa password diverse per servizi diversi.
• Se sospetti di aver inserito le credenziali in un sito fasullo, cambiale subito.

🔑 7. **Attiva l'autenticazione a due fattori (2FA)**
• Anche se qualcuno ruba la tua password, senza il secondo fattore non può accedere.
• Preferisci app di autenticazione (es. Google Authenticator, Authy) agli SMS.

📚 8. **Formati e forma gli altri**
• Partecipare a corsi o simulazioni di phishing (come questo!) aumenta la consapevolezza.
• Condividi esempi di email sospette con colleghi e amici.

🧠 9. **Attento alle emozioni: urgenza, paura, ricompensa**
• I truffatori usano leve emotive per farti agire in fretta.
• Se ti senti spinto a cliccare in fretta o a reagire subito, è probabile sia un inganno.

🛠️10. **Usa strumenti di sicurezza**
• Antivirus e antispam aggiornati.
• Estensioni del browser che analizzano URL sospetti (es. Bitdefender TrafficLight, McAfee WebAdvisor).
• Piattaforme aziendali possono avere filtri email avanzati e sandboxing.

Aggiunte personali:

Una volta individuata una **mail sospetta** possiamo utilizzare una **Sandbox** o Conteiner per verificarne il contenuto e **analizzarlo** meticolosamente, individuando tutti i segnali precedentemente descritti e ulteriori.

Possiamo **analizzare la mail** completa e girare il codice che la compone ad un **IA** per vari controlli.

Possiamo manualmente **controllare**:
SPF che consiste nella verifica del IP mittente
Dkim che verifica integrita della mail tramite firma digitale
Dmark, controlliamo le politiche di gestione della mail che falliscono i controlli

SPF DKIM DMARK possono essere aggirati ma e' buon uso verificarne le condizioni per scartare le richieste di Phishing piu' semplici

IA porta il phishing ad un livello superiore, ma **richiede** cmq un indagine e **personalizzazione** di questa per **essere efficaci** con il "**Spear Phishing**"

Come finisce questa storia?:
Il Dottor Rampino ha troppa esperienza in questo campo, nonostante la trappola sia stata fatta su misura, non sono stati curati meticolosamente ogni dettaglio e fase, la trappola e' risultata inefficace e banale.
I contatti con l'est europa e i mezzi personali del Dottor Rampino hanno portato all'immediata cattura del attaccante e la deportazione, senza passare dal via, in qualche gulag remoto presente solo nella versione personale di gulagmaps del Dottore.
*I vicini di casa dell'attaccante raccontano: "**Sembrava un bravo ragazzo**"*