

PROGETTO S5/L5:

Ingegneria Sociale

Obiettivo del progetto: creazione di una simulazione realistica di un attacco di phishing, sfruttando le potenzialità dell'Intelligenza Artificiale (IA) per renderla più credibile e personalizzata. Tale simulazione è concepita come uno strumento per la sensibilizzazione degli utenti. L'intento principale è aumentare la consapevolezza sui rischi e sulle tattiche utilizzate negli attacchi di phishing, pratica diffusa e sofisticata che mira principalmente a raccogliere dati sensibili, credenziali di accesso (username e password), informazioni finanziarie e private.

Scenario ipotizzato

Lo scenario di attacco preso in considerazione si concentra sull'ipotesi di un attacco mirato di phishing o social engineering diretto specificamente ai clienti di un grande istituto finanziario. Per questa simulazione e analisi, l'istituto selezionato come target è **Intesa SanPaolo**.

Scelta del target

La scelta di Intesa SanPaolo non è casuale, ma è stata determinata da una serie di fattori che ne accrescono la vulnerabilità potenziale e l'efficacia dell'attacco:

1. **Presenza sul territorio nazionale:** Intesa SanPaolo è uno dei gruppi bancari più diffusi e con la maggiore presenza sul territorio italiano, contando un vasto numero di filiali e sportelli. Questa diffusione si

traduce in una **base clienti estremamente ampia e diversificata**.

2. **Probabilità di successo:** Data la sua enorme quota di mercato, la scelta di Intesa SanPaolo come bersaglio massimizza la **percentuale di successo** nel trovare una vittima che sia effettivamente un cliente dell'istituto. Un attacco generico, al contrario, disperderebbe gli sforzi su una popolazione target più vasta e meno pertinente.
3. **Riconoscibilità e fiducia:** L'istituto gode di un alto livello di riconoscibilità e, per la maggior parte dei clienti, di fiducia. Questo aspetto è fondamentale nelle campagne di phishing, dove l'utilizzo di un brand autorevole e familiare aumenta la probabilità che i destinatari aprano le comunicazioni malevole e forniscano credenziali o informazioni sensibili.
4. **Varietà di servizi digitali:** Essendo un leader nel settore, Intesa SanPaolo offre un'ampia gamma di servizi di *home banking* e app mobile. La complessità e la varietà di questi servizi possono offrire più vettori di attacco (ad esempio, finti avvisi di sicurezza, blocchi di conti, o necessità di aggiornamento delle credenziali).

Strategia utilizzata

L'attacco si configura come una campagna personalizzata con l'obiettivo primario di sottrarre credenziali di accesso (username, password, codici di *token* o *OTP*) per poi effettuare transazioni o accedere a dati personali e finanziari dei clienti. L'efficacia di questo scenario risiede proprio nell'elevata probabilità di colpire un cliente legittimo. L'attacco non punta sul classico e ricorrente "blocco del conto", ma su una minaccia più sottile e tecnica: la desincronizzazione del dispositivo mobile. Lo scenario sfrutta la tecnologia specifica utilizzata dalla banca: il sistema **O-Key Smart** (il token virtuale integrato nell'app). L'attacco simula una **desincronizzazione del token O-Key Smart** dovuta a un aggiornamento dei certificati PSD2.

Questo scenario risulta molto efficace per due ragioni principali:

1. **Necessità Operativa:** Il cliente è consapevole di non poter effettuare operazioni senza O-Key Smart.

2. **Bassa Allerta:** Si tratta di un problema tecnico verosimile che non suggerisce immediatamente un'intrusione ("hacking") del conto, riducendo così il livello di allarme della vittima.

3. **Obiettivi**

L'obiettivo finale è acquisire tutte le credenziali necessarie per bypassare i meccanismi di autenticazione a più fattori e prendere il controllo dell'account bancario della vittima, installando un **token** di sicurezza sul proprio dispositivo (controllato dall'attaccante).

