Creiamo una simulazione di un'email di phishing utilizzando ChatGPT.

1. Fase preliminare: Come sapere che il cliente ha Intesa Sanpaolo

Un attaccante può raccogliere questa informazione in diversi modi:

1. **Doxing o social engineering**: Osservare post pubblici sui social (es. lamentele su servizi bancari).
2. **Email compromessa**: Se l'attaccante ha accesso alla casella email della vittima (anche solo per pochi minuti), può cercare email ricevute da Intesa Sanpaolo.
3. **Phishing precedente**: Una campagna generica potrebbe aver raccolto info da chi ha cliccato su un link ("Seleziona la tua banca").
4. **Data breach o dark web**: Informazioni vendute online da altre violazioni.

2. Scenario scelto

- **Contesto**: Email da Intesa Sanpaolo per **conferma urgente di un bonifico non autorizzato**.
- **Obiettivo del phishing**: Rubare le credenziali di accesso all'home banking.

3. Analisi dello scenario

Perché l'email può sembrare credibile:

- Il messaggio è formale e simula il tono reale delle comunicazioni bancarie.
- Il contenuto crea panico (bonifico non autorizzato di quasi 1000€).
- Invita a cliccare per "bloccare", sfruttando l'urgenza emotiva.

Elementi tipici del phishing:

- **Urgenza estrema** (tempo limite di 2 ore).
- **Link sospetto** (il dominio è falso: intesa-verifica-servizi.com).
- **Importo preciso e alto ma non troppo**, per aumentare l'impatto e creare credibilità.
- Potenziali **errori lievi di linguaggio** ("Lei" non sempre maiuscolo, un dettaglio che un'azienda curerebbe).

Nota tecnica

Nel corpo dell'email saranno **intenzionalmente inseriti piccoli errori ortografici e stilistici**, per riflettere i tratti distintivi delle reali email di phishing.

4. Indirizzo del mittente (visibile al cliente)

Un attaccante **non può inviare email realmente da** @intesasanpaolo.com, ma può **falsificare** (spoofare) l'indirizzo o **usarne uno simile** per trarre in inganno.

Esempi realistici di indirizzi che potrebbero apparire al cliente:

Tipo	Esempio di mittente visibile	Note
Falsificato (spoofed)	servizio.clienti@intesasanpaolo.com	Appare autentico, ma richiede un server mal configurato o vulnerabilità DNS (molto rischioso e difficile da realizzare su larga scala oggi).
Simile (truffaldino)	intesa.clienti@supporto-sicurezza.com	Dominio diverso ma costruito per sembrare legittimo.
Ingannevole (con nomi simili)	notifiche@intesasanpaIo.it *(nota: la "L" è una i maiuscola "I")*	Tecnica tipografica per ingannare visivamente.
Generico ma "credibile"	avvisi@banche-online.it	Non riconducibile a Intesa, ma inserito in un messaggio costruito bene può trarre in inganno.

L'email che il cliente riceverà oggi sarà da **notifiche@intesasanpaIo.it.**

Come l'utente può accorgersene

- Guardando **l'indirizzo reale**, non solo il nome visualizzato (es. "Intesa Sanpaolo Servizi").
- Passando il mouse sul **link** contenuto nel messaggio per vedere il vero URL.
- Controllando **piccoli errori** nel dominio (es. .co, .it al posto di .com, lettere simili, ecc.).

Email di phishing (falsa notifica Intesa Sanpaolo)

Oggetto: POSTA CERTIFICATA - Conferma Avvenuto Pagamento
Mittente: notifiche@intesasanpaIo.it
A: Mattaluciano@gmail.com

Gentile Cliente,
La informiamo che in data **02/05/2025** è stato eseguito con successo un **bonifico SEPA** dal Suo conto corrente, per un importo pari a **960,00 €**.

In allegato trova il **documento PDF** con i dettagli dell'operazione.

Se **lei ha autorizzato il pagamento**, non è richiesta alcuna azione.

