Esercizio: Creazione di un email di phishing

Nell'esercizio di oggi andremo a vedere come creare un email di phishing per appropiarci di dati sensibili di un utente target.

Il **phishing** è un tipo di truffa online in cui un malintenzionato cerca di ingannare le vittime per ottenere informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in comunicazioni digitali. Nel nostro caso, andremo a fingere di essere la compagnia **Paypal,** andando ad allarmare l'utente sulla sicurezza del suo account.

1.Descrizione dettagliata dello scenario

Immagina un utente medio che utilizza PayPal per fare acquisti online. Questo utente potrebbe ricevere un'email all'apparenza legittima che sembra provenire proprio da PayPal.

Il messaggio comunica che c'è stato un tentativo di accesso sospetto al conto da un dispositivo non riconosciuto e che il conto è stato temporaneamente bloccato per sicurezza. L'email invita l'utente a cliccare su un link per "verificare la propria identità" e sbloccare l'account.

Obiettivo dell'attacco:
Indurre l'utente a cliccare su un link malevolo e inserire **le proprie credenziali PayPal** su un sito di **phishing** (una copia visivamente identica al sito ufficiale). Queste credenziali vengono poi rubate dagli attaccanti, che possono usarle per sottrarre fondi, fare acquisti fraudolenti o vendere l'accesso ad altri criminali.

2. Email di Phishing

Andiamo a chiedere a ChatGPT di creare l'email esca, dandogli il contesto per essere più efficiente possibile.

Ecco l'email incriminate:

Da: servizio-clienti@notifiche-paypol.com

Oggetto: ⚠ Azione richiesta: Accesso sospetto rilevato sul tuo conto PayPol

Gentile Cliente,

Noi abbiamo rilevato tentativo di accesso al tuo conto da luogo non familiare.

Per evitare la perdita, il sistema ha effettuato il blocco temporaneo del conto.

👉 Clicca qui per confermare la tua identità e riattivare il tuo conto:

https://secure-paypol.it-verifica.com

Se non completi la verifica entro 24 ore, il tuo conto sarà sospeso per motivi di sicurezza. Questa azione è richiesta per sicurezza totale del tuo account e protezione fondi.

Grazie per la tua collaborazione.

Servizio Clienti PayPol

Il link fornito nell'email, rimanderà ad un sito clone generato da noi tramite SET **(Social Engineering Toolkit).** La vittima, pensando che il sito sia autentico, inserirà il suo username e la sua password. Noi potremo vedere le credenziali inserite e rubare i dati.

---

3. Analisi dello scenario

Perché l'email potrebbe sembrare credibile:

1. **Brand conosciuto**
   PayPal è un'azienda molto diffusa e affidabile, quindi in termini percentuali, la metà degli utenti alla quale questa email arriverà,

avrà un conto PayPal. Inoltre ricevere comunicazioni da loro è plausibile, soprattutto per chi ha effettivamente un conto.

2. **Contesto realistico**
   L'idea di un accesso non autorizzato da una località diversa induce preoccupazione. È un tipo di notifica che **realmente PayPal potrebbe inviare**.
3. **Grafica e linguaggio coerente**
   Anche se il testo è semplice, lo stile ricorda quello delle email automatiche. Non ci sono frasi esagerate o evidentemente assurde.
4. **Pressione temporale**
   Dare un tempo limite ("entro 24 ore") genera **urgenza** e riduce la capacità critica dell'utente: è una pressione psicologica classica del phishing.

Elementi che indicano un potenziale phishing

1. **Dominio sospetto nel link e nel mittente**
   - Il link non è **paypol.com** ma **secure-paypol.it-verifica.com**, un dominio ingannevole.
   - L'indirizzo email @notifiche-paypal.com è simile, ma **non è un dominio ufficiale**.
2. **Link testuale mascherato**
   Anche se il testo dice "Verifica la tua identità", l'**URL porta a un sito non ufficiale**.
3. **Mancanza di personalizzazione**
   Viene usata la formula generica "Gentile Cliente", ma PayPal **utilizza sempre il nome e cognome reale** dell'intestatario.
4. **Grammatica leggermente sospetta**
   L'italiano è corretto ma leggermente **"meccanico"**. Questo perchè molte email di phishing sono tradotte automaticamente. Inoltre il nome dell'azienda indicato nell'email è **"Paypol"**.

5. **Nessuna possibilità di contatto reale**
   L'email non offre canali alternativi per contattare il supporto (es. numero verde, app ufficiale), e vieta esplicitamente di rispondere.

Conclusione

Questo esempio è efficace perché **mima una situazione reale**, usa **tecniche di pressione psicologica** e ha un'apparenza credibile. Tuttavia, un occhio esperto può **identificare gli elementi anomali** e riconoscere il tentativo di truffa. Inoltre, per evitare di essere "presi all'amo" è quello di implementare tecnologie di autenticazione email

- **SPF**: Che riesce ad identificare gli indirizzi IP autorizzati a inviare email dal dominio emittente.
- **DKIM**: Che riconosce **la chiave pubblica associata alla firma digitale** della mail del mittente.
- **DMARC**: Che specifica la politica di gestione delle email che falliscono l'autentificazione **SPF** e **DKIM**