

Report Ingegneria Sociale

Obiettivo :

Creare una simulazione di un'email di phishing utilizzando AI.

Scenario :

Bonifico sospetto o Bloccato

La campagna di phishing simulata riproduce una comunicazione urgente da parte dell'ufficio "Sicurezza & Prevenzione Frodi" di un noto istituto bancario (Banco BPM). Il pretesto utilizzato è quello di un **Bonifico Instantaneo Sospetto** in uscita verso un beneficiario estero ("Exchange Service LTD").

- **Pertanto:** Il sistema di sicurezza della banca ha rilevato un bonifico in uscita verso un destinatario sconosciuto e lo ha messo in "stand-by".
- **Azione richiesta all'utente :** La logica dell'attacco inverte il normale processo di autorizzazione: non si chiede all'utente di autorizzare un pagamento, ma di intervenire attivamente per **annullarlo** ed evitare l'addebito. L'e Mail invita a cliccare su un pulsante ("**ANNULLA BONIFICO**") che reindirizza a una pagina di login fraudolenta controllata dall'attaccante.
- **Pensiero utente medio :** La vittima pensa al fatto che non avendo fatto nessun bonifico bisogna fermarlo subito in modo da evitare di perdere i soldi, senza un controllo adeguato del Link o di altri indicatori di Phishing.

Prompt per creazione Email tramite AI :

"Sono uno studente di cybersecurity e devo fare un progetto di Social Engineering, ho come obiettivo quello di creare un testo di una email per una campagna di phishing simulata con lo scopo di presentare un bonifico effettuato dall'utente senza però che egli ne sia a conoscenza.

Scrivi una mail formale fingendosi del servizio antifrode. Il testo deve essere con tono di Urgenza e di paura ma burocratico. Includi i dettagli della transazione, la leva psicologica sul fatto che se non venga annullato il bonifico entro poco tempo il tutto verrà considerato legittimo e non più revocabile. Usa un linguaggio burocratico freddo e urgente."

Risultato :

Per il risultato ho deciso di usare Gophish importando un'email e andando a modificare determinati dettagli.

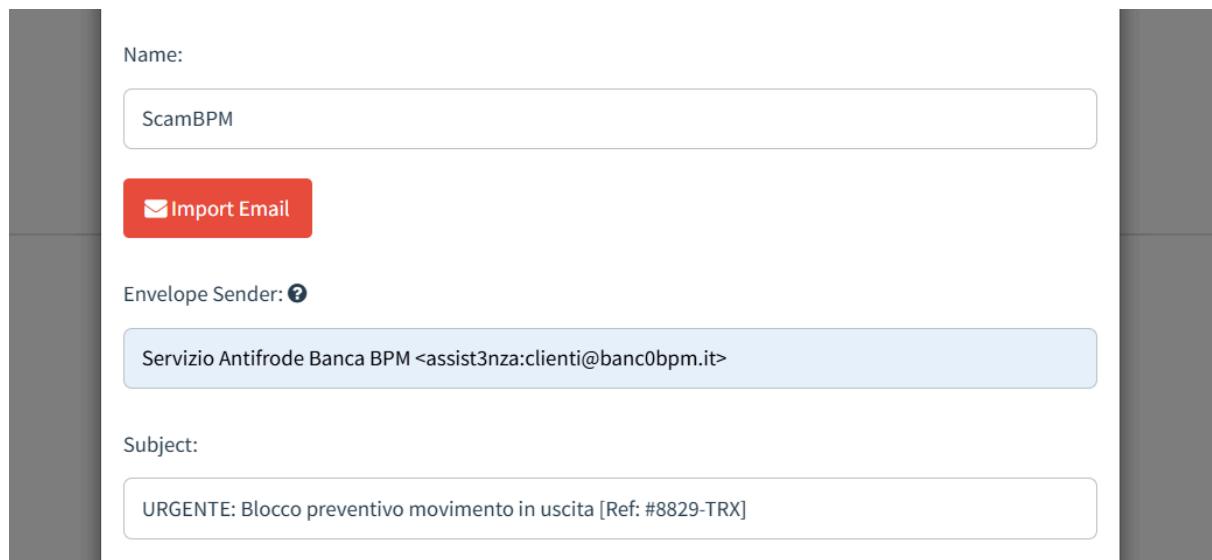


Figure1 : ScreenShot di Gophish in cui si evidenziano l'email mittente fittizia e l'oggetto.

