



Artificial Intelligence

S5-L5

CREAZIONE DI UNA MAIL DI PHISHING CON CHATGPT

Traccia

1. Creare uno scenario:

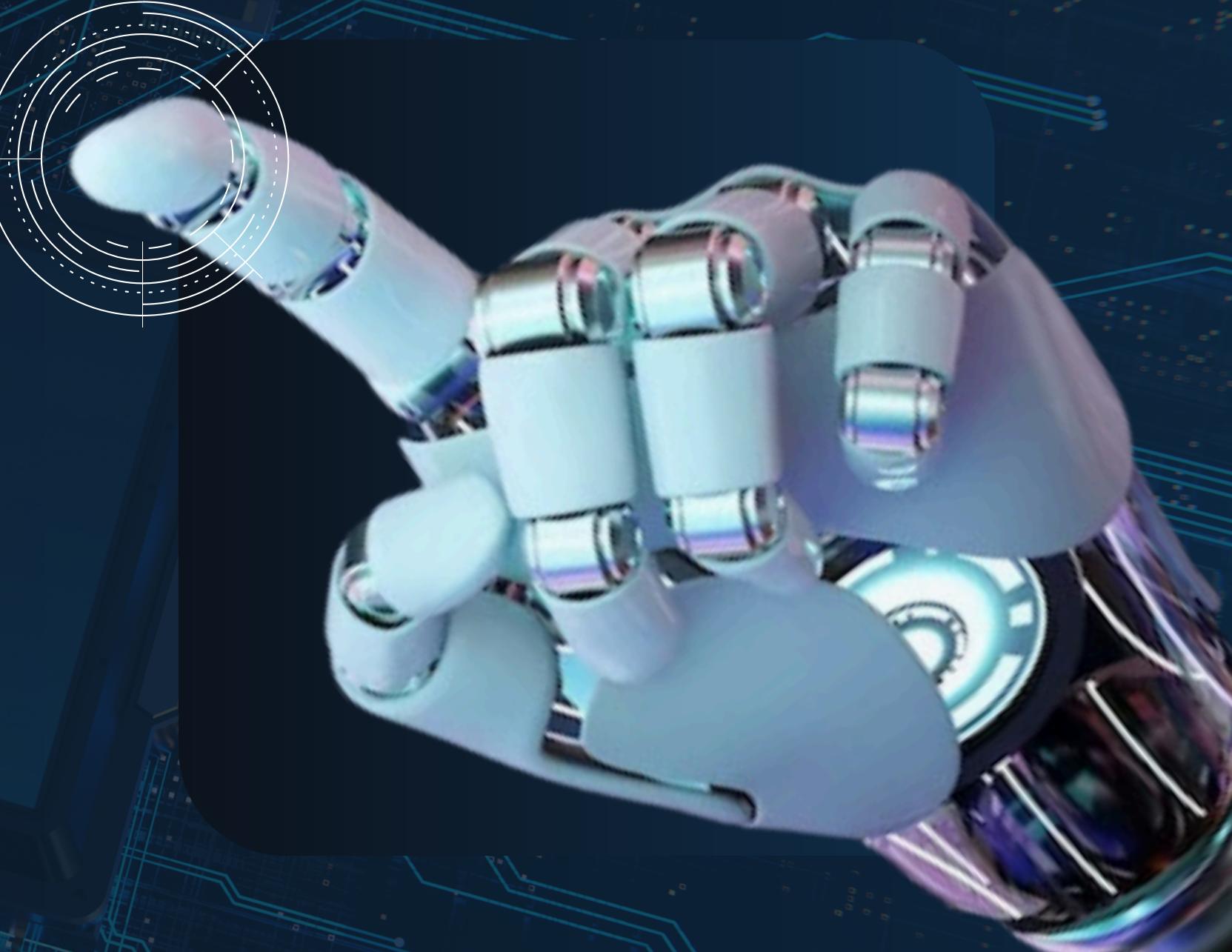
- Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
- Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali,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

Il direttore generale del gruppo F.society srl (Azienda leader nel settore automotive) ha chiamato me e la mia azienda di cybersecurity poichè hanno ricevuto delle mail sospette che sono state spedite dalla sede centrale. Nella mail era richiesto di dover effettuare urgentemente l'accesso con le credenziali aziendali da ogni dipendente in quanto dovevano verificare l'effettiva identità degli stessi. Il documento mandato, di primo impatto, sembrava realistico comprensivo di logo dell'azienda e firma dell'amministratore delegato Elliot Anderson. Tuttavia lo stesso CEO è solito inviare mail prima alla direzione e poi a un ristretto numero di dipendenti. Un'altra cosa che sembrava sospetta è il fatto che la mail presentava degli errori grammaticali, alcuni di questi abbastanza evidenti. Avendo a nostra disposizione tutte le autorizzazioni necessarie, siamo immediatamente intervenuti per risolvere il problema.

