Federico
Cuccu

Email di phishing: esempio, credibilità e criticità

Pratica S5/L5

Cosa sono le email di phishing

Le email di phishing sono messaggi ingannevoli inviati per ottenere **informazioni sensibili** come credenziali di accesso, numeri di carta di credito o altri dati personali e utilizzarli per attività fraudolente, come furto d'identità e acceso non autorizzato a conti bancari.

Queste email sembrano provenire da **fonti affidabili**, come banche, fornitori di servizi o aziende conosciute, e inducono le vittime a cliccare su link dannosi o a fornire informazioni direttamente.

Alcuni attacchi di phishing possono anche eseguire **script malevoli** sul dispositivo della vittima, rendendo il sistema vulnerabile o utilizzandolo come punto di accesso per attacchi futuri.

Perché sono sempre più pericolose

Le email di phishing sono diventate più pericolose perché:

- **Sono più sofisticate**: Gli attacchi moderni sono personalizzati (spear phishing) e mirano a specifiche persone o organizzazioni, utilizzando informazioni reali per sembrare credibili.

- **Usano tecniche avanzate**: Alcune email di phishing utilizzano pagine di login false, tecniche di spoofing e persino contenuti interattivi per ingannare le vittime.

- **Difficili da rilevare**: I truffatori perfezionano continuamente i loro metodi per aggirare i filtri antispam e le difese di sicurezza, rendendo difficile individuare queste email.

Esempio di email di phishing

Scenario dell’email

Andremo a generare con ChatGPT una finta (ma realistica) email di phishing.

Lo scopo dell'esercizio è quello di creare un email manipolatoria e di individuarne poi le criticità, ovvero quali sono gli elementi che rendono l'email meno credibile.

Lo scenario dell'email è il seguente:

- **Oggetto**: il tuo ordine amazon non è stato evaso.
- **Obiettivo e CTA dell'email**: conferma i dati della tua carta per evadere l'ordine.
- **Urgenza**: hai 24 ore di tempo, dopodiché l'ordine verrà annullato.

Oggetto: Il tuo ordine Amazon non è stato evaso
Da: supporto@amazon-ordini.com

Caro cliente,
Ti informiamo che il tuo ordine effettuato su Amazon **non è stato evaso** a causa di un problema riscontrato con il pagamento.

Per completare l'acquisto, è necessario confermare i dettagli della tua carta di pagamento **entro le prossime 24 ore**. Se non riceveremo una conferma entro questo termine, l'ordine verrà annullato automaticamente.

Per confermare i tuoi dati di pagamento, clicca sul seguente link sicuro:
Conferma il pagamento
In alternativa, scansiona il codice QR e conferma i tuoi dati di pagamento:

Grazie per aver scelto Amazon. Restiamo a tua disposizione per qualsiasi domanda.
Cordiali saluti,
Il Team di Supporto Amazon

Motivi per cui potrebbe essere credibile

Motivi per cui l'email potrebbe sembrare credibile

- **Oggetto**: L’oggetto sfrutta la paura di un ordine non completato e crea urgenza, inducendo la vittima a controllare immediatamente la situazione.
- **Struttura e stile formale**: L’email è scritta con un tono formale, emulando le comunicazioni ufficiali di Amazon, e contiene termini come "confermare i dettagli della carta", che rispecchiano un linguaggio tecnico.
- **CTA ben evidenziata**: Il link di conferma del pagamento è presentato come "sicuro", il che potrebbe convincere la vittima a cliccare senza sospettare.
- **Scadenza ravvicinata**: L’avviso di 24 ore per risolvere il problema crea pressione, una tattica comune per evitare che la vittima abbia tempo di riflettere.

Motivi per cui non dovrebbe essere credibile

Motivi per cui l'email non dovrebbe sembrare credibile

- **Indirizzo email del mittente**: La mail arriva da un indirizzo non ufficiale, supporto@amazon-ordini.com, che non è legato al dominio ufficiale di Amazon (@amazon.com). Questo è un segnale chiaro di phishing.

- **Errore nel link di verifica**: Il link proposto non conduce a un dominio Amazon ufficiale, bensì a un sito sospetto (amazon-verifica-pagamento.com), che non appartiene ad Amazon.

- **Assenza di personalizzazione**: L'email si rivolge a un generico “**Caro cliente**” invece di usare il nome completo del destinatario, come farebbe un'email autentica di Amazon.

Motivi per cui l'email non dovrebbe sembrare credibile

- **Mancanza di riferimenti specifici all’ordine**: Non ci sono dettagli sull’ordine specifico (es. numero di ordine, articoli acquistati), una mancanza comune nelle email di phishing che non riescono a personalizzare le informazioni.

- **Errori minimi nella formattazione**: La frase "Restiamo a tua disposizione per qualsiasi domanda" potrebbe suonare leggermente inusuale e meno formale rispetto alle comunicazioni ufficiali di Amazon, che seguono sempre uno stile ben definito.

- **Codice QR**: nell’email è stato inserito un codice QR (come richiesto dall’esercizio) che rimanda al link malevolo, ma amazon non inserisce mai un codice QR nelle loro email e questo potrebbe generare ulteriori sospetti.

Motivi per cui l'email non dovrebbe sembrare credibile

L’email potrebbe non passare i controlli SPF, DKIM e DMARC.

Il server effettua dei controlli e restituisce ‘PASS’ o ‘BLOCK’ in base all’esito del controllo.

- **SPF**: controlla l’indirizzo IP del mittente
- **DKIM**: controlla la firma digitale del mittente
- **DMARC**: l’email viene inviata se SPF e DKIM sono legittimi.

Se non sono presenti, allora l’email è sicuramente fake. Se l’email per qualche motivo viene comunque inviata dal server di posta, l’utente medio non avrà le conoscenze per accorgersi di questa falla.

Conclusioni

Conclusioni

Questa email usa tattiche di urgenza e toni formali per apparire credibile, ma la mancanza di dettagli personalizzati (come il nome del destinatario a inizio email), il dominio email del mittente non conforme e il link sospetto rivelano che si tratta di una truffa.

Uno strumento come ChatGPT, però, se utilizzato con fini malevoli, potrebbe insegnare agli attaccanti dove sono le falle delle email di phishing che generano e **migliorare l'efficacia** dei loro attacchi.