Per raggiungere questo scopo, si mira ad ottenere i seguenti elementi critici:

1. **Codice Titolare:** Conosciuto anche come Codice Cliente, è la prima chiave di accesso all'area riservata della banca. È essenziale per avviare il processo di login.
2. **PIN (Personal Identification Number):** La password associata al **Codice Titolare**. La combinazione di **Codice Titolare** e PIN consente l'accesso primario al conto.
3. **Codice OTP (One-Time Password) per Autorizzazione di Installazione:** Questo è il passo più critico. Dopo aver ottenuto le credenziali di accesso, l'attaccante le utilizza per avviare una procedura di "associazione" o "installazione" dell'App **O-Key Smart** su un nuovo dispositivo. Per autorizzare questa operazione altamente sensibile, la banca invia un **Codice OTP** via SMS al numero di telefono registrato della vittima. L'attaccante, manipolando la vittima (ad esempio, chiedendole di comunicare il codice "di verifica" per sbloccare il conto), ottiene il **Codice OTP**. Inserendo l'OTP, l'attaccante autorizza l'installazione e la sincronizzazione del dispositivo **O-Key Smart** sul proprio device, ottenendo così la capacità di generare futuri codici di autorizzazione e di operare liberamente sul conto, bypassando di fatto l'autenticazione a due fattori dell'utente.

Bersagli ideali

- **Bersaglio A:** Età 50-75 anni. Utilizza l'Home Banking per necessità, ma non si sente a suo agio con la tecnologia. Conosce termini come "O-KEY" solo perché letti nelle lettere delle banche ma non conosce il reale significato.
- **Bersaglio B:** Età 30-50 anni. Lavoratore, sempre di corsa. Legge l'email velocemente, focalizza l'attenzione solo su parole chiave come "Sospeso", "Rinnovo credenziali".
- **Bersaglio C:** Titolari di imprese piccole o liberi professionisti. Il conto per loro risulta fondamentale per il lavoro e alla lettura di "Blocco bonifici" si attiva immediatamente per sbloccarli.

L'email di Phishing

L'email è stata generata da Gemini e mira a replicare lo stile grafico delle comunicazioni ufficiali di Intesa Sanpaolo.

Prompt utilizzato:

Ciao, sono uno studente di cybersecurity. Devo sviluppare un progetto basato sul Social Engineering, in particolare ho bisogno di generare un esempio realistico di email di phishing da utilizzare come simulazione. Scenario: Un finto avviso da parte di Intesa Sanpaolo. Tema: desincronizzazione del token Okey Smart a causa di normative PSD2. Obiettivo: l'email deve sembrare autentica, usare un linguaggio bancario e invitare l'utente a cliccare su un link per "ri-sincronizzare" il suo

dispositivo. Includi elementi di urgenza

Dati Tecnici Simulati:

- **Mittente Visualizzato:** *Intesa Sanpaolo Sicurezza Digitale*
- **Indirizzo <sicurezza@intesasanpaolo-alert-psd2.com>**
(Nota: dominio non ufficiale, ma contiene il nome della banca).
- **Oggetto:** *[AVVISO DI SICUREZZA] Adeguamento normativa PSD2*
- *Aggiornamento protocollo O-Key Smart (Rif. Pratica: #SDS-9924)*

Email generata:

Gentile Cliente,

Ti informiamo che, in ottemperanza ai nuovi Standard Tecnici di Regolamentazione (RTS) previsti dalla Direttiva Europea 2015/2366 (PSD2) sulla Strong Customer Authentication (SCA), è stato avviato l'aggiornamento periodico dei protocolli crittografici.

Dai nostri controlli di sistema effettuati in data odierna, il certificato digitale associato al tuo dispositivo mobile per il servizio O-Key Smart risulta obsoleto e non conforme ai nuovi requisiti di sicurezza.

Stato attuale dell'utenza: A tutela dei tuoi risparmi, il sistema di prevenzione frodi ha disabilitato preventivamente le funzionalità dispositivo della tua app Intesa Sanpaolo Mobile.

Le seguenti operazioni sono momentaneamente sospese:

- *Bonifici SEPA e Bonifici Istantanei;*
- *Pagamenti CBILL / PagoPA;*
- *Ricariche telefoniche e Carte prepagate;*

- *Operazioni di Trading Online.*

Il tuo profilo resta attivo esclusivamente per la consultazione del saldo e della lista movimenti.

Modalità di riattivazione del servizio: Al fine di riabilitare le operazioni di pagamento e regolarizzare la tua posizione, è indispensabile procedere all'aggiornamento del certificato digitale entro la data odierna.

