Gophish

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

Istruzioni:

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.

Fattura Pendente - URGENTE

Posta in arrivo ×

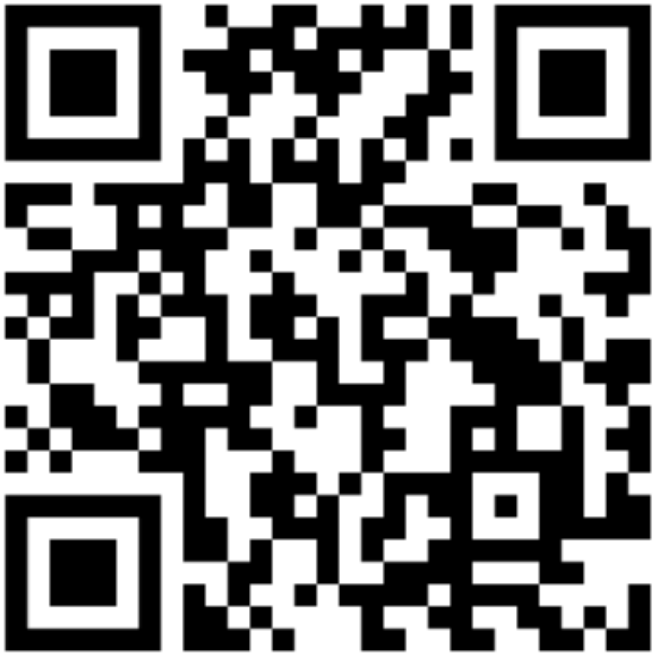
d3.dngst3@gmail.com
a me

Gentile Cliente,

Abbiamo notato che la Sua ultima fattura non è stata saldata e risulta ancora pendente. Questo potrebbe causare l'interruzione del servizio se non viene saldata entro le prossime 24 ore. Ci teniamo a garantire la continuità del servizio e La invitiamo a regolarizzare il pagamento il prima possibile.

Numero Fattura: 389173
Importo: € 68,00
Scadenza: Immediata

Per saldare l'importo, La preghiamo di scansionare il codice QR qui sotto e seguire le istruzioni riportate sulla pagina di pagamento.



IMPORTANTE: Ignorando questa notifica, procederemo con la sospensione temporanea del servizio. La preghiamo di agire immediatamente.

Grazie per la collaborazione,
Gemini Luce - Assistenza Clienti
Email: assistenza@gemini-luce.it
Tel.: 800 123 456

Un allegato • Scansione eseguita da Gmail ⓘ

qr

Per la realizzazione di questo compito, ho chiesto a ChatGPT di crearmi un template per l'invio di una mail fittizia dove si informa un ipotetico cliente del mancato pagamento di una fattura della luce per un importo di 68,00€.

Da: assistenza@gemini-luce.it
Oggetto: Fattura Pendente - URGENTE

Gentile Cliente,

Abbiamo notato che la Sua ultima fattura non è stata saldata e risulta ancora **pendente**. Questo potrebbe causare l'interruzione del servizio se non viene saldata entro le prossime 24 ore. Ci teniamo a garantire la continuità del servizio e La invitiamo a regolarizzare il pagamento il prima possibile.

Numero Fattura: 389173
Importo: € 68,00
Scadenza: Immediata

Per saldare l'importo, La preghiamo di **scansionare il codice QR** qui sotto e seguire le istruzioni riportate sulla pagina di pagamento.

![QR Code]

IMPORTANTE: Ignorando questa notifica, potremmo procedere con la sospensione temporanea del servizio. La preghiamo di agire immediatamente.

Grazie per la collaborazione,
Gemini Luce - Assistenza Clienti
Email: assistenza@gemini-luce.it
Tel.: 800-123-456

Dopo la creazione del template, ho installato gophish su kali, e ho impostato i vari parametri per l'invio della mail. Sono tornato su chatgpt, e gli ho chiesto di trasformare il codice in forato html e aggiungere uh po' di html per renderlo più reale.

Questo è il codice generato da ChatGPT, ho creato un codice qr, che ho aggiunto su Drive, e ho chiesto a ChatGPT di aggiungerlo cosi che i clienti potessero effettuare il pagamento di tale fattura solamente scannerizzando il codice.

```
<!DOCTYPE html>
<html lang="it">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Gentile Cliente - Fattura Pendete</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f2f2f2;
      margin: 0;
      padding: 0;
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
    }
    .container {
      background: white;
      padding: 20px;
      border-radius: 5px;
      box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
      max-width: 500px;
      text-align: left;
    }
  </style>
</head>
<body>
  <div class="container">
    <h2>Gentile Cliente,</h2>
    <p>Abbiamo notato che la Sua ultima fattura non è stata saldata e risulta ancora pendente. Questo potrebbe causare l'interruzione del servizio se non viene saldata entro le prossime 24 ore. Ci teniamo a garantire la continuità del servizio e La invitiamo a regolarizzare il pagamento il prima possibile.</p>

    <p>Numero Fattura: 389173<br>
    Importo: € 68,00<br>
    Scadenza: Immediata</p>

    <p>Per saldare l'importo, La preghiamo di scansionare il codice QR qui sotto e seguire le istruzioni riportate sulla pagina di pagamento.</p>

    <!-- Codice QR integrato -->
    <img src="https://drive.google.com/uc?id=1juuZO6QX7wfb2MZd-vgblgqkquH-xu5M" alt="Codice QR per il pagamento" style="width: 100%; height: auto;">

    <p><strong>IMPORTANTE:</strong> Ignorando questa notifica, procederemo con la sospensione temporanea del servizio. La preghiamo di agire immediatamente.</p>

    <p>Grazie per la collaborazione,<br>
    Gemini Luce - Assistenza Clienti<br>
    Email: assistenza@gemini-luce.it<br>
    Tel.: 800 123 456</p>
  </div>
</body>
</html>
```

Una volta impostato i vari parametri ho inviato la mail e scannerizzato il codice, il risultato del codice vi invito a verificarlo voi stessi :D .

