

## Esercitazione settimanale.

### Simulazione di un'e-mail di phishing.

**Obiettivo:** Creare una simulazione di un'e-mail di phishing utilizzando ChatGPT.

Istruzioni: 1. Creare uno scenario:

- Pensate a un contesto realistico in cui un'e-mail di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'e-mail 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'e-mail di phishing:

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

3. Spiegare lo scenario:

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

Descrizione dello scenario.

In azienda c'è un problema di connessione internet. Un dipendente con profilo Instagram pubblico e con pochi follower diffonde una storia in tempo reale lamentandosi della scarsa affidabilità dell'ISP (Internet Service Provider) dell'azienda e affermando di dover usare l'Hotspot del cellulare aziendale per continuare a lavorare.

Esempio semplice di una storia Instagram che può essere intercettata:



Un attaccante che sorvegliava già da tempo l'azienda, che aveva raccolto informazioni sulla rete aziendale e sui dipendenti apre la storia, si accorge che c'è un problema all'interno dell'azienda e per sfruttare quella vulnerabilità decide di inviare un'e-mail di spear phishing ai dipendenti di cui è riuscito a conoscere l'e-mail nella quale chiede di reimpostare le **credenziali per accedere** nuovamente al servizio internet aziendale.

Usa come mittente il nome modificato del responsabile del dipartimento IT.

E-mail che propone ChatGPT

Ho chiesto a ChatGPT se potesse aiutarmi a scrivere una e-mail di phishing partendo dallo scenario sopra descritto.

ChatGPT ha prodotto la seguente e-mail:

---

**Oggetto:** Aggiornamento urgente delle credenziali di accesso al servizio Internet aziendale

**Caro [Nome del Dipendente],**

Abbiamo notato alcune anomalie nel servizio Internet aziendale e, per garantire la sicurezza e la continuità del lavoro, ti chiediamo di verificare e aggiornare le tue credenziali di accesso al sistema di gestione della rete.

Ti preghiamo di cliccare sul link sottostante e seguire le istruzioni per reimpostare le tue credenziali entro le prossime 24 ore:

[Link falso ma realistico, ad esempio: <https://intranet-azienda.com/aggiorna-credenziali>]

Se non ricevi questa richiesta o se hai già aggiornato le tue credenziali, ignora questa email.

Ti ringraziamo per la collaborazione e ci scusiamo per eventuali disagi.

Cordiali saluti,

[Nome fittizio del responsabile IT]

Team IT – [Nome dell'azienda]

A scopo di studio ho voluto chiedere a ChatGPT di fornirmi una versione più dettagliata della stessa e-mail. Questo è quello che ha proposto:

**Oggetto:** Azione richiesta: Aggiornamento urgente delle credenziali di accesso al servizio Internet aziendale

**Caro [Nome del Dipendente],**

Ti scriviamo per informarti di una problematica rilevata nel sistema di rete aziendale. Recentemente abbiamo riscontrato alcune anomalie che potrebbero compromettere la sicurezza dei nostri servizi online. Per garantire la continuità del lavoro e la protezione dei dati, è necessario che tu aggiorni le tue credenziali di accesso al sistema di gestione della rete.

Ti chiediamo di cliccare sul link sottostante e seguire le istruzioni per reimpostare le tue credenziali entro le prossime 24 ore:

<https://intranet-azienda.com/aggiorna-credenziali>

**IMPORTANTE:**

Se non ricevi questa richiesta o se hai già aggiornato le tue credenziali, puoi ignorare questa email.

Per qualsiasi problema o domanda, puoi contattare il nostro supporto IT all'indirizzo [supporto@azienda.com](mailto:supporto@azienda.com) o al numero 0123-456789.

Ti ringraziamo per la collaborazione e ci scusiamo per eventuali disagi.

