

Progetto S5/L5

Obiettivo: simulare un attacco di phishing tramite una mail malevola. L'obiettivo è mostrare come un attacco apparentemente innocuo possa diventare un punto di ingresso per compromettere non solo account personali, ma anche risorse aziendali. In questo scenario la vittima lavora per **GLS Italia**.

1) Scenario

Profilo della vittima:

Nome: Luca Bianchi

Età: 31 anni

Professione: analista logistica digitale

Azienda: GLS (sede di Milano)

Account social attivi: Instagram, Facebook, LinkedIn

Dispositivi: iPhone personale, laptop aziendale (Windows), tablet aziendale Android

Informazioni su GLS Italia

GLS è uno dei principali operatori europei nel settore di spedizioni, con migliaia di clienti business, come Amazon, Zalando, e-commerce e pubbliche amministrazioni. L'infrastruttura IT di GLS gestisce ogni giorno:

- Dati di tracciamento in tempo reale
- Informazioni su clienti, ordini e mittenti
- Documenti doganali e bolle di trasporto
- Accessi riservati al sistema gestionale logistico

In questo contesto abbiamo Luca, impiegato di 31 anni che lavora nel reparto logistica digitale di GLS Italia. Usa regolarmente Instagram da mobile e riceve spesso e-mail legittime che gli notificano i nuovi accessi.

2) Contesto del Phishing

Luca un giorno riceve una mail con le seguenti caratteristiche:

- **Mittente:** security@mail.instagram-alert.com
- **Oggetto:** "Abbiamo notato un nuovo accesso, luca.bianchi"

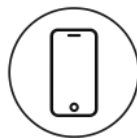
(nella pagina successiva è presente la mail di phishing scritta con l'ausilio di ChatGPT)



Abbiamo notato un nuovo accesso,

luca.bianchi

Abbiamo notato un accesso da un dispositivo
che non usi abitualmente.



Apple iPhone · Chrome Mobile · Milan,


Italy


August 1 at 10:24 AM (PDT)

Se l'azione non è stata eseguita da te, non
potrai accedere ad alcune impostazioni
dell'account e di sicurezza per qualche giorno.

Potrai continuare ad accedere a queste impostazioni
da un dispositivo con cui hai
effettuato l'accesso in passato.

 **PROTEGGI SUBITO IL TUO ACCOUNT DA ACCESSI NON AUTORIZZATI:**

 <https://instagram-secure-login.help/auth>

 **IGNORARE QUESTA RICHIESTA POTREBBE COMPORTARE UNA SOSPENSIONE
TEMPORANEA DEL TUO ACCOUNT SE NON PROCEDI ENTRO 24 ORE.**

from



© Instagram. Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025

La mail presenta un layout molto realistico e i loghi ufficiali (scaricati dal Brand Resource Center di Meta).

Luca, leggermente preoccupato, clicca sul link senza controllare l'URL. Viene reindirizzato a un sito identico a Instagram, ma, a sua insaputa, ospitato su un dominio falso. Inserisce nome utente e password, convinto di mettere al sicuro il suo account. In realtà ha appena consegnato le sue credenziali ad un attaccante, che ora non solo ha accesso al suo profilo Instagram ma a un'informazione ancora più preziosa.

3) Obiettivo reale dell'attaccante

L'attaccante non è interessato solo a rubare l'account Instagram, ma spera che Luca:

- Usi la stessa e-mail e password per altri servizi.
- Non abbia attivato l'autenticazione a due fattori (2FA).
- Abbia accesso ad ambienti aziendali, ad esempio attraverso la sua e-mail di lavoro o software aziendale.

Infatti, Luca usa la stessa combinazione e-mail + password anche per:

- Il suo account aziendale (luca.bianchi@gls-italy.com)
- L'accesso ai portali interni di GLS, come il gestionale di tracciamento spedizioni.

GLS potrebbe essere un bersaglio interessante per un attaccante in quanto con un accesso rubato potrebbe:

- Intercettare o modificare spedizioni
- Rubare dati commerciali riservati
- Iniettare malware nel sistema tramite un utente compromesso
- Avviare attacchi supply chain a clienti partner (es. Amazon, Zalando)

4) Tecniche di attacco usate

Tecnica	Descrizione
Spoofing visivo	L'email è identica a quelle vere, quindi genera fiducia automatica.
Ingegneria sociale	Fa leva sulla paura di un accesso non autorizzato.
Familiarità	Copia stile, font, struttura già nota all'utente.
Phishing mirato (spear phishing)	L'attacco è pensato contro una persona che lavora in un'azienda sensibile.
Credential stuffing	Se le credenziali Instagram funzionano altrove, vengono testate in massa.

5) Impatto potenziale per l'azienda attaccata

Un attacco del genere potrebbe provocare dei danni irreparabili e gravissimi per l'azienda, sia a livello tecnico che economico.

Ad esempio:

- Violazione dell'infrastruttura di rete aziendale
- Accesso a credenziali di colleghi
- Perdita di fiducia di clienti e partner
- Potenziale richiesta di riscatto in caso di ransomware
- Sanzioni in base al GDPR (Regolamento Generale sulla Protezione dei Dati) per mancata protezione dei dati
- Notorietà negativa sui media
- Diffusione dell'incidente su forum o canali pubblici
- Impatto su collaborazioni internazionali e appalti pubblici

6) Difese e contromisure

Per evitare questo tipo di attacchi, sia l'utente che l'azienda devono adottare una serie di difese e contromisure.

Utente:

- Usare password univoche con un password manager
- Mai cliccare su link in e-mail
- Abilitare 2FA su tutti i servizi, non solo la mail
- Verificare l'URL effettivo del link allegato nella mail

Azienda:

- Formazione sulla sicurezza obbligatoria per tutti i dipendenti ogni 6 mesi.
- Simulazioni di phishing
- Protezione anti-phishing nei client di posta (Microsoft Defender, Proofpoint)
- Segmentazione della rete per contenere movimenti laterali
- Controllo accessi con Zero Trust Architecture

7) Conclusione

Questa simulazione evidenzia come una semplice e-mail apparentemente innocua possa diventare il punto di accesso a un'infrastruttura critica aziendale, sfruttando l'ingegneria sociale, la fiducia nell'interfaccia e la debolezza delle abitudini umane. Il caso di Luca dimostra come la paura di perdere l'accesso a un account personale possa spingere un dipendente a compiere un'azione impulsiva, aprendo involontariamente le porte a un attacco ben più grande e pericoloso per l'intera azienda.