Punti di credibilità:

Fattura Pendente - URGENTE crea un senso di urgenza e preoccupazione nel destinatario, spingendolo ad agire rapidamente.

Il tono formale e professionale dell'email contribuisce a rafforzare l'impressione di legittimità.

Riferimento a un servizio specifico: Il riferimento a una fattura pendente e alla possibile interruzione del servizio crea un senso di familiarità per coloro che hanno contratti con fornitori di servizi.

L'inserimento di un numero di fattura, un importo esatto e una scadenza imminente rende l'email più credibile.

Il codice QR aggiunge un tocco di modernità e semplicità al processo di pagamento, invitando il destinatario a seguire le istruzioni.

Punti non credibili:

L'email è generica e non contiene alcun riferimento personalizzato al destinatario (nome, cognome, dettagli specifici del contratto).

Non è presente l'allegato con la fattura pendente.

Manca logo aziendale, e la mail è spoglia.

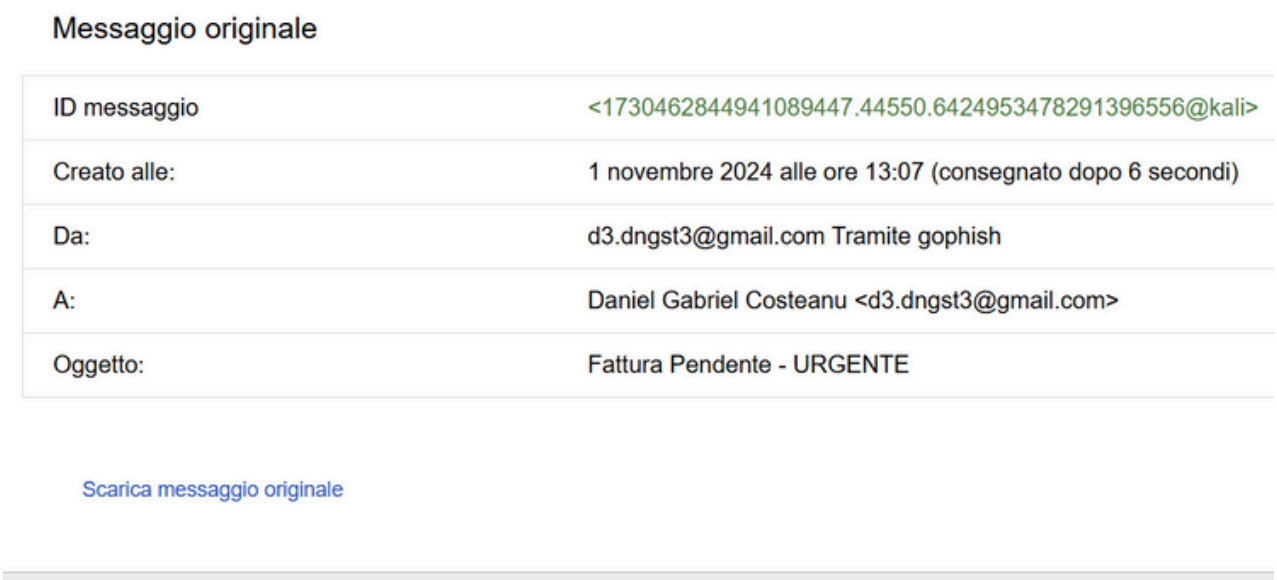
Non è presente nessun link che conduce alla pagina dell'azienda.

Inoltre come abbiamo visto nell'ultima lezione, l'assenza di verifiche dei 3 protocolli:

- SPF (Sender Policy Framework): Verifica che il server di invio dell'email sia autorizzato a inviare email per conto del dominio del mittente. Controlla l'indirizzo IP del server di invio contro un elenco di indirizzi IP autorizzati specificato nel record SPF del dominio.

- DKIM (DomainKeys Identified Mail): Aggiunge una firma digitale all'intestazione dell'email, permettendo al destinatario di verificare che l'email non sia stata alterata durante il transito e che provenga realmente dal dominio dichiarato. La firma viene generata utilizzando una chiave privata e può essere verificata con una chiave pubblica pubblicata nel DNS del dominio.

- DMARC (Domain-based Message Authentication, Reporting & Conformance): Si basa su SPF e DKIM e permette ai proprietari dei domini di specificare come gestire le email che non superano le verifiche SPF e DKIM. DMARC consente anche di ricevere report sulle email che falliscono le verifiche, fornendo così visibilità sulle potenziali frodi.



Messaggio originale

ID messaggio	<1730462844941089447.44550.6424953478291396556@kali>
Creato alle:	1 novembre 2024 alle ore 13:07 (consegnato dopo 6 secondi)
Da:	d3.dngst3@gmail.com Tramite gophish
A:	Daniel Gabriel Costeanu <d3.dngst3@gmail.com>
Oggetto:	Fattura Pendente - URGENTE

Scarica messaggio originale