Simulazione di un'Email di Phishing: Creazione e Analisi con l'Aiuto di ChatGPT

Introduzione

Questa simulazione è stata realizzata con l'obiettivo di comprendere meglio le tecniche di phishing e i modi per riconoscere email fraudolente. L'email scelta per la simulazione riproduce una comunicazione bancaria falsa, progettata per rubare informazioni sensibili agli utenti meno attenti.

Scenario: Notifica di Sicurezza Bancaria

Contesto:
Un utente riceve un'email apparentemente dalla propria banca, che lo informa di un tentativo di accesso non autorizzato al proprio conto corrente. L'email richiede un'azione immediata per proteggere l'account, suggerendo di cliccare su un link per verificare la propria identità e garantire la sicurezza del proprio conto.

Obiettivo del phishing:
L'obiettivo dell'attaccante è spingere la vittima a cliccare sul link malevolo "Verifica Ora", che in realtà porterà a una pagina falsa progettata per rubare informazioni sensibili: username, password o dati bancari.

Testo Email di Phishing

***Oggetto**: Urgente: Tentativo di Accesso Non Autorizzato Rilevato!!*

Caro Cliente,

*Abbiamo rilevato un tentativo di accesso non autorizzato al tuo conto corrente. Per proteggere il tuo account, ti chiediamo di verificare **immediatamente** le tue credenziali.*

Clicca sul link sottostante per confermare la tua identità e garantire la sicurezza del tuo conto:
Verifica Ora

***Attenzione**: Se non agisci **entro al massimo 24 ore**, il tuo account potrebbe essere **bloccato** temporaneamente per motivi di sicurezza.*

*Grazie per la tua **collaborazione**,*
Il Team di Sicurezza di Banca FinSecure S.p.a.

Nota Importante**: Non rispondere a questa email. Per ulteriori informazioni, visita il nostro sito **ufficiale.

Spiegazione dello Scenario

Perché l'Email Potrebbe Sembrare Credibile:

1. **Tono Urgente**: L'uso di parole come "urgente" e "tentativo di accesso non autorizzato" crea un senso di emergenza, spingendo la vittima ad agire rapidamente senza riflettere.
2. **Riferimento alla Sicurezza**: Il messaggio si presenta come un avviso di sicurezza, un tema che spesso preoccupa gli utenti e li induce a fidarsi.
3. **Apparente Professionalità**: L'email sembra provenire da un team di sicurezza bancario, con un tono formale e una struttura che imita quella delle comunicazioni ufficiali.
4. **Minaccia di Sospensione**: La menzione di una possibile sospensione dell'account entro 24 ore aumenta la pressione psicologica sulla vittima.

Segnali di Allarme nell'Email:

1. **Link Sospetto**: Il testo "*Verifica Ora*" nasconde un link che potrebbe portare a un sito fraudolento. Un'email legittima di una banca di solito non chiede di cliccare su un link per verificare le credenziali.
2. **Assenza di Informazioni Specifiche**: L'email non menziona il nome del cliente né fornisce dettagli specifici sul presunto tentativo di accesso (ad esempio, data, ora o dispositivo utilizzato).
3. **Errori Grammaticali**:
   - "**Tentativo di Accesso Non Autorizzato Rilevato**"
     L'uso di maiuscole eccessivo nel titolo ("Accesso Non Autorizzato Rilevato") non è coerente con le convenzioni grammaticali italiane. Le maiuscole dovrebbero essere utilizzate solo per la prima lettera di ogni parola principale in un titolo, non per tutte le parole.
   - "**Abbiamo rilevato un tentativo di accesso non autorizzato al tuo conto corrente."**
     L'uso di "conto corrente" è corretto, ma in contesti moderni e internazionali, molte banche utilizzano il termine "account" per riferirsi al conto. L'uso esclusivo di "conto corrente" potrebbe sembrare antiquato o poco professionale in alcune comunicazioni bancarie.
   - "**Clicca sul link sottostante per confermare la tua identità e garantire la sicurezza del tuo conto**."
     La parola "conto" è scritta in modo errato. La forma corretta è "conto corrente".
   - "**Se non agisci entro al massimo 24 ore, il tuo account potrebbe essere temporaneamente sospeso per motivi di sicurezza**."
     L'uso di "account" è corretto, ma in un contesto italiano formale, molte banche preferiscono utilizzare "conto" o "conto corrente" per evitare confusioni.
     "**Se non agisci entro al massimo 24 ore"**
     Uso improprio di "al massimo": l'espressione "al massimo" è ridondante in questo contesto.
   - **"Grazie per la tua collaborazione, Il Team di Sicurezza di Banca FinSecure *S.p.a.*"**
     La virgola dopo "collaborazione" è seguita da una lettera maiuscola ("Il"), il che è grammaticalmente scorretto. Dopo una virgola, la frase dovrebbe continuare con una lettera minuscola.

- “**Nota: Non rispondere a questa email. Per ulteriori informazioni, visita il nostro sito ufficiale.**"
  La frase è grammaticalmente corretta, ma la mancanza di un link diretto al sito ufficiale o di informazioni di contatto specifiche (come un numero di telefono o un indirizzo email verificato) rende il messaggio vago e sospetto.
- **Errore di ortografia**:
  La parola "**immediatemente**" è scritta in modo errato.

4. **Richiesta di Azione Immediata**: Le email che richiedono azioni immediate, specialmente se legate alla sicurezza, sono spesso un segnale di phishing.
5. **Nota Generica**: La frase "**Non rispondere a questa email**" è vaga e non fornisce un metodo dati utilizzabili per il contatto diretto con la banca.
6. **Mancanza di Loghi Ufficiali o Firme Dettagliate**: Un'email autentica di una banca di solito include loghi ufficiali, firme dettagliate e informazioni di contatto verificabili.

Conclusione

Questa email di phishing è progettata per creare nella vittima un clima di paura che la induce ad affrettarsi nel compiere l’azione voluta dall’attaccante anche se contiene diversi elementi sospetti che dovrebbero far dubitare della sua autenticità. È fondamentale che gli utenti verifichino sempre l'autenticità di tali comunicazioni contattando direttamente la banca attraverso canali ufficiali, anziché cliccare su link o fornire informazioni sensibili.