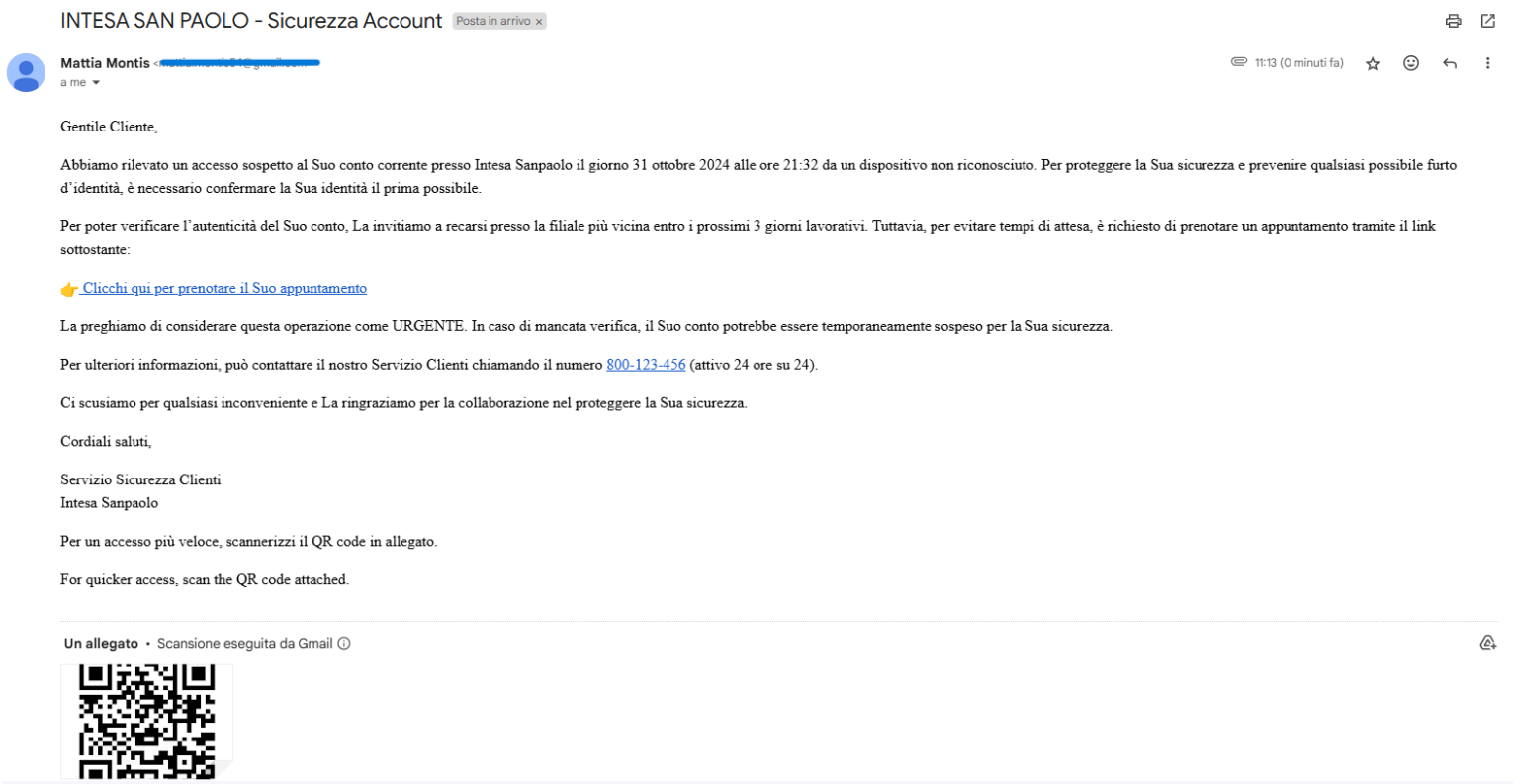
INGEGNERIA SOCIALE (Phishing)

Scenario Creato

In questo progetto, è stata scritta e inviata un'email di phishing fittizia, mascherata da comunicazione ufficiale di Intesa Sanpaolo. L'email avverte il destinatario di un accesso sospetto al proprio conto corrente, avvenuto da un dispositivo non riconosciuto. Si richiede urgentemente la conferma dell'identità per prevenire furti d'identità e il rischio di sospensione del conto. L'email contiene link malevoli per prenotare un appuntamento, un numero di telefono apparentemente valido e un QR code da scannerizzare per un accesso più veloce. Per completare il processo, ho scritto un codice Python (in ambiente Linux) per l'automatizzazione dell'invio della mail ed ho chiesto a ChatGPT di fornire il codice HTML per la mail e per creare un link di reindirizzamento a una pagina progettata per rubare le credenziali.



