Scenario

Contesto:
Una persona X riceve un'email apparentemente da *Revolut*, un'app di pagamento popolare, che annuncia un'offerta limitata per acquistare Bitcoin a un prezzo scontato del 70%, con una scadenza imminente.

Obiettivo del phishing:
Frodare l'utente per fargli fornire informazioni personali, come dati bancari o credenziali di accesso, per rubare fondi o rubare le sue informazioni di pagamento.

Email di phishing

Oggetto: 🚀 Bitcoin alle stelle! Acquista i tuoi Bitcoin con il 70% di sconto!

Mittente: support@revolut-cryptofunds.com

Corpo dell'email:

Gentile cliente Revolut,

🚨 **Offerta Imperdibile!** 🚨
I Bitcoin stanno esplodendo! Il valore è aumentato del 200% nelle ultime 24 ore!

Revolut ti offre un'opportunità unica per acquistare Bitcoin con il 70% di sconto!
Non lasciare che questa occasione ti sfugga! Solo per i nostri utenti selezionati, puoi ottenere fino a 5 BTC a un prezzo mai visto prima!

Hai solo 24 ore per approfittare dell'offerta.
Clicca qui per acquistare subito i tuoi Bitcoin a un prezzo scontato:

Acquista ora e blocca il tuo sconto!

Una volta completato l'acquisto, i Bitcoin verranno automaticamente trasferiti nel tuo portafoglio Revolut!

Non perdere tempo, l'offerta scade tra poco!

Saluti,
Il Team Revolut
(Assicurati di completare l'acquisto entro 24 ore per evitare la perdita dello sconto!)

Perché l'email potrebbe sembrare credibile:

1. **Nome familiare:**
   Revolut è una piattaforma ben conosciuta per la gestione di criptovalute e denaro digitale. Molti utenti si affidano a servizi come Revolut per le loro transazioni quotidiane e l'acquisto di criptovalute. Questo rende l'email apparentemente credibile, poiché il destinatario può riconoscere il nome e fidarsi del marchio. L'idea che Revolut stia promuovendo un'offerta speciale legata ai Bitcoin sembra naturale, considerando che la piattaforma offre già servizi di

scambio di criptovalute. Pertanto, l'utente potrebbe abbassare la guardia e credere che l'email provenga effettivamente dal servizio che già utilizza.

2. **Offerta allettante:**
   Il concetto di acquistare Bitcoin scontati del 70% è estremamente allettante. L'offerta appare come un'opportunità irripetibile, un'occasione che può sembrare troppo vantaggiosa per essere ignorata. Poiché i Bitcoin sono una criptovaluta molto popolare e il loro valore fluttua in modo significativo, un'offerta che promette un grande sconto sembra come un affare unico. Gli investitori, soprattutto quelli meno esperti o i fan delle criptovalute, potrebbero essere tentati di agire rapidamente per ottenere il massimo beneficio, senza riflettere sulle possibili implicazioni di sicurezza.

3. **Urgenza:**
   L'email include una scadenza di 24 ore, una tecnica psicologica comune nelle truffe di phishing. La pressione del tempo spinge il destinatario ad agire senza pensarci troppo, con l'idea che se non lo farà, perderà un'occasione unica. Questa tattica sfrutta la paura di "perdere l'affare" e aumenta la probabilità che l'utente clicchi sul link senza verificare l'autenticità dell'offerta. Le truffe spesso giocano su questa sensazione di urgenza per indurre reazioni impulsive.

4. **Presenza di loghi e design professionale:**
   L'email potrebbe includere loghi ufficiali, colori aziendali e un design che imita fedelmente quello delle comunicazioni autentiche di Revolut. Questo dà l'impressione di un messaggio ufficiale, soprattutto per gli utenti meno attenti ai dettagli. Elementi come un'intestazione professionale, un saluto formale, e una firma del team di Revolut aumentano la credibilità dell'email. Anche piccoli dettagli, come l'uso del font o il layout delle email autentiche, possono essere replicati dai truffatori per ingannare meglio le vittime.

5. **Ignoranza o inesperienza sulle criptovalute:**
   Molti utenti hanno una conoscenza limitata delle criptovalute e delle loro dinamiche di prezzo. Non sapendo quanto sia plausibile uno "sconto del 70% sui Bitcoin", potrebbero considerare l'offerta reale senza verificare. La mancanza di familiarità con il mercato delle criptovalute rende facile per i truffatori sfruttare la curiosità o il desiderio di approfittare di un'opportunità percepita come legittima.

6. **Lingua e tono credibile:**
   L'email utilizza un tono professionale e frasi comuni nei contesti finanziari, come "acquisto sicuro", "offerta limitata", e "transazione crittografata". Questo linguaggio tecnico fa sembrare l'email autentica, specialmente per gli utenti che associano Revolut a innovazioni finanziarie e sicurezza digitale.

