Progetto S5/L5

Marco Falchi

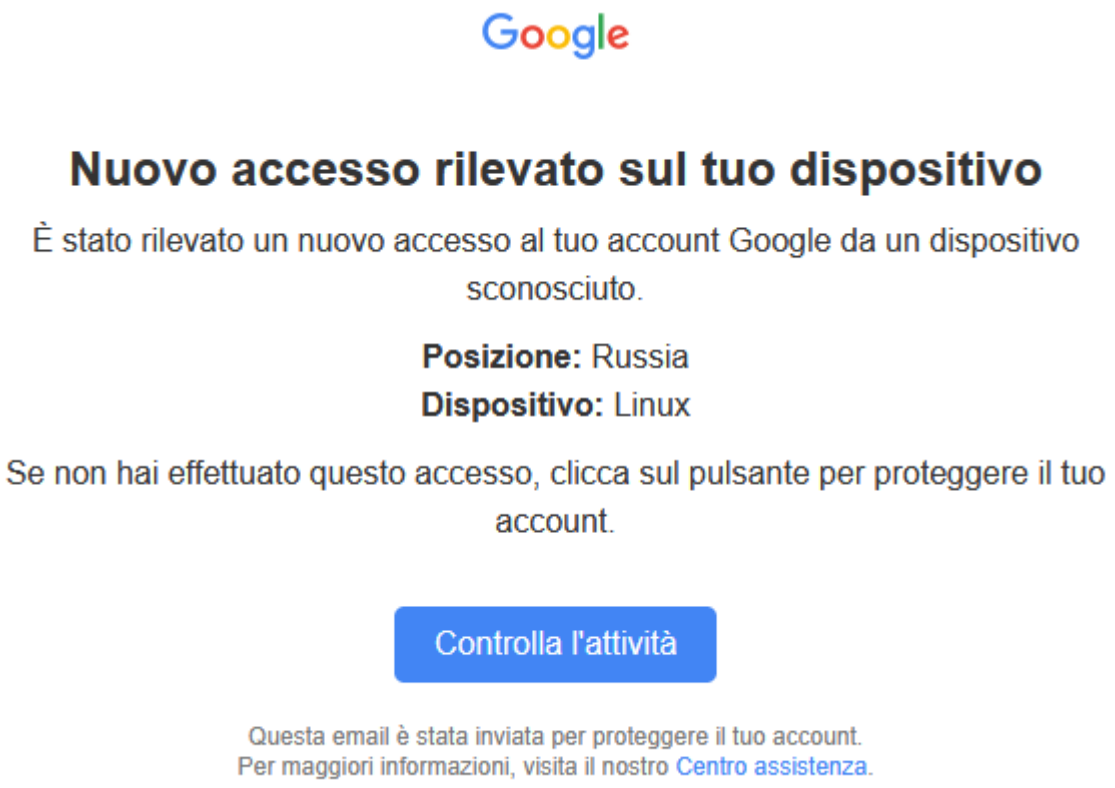
Simulazione di Phishing su Target emulando email di avviso Google

Introduzione

Il progetto consiste nella creazione di una simulazione di phishing realistico indirizzato agli utenti di Google, un target molto comune data l'ampia diffusione di account Google in tutto il mondo. Utilizzando il contesto di una notifica di sicurezza, abbiamo generato un'email che replica accuratamente il design e il tono delle comunicazioni ufficiali di Google.

Scenario Creato

Ho deciso date le mie esperienze pregresse di simulare un'email di notifica di sicurezza inviata da Google, avvisando l'utente di un **accesso non autorizzato** rilevato sul proprio account.



Dettagli dell'email:

- **Mittente:** no-replai@accounts.google.com
- **Oggetto:** "Avviso di sicurezza: Nuovo accesso rilevato sul tuo account Google"
- **Corpo del messaggio:**
    - Un avviso che informa l'utente di un tentativo di accesso sospetto da un dispositivo sconosciuto.
    - Contiene una chiamata all'azione (CTA) per "Controllare l'attività".
- **Pulsante (CTA):** "Controlla l'attività" che reindirizza a un **falso sito di login** progettato per **catturare le credenziali dell'utente**.

L'email è stata progettata in HTML, replicando quasi fedelmente il design delle notifiche ufficiali di Google, inclusi:

- **Logo ufficiale Google.**
- Colori e font simili o uguali alle comunicazioni originali di google.

Perché l'email potrebbe sembrare credibile

L'email è progettata per sembrare autentica grazie ai seguenti fattori:

1. **Mittente realistico:** L'indirizzo email del mittente (no-repl**ai**@accounts.google.com) è simile a quello utilizzato da Google, ossia **no-reply@accounts.google.com**.
2. **Design coerente:** Il layout dell'email imita quasi perfettamente le notifiche di sicurezza di Google.
3. **Contenuto contestuale:**
    - La notifica sfrutta un evento comune, come un **accesso sospetto**, per **creare urgenza**.
    - Questo è un classico esempio di **ingegneria sociale** per indurre l'utente ad **agire rapidamente**.
4. **Pulsante visibile e intuitivo:** Il pulsante "Controlla l'attività" è prominente, invitando l'utente a cliccare.

