

Progetto S5L5 – INGEGNERIA SOCIALE

Obiettivo: Creare una simulazione di un email di phishing utilizzando ChatGPT

INTRODUZIONE

L'esercizio settimanale, Progetto S5/L5, richiede nelle sue istruzioni di:

1. Creare uno scenario:
 - Un contesto realistico in cui un'email di Phishing potrebbe essere inviata.
 - Definizione chiara dell'obiettivo del Phishing
2. Scrivere l'email di Phishing:
 - Utilizzare ChatGPT per generare il contenuto dell'email
 - Assicurarsi che sia convincente con elementi tipici delle email di phishing
3. Spiegare lo scenario:
 - Descrivere lo scenario creato
 - Spiegazione del perché l'email potrebbe sembrare credibile alla vittima.
 - Evidenziare gli elementi della email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

1. CREAZIONE SCENARIO

- Nello scenario di Phishing creato, descritto nel paragrafo 3.SPIEGAZIONE SCENARIO, viene rappresentato un contesto nel quale un fornitore di servizi (in questo caso [Amazon.it](#)) notifica, tramite posta elettronica, la presenza di presunti problemi doganali relativi alla consegna di un pacco.
- L'obiettivo principale dell'attacco di phishing è indurre uno stato di allarme nella **Vittima** e indurla a visualizzare il contenuto del link presente nella mail, utile alla risoluzione del problema, fornendo i propri dati finanziari e permettendo così all'**Attaccante** di poter usufruire di tali dati e accedere alle risorse economiche della **Vittima**.

2. SCRITTURA DELL'EMAIL DI PHISHING

In questo paragrafo viene descritto come viene utilizzata lo strumento **IA ChatGPT** (chatgpt.com) per la creazione dell'email di Phishing, partendo dal seguente **Prompt**:

“Sono uno studente di cybersecurity la traccia dell'esercizio mi richiede un report in cui devo simulare una mail di phishing realistica dando un alto senso di urgenza contesto acquirente Amazon problemi dogana necessita invio pagamento doganale”

La risposta iniziale della IA risulta cauta:

“Capisco il contesto accademico. Tuttavia, non posso redigere una mail di phishing “realistica” e pronta all’uso [...]”

Nonostante ciò, procede a soddisfare la richiesta.

Data la forma della mail generata dalla IA, apporto modifiche al testo che in questo Report verranno trascritte in colore rosso (**rosso**) per poter eseguire la traccia.

Qui l'Email generata da ChatGPT con relative modifiche:

from: Servizio Clienti Amazon <support@amazon-sicure.it>

Oggetto: **AZIONE IMMEDIATA RICHIESTA** – Spedizione **Amazon** in sospeso

Gentile **Utente**,

la informiamo che il suo recente ordine **Amazon**, è attualmente **sospeso** presso il centro doganale di **smitsamento** a causa di **oneri doganali non saldati**.

A seguito di un controllo, è stato rilevato un **pagamento doganale mancante pari a €2,94**, necessario per completare lo sdoganamento e consentire la consegna del pacco.

Stato della spedizione

- **Stato attuale: In sospeso – verifica doganale**
- **Motivo del blocco: Costi doganali non saldati**
- **Termine massimo di risoluzione: entro 12 ore**

⚠ ATTENZIONE: In assenza di conferma **entro 12 ore**, l'ordine verrà **automaticamente annullato** e l'importo dell'acquisto potrebbe non essere rimborsabile **secondo le normative doganali vigenti**.

Per evitare la cancellazione della spedizione, La invitiamo a verificare immediatamente i dati di **pagina** **tramite il seguente portale sicuro:**

→ **[VERIFICA PAGAMENTO DOGANALE ATTRAVERSO IL SEGUENTE LINK]**

<https://amazon-sicure.it/spedizioneconsegna.com>

Una volta completata la procedura, la spedizione riprenderà entro poche ore.

La ringraziamo per la collaborazione.

Cordiali saluti,

Ufficio Spedizioni Internazionali

Amazon Logistics Europe

© Amazon EU S.à r.l. – Tutti i diritti riservati

Nota: Questo messaggio è generato automaticamente. Si prega di non rispondere a questa email.”

3. SPIEGAZIONE SCENARIO

Premessa:

Nel seguente scenario l'**Attaccante** prepara il suo attacco creando una pagina che funge da link nella quale viene simulato il sito ufficiale **Amazon.it** il quale contiene delle sezioni per la **Vittima** da compilare:

Indirizzo di spedizione (se diverso da quello di residenza):

Numero di carta:

Scadenza:

CVV:

Successivamente invia ad un certo numero di indirizzi email, acquisiti illegalmente, l'esempio di email di phishing che abbiamo visto nel paragrafo precedente clonando una mail reale.

