REPORT S5/L5

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

SCENARIO E OBIETTIVO

L'email finge di provenire dal reparto di sicurezza di una banca (Revolut) e ha l'obiettivo di spingere il destinatario a cliccare su un link per inserire le proprie credenziali bancarie. Lo scenario è volutamente costruito per sembrare credibile agli occhi di un utente distratto.

L'obiettivo della mail è quello di indurre il destinatario a cliccare sul link e inserire le credenziali bancarie su un sito falso, questo permetterebbe ai malintenzionati di rubare le credenziali e potenzialmente accedere al conto della vittima.

EMAIL

Oggetto: ⚠️ URGENTE: Verifica immediata del tuo conto bancario

Mittente: suport@revolut.com

Corpo del messaggio:

Gentile Cliente,

A causa di attività sospettose rilevata sul tuo conto, è necessario che tu confermi immediatamente le tue informazioni di accesso per evitare il blocco permanente del tuo conto bancario.

Per favore, clica sul link sottostante per verificare i tuoi dati:

👉 Accedi al tuo conto ora

Nota: Se non esegui questa verifica entro 24 ore, il tuo conto sarà disattivato.

Grazie per la collaborazione,
Il Team di Sicurezza Revolut

CREDIBILITÀ DELLA MAIL

L’email potrebbe risultare credibile agli occhi di una potenziale vittima per più motivi che fanno leva su aspetti psicologici e tecnici.

- Uso del nome di un marchio conosciuto

  L'email fa riferimento a una banca che la vittima potrebbe realmente utilizzare, inoltre molte persone non verificano attentamente l'indirizzo email del mittente, quindi un dominio simile può sembrare legittimo.

- Tono urgente e minaccioso

  Frasi come "Devi agire entro 24 ore" o "Il tuo account sarà bloccato" spingono la vittima a reagire d'impulso, senza riflettere o controllare i dettagli, la paura di perdere l'accesso al conto bancario o di subire conseguenze economiche fa abbassare l’attenzione ai dettagli della vittima.

- Linguaggio formale

  il linguaggio usato potrebbe sembrare abbastanza professionale da non sollevare sospetti immediati, soprattutto per persone meno esperte, errori grammaticali leggeri possono passare inosservati soprattutto se il destinatario è distratto o sotto stress.

- Aspetto professionale

  Il messaggio potrebbe includere elementi visivi ufficiali, come il logo della banca o un formato con colori, font e struttura simili a quelli utilizzati nelle comunicazioni reali.

ELEMENTI SOSPETTI

Ci sono diversi segnali d'allarme che potrebbero aiutare una vittima a rendersi conto della falsità della mail, questi segnali riguardano il contenuto, il mittente e i link forniti.

- Mittente sospetto

  L'indirizzo del mittente può sembrare simile a quello dell'ente ufficiale ma con la presenza di piccole variazioni, come un dominio errato o aggiunte anomale, inoltre un'email legittima includerebbe un numero di telefono o altre modalità di contatto.

- Errori grammaticali e ortografici

  Errori di grammatica, ortografia, punteggiatura o un linguaggio troppo informale o artificiale rispetto a quello delle comunicazioni ufficiali potrebbero insospettire la vittima.

- URL sospetto

  Una vittima attenta, dopo una breve ricerca, potrebbe notare una discrepanza tra i domini dell'URL reale e quello della mail di phishing.

- Personalizzazione assente

  Email che iniziano con "Gentile Cliente" invece del nome completo del destinatario risultano meno credibili dato che le banche conoscono i propri clienti e includerebbe dettagli specifici sul conto, transazioni o problematiche che possano confermare la sua autenticità.

BONUS 1

Obiettivo: Creare una simulazione di un'email di phishing irriconoscibile