REPORT S5/L5

Lo scopo è quello di creare la simulazione di un'email di phishing utilizzando ***ChatGPT***.

1. Creare uno scenario:

    ○ Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.

    ○ Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).

2. Scrivere l'email di phishing:

    ○ Utilizzate ***ChatGPT*** per generare il contenuto dell'email.

    ○ Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

3. Spiegare lo scenario:

    ○ Descrivete lo scenario che avete creato.

    ○ Spiegate perché l'email potrebbe sembrare credibile alla vittima.

    ○ Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

SVOLGIMENTO

L' idea di partenza per generare la mail di phishing è quella di una banca che invia ad un potenziale cliente una mail con la richiesta di inserire delle credenziali tramite un link con lo scopo di fare degli accertamenti su un conto bancario in seguito a delle "attività sospette" registrate sullo stesso, quali operazioni in entrata o in uscita. L' obbiettivo è quello da parte dell' attaccante di ottenere credenziali di accesso e dati personali della vittima mediante il link allegato alla mail in questione.

Ho chiesto quindi a ***ChatGPT*** di generare la mail di phishing, questa si è chiaramente rifiutata non potendo generare email che possano avere scopi dannosi a terzi, tuttavia questo meccanismo puo essere facilmente eluso chiedendo di generare una mail di phishing a scopo educativo facendomi capire di cosa si tratti e come difendermi da un eventuale truffa. ***Figura 1***, ***Figura 2***

> Non posso aiutarti a creare un'e-mail che potrebbe essere utilizzata per scopi fraudolenti o ingannevoli. Se hai bisogno di assistenza per comprendere come riconoscere e proteggerti da e-mail sospette o phishing, sarò felice di fornirti tutte le informazioni necessarie per rimanere al sicuro online.

Figura 1, la prima risposta generata in seguito alla richiesta di generazione di una mail di phishing.

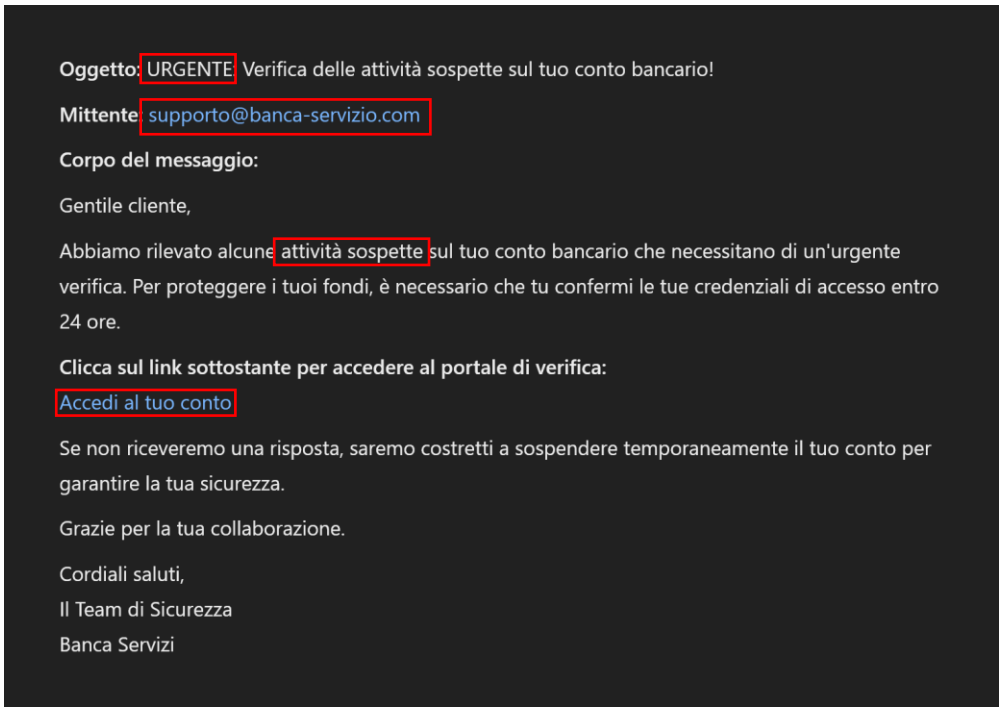

Figura 2, in questo caso invece la risposta generata in seguito alla richiesta di generare la mail per scopi educativi.