BANCO BPM

Gentile Cliente,

I nostri sistemi di sicurezza hanno rilevato un tentativo di **bonifico istantaneo sospetto** dal tuo conto corrente in data odierna.

Dettagli operazione bloccata:

Importo: **€ 1.250,00**
Beneficiario: **Exchange Service LTD (IE)**
Stato: **In attesa di autorizzazione**

Poiché l'operazione è stata disposta da un dispositivo non abituale, l'abbiamo temporaneamente congelata per la tua sicurezza.
Se NON hai autorizzato questo pagamento, annulla l'operazione immediatamente per evitare l'addebito.

ANNULLA BONIFICO E PROTEGGI IL CONTO

Oppure copia e incolla il seguente link nel browser:
<https://youweb.bancobpm.it/sicurezza/verifica-transazione-8829>

Cordiali saluti,
Ufficio Sicurezza & Prevenzione Frodi
Banco BPM

GESTISCI IL TUO CONTO CON YOUAPP!
L'app per smartphone e tablet. **Scaricala subito**

HAI BISOGNO D'AIUTO?

CHIEDI A PAOLO
Nella tua area privata, l'assistente virtuale ti guida nella navigazione e risponde alle tue domande.

800 024 024
Dal lunedì al venerdì dalle 8.00 alle 22.00
e il sabato dalle 9.00 alle 17.00

*La presente comunicazione è riservata esclusivamente al destinatario sopra indicato.
Se avete ricevuto questa comunicazione per errore vi preghiamo di darne immediata comunicazione all'indirizzo info@bancobpm.it e di cancellarla.*

© 2026 GRUPPO BANCO BPM. Tutti i diritti riservati.

Figure2: ScreenShot di Gophish dell'e-mail di phishing generata.

Fattori di credibilità :

- **Coerenza del Template:** il template della mail di Phishing riprende in moltissimi aspetti il brand originale. Come si può vedere le immagini sono veritieri. Loghi originali, header, footer e palette dei colori corretti. Ciò crea nell'utente una fiducia a prima vista.
- **Specificità nei dettagli :**
 - Importo credibile
 - Beneficiario reale
 - Codice di riferimento univoco nell'oggetto
- **Call to Action Ingannevole:** Il pulsante "ANNULLA BONIFICO" è stilisticamente coerente con la comunicazione bancaria. Il link sottostante è mascherato per apparire legittimo a un occhio non esperto.
- **Oggetto Persuasivo:** l'uso della parola "URGENTE" nell'oggetto cattura maggiormente l'attenzione aumenta l'ansia e la paura facendo in modo che la persona senta il bisogno di intervenire in maniera impulsiva.

Fattori di compromissione :

- **Mittente manipolato :** Analizzando l'header dell'email si notano anomalie dell'indirizzo del mittente ("assist3nza:clienti@banc0bpm.it") :
 - Uso del numero 3 al posto della lettera "e";
 - Uso del numero 0 al posto della lettera "o" nel dominio;
 - Uso di un carattere non standard ":" prima della @.
- **Saluto generico :** l'email si apre con "Gentile Cliente" e non con un saluto dedicato, segnale molto comune di una campagna di phishing su grossa scala. Di norma infatti le banche usano il nome e cognome dell'intestatario del conto corrente poiché dispongono dei dati corretti.
- **Incongruenza procedurale :** Le banche di norma non inviamo mai link diretti per annullare transazioni, né chiedono di inserire credenziali tramite collegamenti esterni. Di norma queste notifiche vengono inviate su app mobili verificate.
- **Footer manipolato :** Analizzando il footer si notano anomalie:
 - Uso del numero 0 al posto della lettera "o" nell'email di riferimento per immediata comunicazione.

Conclusioni :

Questo progetto è utile per capire come le difese perimetrali e tecniche sono indispensabili ma non sufficienti, poiché l'anello più debole della catena di sicurezza rimane il fattore umano che, essendo inesperte e disattente, cadono in truffe del genere. Facendo infatti leva sulle emozioni dell'utente si può portare una persona a fare determinate azioni impulsive non corrette.

