Consegna S5L5

Scenario Simulato di Email di Phishing da una "Banca"

Oggetto: Verifica Urgente Richiesta per il Suo Conto Bancario

Da: Servizio Clienti [noreply@bankofitalia.com]
A: [Email del Destinatario]

Gentile Cliente,

Siamo a contattarLa per informarLa di una potenziale violazione della sicurezza che potrebbe aver interessato il Suo conto presso la nostra banca. Per assicurare l'integrità delle Sue informazioni personali, è richiesta una verifica immediata.

Si prega di accedere al Suo conto tramite il seguente link per confermare le Sue informazioni personali: https://www.bank0fditalia.com/verify

La preghiamo di completare questo processo entro 24 ore per evitare la sospensione temporanea del Suo conto. Ci scusiamo per il disagio e La ringraziamo per la Sua collaborazione e comprensione.

Distinti saluti,

Servizio Clienti
Banca d'Italia
Telefono: 800-123-4567
Email: support@bankofitalia.com

Analisi della Credibilità e delle Bandiere Rosse

Credibilità:

- **Tono Formale e Professionale:** L'uso di un linguaggio formale e termini specifici del settore bancario può conferire autenticità all'email.
- **Urgenza:** La richiesta di azione immediata può spingere il destinatario a rispondere senza verificare l'autenticità dell'email.

Bandiere Rosse:

- **URL Sospetto:** Nonostante il link appaia legittimo a una lettura superficiale, l'URL presenta una piccola discrepanza nell'ortografia ("bank0fditalia" invece di "bankofitalia"). Questo è un comune trucco usato nei tentativi di phishing per ingannare le vittime.
- **Richiesta di Informazioni Sensibili:** Una banca legittima non chiederà mai di verificare informazioni sensibili attraverso un link inviato via email.

- **Urgenza Ingiustificata:** La pressione per agire rapidamente è una tattica usata per spingere le vittime a commettere errori e non verificare le informazioni.

Simulazione dell'Email di Phishing per Test di Sicurezza

Per simulare questo scenario di phishing e testare la consapevolezza della sicurezza tra gli utenti, si può utilizzare uno strumento come GoPhish. GoPhish permette di creare campagne di phishing simulate in un ambiente controllato, dove si possono inviare email simulate come quella descritta sopra per vedere come gli utenti reagiscono a tentativi di phishing.

Questo aiuta a identificare vulnerabilità nella consapevolezza degli utenti e a migliorare le formazioni sulla sicurezza informatica, proteggendo così l'organizzazione da attacchi reali.

Questo scenario evidenzia come un'email di phishing possa sembrare convincente e allo stesso tempo presentare segnali di allarme che, se riconosciuti, possono proteggere l'utente da potenziali frodi. È fondamentale esaminare attentamente le email che richiedono informazioni personali o azioni urgenti, soprattutto se contengono link a siti web.