**PROGETTO S5/L5 PEDRANA YURI 10/01/2025**

Nel esercizio di oggi ci è stato chiesto di 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.

## Introduzione

Per rendere questo esercizio il più realistico possibile, ho scelto di utilizzare PayPal, uno dei servizi di pagamento online più sicuri e affidabili a livello globale.

L’obiettivo è simulare un attacco di phishing in cui la vittima riceve una comunicazione falsa, che potrebbe riguardare un errore nelle credenziali di accesso o un accesso non autorizzato al suo account PayPal.

Questo tipo di attacco è molto comune e sfrutta la paura e l’urgenza per spingere la vittima a fornire informazioni personali e sensibili.

Di seguito, entreremo nel dettaglio.

**PROGETTO S5/L5 PEDRANA YURI 10/01/2025**

**Oggetto**: Attenzione: Acceso non autorizzato al tuo account PayPal

**Mittente**: supporto@paypal.com

**Testo del messaggio**:

Caro cliente,

Abbiamo notato un acceso non autorizzato al tuo account PayPal da un dispositivo sconosciuto. Per protegere la tua sicurrezza, abbiamo temporaneamente limitato alcune funzionalità del tuo account.

Ti invitiamo a verifcare immediatamente le tue informazioni accedendo al tuo account tramite il link sottoindicato:

Verifica il tuo account

Se non completi la verfica entro 48 ore, il tuo account potrebbe essere sospeso.

Grazie per la tua attenzione,

iI team di sicurezza PayPal

## Perchè Paypal

Ho creato questo scenario per far capire che attacchi del genere succedono ogni giorno, senza sosta. Ogni giorno ci sono tentativi di phishing di ogni tipo, e a volte anche le persone più attente ci cascano. Ho scelto PayPal come esempio perché è uno dei metodi di pagamento più sicuri e usati da tutti. Proprio per questo, è facile farsi ingannare anche se pensiamo di stare al sicuro.

## E’ attendibilie?

Questo esemipo potrebbe sembrare credibile perché la persona potrebbe essere indirizzata dal phishing, senza nemmeno toccare nulla di sospetto. Spesso le persone, quando non si ricordano una password, potrebbero pensare che sia stata dimenticata o che sia troppo semplice da usare. Inoltre, il messaggio che invita a “verificare il tuo account” sembra rassicurante, quindi la vittima potrebbe pensare che sia solo una procedura normale per controllare se tutto è a posto. Questo rende l’attacco ancora più efficace, perché sfrutta la sensazione di urgenza e la paura che qualcosa non vada.

**PROGETTO S5/L5 PEDRANA YURI 10/01/2025**

## Spiegazione nei singoli elementi:

**Oggetto:** Attenzione: Acceso non autorizzato al tuo account PayPal

Come si può notare, il primo campanello d'allarme risiede nell'uso della parola "Acceso";

**Mittente:** supporto@paypal.com

PayPal non invia mai email da indirizzi di supporto come "supporto@paypal.com" o simili. I messaggi ufficiali provenienti da PayPal sono generalmente inviati da indirizzi come:

**service@paypal.com** o **no-reply@paypal.com**.

**Testo del messaggio:**

Abbiamo notato un acceso non autorizzato al tuo account PayPal da un dispositivo sconosciuto. Per protegere la tua sicurrezza, abbiamo temporaneamente limitato alcune funzionalità del tuo account.

Ti invitiamo a verifcare immediatamente le tue informazioni accedendo al tuo account tramite il link sottoindicato

Se non completi la verfica entro 48 ore, il tuo account potrebbe essere sospeso.

L'inizio del messaggio può sembrare veritiero, ma subito dopo notiamo alcuni errori nelle parole, come: "protegere", "sicurrezza", "verifcare", "verfica". Questi errori sono un chiaro segnale di tentativo di phishing.

**Saluti:** iI team di sicurezza PayPal

Nella seconda frase, "il team di sicurezza PayPal", quasi impercettibile, al posto della "L" in "il" c'è una "i" maiuscola