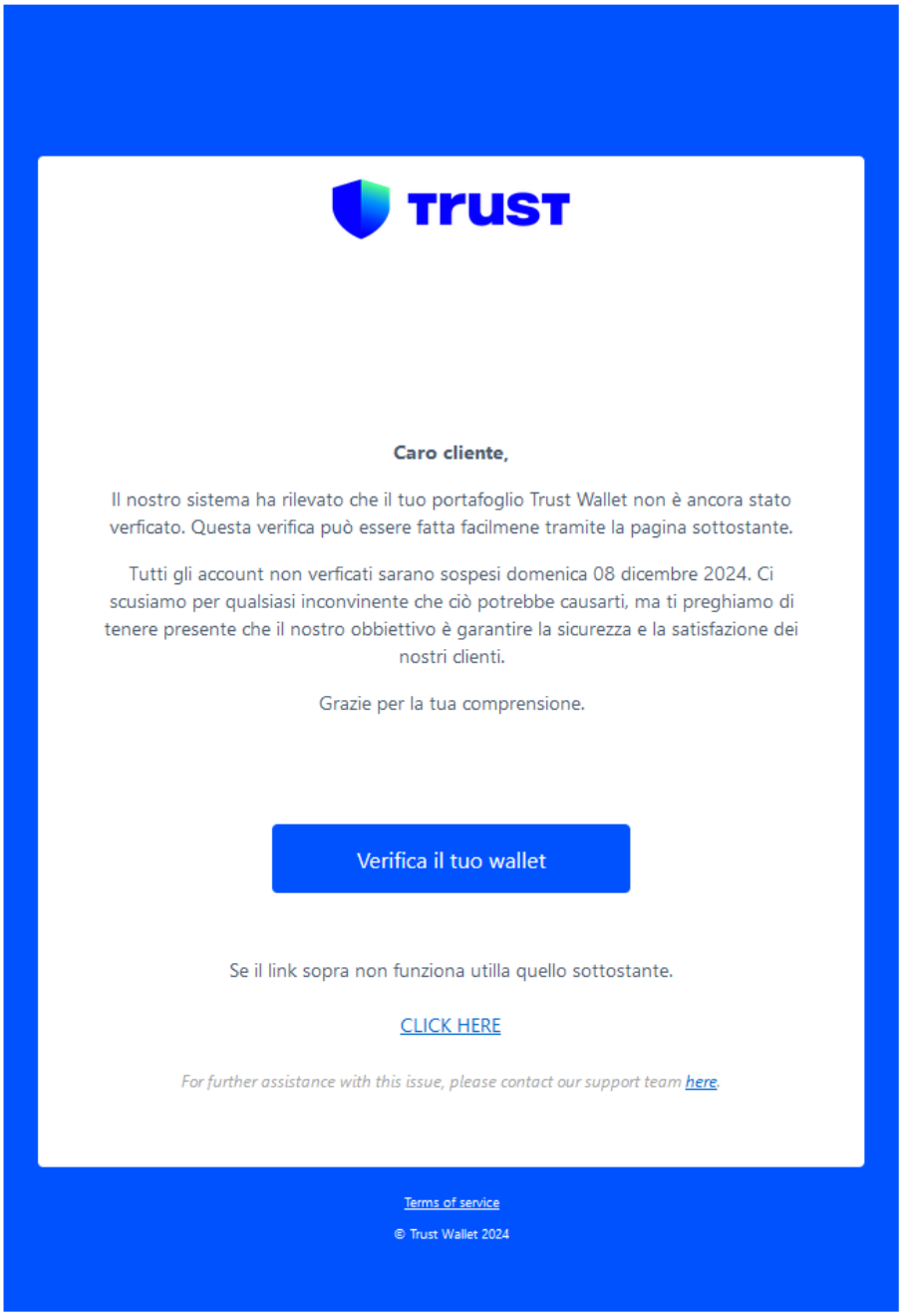
Progetto S5L5

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

Contesto realistico: Un utente ha recentemente creato un wallet con Trust Wallet o su un servizio simile di criptovalute. Dopo aver iniziato a utilizzare il servizio per gestire criptovalute, riceve una notifica via email che sembra provenire dall'assistenza ufficiale del portafoglio. La notifica afferma che il suo portafoglio deve essere verificato per continuare a funzionare correttamente e che, se non viene completata la verifica entro una certa data, l'account verrà sospeso.