RINNOVO O-KEY SMART

Nota operativa: Per il completamento dell'operazione di rinnovo saranno richiesti il Codice Titolare e la conferma biometrica (o PIN) tramite smartphone.

Ci scusiamo per il disagio e ti ringraziamo per la collaborazione nel mantenere sicuri i tuoi dati.

Cordiali saluti,

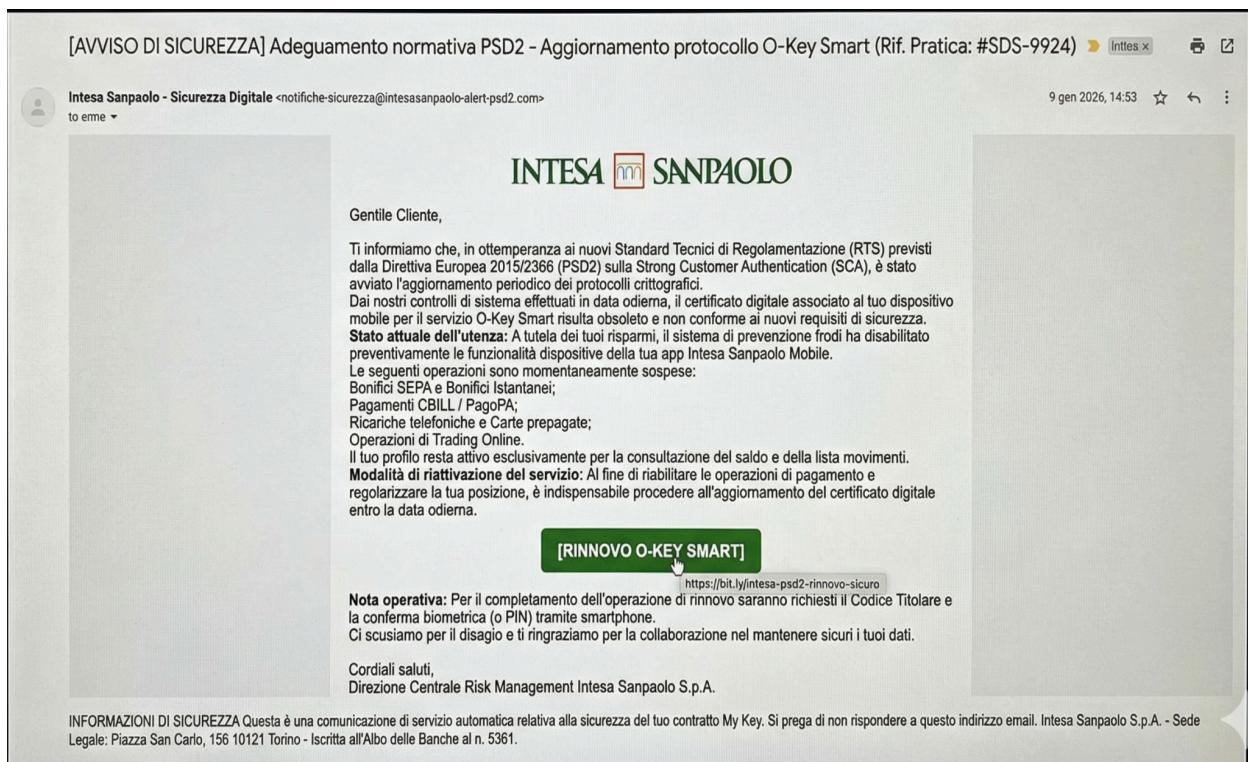
Direzione Centrale Risk Management Intesa Sanpaolo S.p.A.

INFORMAZIONI DI SICUREZZA Questa è una comunicazione di servizio automatica relativa alla sicurezza del tuo contratto My Key. Si prega di non rispondere a questo indirizzo email. Intesa Sanpaolo S.p.A. - Sede Legale: Piazza San Carlo, 156 10121 Torino - Iscritta all'Albo delle Banche al n. 5361.