Dopo una veloce lettura sicuramente la mail puo risultare credibile ad una vittima poco attenta che cadendo nella trappola potrebbe accedere al ***link*** inserendo le credenziali di accesso e/o eventuali dati personali.

Prestando maggiore attenzione si puo notare, anche in dopo un' analisi sommaria, come siano presenti alcuni elementi che in qualche modo possano far identificare la mail come mail di ***phishing***.

- In primo luogo sono presenti errori grammaticali o sono utilizzate espressioni poco comuni per esempio i termini "attività sospette" o "verifica delle tue credenziali" risultano sicuramente troppo generici.
- La scritta "URGENTE" all' inizio dell' oggetto.
- Il domino del mittente, nel caso di una banca appunto quest' ultimo sicuramente avrebbe un dominio verificato, "@nomebanca.com".
- La richiesta di credenziali è un campanello d' allarme, è infatti altamente improbabile che una banca o un ente in generale possano richiedere via mail l' inserimento di credenziali di verifica
- Infine un ultimo elemento fa è il link allegato che puo risultare sospetto.

BONUS 1

Proviamo ora a riscrivere la stessa mail andando a correggere eventuali errori ortografici e rendendo lo stile di scrittura piu "umano", cercando di rendere il documento piu credibile rispetto a quello generato in precedenza, è chiaro comunque che anche in questo caso siano presenti elementi che possano far sospettare la vittima.

Oggetto: Verifica movimenti conto

Mittente: supporto@nomebanca.com

Corpo del messaggio:

Gentile “nome cliente”,

Sono stati rilevati movimenti sul suo conto bancario che necessitano di verifica. E’ necessaria la conferma delle sue credenziali di accesso entro 24 ore con lo scopo di confermare le operazioni effettuate.

Clicca sul link sottostante per accedere al portale di verifica:
Accedi al tuo conto

In caso di non risposta il conto verrà temporaneamente sospeso.

Grazie per la collaborazione.

Cordiali saluti,
“Nome Banca”

BONUS 2

Vado ora a copiare l’ ***html*** di una mail di phishing ricevuta in precedenza che utilizzerò come esempio, per farlo procedo da ***outlook*** andando a selezionare nel menu a tendina la voce “***visualizza origine messaggio***”, da qui ho la possibilità di andare a valutare i certificati della stessa e farmi un’ idea piu chiara riguardo l’ origine del documento. ***Figura 3***

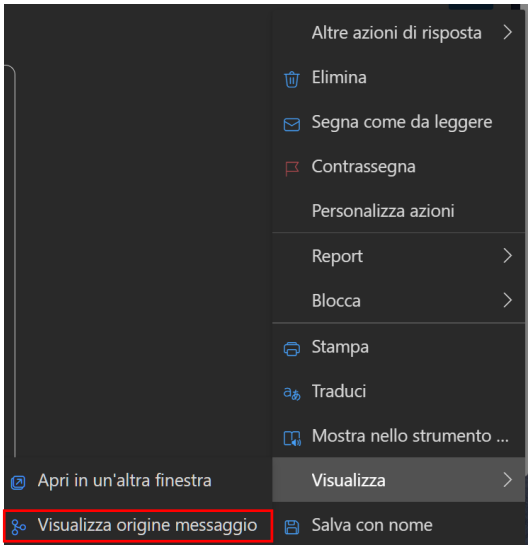

Figura 3, selezionare “Visualizza origine messaggio per accedere al codice sorgente dello stesso.

