Esercizio del Giorno: Simulazione di un'Email di Phishing

INDICE

1. Creazione e introduzione allo scenario
   Lo scenario che ho chiesto a chatgpt, è quella di una mail phishing da parte di un collega, da cui abbiamo raccolto informazioni in precedenza, verso un altro e, più avanti magari a tutti i suoi colleghi. Ho scelto questo perché mi sembrava essere la migliore tra la mail di notifica bancaria e un'email di un fornitore di servizi, dato che quest'ultimi sono più comuni e quelle a cui le persone ormai stanno iniziando a non abboccare più. Quindi, chatgpt mi ha creato questa mail, durante un periodo di lavoro in cui viene chiesta una firma, prima di poter mettere la firma però, vengono chieste le credenziali aziendali per accedere al sito, l'obiettivo della mail mandata sono le credenziali, che ci saranno date e, anche delle informazioni personali sulla vittima e, magari con una sessione di raccolta informazioni riuscire a ricavare anche qualcosa di più.
2. Mail phishing
   La mail che ci è stata creata è la seguente:

Oggetto: Urgente: Firma documento e aggiorna le tue credenziali per completare il progetto

Corpo del messaggio:

Ciao [Nome],
Abbiamo bisogno che tu firmi un documento molto importante per il progetto su cui stiamo lavorando. Il documento è pronto per la firma, ma prima di poterlo firmare, ti chiediamo di confermare le tue credenziali aziendali per motivi di sicurezza e aggiornamento. È urgente che lo faccia entro oggi, così possiamo procedere con la prossima fase.

Passaggi da seguire:

1. Clicca sul link sottostante per firmare il documento.
2. Inserisci il tuo nome utente e password aziendali per confermare la tua identità.
3. Completa la verifica delle tue informazioni personali, incluse la tua data di nascita e indirizzo, per garantire la tua sicurezza.

[Link per firmare il documento e aggiornare le tue credenziali]

Se hai domande o problemi nell’aprire il documento o completare il processo, fammi sapere subito. È fondamentale che tu segua questa procedura rapidamente per evitare interruzioni nel progetto.

Grazie mille per la tua collaborazione,
[Nome del collega]
[Posizione del collega]

3. Codice HTML
   Questa è la mail in questione, i oltre ho anche chiesto a chatgpt di crearmi il codice html di questa mail, così da poterla riutilizzare su gophish

```
<!DOCTYPE html>
<html lang="it">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Firma Documento e Aggiorna le Tue Credenziali</title>
</head>
<body style="font-family: Arial, sans-serif; color: #333;">
  <p>Ciao <strong>[Nome]</strong>,</p>
  <p>Abbiamo bisogno che tu firmi un documento molto importante per il progetto su cui stiamo lavorando. Il documento è pronto per la firma, ma prima di poterlo firmare, ti chiediamo di confermare le tue credenziali aziendali per motivi di sicurezza e aggiornamento. È urgente che lo faccia entro oggi, così possiamo procedere con la prossima fase.</p>

  <h3>Passaggi da seguire:</h3>
  <ol>
    <li><strong>Clicca sul link sottostante per firmare il documento.</strong></li>
    <li><strong>Inserisci il tuo nome utente e password aziendali</strong> per confermare la tua identità.</li>
    <li>Completa la verifica delle tue <strong>informazioni personali</strong>, incluse la tua data di nascita e indirizzo, per garantire la tua sicurezza.</li>
  </ol>

  <p><a href="[link]" style="color: #007BFF; text-decoration: none;">[Link per firmare il documento e aggiornare le tue credenziali]</a></p>

  <p>Se hai domande o problemi nell'aprire il documento o completare il processo, fammi sapere subito. È fondamentale che tu segua questa procedura rapidamente per evitare interruzioni nel progetto.</p>
```

```
  <p>Grazie mille per la tua collaborazione,</p>
  <p><strong>[Nome del collega]</strong><br>
  [Posizione del collega]</p>
</body>
</html>
```

4. Elementi sospetti da analizzare e che potrebbero far scattare il campanello di allarme

- **Richiesta di credenziali**: Un messaggio che ti chiede di inserire il tuo nome utente e password aziendali su un sito esterno è un chiaro segno di phishing.
- **Informazioni personali**: La richiesta di altre informazioni personali, come la data di nascita o l'indirizzo, è sospetta.
- **Link sospetto**: Il link "Link per firmare il documento e aggiornare le tue credenziali" porta a un URL sconosciuto e sospetto. Un vero documento aziendale sarebbe probabilmente ospitato su un dominio aziendale ufficiale o su una piattaforma sicura come Google Drive o Microsoft OneDrive.
- **Richiesta urgente**: La parola "urgente" è spesso utilizzata nelle email di phishing per indurre l'utente a cliccare senza riflettere troppo. La pressione temporale è un modo comune per ridurre la vigilanza dell'utente. Inoltre il collega non spiega perché è così urgente firmare il documento. Un collega reale avrebbe probabilmente fornito una motivazione più chiara e dettagliata.
- **Messaggio generico e mancanza di dettagli**: Il messaggio è vago e non fornisce dettagli concreti sul documento (come il nome del file, il tipo di documento o il motivo per cui è necessario firmarlo). Un vero collega avrebbe specificato meglio di cosa si trattava.
- **Tono informale**: Il tono amichevole e informale potrebbe sembrare autentico, ma le email di phishing spesso usano questo approccio per "abbassare le difese" e fare sembrare la comunicazione più credibile.
- **Assenza di altri metodi di contatto**: In un'email legittima, un collega avrebbe potuto includere anche altri dettagli di contatto o offrire un numero di telefono per risolvere eventuali problemi. In questo caso, manca qualsiasi informazione aggiuntiva utile.

5. Conclusioni

In conclusione possiamo dire che la mail, per una persona che non è molto informata sul phishing, risulta essere molto convincente, sopratutto perché si ritroverebbe davanti una mail di un suo collega, che era stato hackerato molto prima all'insaputa di tutti e anche perché la vittima in questione non riuscirebbe ad accorgersi degli elementi sospetti all'interno di essa.
Però se la mail venisse ricevuta da una persona informata sul phishing, noterebbe alcuni elementi sospetti che abbiamo elencato in precedenza, usufruendo così delle sue conoscenze, competenze e formazioni, al fine di evitare quella mail e prendere le precauzioni giuste.