

Esercizio per il progetto settimanale Unit 2 - S5 - L5

L'esercizio consiste nella creazione di una **simulazione** di un'email di phishing in cui ipotizzare uno scenario pensando ad un contesto realistico, scrivere l'email di **phishing** convincente e originale e infine descrivere lo scenario creato.



Renova è un'azienda moderna e flessibile che offre servizi completi alle imprese, aiutandole a **crescere e innovare**. Grazie a un team con competenze diverse e ben coordinate, Renova affianca i propri clienti in ogni fase del loro sviluppo, proponendo soluzioni pratiche e su misura.

L'azienda è suddivisa in aree operative, ognuna con compiti specifici:

● **Area Marketing e Comunicazione**

Si occupa della promozione e dell'immagine delle aziende clienti: crea campagne pubblicitarie, cura i contenuti per i social, progetta loghi, siti e strategie per migliorare la visibilità e attrarre nuovi clienti.

● **Area Sviluppo Software e IT**

Realizza programmi e strumenti digitali personalizzati, come gestionali, app o piattaforme online, che aiutano le aziende a lavorare meglio e in modo più organizzato.

● **Area Risorse Umane**

Gestisce tutto ciò che riguarda il personale: ricerca nuovi collaboratori, organizza corsi di formazione e supporta le aziende nella creazione di un ambiente di lavoro positivo e produttivo.

● **Area Amministrazione e Logistica**

Si occupa della contabilità, dei pagamenti, delle fatture e di tutte le attività amministrative. Inoltre, gestisce l'acquisto e l'organizzazione delle attrezzature da ufficio, assicurando che ogni reparto abbia ciò di cui ha bisogno per lavorare al meglio.

Esempio email phishing reparto IT e sviluppo Software

Per il reparto Software e IT ho pensato a 2 modelli di possibile phishing:

- **Finto nuovo accesso a bitwarden per nuovo dipendente**
- Finto push fallito su GitHub

Esempio email phishing proveniente da bitwarden



Bitwarden è un gestore di **password** che consente di salvare, organizzare e condividere in modo protetto le credenziali aziendali.

In questo contesto stiamo mandando una mail di phishing riguardo un nuovo dispositivo connesso al servizio all'interno dell'ambiente aziendale (reso reale dalla data e IP veritieri), se un attaccante dovesse venire a conoscenza di una recente assunzione di un nuovo dipendente all'interno dell'azienda (tramite linkedIn per esempio) questo può essere un metodo efficace per ottenere delle preziose credenziali di accesso.

Nuovo dispositivo connesso da Safari



Bitwarden (no-reply[.]bitwarden@cloud-notification-services[.]com)
to soniagrasso@renova[.]com



Il tuo account Bitwarden è appena stato effettuato l'accesso da un nuovo dispositivo.

Data: Fri Aug 01 2025 12:12:55 GMT+0200 (Ora legale dell'Europa centrale)

IP Address: 159.196.12.160

Device Type: Safari

Puoi rimuovere l'autorizzazione di tutti i dispositivi che hanno accesso al tuo account dal [web vault](#) in Impostazioni | Il mio account | Rimuovi l'autorizzazione delle sessioni. Oppure [fai clic qui per eseguire](#) una reimpostazione della password.

Esempio email phishing reparto IT e sviluppo Software

Per il reparto Software e IT ho pensato a 2 modelli di possibile phishing:

- Finto nuovo accesso a bitwarden per nuovo dipendente
- **Finto push fallito su GitHub**