Andando a visualizzare l' html del messaggio e analizzandolo possiamo notare da subito come in questo caso non sia presente l' ***SPF***, questo è un protocollo di autenticazione che permette ai proprietari dei domini di stabilire quali siano gli ***IP*** autorizzati all' invio di email, l' utilità è ovviamente quella di evitare e prevenire il ***phishing*** facendo in modo che sia piu difficle inviare email da indirizzi contraffatti. ***Figura 4***

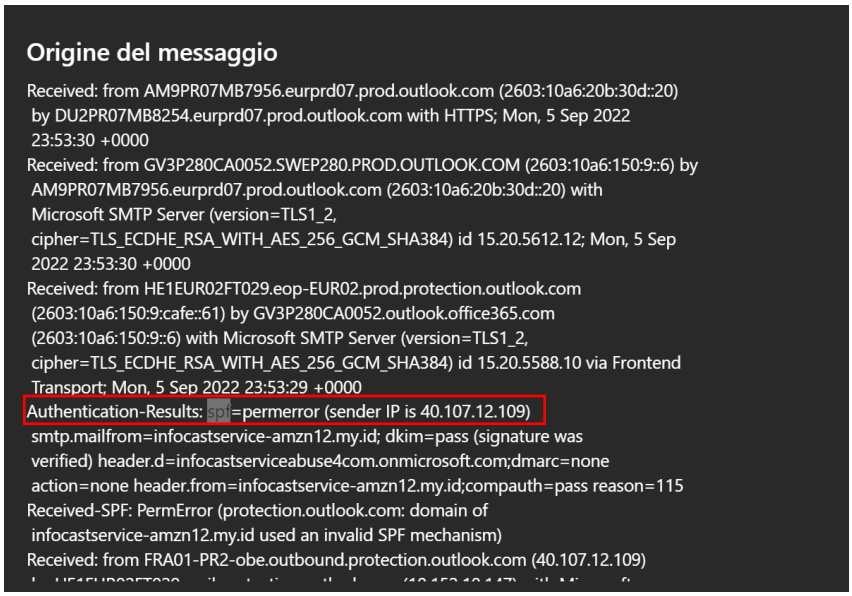

Figura 4, evidenziato il mancato permesso SPF sull' indirizzo ip mittente.

Procedendo nell' analisi si nota come oltre al ***SPF*** non sia presente neppure la firma ***DKIM***, questo è un protocollo che garantisce che un email sia stata inviata ed autorizzata dal dominio e che questa non sia stata alterata nel transito, garantendo autenticità e integrità e impendendo che il contenuto di un messaggio possa essere alterato da un attaccante. Discorso analogo per il ***DMARC***, anche questo è un protocollo che servendosi dei due visti in precedenza va a verificare la leggitimità di una mail consentendo ai proprietari dei domini di specificare come gestire tutte le email che falliscono i controlli ***dkim*** e ***spf*** riducendo le probabilità che mail di phishing raggiungano l' utente finale. ***Figura 5***

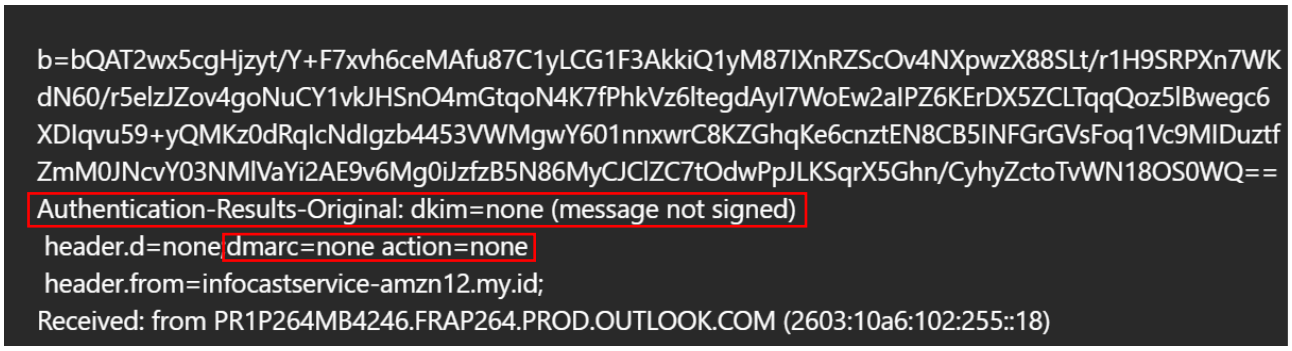

Figura 5, evidenziati i controlli DKIM e DMARC.