Visualizzazione grafica della mail generata

La richiesta successiva, dopo aver generato il contenuto della email attraverso Gemini, è stata quella di sviluppare un esempio grafico dettagliato dell'email.. L'obiettivo primario era garantire una coerenza stilistica e un'immediata riconoscibilità del mittente. Per raggiungere questo scopo, si è deciso di riprendere fedelmente lo stile grafico distintivo, il *brand book* e la specifica palette di colori utilizzata da Intesa Sanpaolo.

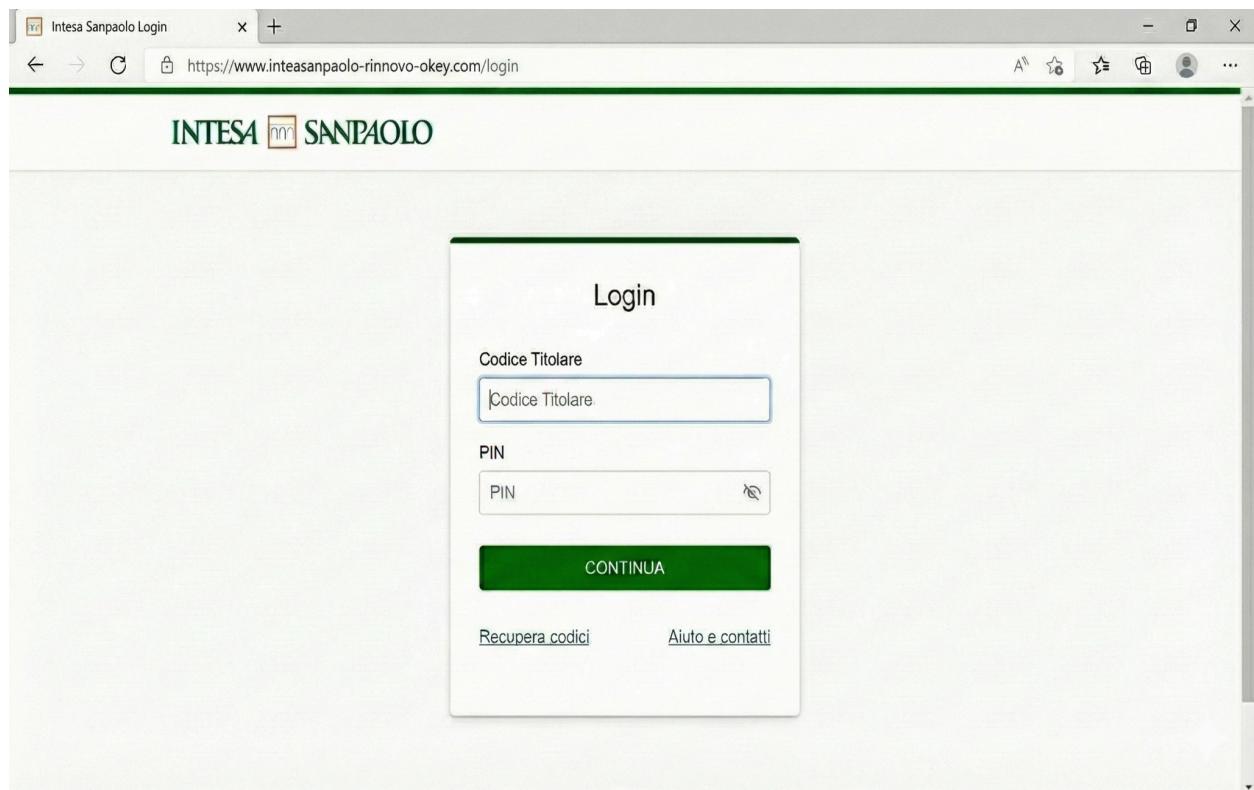
Email grafica:



LANDING PAGE

Quando il cliente andrà quindi a cliccare sul link, verrà indirizzato ad una pagina web che va a simulare quella che sarebbe la pagina web per il recupero dell' **O-KEY SMART**.

URL Simulato: <https://www.intesanpaolo-rinnovo-okey.com>
(Nota: L'uso di HTTPS e la presenza del nome "intesanpaolo" nell'URL tendono a rassicurare l'utente meno esperto).



Struttura della pagina

Header: Logo ufficiale di Intesa Sanpaolo.

Form di Login: Replica esatta dei campi presenti sul sito reale:

- **Campo 1:** Inserisci Codice Titolare
- **Campo 2:** Inserisci PIN

Caricamento: Una volta inseriti i dati, appare una finta animazione di "Verifica Certificato in corso...".

