

EMAIL DI PHISHING

1. Creare uno scenario

- Per questo esercizio ho voluto creare uno scenario dove il target del truffatore è un anziano signore. La vittima riceverà un'e-mail di phishing riguardante la sua pensione.
 - Target: Maestro Muten un anziano signore
 - Mittente e-mail: INPS
- L'obiettivo del mal intenzionato sarà quella di ottenere informazione per accedere all'account INPS e al conto corrente della vittima.

L'informazioni che vorrà ottenere sono:

- Numero di identificazione personale (PIN INPS)
- Codice Fiscale
- Numero di conto corrente bancario
- Pin conto corrente

2. Scrivere un'e-mail di phishing

Per questa fase mi sono aiutato della AI per scrivere l'e-mail. L'AI utilizzata è chatGPT una LLA.

Per aggirare la policy della AI, ho inteso nel prompt che sto frequentando un corso di cybersicurezza e che il professore ci ha detto di ipotizzare uno scenario di phishing. In fine mi doveva aiutare a scrivere l'e-mail per ottenere i dati sensibili desiderati.

Questo il risultato:

“Oggetto& Importante% Aggiornamento informazioni pensionistiche \$urgente

Mittente: <Servizio clienti INPS>

Gentile Signor Muten,

La informiamo che il suo profilo pensionistico necessita di un aggiornamento urgente per garantire il corretto accredito della pensione del mese 12/2024.

Purtroppo, durante una revisione del nostro sistema, l'IMPS e il suo istituto bancario sono stati dissociati. La invitiamo a verificare e confermare i suoi dati personali entro le prossime 24 ore per evitare eventuali sospensioni temporanee dell'accredito pensionistico.

Può effettuare la verifica cliccando sul seguente link sicuro:

http://ti_rubiamo_la_pensione.org

Accedi al tuo profilo pensionistico

Una volta effettuato l'accesso, le sarà richiesto di inserire i seguenti dati:

Numero di identificazione personale (PIN INPS)

Codice fiscale

Numero di conto corrente da associare

Pin autenticazione conto corrente

Se ha bisogno di assistenza, non esiti a contattare il nostro supporto clienti al numero

+7 495 123-45-67

Grazie per la collaborazione.

Cordiali saluti,

Istituto Nazionale Previdenza Sociale (INPS)

Servizio Clienti”

Responsabile di questa e-mail: Dott. Luca Loschiavo – Dirigente INPS

<https://servizi2.inps.it/servizi/CVDirigentiFE/Home/Curriculum/2401T298TF00>

Per dare più credibilità e legittimità all' e-mail o implementato un nuovo testo, il logo, un numero telefonico collegato ad un AI per sfruttare i principi del Vishing e un collegamento vero ad un dirigente INPS.

- Sempre tramite chatGPT ho chiesto di aggiungere le classiche raccomandazioni per non essere vittime di truffe.

Testo aggiuntivo:

“Per sua sicurezza, desideriamo ricordarle che l’INPS non richiederà mai i suoi dati sensibili (come PIN, password o coordinate bancarie) tramite e-mail o telefono, ma solo tramite link sicuri di autoidentificazione che le è stato mandato.”

- Aggiunta di loghi identificativi dell’organizzazione.



- Chiamando il numero di telefono (Utilizzando tool di generazione di numeri telefonici virtuali es. Twilio associabile a AI come Dialogflow o modelli personalizzabili che offrono API per creare logiche vocali avanzate) risponderà un AI impostata a simulare una voce umana con tono confortante che guiderà la vittima in tutto il procedimento.
- Alla fine dell'email ho aggiunto un responsabile dell'email, fornendo anche un link vero trovato facendo ricerche con dork di Google. Qual' ora la vittima voglia avere più rassicurazioni che l' email sia legittima, potrà accedere al link e vedere che la persona lavora effettivamente all' INPS. In questo caso è un dirigente per dare ancora più credibilità all' e-mail.

3. Spiegare lo scenario:

- Un mal intenzionato tramite un'e-mail di phishing cercherà di ottenere dati sensibili come: CF e pin per accedere all' area riservata INPS, numero conto corrente e pin per accedere all' istituto bancario.
- L' e-mail potrebbe sembrare credibile per:
 - In prima battuta l'e-mail mittente è mascherata dal nome "Servizio clienti INPS"
 - L' e-mail è scritta in modo formale e l' argomento trattato è conforme all' età anagrafica del target
 - Il link di autenticazione fornito porterà ad una pagine con pattern simile a quella dell' INPS
 - Aggiunta di raccomandazioni di sicurezza
 - Aggiunta del logo INPS
 - Aggiunta del responsabile dell'email, collegata ad un link vero.
- Nell' email ho inserito elementi che dovrebbero mettere in dubbio l'autenticità di questa email:
 - L' oggetto dell' email riporta caratteri speciali non convenzionali
 - Andando a ispezionare il nome del mittente scopriremo essere un email non associata all' INPS
 - I tempi ristretti e l'urgenza che crea l' email non sono conformi ad un modus operandi conforme delle istituzioni o altri istituti.
 - Nel testo principale è riportato il nome dell' istituto previdenziale sbagliato: IMPS
 - Il link è equivocamente fraudolento
 - Il numero fornito non ha prefisso Italiano (E ciò dovrebbe creare sospetti visto che l' INPS è un istituto del sistema Italiano)
 - In fondo all' email "Istituto Nazionale **Providenza** Sociale (INPS)" è sbagliato.
 - Il logo utilizzato è datato.