Phishing

Obiettivo: Creare una simulazione di un'email di phishing utilizzando ChatGPT.

1. Creazione dello scenario

   Lo scenario che ho pensato è la ricezione da parte di un utente PayPal, che riceve una mail dal servizio clienti in cui viene notificata una finta transazione di alto livello da parte dell'utente. L'obiettivo del phishing è ottenere le credenziali d'accesso dell'utente a scopo malizioso.

2. Scrittura dell'email

   Per la scrittura di una mail di phishing più accurata possibile si devono mettere in conto alcuni parametri:

   - Urgenza: creare un senso di urgenza, spingendo l'utente ad agire rapidamente, ad esempio un avviso che comunica la chiusura dell'account
   - Link sospetti: link che il mittente invita a cliccare. Responsabile, la maggior parte delle volte, del furto di credenziali
   - Informazioni del mittente falsificate: spesso sembrano provenire da fonti legittime, imitando l'aspetto e il tono delle comunicazioni ufficiali.
     Esempio:
     mittente originale = service@paypal.com
     mittente falsificato = servizio-paypal@support0-0nline.com
   - Errori grammaticali e ortografici: molte email di phishing contengono errori nella loro stesura

3. Email

   L'email che appare all'utente è questa:

Oggetto: Avviso di Sicurezza Importante: Transazione non Autorizzata

Mittente: PayPal *servizio-paypal@support0-0nline.com*

Gentile Cliente,
Abbiamo rilevato un'attività insolita sul tuo conto PayPal, relativa a una transazione effettuata il 1/08/2025 per un importo pari a € 3799,99 presso www.amazon.com .

Ti invitiamo a verificare immediatamente l'attività recente accedendo al tuo conto tramite il nostro sito:

👉 Clicca qui per verificare il tuo conto

Teniamo a precisare che, se non si agisce entro 12 ore dalla ricezione di questo messaggio l'account verrà sospeso per motivi di sicurezza

Grazie per l'attenzione La nostra squadra resta a disposizione per ulteriori chiarimenti

Cordiali saluti,
Il Team PayPal
www.paypal.com

4. Spiegazione

Questa mail ha le carte in regola per essere classificata email di phishing, partendo dal mittente che usa un dominio falso che, ad occhi inesperti, può sembrare autentico, e dall'oggetto che dà senso di allarme. Successivamente notiamo che l'email inizia con "Gentile Cliente", non c'è un nome personale, l'azienda PayPal nelle comunicazioni utilizza il nome del cliente.
Poi troviamo la finta transazione su un sito comunemente usato per rendere il tutto più credibile.
In seguito, abbiamo il link malevolo che viene nascosto nella scritta "Clicca qui per verificare il tuo conto", Il link che appare cliccando la scritta è:

L'utente viene portato a questo link malevolo cliccando anche sul link www.paypal.com che trova in fondo alla mail.
Come possiamo vedere il link non è legittimo e non è HTTPS, quindi una volta inserite le credenziali, chi controlla il sito può vederle in chiaro. Tengo a specificare che un sito può avere HTTPS ed essere comunque non autentico.
Sotto il link troviamo la frase "*Teniamo a precisare che, se non si agisce entro 12 ore dalla ricezione di questo messaggio l'account verrà sospeso per motivi di sicurezza*" che ha come obiettivo quello di trasmettere un senso di urgenza facendo vera e propria pressione psicologica, portando la vittima a cliccare sul link e a inserire le credenziali il prima possibile.
Per concludere ci sono anche degli errori grammaticali come la mancanza di punteggiatura.

Conclusione

La simulazione dell’email di phishing evidenzia che la consapevolezza e il riconoscimento di questi segnali sono fondamentali per riconoscere ed evitare tentativi di phishing proteggendo i propri dati sensibili.