# Simulazione di Email di Phishing

Report di analisi – Cybersecurity e Ingegneria Sociale

## 1. Introduzione

Il presente documento costituisce un report di analisi relativo a una simulazione di email di phishing, realizzata a scopo esclusivamente didattico. L'obiettivo è analizzare le tecniche di ingegneria sociale utilizzate negli attacchi di phishing e sviluppare una maggiore consapevolezza nella valutazione delle comunicazioni digitali in ambito aziendale.

## 2. Contesto aziendale e scenario

Lo scenario è ambientato all'interno dell'azienda fittizia **TechNova S.p.A.**, operante nel settore dei servizi digitali. I dipendenti utilizzano quotidianamente account di posta elettronica aziendali per comunicazioni interne, accesso agli strumenti di lavoro e ricezione di notifiche ufficiali.

L'email di phishing simulata si presenta come una comunicazione proveniente dal Supporto IT interno dell'azienda.

## 3. Obiettivo dell'attacco simulato

L'obiettivo dell'attacco di phishing simulato è indurre il destinatario a inserire le proprie credenziali di accesso alla posta elettronica aziendale, facendo leva su un presunto problema di sicurezza e sulla minaccia di una sospensione imminente del servizio.

## 4. Email di phishing simulata

**Oggetto:** Azione richiesta: verifica di sicurezza account email
**Mittente:** Supporto IT – TechNova S.p.A.

---

Gentile utente,

il nostro sistema di monitoraggio ha rilevato un accesso anomalo al tuo account email aziendale. Per motivi di sicurezza, l'account verrà temporaneamente sospeso entro **2 ore** se non viene completata la procedura di verifica.

Per evitare l'interruzione del servizio, accedi al portale di verifica e conferma le tue credenziali al seguente indirizzo:

**[link di verifica simulato – non reale]**

In assenza di verifica, non sarà possibile inviare o ricevere messaggi di posta elettronica.

Cordiali saluti,
**Supporto IT**
TechNova S.p.A.

## 5. Perché l'email può sembrare credibile

L'email risulta credibile perché inserita in un contesto aziendale familiare al destinatario. Il riferimento a controlli di sicurezza è coerente con le pratiche adottate dalle aziende moderne. Il linguaggio utilizzato è formale, professionale e privo di errori evidenti.

L'uso del nome dell'azienda e del supporto IT rafforza la percezione di autenticità, mentre l'urgenza temporale riduce la propensione del destinatario a effettuare verifiche approfondite.

## 6. Indicatori di possibile phishing

Nonostante l'apparente legittimità, l'email presenta diversi segnali tipici di un tentativo di phishing:

- Creazione di un senso di urgenza artificiale con una scadenza ravvicinata.
- Richiesta di inserimento delle credenziali tramite un link.
- Messaggio generico, privo di riferimenti personali al destinatario.
- Minaccia di sospensione del servizio come leva psicologica.
- Presenza di un link non chiaramente riconducibile a un dominio ufficiale.

## 7. Conclusioni e Best Practice

La simulazione dimostra come le email di phishing moderne possano apparire altamente professionali, credibili e coerenti con il contesto aziendale in cui vengono ricevute. A differenza delle campagne di phishing più rudimentali, queste comunicazioni non fanno leva su errori evidenti, ma sfruttano dinamiche psicologiche come l'urgenza, l'autorità percepita e la paura di una perdita imminente del servizio.

Il riconoscimento di tali minacce non può quindi basarsi esclusivamente su competenze tecniche, ma richiede attenzione, consapevolezza del contesto e capacità di analisi critica delle comunicazioni digitali. In ambienti lavorativi caratterizzati da ritmi elevati e carichi cognitivi significativi, anche utenti esperti possono commettere errori di valutazione.

Alla luce di quanto analizzato, è possibile individuare alcune **best practice fondamentali** per ridurre il rischio di compromissione:

- Diffidare da comunicazioni che impongono scadenze molto ravvicinate o che richiedono azioni immediate, soprattutto se associate a minacce di sospensione o limitazione del servizio.
- Non inserire mai credenziali di accesso a seguito di link ricevuti via email. In caso di dubbio, accedere al servizio digitando manualmente l'indirizzo ufficiale nel browser.
- Verificare sempre il mittente e il contesto della comunicazione, prestando attenzione a messaggi generici che non fanno riferimento diretto al destinatario.
- Segnalare tempestivamente al reparto IT o al team di sicurezza eventuali email sospette, anche nel caso in cui non siano stati compiuti errori o interazioni con il messaggio.
- Promuovere attività di formazione continua e simulazioni periodiche di phishing per rafforzare la consapevolezza degli utenti e migliorare la postura di sicurezza complessiva dell'organizzazione.

In conclusione, il phishing rappresenta una minaccia che evolve costantemente e che colpisce il fattore umano prima ancora che quello tecnologico. Un approccio efficace alla sicurezza informatica deve quindi integrare strumenti tecnici, processi chiari e una solida cultura della sicurezza condivisa da tutti gli utenti dell'organizzazione.