ESERCIZIO

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

Istruzioni: 1. Creare uno scenario:

- Pensate a un contesto realistico in cui un'e-mail di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'e-mail 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'e-mail di phishing:

- Utilizzate ChatGPT per generare il contenuto dell'e-mail.
- Assicuratevi che l'e-mail sia convincente, ma anche che contenga gli elementi tipici delle e-mail di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

3. Spiegare lo scenario:

- Descrivete lo scenario che avete creato.
- Spiegate perché l'e-mail potrebbe sembrare credibile alla vittima.
- Evidenziate gli elementi dell'e-mail che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

1. Creare uno scenario

Ai fini del nostro esempio lo scenario che ho immaginato è quello di ricevere una mail da un servizio di cloud storage. Servizi come Dropbox sono molto utilizzati in contesti aziendali (e non) per la condivisione di documenti tra colleghi. Per rendere il tutto più verosimile, supponendo che ci sia già stata una fase di information gathering, si potrebbero usare nomi reali (come mittente e destinatario) di dipendenti dell'azienda target. Questo sarebbe un caso di **spear phishing**, in quanto avrebbe come bersaglio individui specifici, o un gruppo ristretto, in una specifica organizzazione.

L'obiettivo della mail è quello di ottenere le credenziali di accesso di un utente (nome utente e password) al servizio Dropbox, utilizzando il link presente nella mail per redirezionare l'utente ignaro su una falsa pagina di login Dropbox.

2. Scrivere l’e-mail di phishing

Oggetto: [Nuovo documento condiviso] Mario Bianchi ha condiviso un file con te su Dropbox

Mittente: noreply@dropbox-share.net
Data: 2 maggio 2025, 11:20
A: luca.verdi@gmail.it

Ciao Luca,

Hai ricevuto un nuovo documento importante da Mario Bianchi. Per visualizzare il file, accedi al tuo spazio Dropbox cliccando sul pulsante qui sotto:

📄 **Visualizza Documento**

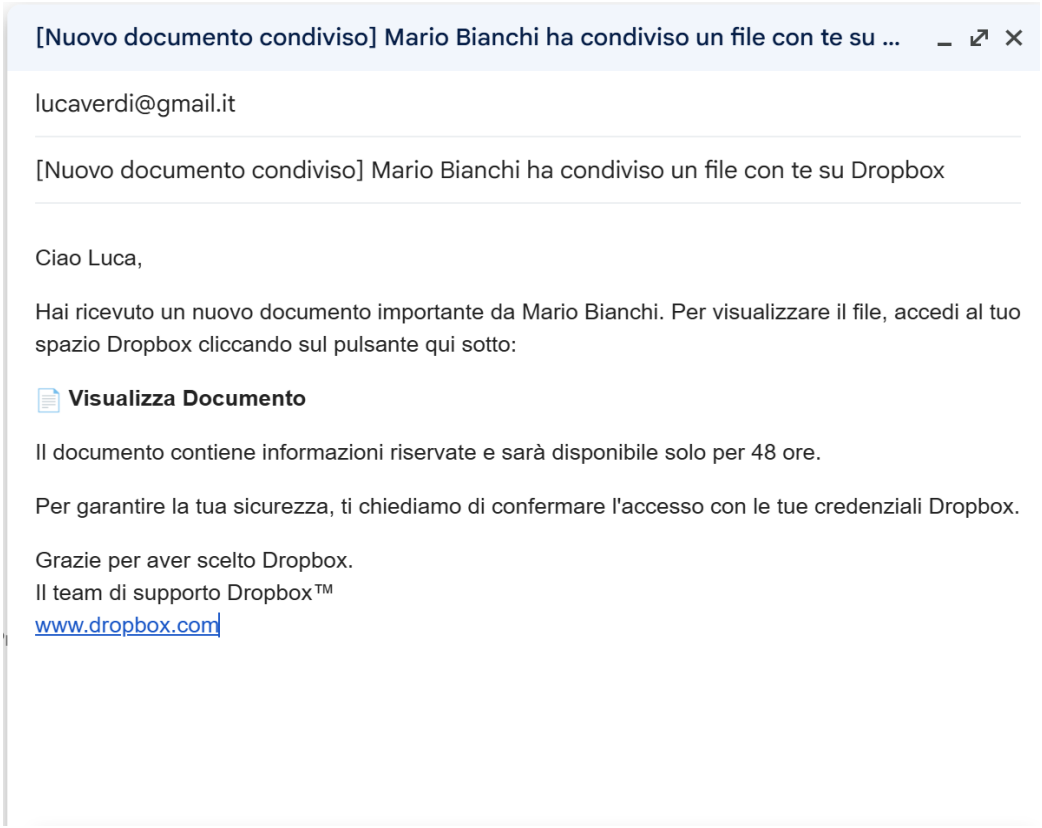
*(http://dropbox-share-access-document.net/verify)