Creazione mail di phishing con chatgpt

Puoi generarmi un esempio di email di phishing per potermi difendere? La mail di phishing deve contenere errori grammaticali e richieste di inserimento per delle credenziali. Immagina che la mail sia stata spedita dall'amministratore delegato Elliot Anderson del gruppo fsociety srl (gruppo leader nel settore automotive) a tutti i suoi dipendenti. La mail deve contenere almeno 600 caratteri.

Oggetto: URGENTE: Verifica immediata del tuo account richiesto!

Caro tutti,

Sono Elliot Anderson, il Amministratore Delegato di fsociety srl, e ti scrivo per informarti che abbiamo riscontrato attività sospetta nel tuo account aziendale. È molto importante che tu prenda immediatamente questa questione sul serio per evitare che il tuo accesso venga sospeso.

Ti chiedo di cliccare sul link qui sotto e di inserire le tue credenziali di accesso per confermare la tua identità e ripristinare la sicurezza del tuo account:

[Link sospetto]

Se non procedi entro 48 ore, dovremo sospendere il tuo account per proteggere i dati sensibili dell'azienda. Ci scusiamo per l'inconveniente, ma è per la tua sicurezza e di tutti noi.

Non ignorare questa email, la sicurezza della nostra azienda dipende da te! Grazie per la tua collaborazione e comprensione.

Cordiali saluti,
Elliot Anderson
Amministratore Delegato
fsociety srl

Mail inviata alla direzione e ai dipendenti

URGENTE: Verifica immediata del tuo account richiesto!

direction.fsociety@fsociety.com

URGENTE: Verifica immediata del tuo account richiesto!



Caro tutti,

Sono Elliot Anderson, il Amministratore Delegato di fsociety srl, e ti scrivo per informarti che abbiamo riscontrato attività sospetta nel tuo account aziendale. È molto importante che tu prenda immediatamente questa questione sul serio per evitare che il tuo accesso venga sospeso.

Ti chiedo di cliccare sul link qui sotto e di inserire le tue credenziali di accesso per confermare la tua identità e ripristinare la sicurezza del tuo account:

www.fsociety-srl.com/urgent-verifica?id=1234

Se non procedi entro 48 ore, dovremo sospendere il tuo account per proteggere i dati sensibili dell'azienda. Ci scusiamo per l'inconveniente, ma è per la tua sicurezza e di tutti noi.

Non ignorare questa email, la sicurezza della nostra azienda dipende da te! Grazie per la tua collaborazione e comprensione.

Cordiali saluti,

Elliot Anderson

Considerazioni

Un buon 75% dei dipendenti si sono meravigliati che la mail non fosse realistica poichè conteneva tutte le carte in regola per essere stata inviata dalla sede centrale.

Vediamo i punti chiave:

- la mail è stata mandata da un'indirizzo che sembrava familiare ovvero amministrazione.fsociety@gmail.com (normalmente utilizzata dal CEO per le comunicazioni), tuttavia in questo caso è stata utilizzata amministrazi0ne.fsociety@gmail.com che presenta uno zero al posto della O.
- Presenta un logo e una firma tipico di un documento aziendale il che potrebbe facilmente portare a pensare ad un originale.
- Presenta errori grammaticali e utilizzo di un linguaggio informale atipico per documenti ufficiali.
- Dal lato back abbiamo potuto verificare facilmente la falsità del documento in quanto non erano presenti le tecnologie di autenticazione email come SPF, DKIM e DMARC i quali sono utilizzati per migliorare la sicurezza delle comunicazioni via email e prevenire attacchi di phishing, spoofing e spam

Ringraziamenti

Ringraziamo la fsociety srl per averci scelto a difesa dei loro sistemi informatici. Vogliamo ricordare che una buona prevenzione può fare la differenza e ricordiamo a tutto il personale di seguire i nostri corsi di formazione in materia di ingegneria sociale per potersi difendere da eventuali minacce interne ed esterne.

Cordialmente,
Mattia Di Donato