

Unità 2 - S5-L5

Data: 24 Ottobre 2025

Alessandro Pietro Salerno

Report su vari scenari di Phishing

Oggetto: Report in merito la descrizione di diversi scenari realistici e alcune delle possibili tecniche di phishing che possono essere adottate , per raggiungere l' obiettivo .

Introduzione

Ci è stato richiesto di simulare un' email di phishing utilizzando un LLM , ed inoltre di creare uno scenario realistico , e spiegare lo scenario . La stesura dell' email è stata completamente affidata al LLM , in questo caso gemini . Partendo dalla semplice premessa che le tecniche di phishing sono "infinite" e che se il nostro obiettivo sia quello di creare un' esca , basterebbe semplicemente mettere un QrCode con scritto "Free Wifi" ed aspettare che abbocchino , ho comunque ed ovviamente rispettato la traccia della consegna ed ho riportato ed analizzato diversi casi realistici , partendo dal più "popolare" e semplice , per poi arrivare ad un caso più specifico , complesso ed articolato.

BANCA SICURA.IT

1) Creare uno Scenario

Contesto Realistico: Immaginiamo uno scenario molto comune ; un utente riceve un'email che sembra provenire dalla sua banca, chiamiamola "Banca Sicura". L'email avvisa l'utente di un presunto accesso non autorizzato al suo conto online e lo invita a verificare la sua identità cliccando su un link per proteggere il conto. Questo scenario sfrutta la **paura dell'utente** di perdere i propri soldi o subire un furto d'identità e fa leva sulla **fiducia** che normalmente si ripone nella propria banca.

Obiettivo del Phishing: L'obiettivo primario di questa email di phishing è **ottenere le credenziali di accesso** (username e password) dell'utente per il suo servizio di online banking. Una volta ottenute, l'attaccante potrebbe accedere al conto per sottrarre fondi, raccogliere ulteriori informazioni personali o compiere altre azioni fraudolente.

2) Scrivere l'Email di Phishing (Generata con LLM Gemini)

Ecco un esempio di email di phishing che potrei generare basandomi sullo scenario definito. Cercherò di renderla convincente, includendo elementi tipici del phishing come richiesto. Tra le virgolette "" ho inserito tutta la parte generata dal LLM , limitandomi ad evidenziare in grassetto le parti più importanti e significative per l'analisi successiva , sia per la seguente email che per le successive .

“ Oggetto: Avviso Urgente: Accesso Sospetto Rilevato sul Tuo Conto Banca Sicura

Mittente: Servizio Sicurezza Banca Sicura
alert@bancasicura-servizi-online.com

Corpo dell'email:

Gentile Cliente,

Abbiamo recentemente rilevato un tentativo di accesso al tuo conto online Banca Sicura da un dispositivo e una località non riconosciuti (Indirizzo IP: 89.152.XX.XX, Luogo: Estero) avvenuto pochi minuti fa.

Per la tua protezione e per prevenire accessi non autorizzati, abbiamo temporaneamente limitato alcune funzionalità del tuo conto. È **richiesta un'azione immediata** da parte tua per verificare che l'accesso sia stato effettuato da te e per ripristinare la piena operatività.

La mancata verifica **entro le prossime 12 ore** potrebbe comportare una sospensione prolungata del tuo accesso online per motivi di sicurezza.

Per favore, accedi al nostro portale di sicurezza **tramite il link** sottostante per confermare la tua identità e rivedere le recenti attività. È un passaggio fondamentale per assicurare la protezione del tuo conto.

[Accedi e Verifica la Tua Identità Ora]

Se l'accesso sospetto non è stato effettuato da te, ti preghiamo di seguire comunque la procedura per mettere in sicurezza il tuo conto immediatamente. Ignora questo messaggio se hai già provveduto alla verifica. Ci scusiamo per l'eventuale disagio, la vostra sicurezza è la nostra priorità.

Cordiali Saluti,

Il Team Sicurezza Clienti Banca Sicura www.bancasicura.it “

3. Spiegare lo Scenario

Descrizione: Lo scenario simula un avviso di sicurezza inviato da una banca fittizia, "Banca Sicura", riguardo un presunto accesso non autorizzato al conto online del destinatario. L'email spinge l'utente a cliccare un link per verificare la propria identità e proteggere il conto.

