Progetto settimanale sull’ingegneria sociale

Supponiamo di ricevere una mail di phishing sulla verifica del conto bancoposta da parte di Poste Italiane:

Oggetto: Urgente: Verifica necessaria per la modifica delle impostazioni del tuo conto BancoPosta

---

Da: assistenza.clienti@bancoposta.it
A: [tuaemail@example.com]
Data: 13 Settembre 2024
Oggetto: Urgente: Verifica necessaria per la modifica delle impostazioni del tuo conto BancoPosta

---

Gentile Cliente,

A causa di recenti aggiornamenti ai nostri sistemi di sicurezza, è stata rilevata una richiesta di modifica delle impostazioni del tuo conto BancoPosta. Per garantire la tua protezione e prevenire l'uso non autorizzato del tuo account, è necessario confermare le tue informazioni entro **24 ore**.

Se non confermi la tua identità entro il termine indicato, il tuo conto sarà temporaneamente bloccato per motivi di sicurezza.

Ti invitiamo a cliccare sul link sottostante e seguire le istruzioni per completare la verifica:

Clicca qui per verificare il tuo conto BancoPosta

Una volta completata la procedura, riceverai una notifica di conferma. Se non hai richiesto modifiche al tuo account, ti invitiamo a procedere ugualmente con la verifica per proteggere il tuo conto.

Grazie per la collaborazione e per aver scelto BancoPosta.

Cordiali saluti,
Servizio Clienti BancoPosta
Numero Verde: 800-000-000
E-mail: assistenza.clienti@bancoposta.it
[www.bancoposta.it]

Nota Bene: Questa è un'email automatica. Non rispondere a questo messaggio.

Come funziona l'attacco:

1. Il destinatario viene allarmato dall'urgenza della richiesta di verifica delle informazioni.
2. Cliccando sul link, l'utente viene indirizzato a un sito di phishing che replica il sito ufficiale di BancoPosta.
3. Sul sito falso, l'utente inserisce le credenziali di accesso al proprio conto (username, password, codice OTP, ecc.), che vengono intercettate dai truffatori.

Questo tipo di attacco sfrutta il senso di urgenza e la preoccupazione per la sicurezza del conto per convincere l'utente a fornire i propri dati.

Ecco un'immagine di una mail di phishing:


Da: PostePay.it /Assistenza <info@barbellini.it>
A: <[redacted]>
Data: martedì 20 aprile 2021, 16:25 +0200
Oggetto: Il tuo account è stato sospeso per motivi di sicurezza. .

Gentile [redacted],

La sua utenza sul sito di Poste é stata temporaneamente sospesa perché non ha ancora effettuato l'aggiornamento obbligatorio del suo profilo,

come richiesto in precedenza dal nostro servizio di assistenza.

Ti ricordiamo inoltre che non avrai accesso ai servizi che forniamo finché non avrai terminato questo passaggio.

Accedi ai servizi online

NOTA

Ti ricordiamo che non potrai piu effettuare dei pagamenti con la carta se questa verifica non viene eseguita entro 48 ore dalla sua ricezione.

Spiegazione dello scenario di una Mail di Phishing BancoPosta

Il contesto della mail di phishing descritto rappresenta un tipico attacco informatico mirato a rubare le credenziali di accesso al conto BancoPosta. Ecco come si sviluppa lo scenario:

---

1. Creazione di Allarme:

Il destinatario riceve un'email che sembra provenire da **BancoPosta** o da un servizio

legato a **Poste Italiane**. Il messaggio contiene un avviso urgente: l'utente deve verificare le proprie informazioni per evitare problemi come il blocco del conto o attività sospette. Questo genera una reazione emotiva, inducendo paura e urgenza, con lo scopo di far agire rapidamente il destinatario senza riflettere.

---

2. Clic sul Link:
Spinto dal timore di perdere l'accesso al proprio conto, l'utente clicca sul link fornito nella mail. Questo link sembra legittimo, ma in realtà indirizza a un sito di phishing che replica in modo accurato il portale ufficiale di BancoPosta.

---

3. Sito di Phishing:
Il sito falso è progettato per imitare fedelmente la pagina di login di BancoPosta. Quando l'utente arriva su questo sito, non si accorge della differenza, poiché l'aspetto grafico e l'interfaccia sono molto simili a quelli originali.

---

4. Inserimento delle Credenziali:
L'utente, credendo di essere sul sito autentico, inserisce il proprio username, la password e, in molti casi, anche il **codice OTP** (One Time Password) che riceve sul cellulare. Il codice OTP è una misura di sicurezza reale che però in questo caso viene manipolata dagli attaccanti.

---

5. Intercettazione delle Informazioni:
Le credenziali inserite non vengono trasmesse al vero BancoPosta, ma direttamente ai truffatori. A questo punto, i criminali hanno accesso completo al conto del destinatario e possono effettuare operazioni finanziarie, come trasferimenti di denaro o prelievi.

---

6. Sfruttamento della Psicologia:
Questo attacco sfrutta una combinazione di **urgenza** (paura di perdere l'accesso al conto) e **fiducia** (l'apparente legittimità del sito e del messaggio) per convincere l'utente a fornire spontaneamente le proprie informazioni personali e di accesso.

In sintesi, l'attacco è progettato per sembrare urgente e necessario, inducendo l'utente a non verificare accuratamente i dettagli e a fornire informazioni sensibili senza accorgersi della truffa.

Conclusione

Come abbiamo visto gli attacchi di phishing sono all’ordine del giorno e per evitare di esserne vittima, è estremamente necessaria la continua formazione del personale, non solo per questo tipo di attacchi, ma anche per altre tecniche volte a rubare dati in modo tale da essere sempre pronti.