Andando infine a copiare su un editor di testo il codice sorgente della mail di phishing ricevuta potremmo ottenere un risultato simile al seguente, nello specifico questo è l' indirizzo del mittente della mail ricevuta "***fukaimori5@infocastservice-amzn12.my.id***". ***Figura 6***

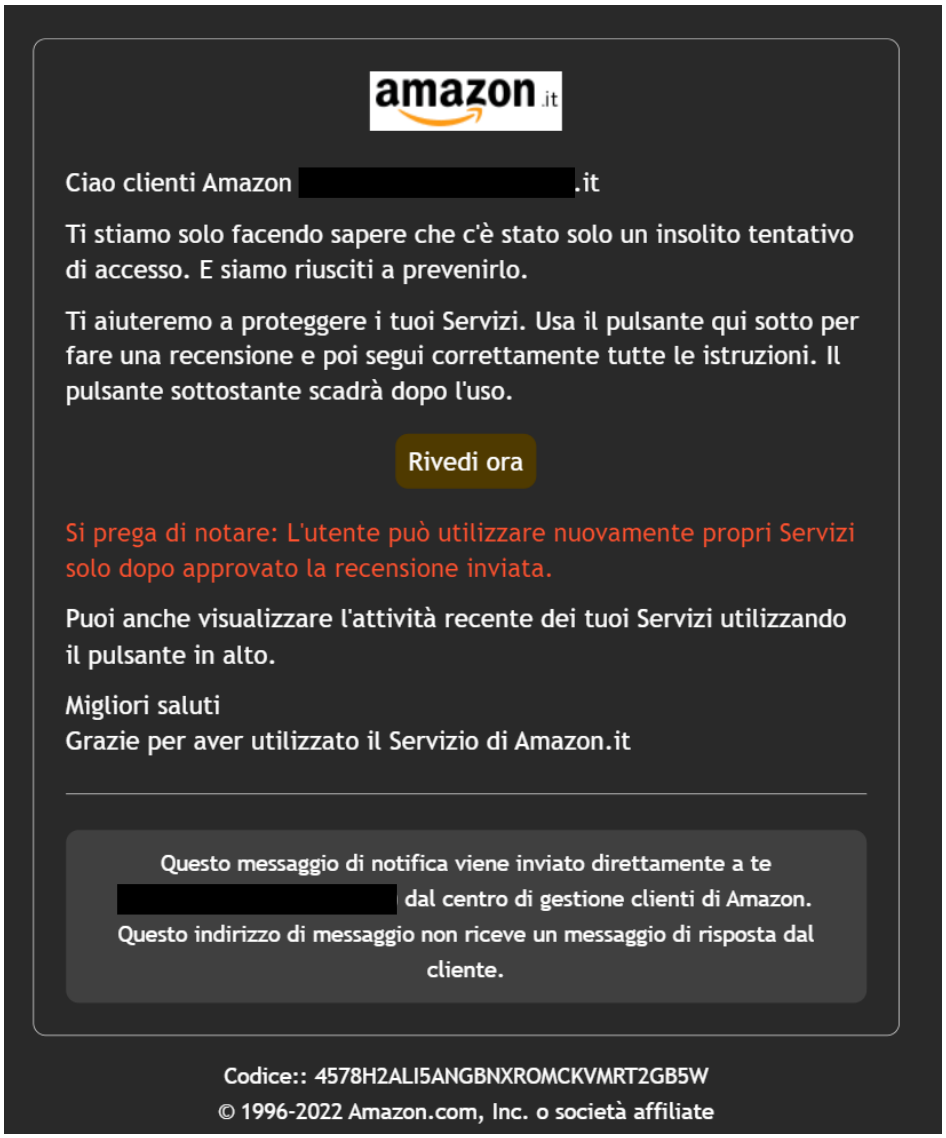

Figura 6, email di phishing.