Progetto settimanale - Phishing

Contesto: Servizi di streaming o abbonamenti (es. Netflix, Spotify)

Il contesto pensato è quello di un'e-mail da parte di un servizio in abbonamento (Netflix) che avvisa che il pagamento per il rinnovo automatico del servizio non è andato a buon fine e invita la vittima a reinserire i dati della sua carta. Tale contesto è stato pensato per rubare dati finanziari e fa leva, sia sulla popolarità di Netflix per colpire un grande quantitativo di persone , ché sull'urgenza di rinnovo dettata dalla dipendenza da serie tv da cui è afflitta la nostra società.

- **Oggetto:** "Problema di pagamento sul tuo abbonamento Netflix"
- **Tattica:** Sfrutta l'importanza dell'accesso ai servizi per indurre le vittime ad agire.
- **Obiettivo:** Rubare dati finanziari sfruttando la popolarità di un servizio di streaming noto come Netflix.

E-mail di Phishing (simulazione)

Oggetto: *"Problema di pagamento: Aggiorna il tuo abbonamento Netflix entro 24 ore"*

Corpo dell'e-mail:

Il pagamento non è andato a buon fine

Gentile [Nome Utente],

Ci dispiace informarti che non siamo riusciti a elaborare il pagamento per il tuo abbonamento a Netflix. A causa di questo problema, il tuo account verrà sospeso temporaneamente a partire da *domani*, impedendoti di accedere ai tuoi contenuti preferiti.

Per risolvere questa situazione e continuare a utilizzare il servizio senza interruzioni, ti invitiamo ad aggiornare i dati di pagamento cliccando sul link sottostante:

Aggiorna metodo di pagamento

Ti ricordiamo che l'aggiornamento è obbligatorio e deve essere completato entro 24 ore per evitare la sospensione dell'account.

Se hai già aggiornato i tuoi dati di pagamento, ti preghiamo di ignorare questa comunicazione.

Grazie per aver scelto Netflix,
Il Team Netflix

--
Nota: Questa è una comunicazione automatica. Si prega di non rispondere a questa e-mail.

Analisi degli elementi tipici dell’e-mail di phishing e come riconoscerli

Di seguito analizziamo gli elementi che caratterizzano un'e-mail di phishing come quella sopra e forniamo indicazioni su come riconoscerli:

---

1. Linguaggio che crea urgenza o paura

- **Nell'e-mail:** Viene detto che l’account sarà sospeso entro 24 ore se non si aggiornano i dati di pagamento.
- **Come riconoscerlo:** I criminali spesso sfruttano la psicologia dell’urgenza per forzare decisioni rapide, riducendo il tempo di riflessione. Diffida sempre di richieste che richiedono azioni immediate o minacce di conseguenze drastiche.

---

2. Link sospetti o falsi

- **Nell'e-mail:** Il link **"http://netflix-pagamenti-sicuri.net"** sembra credibile a prima vista ma non è il dominio ufficiale di Netflix (*netflix.com*).
- **Come riconoscerlo:** Passa il cursore del mouse sul link (senza cliccarci sopra!) per vedere l'URL reale. Controlla se il dominio è corretto. Un dominio ufficiale di Netflix, ad esempio, non includerà termini come "sicuri", "pagamenti", o suffissi strani come *.net*. Inoltre, verifica la presenza del protocollo HTTPS.

---

3. Personalizzazione apparente ma generica

- **Nell'e-mail:** Utilizza un generico "*Gentile [Nome Utente]*" anziché il vero nome dell'utente.
- **Come riconoscerlo:** Le aziende autentiche (come Netflix) di solito personalizzano le e-mail con il tuo nome e cognome reale, non con formule vaghe. Se non c’è personalizzazione o è molto generica, è un campanello d’allarme.

---

4. Mittente sospetto

- **Nell'e-mail:** Non viene mostrato direttamente il mittente, ma in un caso reale il mittente potrebbe essere qualcosa come:
  support@netflix-assistenza.com oppure **pagamenti@netfliix.com**.
- **Come riconoscerlo:** Controlla sempre l'indirizzo e-mail del mittente. Gli attaccanti spesso usano domini simili a quelli legittimi, con piccole variazioni (es. aggiungono lettere, cambiano una "l" con una "i", ecc.).

---

5. Assenza di riferimenti chiari all'account

- **Nell'e-mail:** Non ci sono dettagli specifici legati all'account, come il numero cliente o l'abbonamento attivo.
- **Come riconoscerlo:** Le comunicazioni ufficiali includono quasi sempre informazioni legate all'utente (ad esempio, dettagli sull'abbonamento o sull'ultimo pagamento).

---

6. Invito a cliccare su un link per aggiornare informazioni

- **Nell'e-mail:** Si richiede esplicitamente di aggiornare i dati di pagamento tramite un link.
- **Come riconoscerlo:** Le aziende autentiche raramente richiedono di aggiornare dati personali direttamente tramite un link in un'e-mail. È sempre meglio accedere al sito ufficiale digitando manualmente l'indirizzo nel browser.

---

7. Errori grammaticali o sintattici

- **Nell'e-mail:** In questo esempio non ci sono errori evidenti, ma molti attacchi di phishing presentano errori grammaticali, di formattazione o traduzioni scadenti.
- **Come riconoscerlo:** Errori di scrittura, spaziature anomale o formattazioni strane (es. parole in maiuscolo inutilmente) sono segnali di un'e-mail non professionale.

---

8. Promemoria che l'e-mail è "automatica"

- **Nell'e-mail:** La frase "*Questa è una comunicazione automatica. Si prega di non rispondere*" aggiunge credibilità.
- **Come riconoscerlo:** Questo elemento da solo non è sufficiente per classificare l'e-mail come phishing, ma se combinato con altri segnali sospetti può essere un indizio.