Il documento contiene informazioni riservate e sarà disponibile solo per 48 ore.

Per garantire la tua sicurezza, ti chiediamo di confermare l'accesso con le tue credenziali Dropbox.

Grazie per aver scelto Dropbox.
Il team di supporto Dropbox™
www.dropbox.com

*questo è un esempio del link di redirezionamento cliccando su “Visualizza Documento”



3. Spiegare lo scenario

Con l'aiuto di ChatGPT abbiamo creato una mail che potrebbe sembrare verosimile ad un occhio inesperto. In questo scenario di **spear phishing** abbiamo i nomi reali (presupponendo una precedente fase di information gathering) di due dipendenti dell'azienda target. Abbiamo simulato che il mittente, Mario Bianchi, abbia condiviso un file, mediante l'utilizzo di Dropbox, con il destinatario Luca Verdi. In questo caso, il reale target del phishing è proprio Luca Verdi.

Qualora Luca Verdi aprisse la e-mail e cliccasse su "Visualizza Documento" verrebbe reindirizzato su una falsa pagina di login Dropbox, dove, qualora inserisse il suo nome utente e password, gli verrebbero sottratti i suoi dati di accesso.

Una volta ottenuti i dati di accesso, l'attaccante potrebbe usufruire di documenti aziendali riservati, dati personali e/o sensibili, informazioni contenute in cartelle condivise. Inoltre, potrebbe tentare di accedere ad altri servizi utilizzando le stesse credenziali, dato che mediamente si tende ad utilizzare le stesse credenziali per diversi servizi.

Chiaramente, più sarà stata accurata la fase di information gathering e più questo tentativo di **spear phishing** potrà risultare verosimile per la vittima.

Supponendo che i nomi utilizzati siano reali e che la condivisione di file mediante l'uso di Dropbox sia una pratica comune all'interno dell'azienda, la percentuale di successo della mail è elevata. La percentuale potrebbe incrementare ulteriormente qualora fossimo a conoscenza di un reale scambio previsto tra Mario Bianchi e Luca Verdi, e l'aspettativa di quest' ultimo di ricevere un file.

Inoltre, la e-mail è scritta in maniera professionale, con layout e linguaggio coerenti con quelli di veri servizi online.

Tuttavia, nella mail sono anche presenti elementi che dovrebbero far scattare un campanello di allarme.

Primo fra tutti è sicuramente quello della pressione temporale. Questo è un elemento comune a molte e-mail di phishing. La natura disonesta di queste mail cerca di far leva sull'urgenza e di lasciare il minor tempo possibile alla vittima di pensare o di verificare meglio le informazioni

Inoltre, il link di direzionamento (`http://dropbox-share-access-document.net/verify`) non è quello ufficiale di dropbox (`dropbox.com`).

È anche inverosimile che un servizio come Dropbox ci chieda di fare login per la visualizzazione di un file, soprattutto se si è già connessi.

L'uso improprio del marchio ™ può essere un ulteriore campanello di allarme.

Infine, anche la mail del mittente, per quanto possa essere ben contraffatta, non rispecchierà mai quella ufficiale