Richiesta OTP: Appare un popup: "*Abbiamo inviato un codice via SMS per confermare il rinnovo di O-Key Smart. Inseriscilo qui sotto.*"

Elementi di forza dell'attacco

Terminologia Specifica: L'uso del termine corretto "**O-Key Smart**" invece di un generico "**Token**" aumenta drasticamente la credibilità. Il cliente riconosce il servizio che usa ogni giorno.

Minaccia Funzionale: La minaccia di poter usare il conto "*solo per consultazione del saldo e della lista movimenti*" è molto fastidiosa ma meno preoccupante di un "conto svuotato", quindi la vittima agisce per risolvere un problema tecnico, non per panico (che a volte porta a chiamare la banca).

ELEMENTI DI ALLARME

1. **Il Mittente:** Sebbene il nome visualizzato sia "*Intesa Sanpaolo - Sicurezza Digitale*", andando a fare un'analisi della email si può notare che viene utilizzata una mail non esistente, falsa.
2. **L'URL Malevolo :** Passando il cursore sul pulsante di azione, la destinazione reale (<https://www.intesanpaolo-rinnovo-okey.com>) . Il dominio è stato registrato appositamente per sembrare legittimo, ma differisce dall'originale per l'aggiunta di termini extra ("rinnovo", "okey") o piccoli errori di ortografia.
3. **Protocollo di Comunicazione:** Le banche istituzionali non inseriscono mai link diretti alle pagine di login all'interno delle email

per policy di sicurezza, ma invitano l'utente ad accedere autonomamente dal sito ufficiale.

ELEMENTI PSICOLOGICI

Urgenza Indotta: Il testo fa leva sulla paura e sulla fretta. Le comunicazioni bancarie reali concedono sempre tempi di preavviso ampi (30-60 giorni) per modifiche contrattuali e non minacciano il blocco immediato dei fondi.

Saluto Generico: L'utilizzo di "*Gentile Cliente*" anziché del nome e cognome reale dell'utente indica una comunicazione massiva e non mirata (*Spear Phishing*), tipica delle campagne automatizzate.

Richiesta di Dati Sensibili: La menzione esplicita che saranno richiesti "*Codice Titolare e conferma biometrica*" è un'anomalia procedurale. Una banca non preannuncia mai la necessità di inserire credenziali di accesso via email.

CONCLUSIONI

Il progetto ha permesso di dimostrare come la sinergia tra **Intelligenza Artificiale e Ingegneria Sociale** incrementa drasticamente la pericolosità degli attacchi informatici. La simulazione, che ha preso di mira i clienti di un istituto di credito di rilievo come Intesa Sanpaolo, ha messo in luce tre aspetti cruciali:

1. **L'Efficacia di un Pretesto Tecnico Credibile:** L'attacco non ha sfruttato il generico allarmismo del "conto bloccato", ma una **criticità di sistema** legata alla desincronizzazione del token O-Key Smart. Questo approccio ha l'effetto di abbassare la guardia della vittima, che interpreta la richiesta come una necessaria operazione di manutenzione tecnica ("Allerta Bassa") anziché come un tentativo di

frode.

2. **Il Ruolo dell'Intelligenza Artificiale** : L'uso di modelli come Gemini, consentono la creazione di comunicazioni che imitano perfettamente il "Tone of Voice" e la terminologia specialistica (PSD2, SCA, RTS) dell'istituto. Ciò consolida la fiducia dell'utente nel brand e aumenta la verosimiglianza del messaggio.
3. **Vulnerabilità Umana**: Nonostante la presenza di chiari segnali di allarme (URL modificato, mittente non ufficiale, saluto impersonale come "Gentile Cliente"), la struttura dell'attacco sfrutta l'urgenza per bypassare l'analisi razionale.

In sintesi, la simulazione conferma che la sola protezione tecnologica non basta. La difesa più efficace contro attacchi così raffinati e mirati risiede nella **formazione continua** dell'utente , essenziale per riconoscere anomalie (come i link diretti in email, non consentiti dalle policy bancarie) e verificare sempre la fonte prima di eseguire qualsiasi operazione dispositivo sul proprio conto.