Perché è realistico e potrebbe sembrare credibile:

- **Fonte Apparentemente Affidabile:** L'email sembra provenire dalla banca, utilizzando un nome e un logo (se inserito in formato HTML) simili a quelli ufficiali. Il mittente alert@bancasicura-servizi-online.com può ingannare un utente distratto.
- **Motivazione Legittima:** Gli avvisi di sicurezza sono comunicazioni standard inviate dalle banche. La preoccupazione per la sicurezza del proprio conto è un forte motivatore.
- **Linguaggio Formale:** Il tono e lo stile dell'email cercano di imitare le comunicazioni bancarie ufficiali.
- **Dettagli Tecnici (Falsi):** L'inclusione di un (falso) indirizzo IP e di una località estera aggiunge un elemento di specificità che può aumentare la credibilità percepita.

Elementi d'Allarme (Red Flags): Ecco gli elementi nell'email che dovrebbero far scattare un campanello d'allarme:

1. **Mittente Sospetto:** L'indirizzo email alert@bancasicura-servizi-online.com non corrisponde al dominio ufficiale della banca (che ipotizzando, presumibilmente è bancasicura.it). I phisher spesso usano domini simili ma non identici.

2. **Saluto Generico:** L'uso di "Gentile Cliente" invece del nome specifico del cliente è un classico segnale di phishing. Le banche solitamente personalizzano le loro comunicazioni.
3. **Senso di Urgenza Eccessivo:** Frasi come "azione immediata richiesta" e la minaccia di sospensione "entro le prossime 12 ore" sono tattiche comuni per mettere fretta all'utente, impedendogli di riflettere attentamente.
4. **Link Sospetto:** Anche se il testo del link "[Accedi e Verifica la Tua Identità Ora]" sembra legittimo, passando il mouse sopra (senza cliccare) o analizzando il codice HTML si scoprirebbe che l'URL reale (<http://bancasicura-servizi-online.com/verifica-sicurezza/login.html>) è diverso dal sito ufficiale della banca e ospitato su un dominio non correlato. Questo è il cuore dell'attacco: portare l'utente su una pagina di login falsa.
5. **Richiesta Implicita di Credenziali tramite Link:** Le banche legittime raramente chiedono di cliccare su un link in un'email per inserire le proprie credenziali a seguito di un alert. La procedura corretta è solitamente quella di accedere al sito ufficiale digitando l'indirizzo manualmente nel browser o tramite l'app ufficiale.
6. **Errori Sottili o Linguaggio Non Standard (Possibile):** A volte, le email di phishing contengono piccoli errori grammaticali o frasi leggermente innaturali (qui ho cercato di evitarli per renderla più credibile, ma è un elemento da cercare). Ad esempio, la frase "assicurare la protezione del suo conto" usa "suo" invece di "tuo", creando una leggera incoerenza.
7. **Link Testuale Diverso dal Link Reale:** In fondo, viene mostrato www.bancasicura.it come testo, ma non è il link cliccabile principale, cercando di confondere l'utente.

Essendo dunque abbastanza semplice generare un' email così generica e con una così probabile e scontata motivazione , aspettando che qualcuno caschi nel tranello e ci dia le credenziali , ho di seguito riportato un caso diverso , più strutturato e mirato che adotta la tecnica vista a lezione dello Spear Phishing.

“...troppo comodo , troppo comodo e troppo facile, ... troppo comodo , troppo facile e troppo semplice...”

THE HELPFUL AI

1) Creare uno Scenario

Contesto Realistico: Il nostro bersaglio è uno studente di informatica o un giovane sviluppatore che ha dei *repository* pubblici su GitHub. È risaputo che gli sviluppatori sono molto attenti alla sicurezza del loro codice e sono curiosi di provare nuovi strumenti, specialmente quelli basati sull'IA.

Lo scenario non si basa sulla *paura* (come la banca), ma sulla curiosità, sull'orgoglio e sul desiderio di migliorarsi.