INTESA SAN PAOLO - Sicurezza Account Posta in arrivo ×

Mattia Montis <[redacted]>
a me

11:13 (0 minuti fa)

Gentile Cliente,

Abbiamo rilevato un accesso sospetto al Suo conto corrente presso Intesa Sanpaolo il giorno 31 ottobre 2024 alle ore 21:32 da un dispositivo non riconosciuto. Per proteggere la Sua sicurezza e prevenire qualsiasi possibile furto d'identità, è necessario confermare la Sua identità il prima possibile.

Per poter verificare l'autenticità del Suo conto, La invitiamo a recarsi presso la filiale più vicina entro i prossimi 3 giorni lavorativi. Tuttavia, per evitare tempi di attesa, è richiesto di prenotare un appuntamento tramite il link sottostante:

👉 Clicchi qui per prenotare il Suo appuntamento

La preghiamo di considerare questa operazione come URGENTE. In caso di mancata verifica, il Suo conto potrebbe essere temporaneamente sospeso per la Sua sicurezza.

Per ulteriori informazioni, può contattare il nostro Servizio Clienti chiamando il numero 800-123-456 (attivo 24 ore su 24).

Ci scusiamo per qualsiasi inconveniente e La ringraziamo per la collaborazione nel proteggere la Sua sicurezza.

Cordiali saluti,

Servizio Sicurezza Clienti
Intesa Sanpaolo

Per un accesso più veloce, scannerizzi il QR code in allegato.

For quicker access, scan the QR code attached.

Un allegato • Scansione eseguita da Gmail ⓘ

Credibilità dell'Email

L'email potrebbe apparire credibile per diversi motivi:

1. **Formato Professionale**: Utilizza un layout e un linguaggio formale tipico delle comunicazioni bancarie, creando un'illusione di autenticità.
2. **Minaccia di Urgenza**: L'enfasi sull'urgenza e la possibilità di sospensione del conto spinge i destinatari a reagire rapidamente, un metodo comune per indurre errori.
3. **Dettagli Specifici**: La menzione di un accesso da un "dispositivo non riconosciuto" rende la situazione personale e allarmante, rendendo la vittima più propensa a rispondere.
4. **Richiesta di Azioni Personali**: L'email richiede al destinatario di recarsi di persona presso una filiale per verificare l'autenticità del proprio conto, emulando il comportamento tipico delle banche. Questa strategia non solo crea un senso di urgenza, ma genera anche fiducia nel lettore, facendogli credere che sia fondamentale seguire queste istruzioni per proteggere il proprio conto. Le banche frequentemente incoraggiano le interazioni faccia a faccia per questioni sensibili, rendendo l'email più plausibile. Trovo che la richiesta di azioni fisiche, quindi, è una tattica astuta per persuadere le vittime a compiere operazioni che potrebbero esporre le loro informazioni personali senza destare sospetti.
5. **Mancata richiesta pecuniaria:** Trovo che un altro elemento di forza sia la mancanza di una richiesta di denaro, la quale insospettirebbe la vittima.

Elementi di Allerta

Nonostante la credibilità apparente, ci sono diversi segnali che dovrebbero far scattare un campanello d'allarme:

1. **Link Malevoli**: Il link per prenotare un appuntamento è sospetto. Anche se l'URL sembra legittimo, potrebbe reindirizzare a un sito di phishing progettato per rubare dati personali. Gli utenti dovrebbero sempre controllare attentamente l'URL prima di cliccarvi.
2. **Numero di Telefono**: Anche se il numero di telefono sembra autentico, potrebbe essere un numero tracciato o non affiliato realmente alla banca. È consigliabile verificare i numeri sui siti ufficiali anziché fare affidamento sulle informazioni fornite in email sospette.