Se **non ha autorizzato** tu questa operazione, la invitiamo a bloccare tempestivamente il bonifico tramite il nostro **portale di sicurezza dedicato**:

Accedi per bloccare l'operazione

Attenzione: ha a disposizione **solo 2 ore** per richiedere modifiche o l'annullamento dell'operazione, prima che l'importo venga trasferito in modo definitivo.

Cordiali saluti,
Servizio Clienti Intesa Sanpaolo

Il PDF allegato è un documento reale, reperito online e successivamente modificato da me tramite Photoshop per includere tutti i dati del cliente. Tuttavia, presenta alcuni piccoli errori che un occhio attento potrebbe individuare: sono evidenziati in rosso

INTESA SANPAOLO

LA BANCA HA PRESO IN CARICO IL SUO BONIFICO

Numero ordine INTER20160104BOSBE648852832 - Data ordine 02.05.2025

Conto corrente di addebito
1000/8589

Ordinante
Matta Luciano

Beneficiario
Insieme Salute Societa' Di Mutuo Soccorso
Piazza Di Pietra 26-Roma-Italia

IBAN
IT39 C030 6905 0201 0000 0014 907

BIC/SWIFT
BCITITMMXXX

Banca
Intesa Sanpaolo 2 **- Roma - Via Del Corso 226 - Via Del Corso, 226**

TRN
03069977711379084803200032001T

Data regolamento
02.05.2025

Data contabile ordinante
02.05.2025

Data valuta ordinante
02.05.2025

Descrizione - Causale
rinnovo contributo associativo 2025

Debitore effettivo
Luciano Matta

Creditore effettivo

Identificativo bonifico

Tipologia

Importo
960,00 Euro

Commissioni
0,00 Euro

Totale operazione
960,00 Euro

L'operazione sarà eseguita al cut-off delle ore 17:30 del 02.05.2025. Sarà possibile revocare la disposizione fino alle ore 17:29 del 02.05.2025 cliccando su

L'operazione potrebbe essere conteggiata e assoggettata al pagamento del "Costo unitario per operazione" secondo le modalità concordate in sede di stipula del contratto di conto corrente e/o di successive variazioni concordate, nel quale potrà trovare ogni dettaglio in proposito. In sede di liquidazione periodica di queste spese potrà verificare il dettaglio dei conteggi, che viene esposto all'interno del Suo estratto conto di conto corrente, alla voce "Spese" della sezione "Dettaglio competenze di chiusura".

Le operazioni disposte nelle giornate festive si considerano ricevute il primo giorno lavorativo seguente.

Pagina 1 di 1

Nota tecnica

Il corpo del PDF presenta volutamente errori ortografici e discrepanze visive, studiati per simulare in modo credibile i segni distintivi di una falsificazione documentale.

5. Analisi degli errori nel PDF allegato

Nel documento PDF allegato emergono **tre errori chiave** che ne rivelano la natura contraffatta:

1. **Intestazione errata dell'istituto bancario**
   Nell'intestazione compare la dicitura "*Intesa Sanpaolo 2*", che è anomala e imprecisa. La corretta denominazione, come da registro ufficiale, è **"Intesa Sanpaolo S.p.A."**.
   Questo tipo di errore è tipico nei documenti falsificati, dove l'autore — probabilmente un hacker — commette imprecisioni nei dettagli istituzionali, compromettendo la credibilità del documento.

2. **Disallineamento nell'importo numerico**
   Come evidenziato nelle due caselle rosse, l'importo "**960,00 €**" mostra un lieve disallineamento grafico tra le prime tre cifre ("960") e i decimali ("00").
   Questo difetto grafico suggerisce una **manipolazione del documento**, probabilmente effettuata tramite software di grafica o editor PDF.
   Gli strumenti di scrittura automatica tendono ad allineare in modo coerente numeri e simboli; un'anomalia di questo tipo è un chiaro segnale di editing manuale.