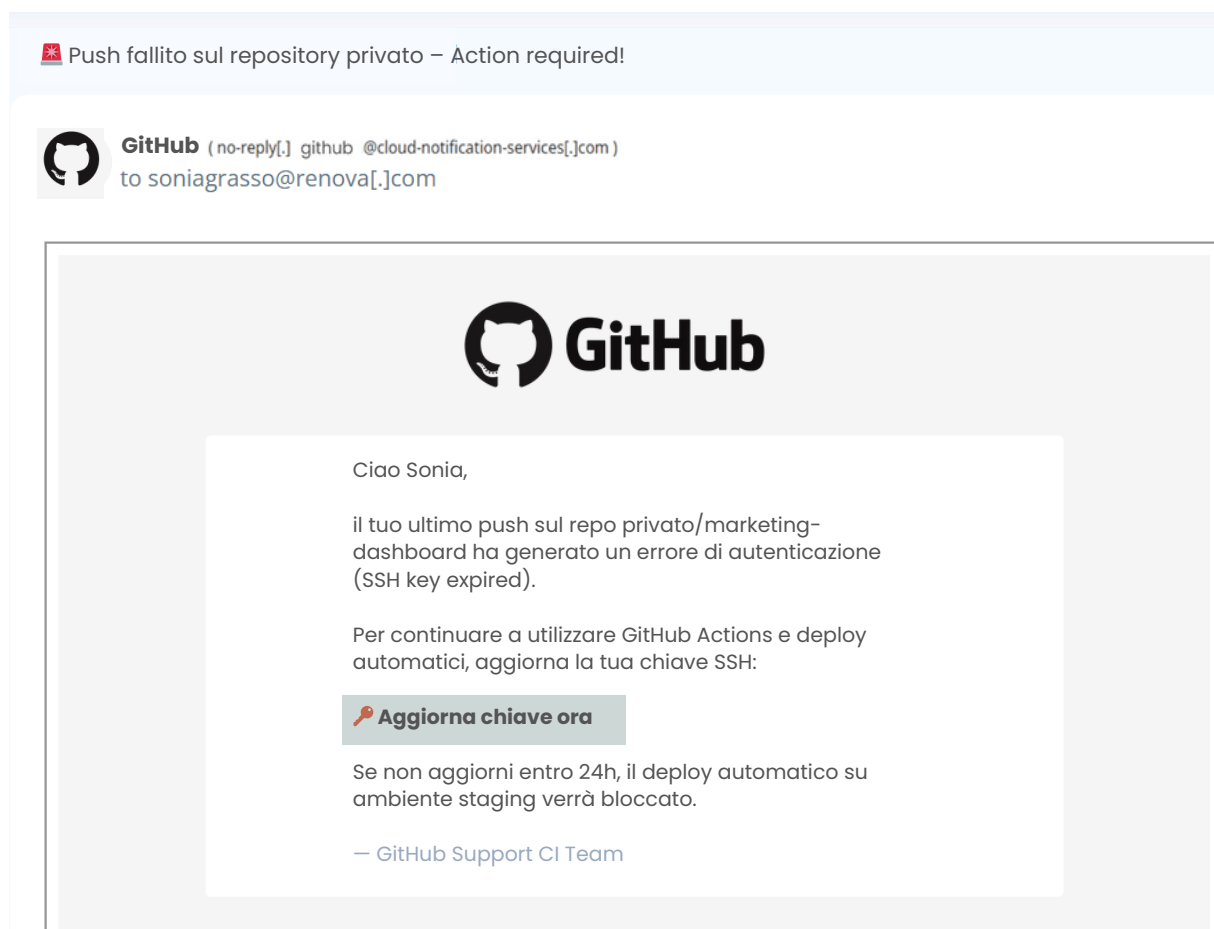
Esempio email phishing proveniente da GitHub



GitHub è una piattaforma online che permette agli sviluppatori di salvare, gestire e condividere il codice sorgente dei loro **progetti**.

In questo contesto credere a una finta email che segnala un push fallito su GitHub è pericoloso perché spinge l'utente a cliccare su un link e Inserire le proprie credenziali o aggiornando chiavi SSH su questo falso portale, l'attaccante può ottenere l'accesso al codice sorgente, strumenti di sviluppo e documentazione privata dell'azienda mettendo a rischio la sicurezza dell'intera infrastruttura software e causando danni all'azienda.

Varianti: una mail per partecipare ad un finto corso di aggiornamento di HTML



Esempio email phishing reparto HR Risorse Umane

Per il reparto HR Risorse Umane ho pensato ad un metodo di phishing che richiama una call to action per scaricare un documento riguardo le prestazioni dei dipendenti, molto utile nell'ambito delle risorse umane.

Esempio email phishing proveniente da Microsoft



Microsoft OneDrive è uno spazio cloud che consente di archiviare e condividere file online, mentre **Word** permette di creare e modificare documenti, anche in modo collaborativo condividendo i documenti tra i reparti dell'azienda. In ambito aziendale, questi strumenti sono spesso usati per condividere documenti riservati, contratti, report o dati interni. Una finta email di phishing che richiede le credenziali dell'account Microsoft può essere estremamente pericolosa: se un dipendente cade nella trappola, un attaccante può accedere a OneDrive e Word online, visualizzando, copiando o modificando documenti sensibili, con gravi rischi per la sicurezza dei dati aziendali.

Microsoft 365 Support ha condiviso con te «Rapporti sulle prestazioni dei dipendenti».



Microsoft 365 Support (support@office-365-notifications[.]com)
to ilariacorsi@renova[.]com

Microsoft 365 Support ha condiviso un file con te



Questo link funzionerà per chiunque faccia parte della tua organizzazione.



Rapporti sulle prestazioni dei dipendenti

Aperto



Microsoft OneDrive

Il mittente riceverà una notifica quando aprirai questo link per la prima volta.