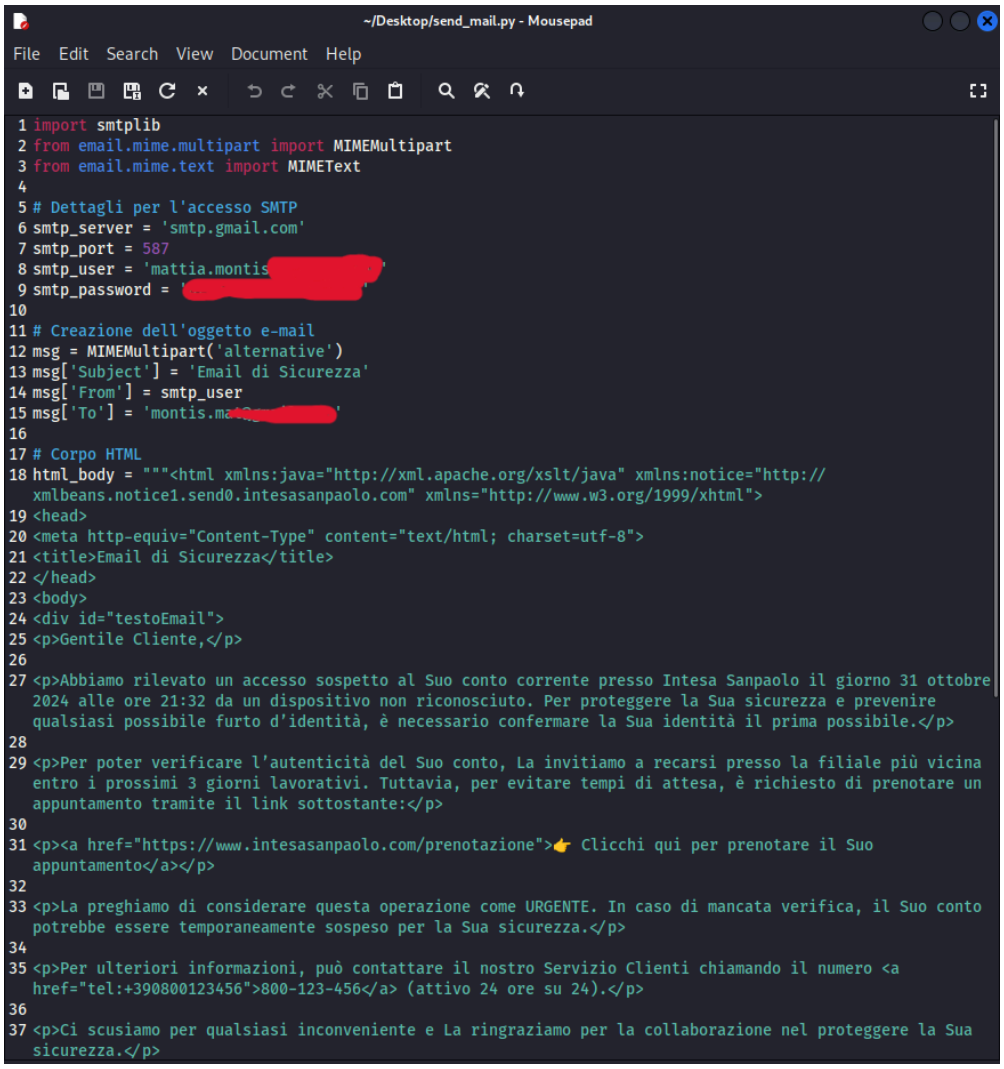
3. **QR Code**: La richiesta di scannerizzare un QR code per un accesso veloce è pericolosa, poiché gli utenti non possono vedere dove verranno indirizzati. Questo metodo è particolarmente insidioso perché bypassa la necessità di cliccare su un link, rendendo più difficile la verifica dell'autenticità.

