Questa email finge di provenire da un amico fidato, con l'obiettivo di ottenere credenziali di accesso a un servizio (ad esempio, un account email o social media).

Oggetto: Urgente! Ho bisogno di un favore con il tuo account

Ciao [Nome del destinatario],

spero che tu stia bene! Ho un problema urgente e ho pensato di chiedere il tuo aiuto. Ti scrivo qui perché è l'unico modo in cui al momento posso mettermi in contatto. Sto cercando di accedere a un vecchio account ma non riesco a recuperare la password. Mi è stato suggerito di utilizzare un accesso condiviso per verificare alcune informazioni.

Potresti accedere al link qui sotto con il tuo account [email/social media] e confermare una cosa per me? È davvero importante e ti prometto che ci vorranno solo pochi minuti.

Accedi qui al mio account

Fammi sapere appena l'hai fatto, così ti spiego tutto. Grazie mille, sei un vero amico!

Un abbraccio,
[Nome del presunto amico]

Elementi di phishing inclusi:

1. **Appello all'urgenza:** Il messaggio enfatizza l'urgenza per spingere il destinatario ad agire senza riflettere.
2. **Sfruttare la fiducia:** Simula un messaggio personale da un amico.
3. **Collegamento fraudolento:** Il link conduce a un sito contraffatto progettato per rubare credenziali.
4. **Richiesta generica:** L'ambiguità nella richiesta ("confermare una cosa") evita dettagli che potrebbero insospettire.

Struttura dettagliata della mail di phishing:

Oggetto:

"Urgente! Ho bisogno di un favore con il tuo account"

- **Perché funziona:** L'urgenza cattura l'attenzione del destinatario e spinge a leggere subito la mail. Usare un tono informale rafforza l'idea che provenga da un amico.

Saluto:

"Ciao [Nome del destinatario],"

- **Perché funziona:** Personalizzare il saluto con il nome del destinatario crea fiducia e abbassa la guardia. Se l'attaccante ha ottenuto il nome da una precedente violazione dei dati o social network, può rendere il messaggio ancora più credibile.

Contesto e problema:

"Ho un problema urgente e ho pensato di chiedere il tuo aiuto. Ti scrivo qui perché è l'unico modo in cui al momento posso mettermi in contatto. Sto cercando di accedere a un vecchio account ma non riesco a recuperare la password."

- **Perché funziona:** Presenta un problema comune (perdere l'accesso a un account) e una soluzione apparentemente innocua. Utilizza il tono di un amico in difficoltà per sfruttare l'empatia. Inoltre toglie i dubbi sul perché l'amico contatti per mail e non tramite il numero di telefono.

Richiesta d'azione:

"Potresti accedere al link qui sotto con il tuo account [email/social media] e confermare una cosa per me?"

- **Perché funziona:** La richiesta è vaga e non sembra rischiosa, ma spinge il destinatario a cliccare. Non vengono forniti troppi dettagli per non insospettire.

Link fraudolento:

"http://phishing-link-fraudolento.com"

- **Perché funziona:** I criminali usano URL che somigliano a siti legittimi, magari con un piccolo errore (es. **www.faceb0ok.com** invece di **www.facebook.com**). Possono anche camuffare il link con un testo come "Clicca qui".

Ad esempio, il testo del link potrebbe sembrare legittimo:
"**Accedi al tuo account**"
Ma in realtà punta a: **http://malicious-fake-login.com**

Chiusura:

"Fammi sapere appena l'hai fatto, così ti spiego tutto. Grazie mille, sei un vero amico!"

- **Perché funziona:** Il tono amichevole e la promessa di spiegare tutto dopo abbassano ulteriormente le difese del destinatario.

Firma:

"[Nome del presunto amico]"

- **Perché funziona:** Usare un nome familiare (spesso preso dai social o dalle email precedenti) rende la mail più convincente.

Segnali di allarme nella mail (per identificare un phishing):

1. **Errore grammaticale o ortografico:**
   Anche se il testo sembra fluido, gli errori (come punteggiatura mancante o grammatica strana) sono comuni nelle mail di phishing.
   Esempio: "Ti prometto che ci vorranno solo pochi minuti" potrebbe sembrare strano in certi contesti.

2. **Indirizzo email del mittente sospetto:**
   Anche se il mittente sembra essere un amico, controlla l'indirizzo email. Spesso gli attaccanti usano email che sembrano legittime ma contengono piccoli errori, come **amicofinto@gmail.con** invece di **amicofinto@gmail.com**.
3. **Urgenza non giustificata:**
   Frasi come "urgente" o "fallo subito" sono fatte apposta per far agire senza pensare.
4. **Link sospetto:**
   Passa il mouse sopra il link (senza cliccare!) per vedere dove conduce. Se non corrisponde al dominio ufficiale del servizio (es. **facebook.com**, **gmail.com**), è probabile che sia un tentativo di phishing.
5. **Richiesta insolita:**
   Gli amici non chiedono mai di accedere al tuo account per risolvere problemi loro. Questo è sempre un campanello d'allarme.

Come proteggersi dal phishing:

- **Non cliccare su link sospetti:** Se non sei sicuro della legittimità del messaggio, contatta direttamente il mittente tramite un altro canale.
- **Attiva l'autenticazione a due fattori (2FA):** Anche se le tue credenziali vengono rubate, 2FA protegge il tuo account da accessi non autorizzati.
- **Usa un password manager:** Ti aiuta a riconoscere siti fraudolenti, perché inserirà le credenziali solo su siti legittimi.
- **Segnala il phishing:** Aiuta a proteggere altre persone inviando il messaggio al team di sicurezza del servizio (es. **phishing@azienda.com**).