PROGETTO SETTIMANALE S5/L5

TRACCIA:

Creare uno scenario: Pensate a un contesto realistico in cui un'e-mail di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'e-mail 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.).

Scrivere l'e-mail di phishing: Utilizzate ChatGPT per generare il contenuto dell'e-mail. Assicuratevi che l'e-mail sia convincente, ma anche che contenga gli elementi tipici delle e-mail di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

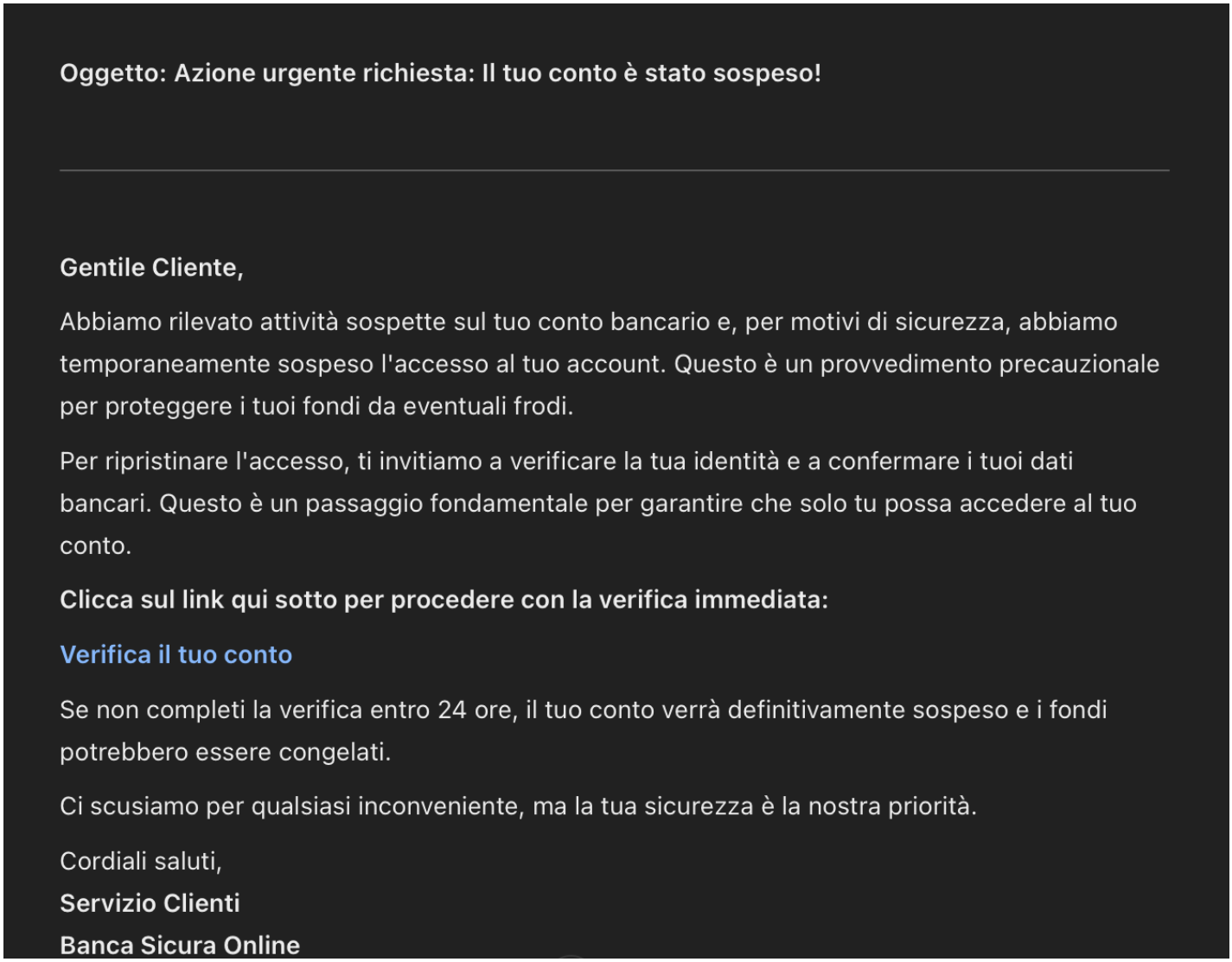
Spiegare lo scenario: Descrivete lo scenario che avete creato. Spiegate perché l'e-mail potrebbe sembrare credibile alla vittima. Evidenziate gli elementi dell'e-mail che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

SCENARIO:

Una banca online invia una notifica urgente a un cliente, informandolo di un presunto problema con il suo conto bancario. L'email utilizza un linguaggio che crea un senso di urgenza e paura, spingendo la vittima a cliccare su un link per risolvere il problema prima che l'account venga sospeso.