3. **Manomissione tipografica evidente**
   L'incoerenza tra il font o l'allineamento dei numeri può derivare dall'inserimento artificiale dell'importo nel secondo momento.
   Chi ha familiarità con programmi come **Photoshop** o editor di testo avanzati sa che l'aggiunta posticcia di cifre o parole spesso produce differenze minime ma rilevabili nel layout.
   Questo supporta ulteriormente l'ipotesi di falsificazione.

in questo caso il file da me modificato, alterato con strumenti di grafica come Photoshop, presenta chiari indicatori di manipolazione tipici dei documenti contraffatti impiegati in attività fraudolente.

6. Analisi tecnico-psicologica e recap

Il messaggio oggetto di questo studio è costruito per replicare una tipica truffa via email a tema bancario, con lo scopo di indurre la vittima a compiere un'azione impulsiva, come cliccare su un link fraudolento, senza eseguire le necessarie verifiche.

1. Leva psicologica: urgenza e perdita di controllo

Il testo si basa su una combinazione di urgenza temporale e pressione emotiva. Il riferimento a un bonifico non autorizzato di 960,00 € provoca un'immediata sensazione di allarme nel destinatario.
L'aggiunta di un limite di 2 ore per bloccare l'operazione accentua la paura di perdere denaro e di non avere il controllo della propria situazione finanziaria.

Questo mix di ansia e urgenza abbassa rapidamente le difese cognitive del lettore, inducendolo a saltare i passaggi di verifica e a cliccare sul link fornito per "bloccare" la transazione, senza accertarsi della reale autenticità del messaggio.

Uno degli effetti più insidiosi di questa pressione psicologica è che l'attenzione viene distolta dai dettagli tecnici che svelano la truffa. Ad esempio, il mittente dell'email appare come:
notifiche@intesasanpaIo.it

Tuttavia, il dominio contiene una lettera "i" sostituita con una "L" maiuscola ("PaIo" → "PaLo"), inganno che l'occhio del destinatario, sotto stress, difficilmente nota. Questo tipo di camuffamento è una tecnica comune nel typosquatting.

2. Elementi di ingegneria sociale e credibilità visiva

La struttura formale del messaggio, il lessico tecnico-bancario e la presenza di un documento PDF in allegato rafforzano la percezione di legittimità. Questi dettagli sono pensati per costruire un contesto verosimile, dove la comunicazione sembra provenire da un ente affidabile come una banca.

3. Analisi tecnica del PDF falsificato

Il documento PDF allegato è stato realizzato ad hoc, al fine di simulare una reale ricevuta bancaria. Al suo interno, sono stati intenzionalmente inseriti errori per riflettere le caratteristiche distintive di una contraffazione:

- Errore nell'intestazione
- Anomalia nell'importo numerico: l'importo "960,00 €" presenta un disallineamento visivo tra le cifre e i decimali, dovuto a una manipolazione grafica.
- Errori di formattazione e tipografia: chi utilizza programmi di grafica o word processor riconosce che il layout dei testi alterati spesso presenta incoerenze minime, come spaziature irregolari o allineamenti difettosi. Anche in questo caso, tali difetti sono visibili.

Questi difetti non sono casuali, ma rappresentano un utile strumento didattico, perché permettono di comprendere meglio come si costruisce un falso credibile e quali dettagli osservare per smascherarlo.

Conclusione

Questo esempio integra sia la **manipolazione emotiva** sia la **contraffazione tecnica** per costruire una simulazione di attacco phishing estremamente realistica.
Capire **come viene sfruttato lo stress per manipolare la percezione** e **quali dettagli tradiscono un documento falsificato** è essenziale per sviluppare un'efficace cultura della **cybersecurity**.

Educare gli utenti a riconoscere questi segnali — sia psicologici che visivi — rappresenta una delle strategie più efficaci per prevenire frodi informatiche e violazioni della sicurezza personale.

Anais Fabriani – Cybersecurity Specialist