L'attaccante impersona un nuovo, fantomatico servizio "OpenSource" chiamato "**CodeGuardian AI**". Questo servizio (fittizio) sostiene di usare un LLM avanzato per scansionare gratuitamente i repository pubblici su GitHub alla ricerca di vulnerabilità di sicurezza "nascoste" (come *hardcoded secrets* o *API keys*). L'email informa la vittima che il suo repository è stato scansionato e che sono stati trovati dei "problemi critici".

Obiettivo del Phishing: L'obiettivo è duplice e più sofisticato del solito furto di password:

1. **Furto di Credenziali GitHub:** Portare l'utente su una pagina clone di GitHub per "autenticarsi" e "vedere il report" rubando username e password.
2. **(Obiettivo Avanzato) Furto di Token OAuth:** In alternativa, la pagina falsa potrebbe implementare un attacco di Consent Phishing. Chiede all'utente di "Autorizzare CodeGuardian AI a scansionare i tuoi repository" tramite un pop-up OAuth. Se l'utente accetta, concede all'applicazione malevola dell'attaccante un **token di accesso permanente al suo account GitHub**, permettendogli di leggere codice privato, rubare chiavi API e persino inserire codice malevolo nei suoi progetti.

2. Scrivere l'Email di Phishing (Generata con LLM Gemini)

Ecco l'email di phishing, progettata per essere altamente credibile per un target tecnico.

“ **Oggetto:** CodeGuardian AI ha trovato 3 problemi di sicurezza critici nel tuo repository `[Nome_Repo_Vittima]`

Mittente: CodeGuardian AI Security alerts@codeguardian-ai.io

Corpo dell'email:

Ciao `[Username_GitHub_Vittima]`,

Siamo il team di **CodeGuardian AI**, un nuovo strumento di analisi statica (SAST) potenziato da IA, dedicato a migliorare la sicurezza della community open-source.

Durante una scansione di routine dei nuovi *commit* pubblici, il nostro motore di analisi ha identificato **3 problemi di sicurezza** nel tuo repository `[Nome_Repo_Vittima]`, di cui uno classificato come **Critico**.

Riepilogo dei Problemi Rilevati:

- **Critico (1):** Esposizione di una *API Key* (hardcoded secret) nel file `src/config/settings.py` (Commit: `8a2fe...`).
- **Alto (1):** Potenziale *SQL Injection* nel gestore della route `/api/user/profile`.
- **Medio (1):** Utilizzo di una dipendenza deprecata con vulnerabilità note (CVE-2023-XXXX).

Per prevenire abusi, i dettagli completi e le *patch* suggerite dalla nostra IA sono disponibili solo per il proprietario del repository.

Puoi visualizzare il report di sicurezza completo e connettere il tuo account per scansioni future (gratuite per l'open-source) accedendo al nostro pannello di controllo.

[Accedi con GitHub per vedere il tuo Report di Sicurezza] ``

Siamo entusiasti di aiutarti a rendere il tuo codice più sicuro.

Buona programmazione, Il Team di CodeGuardian AI

--- © 2025 CodeGuardian AI | Fai l'unsubscribe se non vuoi più ricevere avvisi di sicurezza gratuiti. .“

Prima di procedere con la spiegazione dello scenario , voglio spiegare e riportare le differenze tra i due tipi d' attacco in questione , il "Furto delle credenziali Github" e il "Furto di token OAuth" .

Chiaccherando con Gemini , prima di esaurire le domande a disposizione ho chiesto , se la vittima cambiasse le credenziali l' accesso a Github sarebbe possibile per l' attaccante ? Mi ha risposto ovviamente di no . Però ha anche aggiornato la risposta creando un attacco diverso ovvero quello dei Token OAuth. Riporto una sintesi della spiegazione che ho ottenuto , ed anche una tabella , che per correttezza comunico di non avere creato io ma semplicemente riportato dall LLM.