Elementi che potrebbero far sorgere sospetti nel target

Nonostante l'email sembri autentica, ci sono alcuni **piccoli dettagli** che potrebbero destare sospetti nel target:

1. **Assenza di personalizzazione:**
    - Non viene riportato l'indirizzo email del destinatario sotto il titolo "Nuovo accesso rilevato", questo perché ho pensato a questa email come **un'email di massa** e quindi non personalizzabile, ma nel caso di target singolo è **facilmente implementabile**.
2. **Link sospetto:**
    - Il pulsante "Controlla l'attività" reindirizzerebbe a un dominio falso (http://google-support-securechangepassword-login.com) invece che al dominio ufficiale (https://accounts.google.com).
3. **Errori di sintassi o stilistici:**
    - Piccole incongruenze stilistiche (come il logo più piccolo) potrebbero insospettire un utente esperto.
4. **Aggiunta di informazioni non presenti in originale:**
    - Ho aggiunto anche la provenienza dell'accesso e il dispositivo, quindi nel nostro caso Russia come provenienza e dispositivo Linux in quanto questo a parer mio aiuta ad "**aumentare l'urgenza nel target"** in quanto la Russia è famosa per attacchi hacking e Linux è il sistema operativo più usato.

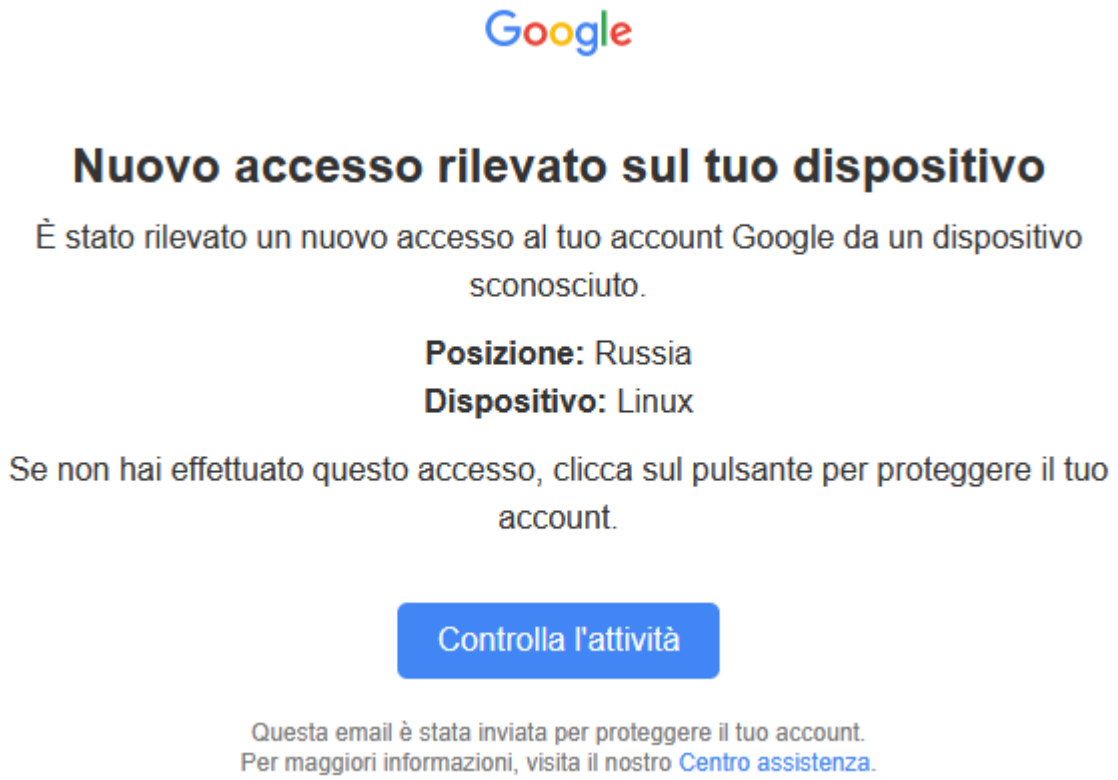
Tuttavia, l'utente medio potrebbe **non notare questi segnali**, lasciandosi ingannare facilmente.

Differenze fra email reale e email creata da me:

Email reale:

Mittente: no-reply@accounts.google.com

Email creata da me:



Mittente: no-replai@accounts.google.com

Conclusioni

Il progetto ha dimostrato come un'email di phishing possa essere resa credibile utilizzando:

- Tecniche di **ingegneria sociale**.
- Design **visivamente autentico**.
- Creando **urgenza** nel target.

Questa simulazione evidenzia:

- La necessità di educare gli utenti su come riconoscere i segnali di phishing.
- L'importanza di verificare sempre i dettagli di un'email (es. dominio, personalizzazione) prima di interagire con essa.