7. **Riferimenti a trend attuali:**
   L'email fa leva sulla popolarità e l'hype delle criptovalute, che sono spesso in prima pagina nelle notizie. Il destinatario potrebbe credere che sia plausibile ricevere un'offerta speciale, dato l'interesse generale attorno ai Bitcoin e al loro valore crescente. Usare argomenti di attualità rafforza l'illusione che l'offerta sia reale.

8. **Personalizzazione parziale:**
   Sebbene la mail possa non includere il nome completo dell'utente, potrebbe comunque utilizzare un saluto generico come "Ciao utente di Revolut" o "Gentile cliente". Per chi non è abituato a distinguere le email autentiche da quelle fraudolente, questo potrebbe sembrare un

dettaglio normale, specialmente considerando che non tutte le comunicazioni ufficiali personalizzano il destinatario.

9. **Simulazione di sicurezza:**
   L'email potrebbe includere dichiarazioni che sottolineano la sicurezza dell'offerta, come *"Tutti i pagamenti sono protetti"* o *"Offerta esclusiva per utenti verificati"*. Includere queste rassicurazioni è una tecnica comune per calmare le paure iniziali dei destinatari e indurli a credere che l'offerta provenga da una fonte affidabile.

10. **Appello all'esclusività:**
    L'email potrebbe contenere frasi come *"Solo per utenti selezionati"* o *"Offerta riservata ai primi 100 iscritti"*. Questo tipo di linguaggio crea un senso di privilegio, inducendo il destinatario a sentirsi speciale e a temere di perdere un'opportunità unica.

11. **Promessa di facilità d'uso:**
    L'email potrebbe sottolineare che la transazione è semplice e veloce, ad esempio: *"Basta un clic per completare l'acquisto e i Bitcoin saranno immediatamente trasferiti nel tuo portafoglio Revolut."* L'idea di un processo senza complicazioni può convincere l'utente che si tratti di una procedura autentica e conforme agli standard del servizio.

12. **Presa in carico di "domande frequenti" anticipate:**
    L'email potrebbe includere una piccola sezione di "FAQ" con risposte a potenziali dubbi.

13. **Dettagli fittizi ma convincenti:**
    I truffatori potrebbero aggiungere dettagli pseudo-legittimi come un numero di transazione, un codice promozionale, o una data di scadenza precisa, come: *"Codice promozionale: BTC70R. Valido fino alle 23:59 di oggi."* Questi dettagli possono sembrare reali, aumentando la fiducia nell'email.

Elementi di allarme nella struttura dell'email:

1. **Mittente sospetto:**
   Il mittente dell'email, *revolut-cryptofunds.com*, non corrisponde al dominio ufficiale di Revolut, che dovrebbe essere qualcosa come *@revolut.com*. Questo è un primo segnale di allarme: i truffatori cercano di imitare marchi e aziende conosciuti, ma spesso sbagliano un piccolo dettaglio, come il dominio dell'email, che può sembrare strano o leggermente modificato. Se l'utente non è attento, potrebbe non notare questa discrepanza, ma è una chiara indicazione che l'email potrebbe non essere legittima.

2. **Link falso:**
   Il link che appare nell'email, *revolut-bitcoin-discount.com*, non corrisponde al sito ufficiale di Revolut. Anche se il link sembra inizialmente convincente, il dominio utilizzato dai truffatori è sospetto. I truffatori cercano di far sembrare il link simile a quello originale, ma con piccole modifiche, come l'aggiunta di parole o l'uso di un dominio non ufficiale. Cliccando su questo link, l'utente potrebbe essere indirizzato a un sito fraudolento che raccoglie le sue credenziali di accesso o altre informazioni sensibili.

3. **Richiesta di agire velocemente:**
   L'email fa pressione sul destinatario per agire immediatamente, mettendo in evidenza che l'offerta scade entro 24 ore. Questo è un altro trucco utilizzato dalle truffe di phishing per

indurre l’utente a cliccare senza pensare troppo. Le offerte genuine raramente richiedono una risposta così rapida, mentre le truffe cercano di sfruttare il senso di urgenza per ridurre il tempo di riflessione e aumentare la probabilità che l'utente prenda decisioni affrettate senza controllare attentamente i dettagli.

4. **Offerta troppo vantaggiosa:**
   Un'offerta che promette uno sconto del 70% sui Bitcoin è quasi certamente troppo vantaggiosa per essere vera. Le criptovalute sono già abbastanza costose e un tale sconto solleva immediatamente dei dubbi. Le truffe spesso si presentano con offerte che sembrano troppo belle per essere vere per attrarre utenti ignari. Un’offerta che promette un grande guadagno in cambio di un piccolo investimento iniziale è uno dei metodi più comuni utilizzati dai truffatori per ingannare le vittime.

Nota Finale

Le email come questa sono progettate per sfruttare l'entusiasmo degli utenti riguardo le criptovalute e per spingerli a compiere azioni impulsive. È fondamentale non cliccare su link sospetti e verificare sempre l'autenticità delle offerte, specialmente quando sembrano troppo buone per essere vere. Se hai dubbi, contatta il servizio clienti ufficiale di Revolut o visita il loro sito web tramite canali sicuri.