Report sull’email di phishing simulata

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

1. Descrizione dello scenario:

Abbiamo simulato un’email apparentemente inviata dalla Banca Centrale Europea con oggetto “*ATTENZIONE: Il tuo conto è stato segnalato per transazioni fraudolente*”.

Lo scenario si basa sull’idea che l’utente riceva una comunicazione urgente che lo avvisa di transazioni fraudolente rilevate sul proprio conto bancario. L’email sfrutta l’urgenza e la paura della perdita totale dei fondi per convincere la vittima a cliccare su un link malevolo e fornire le proprie credenziali bancarie.

Il mittente è stato scelto appositamente per aggiungere credibilità, sfruttando l’autorità di un ente come la Banca Centrale Europea.

Scenario:

- **Mittente falso**: Banca Centrale Europea (alert@eu-banksecure.com)
- **Oggetto**: “*ATTENZIONE: Il tuo conto è stato segnalato per transazioni fraudolente*”
- **Contesto**: L’utente riceve un’email che lo avvisa di attività sospette e di transazioni fraudolente rilevate sul suo conto corrente. La comunicazione specifica che, per motivi di sicurezza, l’account è stato bloccato temporaneamente. Viene chiesto di verificare immediatamente il proprio conto per evitare la perdita completa dei fondi a causa di un possibile attacco hacker.
- **Obiettivo del phishing**: Indurre l’utente a cliccare su un link e accedere a un portale falso che richiede credenziali bancarie o PIN, oppure eseguire un trasferimento di denaro su un conto sicuro (in realtà controllato dagli attaccanti).

Questo scenario gioca sulla paura di perdere i risparmi, sfruttando l’urgenza e il tono autoritario di una banca centrale.

Testo dell'email:

Mittente: Banca Centrale Europea (alert@eu-banksecure.com)

Oggetto: "*ATTENZIONE: Il tuo conto è stato segnalato per transazioni fraudolente*"

Gentile [Nome Cognome],

Abbiamo rilevato una serie di transazioni insolite e non autorizzate sul tuo conto corrente, effettuate da un indirizzo IP sconosciuto. Per motivi di sicurezza, il tuo conto è stato temporaneamente sospeso al fine di prevenire ulteriori rischi.

Ti invitiamo a verificare immediatamente i tuoi dati per evitare la perdita totale dei fondi disponibili sul tuo conto corrente.

Passaggi da seguire per sbloccare il tuo conto:

1. Accedi al nostro portale di sicurezza esclusivo tramite questo link:
   Verifica e Sblocca il tuo conto
2. Effettua l'accesso utilizzando le tue credenziali bancarie.
3. Conferma la tua identità per ripristinare l'accesso completo al conto.

⚠ Avviso importante:

- Hai tempo **fino alle ore 23:59** di oggi per completare la procedura di verifica, altrimenti il conto sarà **completamente bloccato** e sarà necessaria una procedura di recupero più lunga e complessa.
- La mancata verifica potrebbe comportare **la perdita completa dei fondi**, in caso di accessi non autorizzati successivi.
- In caso di domande, puoi contattare il nostro Servizio Clienti al numero ufficiale indicato sul nostro sito web.

Ti ringraziamo per la collaborazione nel garantire la sicurezza del tuo conto.

Cordiali saluti,

Ufficio Sicurezza Bancaria

Banca Centrale Europea

www.ecb.europa.eu

2. Perché l'email potrebbe sembrare credibile alla vittima

Ci sono diversi punti per cui questa mail potrebbe sembrare credibile:

- **Uso di un tono professionale**: Il linguaggio utilizzato imita quello ufficiale, tipico delle comunicazioni bancarie, e include termini come "temporaneamente sospeso", "verifica immediata" e "ripristino dell'accesso".
- **Falsa urgenza**: Viene sottolineato che il problema deve essere risolto entro 23:59 dello stesso giorno, aumentando la pressione psicologica sulla vittima.
- **Mittente autorevole**: Il nome della Banca Centrale Europea e un indirizzo email apparentemente legittimo (alert@eu-banksecure.com) aumentano la fiducia.
- **Link camuffato**: L'URL sembra appartenere a un sito ufficiale, ma in realtà conduce a un portale fasullo (http://secure-eu-bank.com/login-verifica).
- **Menzione di una conseguenza grave**: L'idea di perdere tutti i fondi spinge la vittima ad agire senza riflettere.

3. Elementi che dovrebbero far scattare un campanello d'allarme

Altrettanti sono i punti che però dovrebbero insospettire l'utente:

- **Indirizzo email sospetto**: Anche se sembra legittimo, il dominio "eu-banksecure.com" non appartiene alla Banca Centrale Europea. I domini ufficiali sono solitamente ben noti (es. ecb.europa.eu).
- **Tono allarmistico**: Le email ufficiali raramente usano minacce dirette o imposizioni con scadenze così strette, come "entro oggi o il blocco sarà permanente".
- **Link sospetto**: Anche se sembra autentico, passando il cursore sopra il link, l'utente può notare che conduce a un dominio diverso da quello ufficiale.
- **Assenza di personalizzazione completa**: Nonostante il saluto "Gentile [Nome Cognome]", alcune email di phishing non includono ulteriori dati personali, come il numero del conto o altre informazioni verificate dalla banca.
- **Richiesta di credenziali bancarie**: Le banche e gli istituti ufficiali non richiedono mai l'inserimento di credenziali tramite email.

Conclusioni

Questa simulazione evidenzia come un'email di phishing ben costruita possa apparire credibile, sfruttando fattori psicologici come l'urgenza e la paura, nonché dettagli visivi e linguistici che simulano una comunicazione ufficiale.

L'attacco è particolarmente efficace per i seguenti motivi:

1. **Autorità del mittente**: Utilizzare un ente noto e autorevole come la Banca Centrale Europea aumenta la fiducia dell'utente, poiché difficilmente si sospetterebbe una frode proveniente da un'organizzazione di tale prestigio.
2. **Emotività e pressione temporale**: La paura di perdere tutti i fondi in breve tempo spinge la vittima ad agire d'istinto, ignorando eventuali segnali di allarme.
3. **Apparenza di legittimità**: L'uso di un linguaggio professionale, di un link apparentemente autentico e di riferimenti tecnici (ad esempio, "indirizzo IP sconosciuto") contribuisce a creare una falsa sensazione di sicurezza.

Tuttavia, è altrettanto importante sottolineare che, prestando attenzione ai dettagli, l'utente può identificare elementi sospetti che tradiscono l'autenticità dell'email. Ad esempio:

- **Un dominio web non ufficiale**, facilmente verificabile.
- **Una richiesta di informazioni sensibili** (credenziali) tramite email, che nessuna banca o ente istituzionale farebbe mai.
- **Un tono eccessivamente allarmistico** o **scadenze troppo strette**, che non sono tipiche delle comunicazioni bancarie ufficiali.

Questa esercitazione dimostra quanto sia cruciale formare gli utenti a riconoscere i segnali di phishing e verificare ogni comunicazione prima di fornire dati personali o cliccare su link non verificati. Una maggiore consapevolezza può ridurre significativamente il rischio di cadere vittima di questi attacchi.