

Progetto S5L5



Progetto di ricerca: **Creazione email di phishing**

Corso: **Cyber Security**

Data: **03/11/2024**

Punti Salienti

CREARE UNO SCENARIO

Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.

○ Definire chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).

1. Scrivere l'email di phishing:

○ Utilizzate ChatGPT per generare il contenuto dell'email.

○ Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

2. Spiegare lo scenario:

○ Descrivete lo scenario che avete creato.

○ Spiegate perché l'email potrebbe sembrare credibile alla vittima.

○ Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

CONTESTO E OBIETTIVO

Un cliente riceve un'email apparentemente proveniente dalla sua banca, con oggetto: "Importante: Tentativo di pagamento non riuscito sul Suo conto corrente."

&

Obiettivo del phishing:

L'obiettivo è ottenere le credenziali di accesso del cliente al servizio di online banking.

(dato in "pasto" a Chatgpt")

Scenario: Finto avviso di pagamento non riuscito da una banca

Contesto:

Un cliente riceve un'email apparentemente proveniente dalla sua banca, con oggetto: "Importante: Tentativo di pagamento non riuscito sul Suo conto corrente."

Obiettivo del phishing:

L'obiettivo è ottenere le credenziali di accesso del cliente al servizio di online banking.

Email di phishing:

Oggetto: Importante: Tentativo di pagamento non riuscito sul Suo conto corrente

Mittente: notifiche@bancaxyz.com

Corpo dell'email:

Gentile Cliente,

Abbiamo rilevato un tentativo di pagamento non riuscito dal Suo conto corrente per l'importo di €150,00. Questo può essere dovuto a una mancata autorizzazione o a un problema tecnico temporaneo.

Per completare il pagamento, La preghiamo di accedere al Suo account e verificare i dettagli del pagamento. Clicchi sul link qui sotto per accedere:

[ACCEDI AL TUO ACCOUNT](#)

Ignorare questo messaggio potrebbe comportare la sospensione temporanea del Suo conto per motivi di sicurezza.

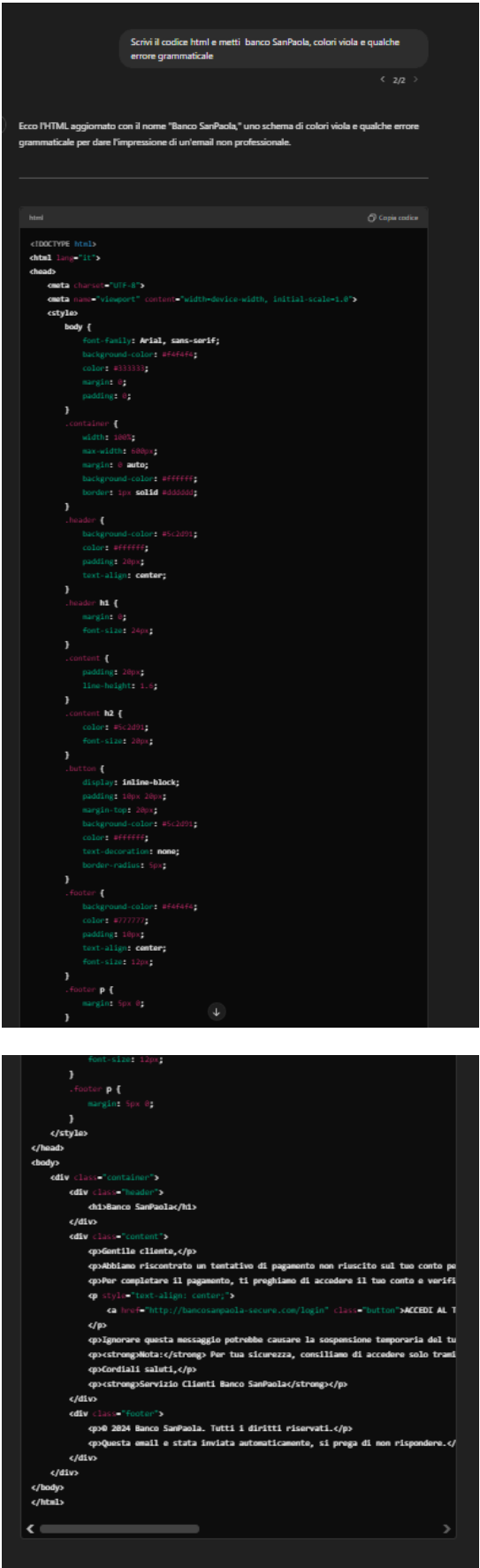
Nota: Per garantire la Sua sicurezza, consigliamo di accedere esclusivamente tramite il link indicato e completare la verifica entro 24 ore.

