

Esercizio del Giorno: Simulazione di un'Email di Phishing

1. Scenario Creato

Per questa simulazione, ho scelto di creare un'email di phishing che imita una comunicazione ufficiale di **PayPal**, uno dei servizi di pagamento più utilizzati al mondo. L'obiettivo dell'attacco di phishing è **rubare le credenziali di accesso** dell'utente (email e password) convincendolo a cliccare su un link fraudolento che lo porta su un sito web che replica quello ufficiale di PayPal.

Questa tipologia di phishing è molto diffusa perché sfrutta il timore degli utenti di perdere l'accesso al proprio conto e quindi di subire danni economici diretti.

2. Email di Phishing Creata

Oggetto:

⚠ Attività sospetta rilevata sul tuo account PayPal

Da:

security@paypalsecure-alert.com

Gentile cliente PayPal,

Abbiamo rilevato un tentativo di accesso non autorizzato al tuo account da un dispositivo sconosciuto situato in **Roma, Italia**.

Per proteggere la tua sicurezza, il tuo account è stato **temporaneamente bloccato**.

Ti preghiamo di **verificare immediatamente** la tua identità per evitare la chiusura definitiva del tuo account.

👉 **Clicca qui per verificare il tuo account** 👉

La verifica deve essere completata **entro 24 ore**, altrimenti il tuo account sarà **sospeso definitivamente**.

Se non completi la verifica entro i tempi richiesti, non potrai più effettuare pagamenti o ricevere denaro.

Grazie per la tua collaborazione.

Cordiali saluti,
Il team di sicurezza PayPal

Questa è un'email automatica. Non rispondere a questo messaggio.

3. Spiegazione dello Scenario

Perché l'email può sembrare credibile:

- Simula un servizio molto conosciuto come PayPal.
- Il messaggio comunica un problema di **sicurezza**, creando allarme nell'utente.
- L'email utilizza un linguaggio formale e include elementi visivi simili a quelli di comunicazioni ufficiali.
- Il link inserito **sembra** a prima vista legittimo, ma in realtà porta a un sito malevolo.

Elementi sospetti che indicano phishing:

- **Indirizzo email falso:** il dominio @paypalsecure-alert.com non è quello ufficiale (@paypal.com).
 - **Link sospetto:** il dominio paypalsecure-checkup.com non appartiene a PayPal.
 - **Tono allarmistico:** la minaccia di sospensione definitiva in 24 ore è tipica degli attacchi phishing.
 - **Richiesta di cliccare su un link:** le vere aziende raccomandano di accedere direttamente dal sito ufficiale e non forzano gli utenti a cliccare da un'email.
 - **Piccoli errori di formulazione:** l'uso di espressioni come «verifica immediatamente la tua identità» può risultare anomalo rispetto allo stile comunicativo di PayPal.
-

4. Conclusione

Questa simulazione mostra come un'email di phishing possa risultare **credibile** e allo stesso tempo contenga segnali chiari che, se riconosciuti, possono aiutare a proteggersi da truffe. È importante educare gli utenti a controllare sempre l'indirizzo del mittente, i link e il tono del

messaggio, evitando di cliccare su link sospetti e accedendo sempre manualmente ai servizi online tramite il sito ufficiale.