S5 L5 Luca Calvigioni

INGEGNERIA SOCIALE

Creare una mail di phishing usando ChatGPT

EMAIL: **offerte@anazom.com**

Oggetto: Offerta speciale riservata per te! Accedi ora ad Amazon per riscattare il buono sconto di 100€

Gentile Utente,

Siamo lieti di informarti che come nostro cliente esclusivo, hai diritto a un'offerta speciale per ringraziarti della tua fiducia nei nostri prodotti!

Solo per pochi giorni, hai l'opportunità di usufruire di uno sconto di 100€ su qualsiasi ordine.

Per riscattare questa offerta, accedi al tuo account cliccando sul link qui sotto. Lo sconto potrà essere applicato ai prossimi acquisti.

Accedi al tuo account e riscatta lo sconto ➔

Come fare:

1. Accedi al tuo account tramite QR Code.
2. Usufruisci del tuo buono nei prossimi acquisti.

Questa offerta è valida solo fino alle prossime 24 ore, quindi affrettati, non perdere questa occasione!

Cordiali saluti,

Il team di Amazon.

Scenario:

La **mail di phishing** è una mail fraudolenta creata e inviata con l'obiettivo di ingannare il destinatario e convincerlo a fornire informazioni sensibili, come in questo caso le credenziali di accesso all'account di Amazon, il malcapitato tenterà di accedere al proprio account Amazon per riscattare il buono sconto ma non sulla pagina vera, su un clone che una volta inserite le sue credenziali di accesso queste verranno immediatamente inviate al truffatore.

Perchè l'email può sembrare credibile:

•Imitazione del marchio

Le email di phishing spesso copiano il layout, i colori e il logo delle aziende rendendole simili alle comunicazioni ufficiali, questo aiuta a creare un'impressione di autenticità.

•Indirizzi email simili

I truffatori possono utilizzare indirizzi email che sembrano molto simili a quelli ufficiali, ad esempio cambiando una lettera o aggiungendo un dominio diverso.

•Creazione di urgenza

Molti messaggi di phishing includono frasi per indurre il destinatario a prendere decisioni affrettate, senza fermarsi a riflettere sulla validità del messaggio, ad esempio offerte limitate.

•Codice QR

Il QR code è presentato come un modo rapido per accedere all'account, un metodo che le persone potrebbero considerare sicuro. Il QR evita che la vittima veda l'URL a primo impatto aumentando la probabilità di cliccare senza sospetti.

Perchè l'email è sospetta:

•Indirizzo email del mittente

L'indirizzo email del mittente può contenere errori di battitura o variazioni rispetto a un dominio ufficiale.

•Richieste Urgenti o Minacce

Le aziende legittime generalmente non usano tattiche di intimidazione o messaggi che esortano a cliccare forzatamente su un link.

•Link mascherati o sospetti

Se il link o in questo caso il QR Code che appare nella mail non corrisponde al sito ufficiale è probabile che si tratti di phishing.

•Offerte irrealistiche

Le truffe spesso cercano di attirare l'attenzione con promesse di guadagni facili o premi.

•Mancanza di personalizzazione

Messaggi che iniziano con “Gentile Utente” o simili, senza usare il nome del destinatario, generalizzando, possono essere segnali di phishing.

Conclusione:

L'efficacia del phishing deriva dalla capacità dei truffatori di emulare comunicazioni legittime e sfruttare la psicologia umana, come la paura, l'urgenza e la fiducia. Essere consapevoli di queste tecniche può aiutare le persone a riconoscere le email di phishing e a proteggersi dalle truffe online.