S5.L5

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

Esecuzione:

In questo scenario, la vittima riceve un'email che sembra provenire da PayPal, notificando un presunto "Aggiornamento di sicurezza obbligatorio" necessario per evitare che il suo account venga sospeso.

L'email contiene un link che invita a confermare l'identità e reimpostare la password. L'obiettivo del phishing è convincere la vittima a inserire le proprie credenziali su una copia della pagina originale di PayPal, permettendo così ai truffatori di accedere al suo account PayPal.

Da: sicurezza@paypal-support.com

A: abcd@hotmail.it

Oggetto: 🔒 Aggiornamento urgente di sicurezza richiesto per il tuo account PayPal!

Gentile Cliente,

Per proteggere i nostri utenti e mantenere un ambiente sicuro, **stiamo eseguendo un aggiornamento obbligatorio sui nostri sistemi di sicurezza**. È stato rilevato un accesso insolito che potrebbe mettere a rischio la sicurezza del Suo account.

Dettagli dell'accesso non riconosciuto:

- **Posizione**: Milano, Italia
- **Data**: 30/10 /2024

Azioni richieste:

Per evitare che il Suo account PayPal venga sospeso, La invitiamo a confermare immediatamente la Sua identita e aggiornare la pasword.

Conferma il tuo account ora

Questo passaggio è essenziale per mantenere il Suo account attivo. **Completi la procedura entro le prossime 24 ore** per evitare la sospensione temporanea dell'account.

Se ha bisogno di assistenza, non esiti a contattarci al nostro numero verde: 800 123 789.

Grazie per la collaborazione e per la fiducia che ripone in noi.

Team di Sicureza PayPal

Spiegazione dello Scenario

Questa email di phishing potrebbe sembrare credibile alla vittima per vari motivi:

1. **Aspetto professionale**: L'email è strutturata per imitare lo stile delle comunicazioni ufficiali di PayPal.
2. **Richiesta di conferma immediata**: Il riferimento ad un accesso non riconosciuto possono indurre la vittima ad agire subito per “proteggere” il proprio account.
3. **Link ingannevole:** Il link riporta ad una copia del sito, quindi non alla pagina originale.

Elementi di Allarme nell'Email

- **Indirizzo email falso**: L'email, "paypal-support.com", non è quella ufficiale.
- **Lingua urgente e minacce velate**: Parole come “Aggiornamento urgente” e “sospensione temporanea” sono segnali tipici delle email di phishing.
- **Assenza di personalizzazione**: L'email non contiene il nome del destinatario o dati personali.
- **Errori grammaticali:** L’email contiene alcuni grammaticale

Conclusione:

Per prevenire che le persone cadano vittime delle tecniche di phishing, è fondamentale fornire loro una formazione adeguata. È importante insegnare a controllare alcuni elementi nelle email, come l'indirizzo del mittente, la presenza di errori grammaticali, minacce velate e la verifica dei record DMARC, DKIM e SPF. Questo aiuterà a evitare il clic su link sospetti.