Sintesi spiegazione delle differenze

- **Furto di Credenziali:** L'attaccante costruisce una **pagina di login FALSA** che assomiglia a GitHub. Tu inserisci la tua password e lui te la ruba. È come rubare la chiave di casa tua.
- **Furto di Token OAuth:** L'attaccante usa la **pagina di login VERA** di GitHub. Tu non gli dai mai la tua password. Lo inganni per farti "autorizzare" la sua applicazione malevola, dandogli un "gettone" (token) che gli permette di entrare. È come convincerti a dare la chiave di casa a un finto servizio di pulizie, autorizzandolo a entrare e uscire quando vuole. (esempio che non mi ha convinto tanto , perchè credo simile al primo caso . Comunque ho capito il senso e la logica dietro i 2 attacchi.)

Tabella creata dall' IA

Caratteristica	Attacco 1: Furto di Credenziali (Pagina Clone)	Attacco 2: Furto di Token OAuth (Consent Phishing)

Pagina di Login	FALSA. È un clone (es. auth.codeguardian-ai.io) che imita github.com .	VERA. È la pagina ufficiale github.com .
Cosa Vede l'Utente	Una pagina di login che <i>sembra</i> GitHub.	La <i>vera</i> pagina di login di GitHub, seguita da una <i>verapagina</i> di autorizzazione.
Cosa Inserisce l'Utente	Username e Password (e forse il codice 2FA) nella pagina FALSA.	Username e Password (e codice 2FA) nella pagina VERA. Poi clicca "Autorizza" sulla pagina di consenso.
Cosa Ottiene l'Attaccante	Il tuo Username e la tua Password in chiaro.	Un Access Token (una lunga stringa di testo) delegato alla sua app.
Gestione dell'MFA (2FA)	È un problema per l'attaccante. Deve ingannarti per ottenere anche il codice 2FA <i>in tempo reale</i> .	Bypassato completamente. L'MFA viene gestita tra te e il <i>vero</i> sito di GitHub. L'attaccante ottiene il token <i>dopo</i> che tu ti sei autenticato.
Persistenza	L'attacco fallisce se l'utente cambia password.	L'attacco persiste anche se l'utente cambia password. Il token rimane valido finché non viene <i>revocato manualmente</i> .

Analogia	Rubare la chiave di casa (e il codice dell'allarme).	Convincere il proprietario a dare una chiave di servizio (valet key) a un ladro travestito da fattorino.
-----------------	---	---

Tornando sull' analogia che mi fornito l' IA , non vedo tanta differenza tra i 2 casi . (ovviamente capisco che il rubare e il farsi dare la chiave , siano due cose diverse) . Però cambiando la serratura "credenziali" non posso accedere né il ladro né il fattorino o servizio di pulizie che sia. Piuttosto sia più coerente un esempio di un fabbro che qualsiasi serratura io metta , lui ha sempre l' accesso alla casa , a meno che non si cambi il fabbro , "cambio/revoca manuale del token" .

3. Spiegare lo Scenario

Perché potrebbe sembrare credibile:

1. **Personalizzazione (Spear Phishing):** L'email è altamente personalizzata. Usa il vero `Username_GitHub_Vittima` e un vero `Nome_Repo_Vittima` (informazioni facilmente reperibili su GitHub).
2. **Pretesto Tecnico e Plausibile:** Gli sviluppatori ricevono email da bot e servizi di sicurezza (come Dependabot o Snyk). Un nuovo servizio "basato su IA" è un pretesto moderno e perfettamente plausibile.
3. **Dettagli Specifici:** L'attacco non è vago. Menziona problemi specifici (`API Key`, `SQL Injection`), un percorso di file(`src/config/settings.py`) e persino un hash di commit. Un attaccante può facilmente prendere un repository pubblico, scegliere un file a caso e inventare una vulnerabilità credibile.
4. **"Esca" di Valore (Baiting):** L'esca non è un premio, ma qualcosa di valore per il target: un report di sicurezza gratuito e la soluzione (la patch) a un problema critico. La curiosità e la paura di avere una falla nel proprio codice sono motivatori potentissimi.

5. **Tono Professionale:** Il linguaggio è quello di una startup tech. Il dominio del mittente (.io) è molto comune per questo tipo di servizi, aumentando la credibilità.
6. **Call-to-Action Standard:** Il "Accedi con GitHub" (OAuth) è un metodo di login standard per i servizi per sviluppatori. Questo abbassa la guardia dell'utente.