Obiettivo del phishing: L'obiettivo principale è ottenere le credenziali di accesso del cliente, che vengono poi utilizzate per accedere al suo conto bancario online.

Di seguito la mail di Phishing generata con Chat Gpt:



Oggetto: Azione urgente richiesta: Il tuo conto è stato sospeso!

Gentile Cliente,

Abbiamo rilevato attività sospette sul tuo conto bancario e, per motivi di sicurezza, abbiamo temporaneamente sospeso l'accesso al tuo account. Questo è un provvedimento precauzionale per proteggere i tuoi fondi da eventuali frodi.

Per ripristinare l'accesso, ti invitiamo a verificare la tua identità e a confermare i tuoi dati bancari. Questo è un passaggio fondamentale per garantire che solo tu possa accedere al tuo conto.

Clicca sul link qui sotto per procedere con la verifica immediata:

Verifica il tuo conto

Se non completi la verifica entro 24 ore, il tuo conto verrà definitivamente sospeso e i fondi potrebbero essere congelati.

Ci scusiamo per qualsiasi inconveniente, ma la tua sicurezza è la nostra priorità.

Cordiali saluti,
Servizio Clienti
Banca Sicura Online

SPIEGAZIONE DELLO SCENARIO:

Credibilità dell'e-mail:
L'email cerca di apparire autentica utilizzando il nome di una banca comune e creando un senso di urgenza. Le banche spesso inviano notifiche riguardanti attività sospette sui conti; quindi, la vittima poco attenta potrebbe pensare che sia un'e-mail legittima. Inoltre, la minaccia di sospendere l'account aumenta il panico e la probabilità che l'utente agisca rapidamente senza fermarsi a riflettere.

Elementi di phishing:

Link sospetto: Il link contenuto nell'email non rimanda a un dominio ufficiale della banca, ma a un sito web che somiglia vagamente a quello legittimo (per esempio, "banca-sicura.com" invece di un dominio con ".it" o ".com" riconosciuto). Questo è un chiaro segnale di phishing.

Richiesta urgente e minacciosa: La minaccia di sospensione immediata del conto e il termine "immediato" crea un senso di urgenza che spinge l'utente a cliccare senza pensarci due volte.

Grammatica e formato: Anche se il testo appare ben scritto, l'e-mail potrebbe presentare qualche piccola incongruenza che può sembrare sospetta, come l'uso di "Banca Sicura Online" senza il nome esatto della banca, o l'assenza di un numero di telefono per contattare il servizio clienti.

Richiesta di informazioni sensibili: L'e-mail non richiede esplicitamente la password o i dati bancari nell'email stessa, ma il link porta a una pagina di phishing in cui vengono richieste queste informazioni una volta che l'utente clicca.

PERCHE’ L’E-MAIL POTREBBE SEMBRARE CREDIBILE:

Aspetto ufficiale: L'email appare professionale e il nome del servizio clienti è realistico. L'utente potrebbe non fare caso al dominio sospetto del link.

Minaccia di azione immediata: La pressione è uno degli strumenti più potenti per spingere le persone a compiere azioni affrettate, come cliccare su link o fornire informazioni sensibili.

Appello all'autorità: L'email si presenta come se provenisse da un'entità di fiducia (una banca), quindi le persone potrebbero non dubitare della sua legittimità.

ELEMENTI SOSPETTI CHE POTREBBERO FAR SCATTARE UN CAMPANELLO D’ALLARME:

Verifica del dominio e dell'URL: Controllare sempre l'indirizzo del link. Un dominio che non corrisponde esattamente a quello ufficiale della banca è un segnale di avvertimento (ad esempio, "banca-sicura.com" invece di "banca-sicura.it").

Richiesta di azione urgente: Nessuna banca legittima invia richieste di verifica tramite e-mail minacciando la sospensione immediata di un conto. In caso di dubbi, è sempre meglio chiamare direttamente la banca.

Errore grammaticale o di formattazione: Anche se l’e-mail sembra scritta bene, piccole discrepanze nel linguaggio o nel formato (ad esempio, "Servizio Clienti" senza il nome esatto della banca) possono essere segnali di una comunicazione fraudolenta.

Mancanza di contatti diretti: Le vere banche offrono sempre metodi sicuri di contatto, come numeri di telefono ufficiali, per risolvere problemi. Un'email che non fornisce questi dettagli è sospetta.

Conclusione

L'email di phishing creata è un esempio tipico di come i truffatori possano sfruttare la paura e l'urgenza per spingere le vittime a rivelare informazioni personali sensibili. Essere consapevoli di questi segnali di avvertimento può aiutare a prevenire le truffe e proteggere la propria sicurezza online.