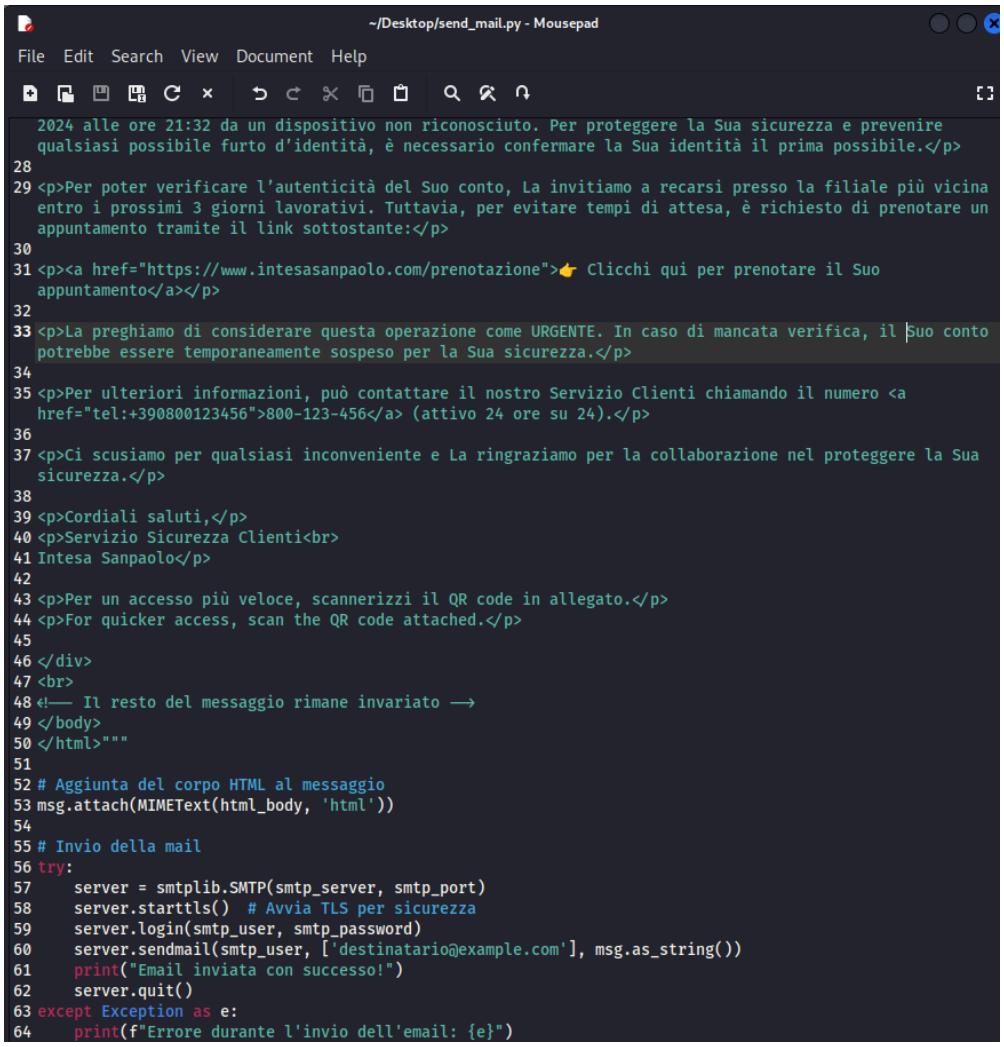
Tipo di Ingegneria Sociale Utilizzata

In questo scenario, è stato utilizzato principalmente il **phishing**, una tecnica di ingegneria sociale in cui l'attaccante si finge un'entità affidabile per indurre le vittime a fornire informazioni sensibili. A differenza del **pretexting**, dove l'attaccante crea una falsa identità specifica per ottenere informazioni, il phishing si basa su una comunicazione generica che può colpire un ampio pubblico. Questo caso, anche se non ho progettato la mail per quel target, può anche essere classificato come **whaling**, che è una forma di phishing mirata a individui di alto profilo all'interno di un'organizzazione, come dirigenti o responsabili finanziari. L'email è progettata per sembrare credibile e coinvolgente.