Elementi d'Allarme (Red Flags):

1. **Servizio Non Richiesto:** Il primo campanello d'allarme. La vittima non ha mai sentito parlare di "CodeGuardian AI" né si è mai registrata per il servizio. Perché la stanno contattando?
2. **Dominio Sospetto (se analizzato):** Anche se `codeguardian-ai.io` sembra legittimo, un controllo su `whois` o una rapida ricerca su Google rivelerebbero che il dominio è stato registrato di recente (un classico) o che non esiste un'azienda reale con quel nome.
3. **Analisi del Link (Hovering):** Passando il mouse sul link (senza cliccare), l'URL di destinazione sarebbe sospetto. Invece di puntare a `github.com` per l'autenticazione, punta a un sottodominio dell'attaccante (`auth.codeguardian-ai.io/...`) che ospita una pagina identica a quella di login di GitHub.
4. **(Per l'attacco OAuth) Richiesta di Permessi Eccessivi:** Se si trattasse di un attacco di Consent Phishing, la pagina di autorizzazione (il pop-up di GitHub) sarebbe reale, ma chiederebbe permessi esagerati. Invece di un permesso read-only per i repo pubblici, chiederebbe: `repo` (accesso completo ai repo, inclusi quelli privati) e `admin:org_hook` (permesso di gestire gli webhook dell'organizzazione). Un utente di fretta potrebbe cliccare "Authorize" senza leggere, consegnando le chiavi del proprio account.
5. **Urgenza Implicita:** La parola "Critico" e la natura del problema (una chiave API esposta) creano un forte senso di urgenza che spinge l'utente ad agire immediatamente senza riflettere.

Infine concludo riportando uno scenario avanzato che combina più vettori d'attacco in una catena. Le tecniche che ho deciso di utilizzare e combinare

tra di loro per l' attacco sono : **Spear Phishing, Clone Phishing , Quishing e Vishing**. Il risultato è un attacco realistico , multivettoriale e sofisticato.

OPERAZIONE RED CARPET

1. Creare lo Scenario (Operazione Red Carpet)

Il Target (Spear Phishing): Il nostro target non è un CEO, ma un individuo molto più vulnerabile e con accessi "interessanti": "Marco Bianchi", *Events & Community Manager* presso "QuantumLeap Solutions", una nota azienda italiana di consulenza IT.

Fase di Information Gathering (OSINT): Prima dell'attacco, abbiamo raccolto informazioni su Marco:

1. **LinkedIn:** È l'*Events & Community Manager*. I suoi post recenti mostrano grande entusiasmo per l'imminente "Milano Digital Week" (MDW). Ha taggato il CEO e il reparto marketing, confermando che QuantumLeap Solutions sarà uno speaker/sponsor principale.
2. **Sito MDW:** Il sito ufficiale della Milano Digital Week conferma che "QuantumLeap Solutions" è uno sponsor *Platinum*. Il loro CEO terrà un keynote il secondo giorno.
3. **Sito QuantumLeap:** La sezione "News" del loro sito ha un comunicato stampa sulla partnership con la MDW, con una foto di Marco e una sua citazione.
4. **Email Aziendali:** Troviamo un'email legittima di una newsletter passata di QuantumLeap. Notiamo che il loro formato email è `nome.cognome@quantumleapsolutions.it`. Quindi, il nostro target è `marco.bianchi@quantumleapsolutions.it`.
5. **Email degli Organizzatori:** Troviamo una vecchia email pubblica degli organizzatori della MDW, "DigitalEvents Italia". Il loro dominio email è `@digitalevents-italia.com`.