L'email di phishing è generata in modo tale da sembrare provenire da Amazon, che è stato scelto in questo esempio per vari fattori:

1. Amazon è un brand globale e altamente riconoscibile, utilizzato quotidianamente da milioni di utenti sia per l'e-commerce sia per servizi digitali aggiuntivi, come streaming, musica etc. Questo elevato livello di familiarità riduce la soglia di diffidenza del destinatario.
2. La frequenza elevata degli acquisti online aumenta la probabilità che il destinatario stia effettivamente aspettando una consegna.
3. L'Utenza ha fiducia in Amazon, percepisce il brand come affidabile anche per l'attenzione e la disponibilità verso il cliente.
4. Amazon produce diversi servizi e prodotti in modo tale da essere presente nella vita quotidiana e puntando ad un senso di familiarizzazione nei confronti dell'Utenza

Quindi, l'autorità e l'affidabilità associate al marchio contribuiscono a rafforzare l'efficacia delle tecniche di ingegneria sociale, portando l'Utente a fidarsi del contenuto del messaggio e a interagire con esso.

-L'Attaccante fa leva su questo.-

Nella mail si descrive che la consegna del pacco è sospeso per problemi doganali, invita tempestivamente l'Utente (**entro 12 ore**) a risolvere il problema pagando la dogana, una cifra piccola, qui **2,94 euro**, cliccando sul link.

Agli occhi di un **Utente** distratto, (la mail sarà scritta in maniera uniforme mantenendo il Grassetto e le dimensioni dei caratteri), il quale sta aspettando una consegna, l'email sembrerebbe legittima e credibile non riscontrando errori grammaticali.

L'Attaccante fa leva sull'**urgenza**, mette in chiaro si ha poco tempo per risolvere il problema, l'Utente **potrebbe perdere il pacco e il denaro** che ha usato per

l'acquisto, propone una cifra irrisoria per risolvere il problema, inducendo la **Vittima** a preoccuparsi poco delle spese doganali e più sulla perdita dell'oggetto acquistato

Usa caratteri grandi e parole in grassetto per portare l'Utente a una lettura veloce e allarmista, usa forme per indurre a pensare che sia tutto sicuro come “**secondo le normative doganali vigenti**” e “**tramite il seguente portale sicuro**”

Il link usato contiene parole come “**sicure**”(secure) e “**spedizioneconsegna**”, un Utente distratto potrebbe non leggere “**amazon**” e sempre ai fini dell'inganno l'**Attaccante** conclude la mail con:

“Ufficio Spiedizioni Internazionali
Amazon Logistics Europe
© Amazon EU S.à r.l. – Tutti i diritti riservati

Nota: Questo messaggio è generato automaticamente. Si prega di non rispondere a questa email.

In modo tale da indurre l'Utente a non cercare spiegazioni rispondendo all'email e a evitare il contatto umano

Qui la mail potrebbe aggirare o ridurre l'efficacia dei protocolli come:

SPF (Sender Policy Framework) perché SPF verifica l'IP del server mittente e non il contenuto es. **amazon-sicure.it**

DKIM (DomainKeys Identified Mail) che garantisce l'integrità del messaggio e l'autenticità del dominio che appartiene all'**Attaccante**

Se DKIM E SPF sono allineati il DMARK non trova irregolarità e non entra in funzione.

Quindi, sebbene SPF, DKIM e DMARC siano correttamente implementati, una campagna di phishing può risultare efficace utilizzando domini simili all'originale e autenticati.

In questo scenario, i controlli di autenticazione email non falliscono, poiché non avviene spoofing diretto del dominio ufficiale, ma una sua impersonificazione.

Inoltre, questo scenario che riguarda problemi doganali è possibile, una potenziale **Vittima** dovrebbe:

- Verificare sempre il mittente reale, cioè prestare attenzione e controllare il dominio dell'indirizzo email del mittente
- Leggere attentamente il contenuto così da trovare errori nel corpo del messaggio (di solito assenti nei veri messaggi)
- Diffidare dalle email disorientanti che creano urgenza
- Ricordarsi che nessun servizio richiede ulteriori informazioni personali
- La mail illustrata nel paragrafo precedente è priva di dati, non c'è un riferimento vero all'ordine (esempio Ordine n.XXXXX tipo di oggetto/servizio con relative immagini) da confrontare con il reale acquisto
- L'Utente dovrebbe contattare subito il SERVIZIO CLIENTI e non cliccare su Link ambigui.

In fine, **la consapevolezza** dell'Utente rappresenta l'ultima linea di difesa contro il phishing, anche in presenza di protocolli tecnici efficaci, l'ingegneria sociale rimane uno dei vettori di attacco più diffusi.