Obiettivo del phishing: L'obiettivo principale dell'email di phishing è **rubare le credenziali dell'utente** (ad esempio, nome utente, password e codici di accesso) o raccogliere **dati sensibili** (come numeri di carte di credito, chiavi private o dettagli di portafogli di criptovalute). I truffatori cercano di ottenere l'accesso al portafoglio o alle informazioni finanziarie dell'utente attraverso un sito web fasullo che replica quello ufficiale di Trust Wallet. Una volta che l'utente inserisce le sue informazioni, queste vengono inviate ai truffatori.

Object: Verifica del wallet
From: Trust<no-reply@trustportafogllo.com>



L'email è progettata per sembrare una comunicazione ufficiale, con l'intento di indurre l'utente a cliccare sul link e fornire informazioni sensibili come credenziali di accesso, chiavi private o altre informazioni legate al suo portafoglio.

Perché l'email potrebbe sembrare credibile alla vittima:

1. Nome e logo riconoscibili: L'email sembra provenire da Trust Wallet, un portafoglio di criptovalute ben noto. Il logo del servizio è presente, il che rende il messaggio visivamente familiare e aumenta la sensazione di legittimità.
2. Urgency e minaccia di sospensione: La minaccia di sospendere l'account entro una data precisa (08 dicembre 2024) crea un senso di urgenza, spingendo la vittima a reagire rapidamente senza pensarci troppo, per paura di perdere l'accesso al suo portafoglio.
3. Tono formale e rassicurante: L'email adotta un linguaggio professionale, con frasi come "Ci scusiamo per qualsiasi inconveniente" e "grazie per la tua comprensione", che potrebbero sembrare un tentativo genuino di supporto da parte di un'azienda ufficiale.
4. Chiarezza nell'azione da compiere: L'email indica in modo molto chiaro cosa fare: cliccare sul link per completare la verifica dell'account. La semplicità dell'istruzione aumenta la probabilità che l'utente compia l'azione richiesta senza riflettere troppo.

Elementi che dovrebbero far scattare un campanello d'allarme:

1. Link sospetto: controlla l'URL, anche se il link sembra indirizzare alla pagina di verifica, l'URL non corrisponde al sito ufficiale di Trust Wallet. L'email contiene un link che porta a un dominio esterno (ad esempio, "https://www.tihofregato.com/"), che non ha alcuna connessione con Trust Wallet. Questo è un segnale evidente di phishing, poiché i servizi legittimi non inviano mai link a domini sconosciuti o non ufficiali.
2. Errori grammaticali e di ortografia: Parole come "inconvinente" invece di "inconveniente" e "satisfazione" al posto di "soddisfazione" sono segnali chiari che l'email potrebbe non provenire da una fonte ufficiale. Aziende come Trust Wallet di solito curano molto la qualità della loro comunicazione, evitando errori di questo tipo.
3. Mancanza di personalizzazione: L'email si apre con un generico "Caro cliente", invece di utilizzare il nome dell'utente o altri dettagli personalizzati. Le comunicazioni ufficiali da parte di servizi legittimi, di solito, sono personalizzate almeno con il nome dell'utente o il numero di account.
4. Richiesta di azione immediata: La scadenza ravvicinata (08 dicembre 2024) e la minaccia di sospensione dell'account sono tattiche comuni nel phishing per creare una pressione psicologica che spinga l'utente a prendere decisioni rapide, senza riflettere sull'autenticità del messaggio.
5. Email del Mittente Sospetta: L'indirizzo email del mittente, no-reply@trustportafogllo.com, non è ufficiale. Un dominio come "trustportafogllo.com" è sospetto e potrebbe essere una variante volutamente simile al dominio ufficiale di Trust Wallet (ad esempio, "trustwallet.com"). I truffatori spesso usano domini che somigliano a quelli legittimi ma con piccole modifiche per ingannare l'utente. I servizi ufficiali, come Trust Wallet, inviano email da indirizzi di posta elettronica ufficiali, facilmente riconoscibili e verificabili. Un indirizzo "no-reply" che non corrisponde al dominio ufficiale è un chiaro segno di allarme.

Extra

Una honeypot è un sistema o una risorsa progettata per sembrare vulnerabile e attraente per gli attaccanti, ma che in realtà serve a monitorare, rilevare e analizzare gli attacchi informatici. Viene utilizzata per studiare il comportamento degli hacker, raccogliere informazioni sulle loro tecniche e prevenire minacce reali.