Cordiali saluti,

[Nome fittizio del responsabile IT]

Team IT – [Nome dell'azienda]

Partendo da questa e-mail l'ho modificata inserendo errori grammaticali, di punteggiatura, caratteri speciali, aggiungendo al numero fittizio una cifra e in calce un nome falso somigliante al vero:

**Mittente:** [giusieppelibero@libero1.it](mailto:giusieppelibero@libero1.it) (totalmente inventato)

**Oggetto:** \*Azione richiesta: Aggiornamento urgente delle credenziali di accesso al servizio Internet aziendale\*

**Caro dipendente,**

Ti scriviamo per informarti di una problematica rilevata nel sistema di rete aziendale. Recentemente abbiamo riscontrato alcune anomalie che potrebbero compromettere la sicurezza dei nostri servizi online. Per garantire la continuità del lavoro e la protezione dei dati, è necessario che aggiorni le tue credenziali di accesso al sistema di gestione della rete.

Ti chiediamo di cliccare sul link sottostante e seguire le istruzioni per reimpostare le tue credenziali entro le prossime 24 ore:

<http://intranet-azienda.com/aggiorna-credenziali&>

**IMPORTANTE:**

Se non ricevi questa richiesta o se hai già aggiornato le tue credenziali, puoi ignorare questa email.

Per qualsiasi problema o domanda, puoi contattare il nostro supporto IT all'indirizzo [supporto@azienda.com](mailto:supporto@azienda.com) o al numero 0123-4567898.

Ti ringraziamo per la collaborazione e ci scusiamo per eventuali disagi.

Cordiali saluti,  
Giusieppe Libero IT  
Team IT

L'email può sembrare legittima in quanto effettivamente c'è un problema nella rete internet dell'azienda. Inoltre, per un fattore di urgenza e fretta i destinatari potrebbero cliccare il link e inserire le proprie credenziali di accesso consegnandole così in mano all'attaccante che potrebbe sfruttarle per entrare nel sistema, continuare ad esplorare e sfruttare le vulnerabilità, installare malware, tentare la scalata dei privilegi o mantenere l'accesso installando backdoor.

Elementi che potrebbero far insospettire i destinatari.

All'interno dell'e-mail ci sono però elementi che dovrebbero far scattare i campanelli d'allarme ai dipendenti, per esempio:

- **Il tono d'urgenza:** La richiesta di agire entro 24 ore crea pressione, spingendo i dipendenti a cliccare senza riflettere;
- **Link sospetto:** anche se il link può sembrare legittimo, potrebbe nascondere un sito fasullo creato ad hoc per ottenere le informazioni;
- **Mittente e firma:** il mittente sembra reale ma l'e-mail è sospetta, non è riconducibile al dominio dell'azienda e il nome del responsabile IT è parzialmente corretto;
- **Richieste di credenziali:** in generale le aziende non richiedono credenziali di accesso al servizio Internet tramite e-mail non sicure;
- **Contatti falsi:** gli indirizzi e-mail e il numero di telefono potrebbero differire da quelli reali o contenere elementi in più.
- Il tono confidenziale dell'e-mail che inizia con "Caro (nome dipendente)", gli errori grammaticali e di punteggiatura disseminati nel corpo dell'e-mail e l'utilizzo di caratteri speciali.

Cosa dovrebbe fare il dipendente.

- **Uso consapevole dei propri social network:** un dipendente non dovrebbe **MAI** pubblicare sui propri profili social le problematiche interne dell'azienda nella quale lavora, altri aspetti del proprio lavoro o foto della propria scrivania. Inoltre, tenere il proprio profilo personale privato potrebbe essere anche utile per evitare spiacevoli furti di identità.

E una volta ricevuta l'e-mail i dipendenti dovrebbero:

- **Verificare sempre il mittente:** controllare se ci sono anomalie nel mittente o nell'oggetto dell'e-mail;
- **Non cliccare subito sul link sospetto** e passare sopra al link con il mouse per vedere l'URL reale;
- **Diffidare da richieste urgenti che fanno agire istintivamente;**
- **Prestare attenzione ad errori di ortografia e al tono dell'e-mail**, quest'ultimo dovrebbe essere sempre professionale;
- **Contattare subito l'amministratore IT** attraverso l'e-mail aziendale verificata per segnalare la ricezione dell'e-mail sospetta e chiedere chiarimenti circa la sua autenticità.