

# Email Phishing Esempio Analisi



Andremo a generare una finta (ma realistica) email di phishing, puramente a scopo educativo. 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, ad esempio piccoli errori grammaticali).

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.

Dopo aver generato l'email, analizzala seguendo questi due criteri:

- spiega perché l'email dovrebbe essere credibile per l'ipotetica vittima
- spiega perché l'email non dovrebbe essere credibile e identifica le criticità.

Ribadisco che la generazione è solo a scopo educativo.



## Email di phishing simulata:

**Oggetto:** Il tuo ordine Amazon non è stato evaso

**Da:** [supporto@amazon-ordini.com](mailto:supporto@amazon-ordini.com)

**A:** [Email destinatario]

**Data:** [Data corrente]

**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](#)

Grazie per aver scelto Amazon. Restiamo a tua disposizione per qualsiasi domanda.

Cordiali saluti,

Il Team di Supporto Amazon

## Analisi dell'email di phishing:

## 1. 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.

## 2. 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.
- **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.

**Conclusione:** Questa email usa tattiche di urgenza e toni formali per apparire credibile, ma la mancanza di dettagli personalizzati, il dominio email del mittente non conforme e il link sospetto rivelano che si tratta di una truffa.

ChatGPT può commettere errori. Considera di verificare le informazioni importanti.