

Simulazione E-mail Phishing

Oggetto: Urgente: Verifica la tua sicurezza del conto



Caro Cliente,

Durante un controllo di sicurezza, abbiamo rilevato attività sospette sul tuo account che potrebbero compromettere la protezione dei tuoi dati. Ti invitiamo a confermare e aggiornare le tue informazioni per evitare la disattivazione permanente.

Dettagli attività sospette:

- Data: 6 dicembre 2024
- Ora: 14:37 GMT+1
- Posizione: San Paolo, Brasile
- Indirizzo IP: 189.12.45.67

Tentativi rilevati:

- Modifica della password.
- Registrazione di un nuovo metodo di pagamento.
- Richiesta di trasferimento fondi di €450,00.

A causa di queste azioni, il tuo account è stato bloccato temporaneamente per garantire la tua sicurezza. Tuttavia, è necessario verificare la tua identità per riattivarlo e prevenire ulteriori tentativi non autorizzati.

1. Accedi al Portale Sicurezza cliccando sul seguente link sicuro:

[Verifica il tuo account](#)

2. Completa il modulo di verifica:

Dopo aver effettuato il login, ti chiederemo di fornire alcune informazioni aggiuntive per confermare la tua identità. Assicurati di inserire correttamente tutti i dettagli richiesti. Il processo richiede solo pochi minuti.

3. Controlla i tuoi dati:

- Nome completo
- Data di nascita
- Numero di telefono
- Indirizzo di fatturazione
- Dati della carta di credito per confermare la proprietà del metodo di pagamento

Questa procedura è necessaria per evitare che il tuo account venga temporaneamente sospeso. L'aggiornamento delle tue informazioni è obbligatorio entro 24 ore. Non completando questa verifica, il tuo account potrebbe essere limitato.

Supporto:

Se hai domande o necessiti assistenza, contatta il nostro supporto clienti:

- Email: bigijol267@secure-bank.com
- Telefono assistenza H24: +1 800-555-0123

Non perdere tempo, completa subito la verifica per evitare interruzioni nel servizio.

Grazie per la tua collaborazione.

Il Team di Sicurezza

Secure Bank

Avvertenza:

Ricorda che le vere banche non chiedono mai di aggiornare i dati sensibili via email. Se ricevi un messaggio del genere, non cliccare mai su link sospetti o fornire informazioni personali.

Descrizione svolgimento compito

Con l'utilizzo di Chat GPT ho creato questa mail Phishing, e ho creato anche un'interfaccia di login e un modulo per la compilazione dei dati la quale simula un'attività anomala di un account bancario e con l'eventuale abboccamento del cliente premendo il link che lo porta ad un login e successivamente ad una compilazione di dati personali un eventuale attaccante potrebbe appropriarsi di tutte queste informazioni.

L'email potrebbe sembrare veritiera, perché la mail crea un senso di urgenza, dichiarando che l'account potrebbe essere sospeso se la verifica non viene completata entro 24 ore. Questo spinge la vittima a prendere decisioni rapide senza riflettere troppo; la presenza di un link apparentemente sicuro, l'inclusione di un logo falso della banca e l'uso di elementi grafici che sembrano provenire da una banca reale aumentano l'illusione di autenticità; l'aggiunta del servizio clienti e del numero di telefono; l'utilizzo di una lingua formale e non molto complessa

Per quanto riguarda gli elementi che possono far suonare un campanello d'allarme sono: principalmente gli errori grammaticali come ad esempio

- "Attività sospetta" invece di "attività sospette" (errore nel numero del sostantivo).
- "Sicurrezza" invece di "sicurezza" (errore di ortografia).
- "Fatturazione" invece di "fatturazione" (errore di ortografia).
- "Controlla i tuoi dati" non è un errore grammaticale in sé, ma la mancanza di dettagli come "Verifica" al posto di "Controlla" potrebbe sembrare meno professionale in una comunicazione bancaria ufficiale.

Questi errori possono sembrare naturali per qualcuno che non è completamente attento, ma per una persona che è abituata a comunicazioni ufficiali potrebbero sembrare strani e sollevare dei dubbi.

Un'altro campanello potrebbe essere l'email e il numero di telefono la quale si notano non essere molto veritieri

Un ultimo campanello d'allarme è la pagina di login non molto dettagliata ad esempio con immagini o altro .



Noel Petralia <noelpetralia2244@gmail.com>

(nessun oggetto)**Amazon** <noelpetralia2244@gmail.com>
A: Noel Petralia <noelpetralia2244@gmail.com>

6 dicembre 2024 alle ore 13:18

Oggetto: Urgente: Verifica la tua sicurezza del conto

Caro Cliente,

Durante un controllo di sicurezza, abbiamo rilevato attività sospette sul tuo account che potrebbero compromettere la protezione dei tuoi dati. Ti invitiamo a confermare e aggiornare le tue informazioni per evitare la disattivazione permanente.

Dettagli attività sospette:

- Data: 6 dicembre 2024
- Ora: 14:37 GMT+1
- Posizione: San Paolo, Brasile
- Indirizzo IP: 189.12.45.67
- Tentativi rilevati:
 - Modifica della password.
 - Registrazione di un nuovo metodo di pagamento.
 - Richiesta di trasferimento fondi di €450,00.

A causa di queste azioni, il tuo account è stato bloccato temporaneamente per garantire la tua sicurezza. Tuttavia, è necessario verificare la tua identità per riattivarlo e prevenire ulteriori tentativi non autorizzati.

1. Accedi al **Portale Sicurezza** cliccando sul seguente link sicuro:

[Verifica il tuo account](#)

2. Completa il modulo di verifica: Dopo aver effettuato il login, ti chiederemo di fornire alcune informazioni aggiuntive per confermare la tua identità. Assicurati di inserire correttamente tutti i dettagli richiesti. Il processo richiede solo pochi minuti.
3. Controlla i tuoi dati:
 - Nome completo
 - Data di nascita
 - Numero di telefono
 - Indirizzo di fatturazione
 - Dati della carta di credito per confermare la proprietà del metodo di pagamento

Questa procedura è necessaria per evitare che il tuo account venga temporaneamente sospeso. L'aggiornamento delle tue informazioni è obbligatorio entro 24 ore. Non completando questa verifica, il tuo account potrebbe essere limitato.

Supporto:

Se hai domande o necessiti assistenza, contatta il nostro supporto clienti:

Email: bigijol267@secure-bank.com

Telefono assistenza H24: +1 800-555-0123

Non perdere tempo, completa subito la verifica per evitare interruzioni nel servizio.

Grazie per la tua collaborazione.

Il Team di Sicurezza

Secure Bank

Avvertenza: Ricorda che le vere banche non chiedono mai di aggiornare i dati sensibili via email. Se ricevi un messaggio del genere, non cliccare mai su link sospetti o fornire informazioni personali.

Qui ho inserito l'immagine di una mail che sono riuscito a mandarmi tramite l'ausilio di Gophis e ho provato a cliccare sul link e funziona correttamente.