L'Attacco Multi-Vettore:

Useremo una combinazione di tecniche:

1. **Clone Phishing:** Cloneremo un'email di "Aggiornamento Logistico" inviata dagli organizzatori della MDW (DigitalEvents Italia).
2. **Spear Phishing:** L'email sarà personalizzata per Marco, menzionando il suo ruolo, la sua azienda e lo **status di sponsor *Platinum***.
3. **Quishing (QR Code):** L'email conterrà un QR code. Il pretesto sarà nuovo e creativo: un "aggiornamento esclusivo per gli speaker e gli sponsor Platinum" per accedere a una *nuova area VIP/Networking* non ancora annunciata pubblicamente. Il QR code serve per "validare" l'accesso a questa nuova area esclusiva.(muahhahha)
4. **Vishing:** La pagina di destinazione del QR code (una pagina clone) ruberà le credenziali. *Subito dopo*, un messaggio di "errore di validazione" chiederà a Marco di aspettare una chiamata dal "Servizio Concierge VIP" per una verifica manuale. Seguirà la telefonata di Vishing per rubare il codice 2FA/MFA.

Obiettivo: Ottenere le credenziali di Single Sign-On (SSO) di Marco e bypassare l'MFA per accedere all'account Microsoft 365 di QuantumLeap Solutions. Con questo accesso, l'obiettivo secondario è trovare documenti sensibili sulla strategia aziendale, liste clienti o rubare il materiale del keynote del CEO prima che venga presentato.

2. L'Email di Phishing (Clone + Spear + Quishing)

Ecco l'email che invieremo. È progettata per sembrare un "resend" o un aggiornamento di un'email legittima.

“ Mittente: Servizio Concierge MDW concierge-vip@digitalevents-italia.org ”

Oggetto: URGENTE: [REPLY] Aggiornamento Accesso VIP per QuantumLeap Solutions alla Milano Digital Week

Corpo dell'email:

Gentile Marco Bianchi,

Facendo seguito alla nostra precedente email del 15 Ottobre e alla conferma del vostro status di Sponsor Platinum, siamo lieti di inviarti questa comunicazione *riservata*.

Abbiamo finalizzato i dettagli per la nuova "Platinum Lounge", un'area networking esclusiva e non pubblica riservata ai nostri sponsor principali, speaker e ospiti VVIP. Quest'area non sarà indicata sulle mappe ufficiali per garantire la massima privacy.

Per motivi di sicurezza e per gestire gli accessi a questa nuova area, abbiamo aggiornato il sistema di pass. La precedente registrazione è stata migrata, ma richiediamo una validazione finale del tuo "Platinum Pass" digitale.

Per evitare code o problemi di accesso il giorno dell'evento, ti preghiamo di convalidare il tuo pass entro oggi, 24 Ottobre, utilizzando il nostro portale di sicurezza unificato (SSO).

Azione richiesta: Per favore, inquadra il QR code sottostante con il tuo smartphone per accedere al portale di validazione e confermare il tuo profilo.

[Immagine di un QR Code grande e chiaro, con il logo "MDW Platinum" al centro]

Questa procedura sincronizzerà il tuo account aziendale (marco.bianchi@quantumleapsolutions.it) con il sistema di accesso sicuro della Platinum Lounge.

Ci scusiamo per questo passaggio aggiuntivo, ma è fondamentale per garantire un'esperienza esclusiva e sicura a partner di valore come QuantumLeap Solutions.

Restiamo a disposizione per qualsiasi necessità.

Cordiali Saluti,

Il Team Concierge VIP DigitalEvents Italia | Organizzatori Milano Digital Week

--- [Footer clonato dall'email originale, con loghi MDW, link ai social media reali, indirizzo e P.IVA reali di DigitalEvents Italia] - "

3. Spiegare lo Scenario (La Catena d'Attacco)

Perché potrebbe sembrare credibile:

1. **Contesto Impeccabile (Spear Phishing):** L'email arriva a ridosso dell'evento, quando le comunicazioni logistiche sono frequenti e spesso urgenti. Cita il *nome reale* di Marco, la sua *azienda reale* e il loro *status reale* di Sponsor Platinum.
2. **Leva Psicologica (Baiting):** Non usa la paura (come una banca), ma l'esclusività e lo status. L'idea di una "Platinum Lounge" segreta è un'esca perfetta per un Community Manager. È un "benefit" che Marco vorrà assolutamente avere.
3. **Clonazione Perfetta (Clone Phishing):** L'email usa la firma, i loghi e il tono di voce esatti degli organizzatori reali (copiati da una loro email legittima). L'oggetto "REPLY" e "URGENTE" la fa sembrare un follow-up importante.
4. **Pretesto Moderno (Quishing):** L'uso di un QR code per l'accesso a un'area VIP è estremamente plausibile. Gli eventi moderni usano continuamente app e QR code per gestire gli accessi. Questo bypassa i filtri email che cercano URL malevoli.
5. **Typosquatting Sottile:** Il dominio del mittente è @digitalevents-italia.org (usato dall'attaccante) invece di quello legittimo @digitalevents-italia.com. In un'email fitta di dettagli, è un errore quasi impossibile da notare a colpo d'occhio.