Cordiali saluti,

Servizio Clienti Banco XYZ



Questa è la risposta di ChatGpt e ho proceduto a chiederle il codice in HTML



RISULTATO EMAIL HTML

Epicode

Html>Email

Banco SanPaola

Gentile cliente,

Abbiamo riscontrato un tentativo di pagamento non riuscito sul tuo conto per l'importo di €150,00. Questo può essere dovuto ad un mancata autorizzazione o a un problema tecnico temporaneo.

Per completare il pagamento, ti preghiamo di accedere al tuo conto e verificare i dettagli del pagamento.

ACCEDI AL TUO ACCOUNT

ignorare questo messaggio

Go to link: <http://bancosanpaola-secure.com/login> | Change | Rem

RELAZIONE

Questa email è stata progettata per apparire come una comunicazione legittima di un'istituzione finanziaria (Banco SanPaola). Il destinatario viene avvisato di un tentativo di pagamento non riuscito sul proprio conto e invitato a cliccare su un link per verificare i dettagli del pagamento; questo simulando l'accesso al sito della banca. L'intero tono del messaggio è urgente, e cerca di rassicurare il lettore sulla sicurezza, caratteristiche tipiche delle comunicazioni delle istituzioni finanziarie. Tuttavia, è importante notare che l'urgenza può essere una strategia manipolativa, perché spesso i truffatori sfruttano questa tecnica per indurre paura e spingere le persone a reagire rapidamente.

Esistono molteplici motivi per cui questa email può apparire credibile. In primo luogo, utilizza il nome di una banca che potrebbe sembrare familiare al destinatario. I colori viola scuro e il layout professionale contribuiscono a conferire un'impressione di autenticità, mentre la struttura dell'email è ben curata e assomiglia a quelle impiegate da vere banche. Inoltre, il messaggio genera un senso di urgenza e spinge il lettore a completare la verifica entro 24 ore, il che potrebbe indurlo a cliccare sul link senza riflettere adeguatamente. Sebbene il linguaggio usato sia formale e rassicurante, con

espressioni come "Gentile cliente" e "Servizio Clienti Banco SanPaola", questo può mettere a proprio agio chi legge e possono essere utilizzati per scopi poco etici.

Tuttavia ci sono dei segnali d'allerta ancora più evidenti. L'email presenta errori grammaticali e di battitura, come "ad un mancata autorizzazzione" e "Questa email e stata inviata automaticamente," indicatori tipici di messaggi non professionali. Inoltre, il link fornito (<http://bancosanpaola-secure.com/login>) non corrisponde al dominio ufficiale della banca; questo rappresenta un chiaro segnale di allerta per chi sa riconoscere il phishing. È fondamentale ricordare che le banche legittime non chiedono mai di accedere ai propri conti tramite link ricevuti via email. Un altro aspetto allarmante è la minaccia implicita: l'email avverte che ignorare il messaggio potrebbe portare alla sospensione temporanea del conto, una tattica comune usata dai truffatori per creare pressione. Infine, l'uso di un saluto generico come "Gentile cliente," senza menzionare il nome del destinatario, riduce ulteriormente l'affidabilità del messaggio.

In sintesi, l'email di phishing in questione illustra chiaramente come sia possibile ingannare le persone, facendole sentire sicure e sotto pressione grazie a un senso di urgenza. È indispensabile che gli utenti imparino a riconoscere questi segnali d'allerta e pericolo. Soprattutto quando ricevono comunicazioni che richiedono informazioni sensibili o l'accesso ai propri conti. L'attacco punta a ottenere le credenziali dell'utente tramite phishing, reindirizzandolo a un sito controllato dall'attaccante in modo "Subdolo" e "Stealthy".