Microsoft rispetta la tua privacy. Per saperne di più, leggi la nostra [Informativa sulla privacy](#).
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Esempio email phishing reparto Marketing e Comunicazione

Per il reparto marketing ho pensato a 2 modelli di possibile phishing:

- **Nuovo accesso del profilo TikTok da parte di una collaboratrice finta**
- Accesso ai tool marketing sospetto

Esempio email phishing proveniente da TikTok

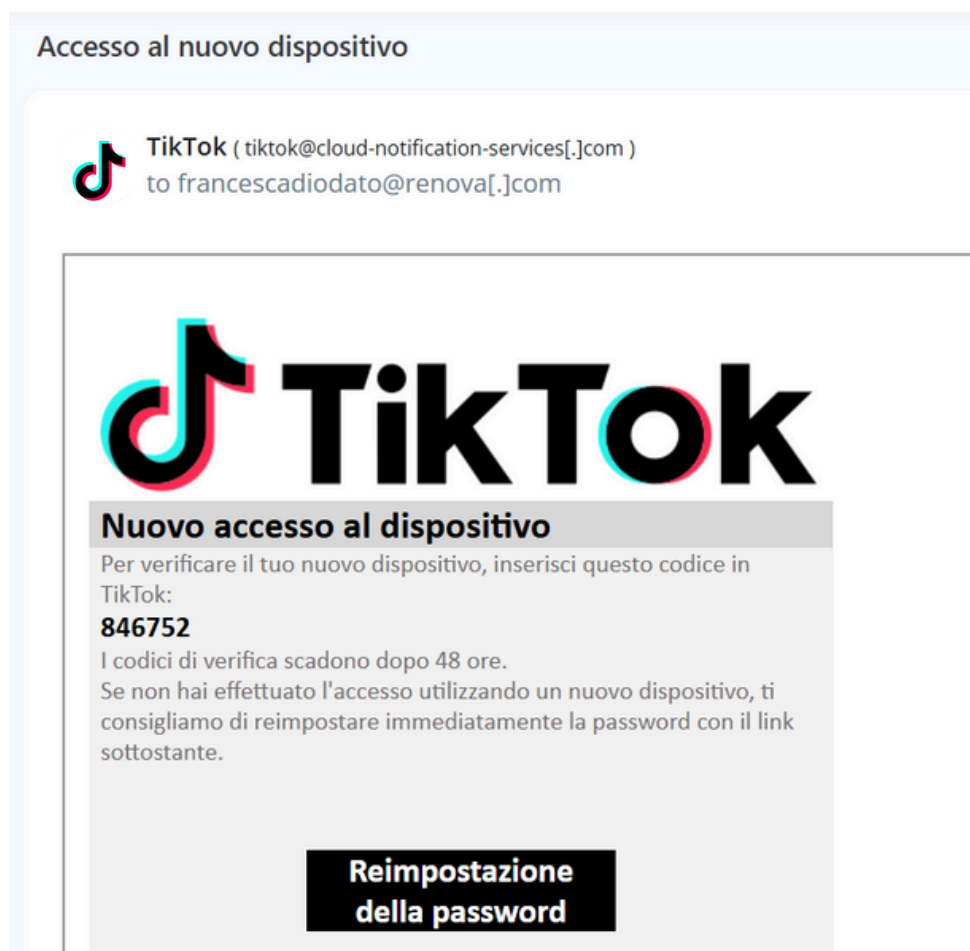


TikTok è una piattaforma di social media sempre più utilizzata nel marketing per aumentare la visibilità del brand, e promuovere **prodotti o servizi**.

Se un attaccante entra in possesso delle credenziali di un profilo TikTok aziendale, può pubblicare contenuti dannosi, cancellare video, compromettere l'immagine del brand o persino contattare follower fingendosi l'azienda.

Delle **varianti** potrebbero essere:

- Essere contattati per un campagna influencer per una collaborazione
- Invito ad un evento marketing e call to action per scaricare file informativi



Esempio email phishing reparto Marketing e Comunicazione

Per il reparto marketing ho pensato a 2 modelli di possibile phishing:

- Nuovo accesso del profilo TikTok da parte di una collaboratrice finta
- **Finti movimenti sospetti nei tool marketing**

Esempio email phishing proveniente da Google Ads



Google Ads è una piattaforma pubblicitaria che consente alle aziende di promuovere i propri **prodotti o servizi** su Google e siti partner, raggiungendo clienti in modo mirato.

Se un attaccante accede all'account Google Ads, può modificare o creare campagne fraudolente e, se ottiene i dati di pagamento, usarli per addebitare costi illeciti, causando danni economici e compromettendo la reputazione dell'azienda nonché avere accesso a dati di altre aziende partner.

Varianti: accesso sospetto non collegato alle coordinate bancarie.