Tipi di Honeypot

1. Bassa Interazione (Low-Interaction Honeypots)
   Questi honeypot emulano solo alcune funzionalità di un sistema vulnerabile, senza l'esecuzione completa di un ambiente operativo. Sono progettati per attirare e monitorare attività di base, come scansioni di porte o tentativi di exploit noti.

2. Alta Interazione (High-Interaction Honeypots)
   Simulano un sistema completo con vari servizi e applicazioni reali. Questi honeypot consentono agli attaccanti di interagire liberamente con il sistema, fornendo informazioni più dettagliate sulle tecniche utilizzate durante un attacco.

3. Honeynets
   Una rete di honeypot che simula un intero ambiente di rete, inclusi più sistemi e dispositivi. Le honeynets offrono una panoramica dettagliata di un'infrastruttura di rete simulata.

4. Honeypot ad Alte Prestazioni (High-Performance Honeypots)
   Questi honeypot sono progettati per attrarre attacchi su larga scala, come quelli su sistemi distribuiti o server web ad alta capacità. Si concentrano sull'emulazione di sistemi complessi in grado di gestire grandi volumi di traffico e interazioni.

5. Honeypot per Malware (Malware Honeypots)
   Questi honeypot sono specializzati nel raccogliere e analizzare malware. Emulano vulnerabilità specifiche, come quelle dei server FTP o dei servizi HTTP, per attirare i malware e monitorarne l'attività.

6. Honeypot per IoT (IoT Honeypots)
   Si tratta di honeypot progettati per emulare dispositivi Internet of Things (IoT) vulnerabili, come telecamere di sorveglianza, router, o termostati. Questi dispositivi sono spesso bersagli di attacchi a causa della loro bassa sicurezza.

7. Honeypot di Sensori (Sensor Honeypots)
   Questi honeypot sono installati su sensori di rete o sistemi di monitoraggio, e sono progettati per rilevare attacchi di scansione o attività sospette come scansioni di rete o tentativi di accesso.

8. Honeypot per Applicazioni Web (Web Application Honeypots)
   Emulano vulnerabilità tipiche delle applicazioni web, come quelle nei server Apache, nei database SQL, o nelle applicazioni PHP, per raccogliere informazioni su attacchi come SQL injection o cross-site scripting (XSS).

9. Honeypot per Sistemi Operativi (Operating System Honeypots)
   Questi honeypot emulano interi sistemi operativi, come Linux o Windows, per attrarre attacchi mirati a vulnerabilità specifiche dei sistemi.

Vantaggi dell'Uso delle Honeypot in una Rete Aziendale

Rilevamento precoce delle minacce: Permettono di scoprire attacchi prima che raggiungano i sistemi reali.
Analisi degli attaccanti: Consentono di raccogliere dati sulle tecniche, gli strumenti e gli obiettivi degli hacker.
Miglioramento della sicurezza: Aiutano a identificare vulnerabilità non ancora note nei sistemi aziendali.

Rischi e Limitazioni

Rischi di sicurezza: Se non configurate correttamente, possono diventare un punto di accesso per gli attaccanti.
Gestione complessa: Le honeypot richiedono monitoraggio continuo per evitare che diventino un rischio per la rete.
Falsi positivi: Potrebbero generare un numero elevato di avvisi che richiedono tempo per essere analizzati.

Esempi di Strumenti Honeypot

1. Honeyd
   Crea e simula honeypot virtuali con diverse configurazioni di sistemi operativi e servizi.
   È un buon strumento per simulare ambienti complessi e analizzare attività sospette.
   Può essere utilizzato per monitorare traffico di rete sospetto e identificare attacchi basati su vulnerabilità conosciute.
2. Dionaea
   Honeypot per il rilevamento di malware e attacchi di exploit.
   Cattura malware reali e informazioni sui metodi di attacco utilizzati dagli hacker.
   Ottimo per raccogliere dati su exploit e malware che cercano di infettare sistemi vulnerabili.
3. Kippo
   Honeypot SSH progettato per simulare un server vulnerabile ad attacchi di brute force.
   Permette di monitorare e analizzare attacchi di password cracking su SSH.
   Usato per raccogliere informazioni su tentativi di accesso non autorizzato tramite SSH e migliorare la protezione delle credenziali.