Tecnica che ho usato in tutto il report è stata quella di evidenziare in verde le cose originali come email indirizzi o ip , in arancione le cose usate dall' attaccante.

La Catena d'Attacco in Dettaglio (Quishing + Vishing):

Fase 1: Il Click (Scan) Marco, entusiasta all'idea della lounge VIP e pressato dall'urgenza, scansiona il QR code.

Fase 2: Il Furto di Credenziali Il QR code apre il browser del suo smartphone su mdw-vip.portal-access.com. Questa pagina è un clone perfetto della pagina di login di Microsoft 365 (SSO) di QuantumLeap Solutions. Pensa che sia il "portale unificato" menzionato nell'email. Inserisce:

- Email: marco.bianchi@quantumleapsolutions.it
- Password: [LaSuaPasswordReale123!](#) L'attaccante riceve e salva queste credenziali in tempo reale.

Fase 3: Il Setup del Vishing Dopo aver inserito la password, la pagina non si blocca. Mostra un messaggio di errore ingegnerizzato: *"Verifica profilo riuscita. Sincronizzazione 2FA... ERRORE (Codice: V-881). Il tuo account richiede una validazione vocale di sicurezza per l'attivazione del Pass Platinum. Un operatore del nostro 'Servizio Concierge VIP' ti contatterà sul numero associato al tuo profilo entro 60 secondi per completare l'attivazione. Non chiudere questa pagina."*

Fase 4: Il Bypass dell'MFA (Vishing) L'attaccante, che ora ha la password di Marco, la inserisce nel vero portale login.microsoftonline.com. Il sistema Microsoft, come previsto, invia a Marco una notifica *push* sulla sua app Microsoft Authenticator (o un SMS con un codice OTP). *Proprio in quel momento*, il telefono di Marco squilla. (muahhhaha)

Risultato: L'attaccante ha bypassato l'MFA (usando l'ingegneria sociale per far approvare la notifica push) e ha ora una sessione valida e autenticata nell'account Microsoft 365 di Marco Bianchi. L'Operazione Red Carpet è riuscita.

Conclusione: L'Importanza della Vigilanza Umana

Questo scenario, sebbene simulato, evidenzia una verità fondamentale della sicurezza informatica: **l'anello umano rimane spesso il più vulnerabile**. L'attacco di phishing "Banca Sicura" dimostra come la manipolazione psicologica, basata su leve emotive come la paura e l'urgenza, sia progettata per bypassare il pensiero critico e indurre a un'azione impulsiva. Manipolazione psicologica che caratterizza anche gli altri 2 attacchi, "Helpful AI" e "operazione red carpet", anche se l'ultimo risulta essere molto più complesso strutturalmente, in quanto l'adozione di diverse tecniche partecipano equamente a renderlo un efficiente attacco multivettoriale, del quale sono soddisfatto. L'aiuto dell'LLM come da consegna è stato fondamentale per la stesura dell'email ed alcune ricerche su web, anche tramite le google dorks che abbiamo visto a lezione, mi hanno chiarito alcune idee e dubbi, perfezionando il report.

Dunque non importa quanto siano sofisticati i filtri anti-spam o le protezioni tecniche; un'email ben congegnata può sempre trovare la sua strada verso la casella di posta di un utente. L'unica difesa veramente efficace, in ultima istanza, è la consapevolezza. Questo esercizio rafforza la necessità di una

formazione continua e di un approccio "zero-trust" a qualsiasi comunicazione non richiesta: **verificare prima di cliccare**, analizzare sempre il mittente e l'URL di destinazione, e trattare ogni richiesta di credenziali con il massimo scetticismo.