Aggiornamento obbligatorio delle coordinate bancarie – Google Ads Billing

 **Google Ads** (no-reply[.] github @cloud-notification-services[.]com)
to soniagrasso@renova[.]com



Gentile cliente,

a seguito di una revisione del vostro account pubblicitario, abbiamo rilevato che le informazioni bancarie associate al profilo di pagamento risultano incomplete o non aggiornate.

Per evitare la sospensione automatica delle campagne attive, vi invitiamo ad aggiornare i dati del conto corrente utilizzato per i pagamenti delle inserzioni:

 [Aggiorna i dati di pagamento](#)

L'aggiornamento è richiesto entro 48 ore. In caso contrario, il sistema non sarà in grado di prelevare i fondi necessari per le campagne in corso.


[Google Ads Billing Support](#)

Esempio email phishing reparto Logistica

Per il reparto di amministrazione e logistica ho pensato ad una situazione in cui l'attaccante potrebbe (o no) venire a conoscenza dell'arrivo di nuove strumentazioni così da poter sfruttare il corriere come mezzo di furto di dati

Esempio email phishing proveniente da FedEx

Cadere nella trappola di questa finta email di FedEx è pericoloso perché, inviando la copia del documento d'identità di un dipendente, si fornisce a un attaccante un dato altamente sensibile che può essere usato per **furti di identità**, attivazione di servizi o conti fraudolenti, falsificazione di richieste aziendali, o per attacchi mirati più sofisticati. L'attaccante potrebbe inoltre sfruttare il documento per fingersi il dipendente verso fornitori, clienti o enti pubblici, compromettendo la sicurezza e la reputazione dell'azienda.

 **FedEx Online** (fedex-online@webnotifications[.]net)
to mario[.]rossi@renova[.]com

Verifica d'identità richiesta – Consegna FedEx in attesa per Renova Srl


Gentile **ufficio amministrativo**,

la spedizione destinata a **Renova Srl** è attualmente trattenuta presso il nostro centro logistico in attesa di verifica.

Come previsto dalle nuove linee guida per consegne aziendali di valore, è richiesta la copia fronte/retro di un **documento d'identità** del referente aziendale autorizzato a ricevere la merce. Vi invitiamo a inviare il documento in risposta a questa email entro 24 ore per evitare ritardi o il rientro del pacco al mittente.

La tua spedizione è stata affidata a FedEx Ground

Tracciamento # 700333134573

Data spedizione: In sospeso		Consegna programmata: In sospeso
REPARTO SPEDIZIONI WESTAMPTON, NEW JERSEY 08060 NOI	In transit	Mario Rossi

Dati relativi alla spedizione

Numero di tracciamento:	700333134573
Numero della fattura:	3249-A745
Numero dell'ordine di acquisto:	10235331
Riferimento:	10235531W
Tipo di servizio:	Consegna FedEx Express

Esempio email phishing reparto Amministrazione e Finanziario

Per il reparto di amministrazione e finanziario ho pensato ad una situazione in cui l'attaccante potrebbe venire a conoscenza di una nuova collaborazione con un partner internazionale e che quindi gli uffici si aspettino dei pagamenti.

Esempio email phishing proveniente da Bank of America



Se un attaccante ottiene i **dati bancari** del reparto finanziario di un'azienda, può usarli per tentare frodi come la modifica delle coordinate su fatture, truffe ai fornitori, pagamenti non autorizzati o furti di fondi. Inoltre, con queste informazioni può simulare comunicazioni credibili per ingannare altri reparti interni o partner esterni, mettendo a rischio la sicurezza economica e la credibilità dell'azienda.

Varianti: Email sulla necessità di revisionare i tassi del cambio valuta, Mail proveniente da un ente italiano del fisco per la revisione dei pagamenti internazionali o attività sospette di scambio di soldi tra stati diversi

Abbiamo rilevato attività insolite sul tuo account



Bank of America (bank-of-america@mail31[.]com)
to carlobonacci@renova[.]com

BANK OF AMERICA



Abbiamo rilevato attività insolite sul tuo account

Carlo Bonacci,

Noi di Bank of America prendiamo molto sul serio la sicurezza del tuo account. Durante il nostro recente monitoraggio di routine, abbiamo rilevato alcune attività insolite sul tuo conto che non sono in linea con i tuoi schemi bancari tipici.

Per la sicurezza del tuo account, abbiamo temporaneamente sospeso qualsiasi altra transazione. Ti chiediamo gentilmente di rivedere l'attività recente sul tuo account accedendo per verificare se le transazioni sono state effettuate da te.

[Accedi al tuo account](#)

Grazie per la pronta attenzione prestata a questo argomento. Ci scusiamo per gli eventuali disagi causati e apprezziamo la tua comprensione mentre lavoriamo per garantire la sicurezza del tuo account.

progetto settimanale svolto da Gioele Parla