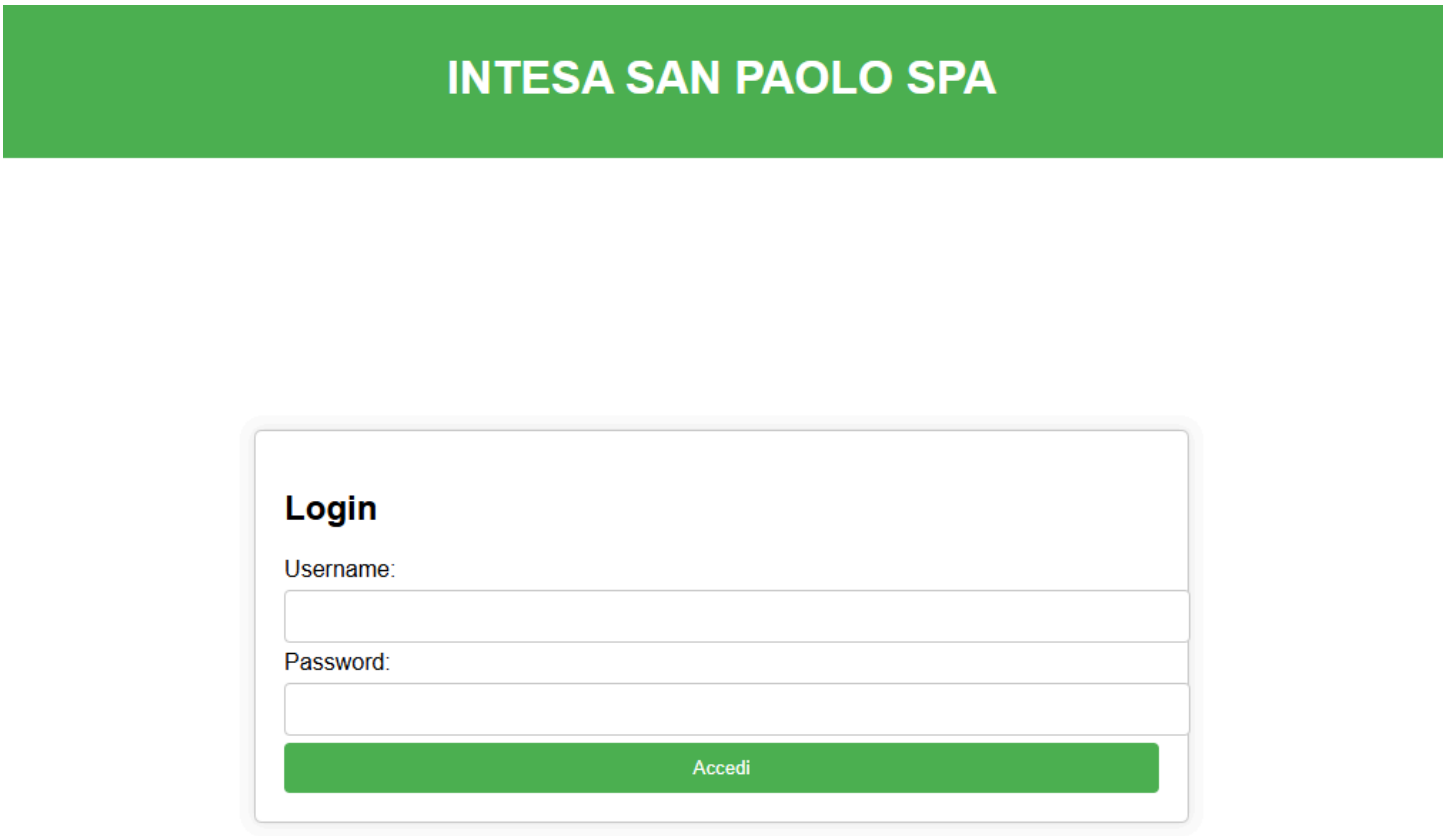
Uso di Codici Python e HTML

Per inviare l'email di phishing, è stato utilizzato un codice Python che sfrutta la libreria smtplib, consentendo di inviare messaggi formattati in HTML. Il codice ha generato un'email con il corpo e i link descritti, compresi quelli per la prenotazione e il numero di telefono, rendendo l'operazione di phishing più efficiente.

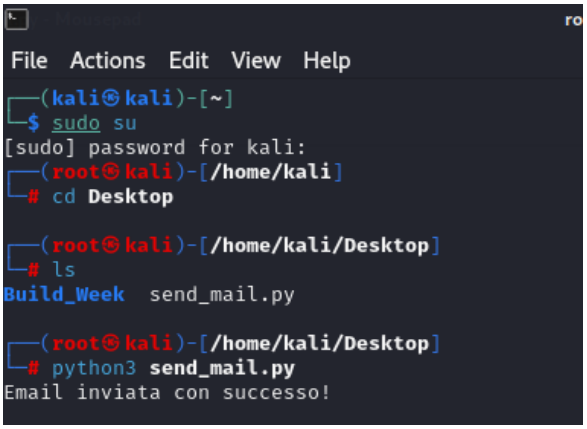




È stato anche chiesto a ChatGPT di fornire il codice HTML per la mail e un codice per creare un link di reindirizzamento a una pagina progettata per rubare le credenziali. L'HTML utilizzato per formattare l'email ha imitato il layout di comunicazioni ufficiali, contribuendo a ingannare le vittime.



Con l'automazione fornita da Python, l'invio di email di phishing diventa un processo semplice e veloce.



Conclusione

Questa simulazione ha messo in evidenza come anche un'email apparentemente innocua possa nascondere intenti malevoli. È cruciale educare le persone a riconoscere i segnali di allerta nel phishing e a prendere precauzioni quando si ricevono comunicazioni sospette. L'uso di strumenti come Python per l'invio di email rappresenta una minaccia

crescente, sottolineando l'importanza di un'adeguata consapevolezza della sicurezza informatica.