Phishing
AI POWERED PROTECTION

GUIDA

Riconoscere un'e-mail di phishing prima che sia troppo tardi: guida operativa

Mittente, dominio, urgenza, link nascosti: tutti i segnali da insegnare al proprio team

A cura del team CENANT di GPI Cyberdefence

2 marzo 2026 www.gpiphishing.com

GUIDA

Mittente, dominio, urgenza, link nascosti: tutti i segnali da insegnare al proprio team

01 La prima linea di difesa è la consapevolezza

Il phishing rimane il vettore d'attacco più comune a livello globale, lo confermano sia l'FBI Internet Crime Report che i dati raccolti da CERT-AGID in Italia. La ragione è semplice: funziona. E funziona perché le persone non sanno esattamente cosa cercare.

Questa guida operativa raccoglie i segnali concreti che ogni dipendente — dal receptionist al CFO — dovrebbe conoscere e saper riconoscere prima di cliccare su qualunque link o aprire qualunque allegato.

02 1. Mittente e dominio: il primo controllo da fare

Il dominio è la parte dell'indirizzo e-mail dopo la @. È il primo elemento da verificare, perché è quello più facile da falsificare a livello visivo. Un messaggio da “Banca XYZ Supporto” con indirizzo “support@bankxyz-secure.com” non viene da Banca XYZ: viene da un dominio controllato dall'attaccante.

> *Tecniche comuni: aggiunta di parole come “-secure2, “-support2”, “-update”; utilizzo di domini con TLD diversi (.com invece di .it); typosquatting con lettere invertite o doppiate (es. “bankxyyz.com”).*

03 2. Oggetto e tono: i campanelli d'allarme

Oggetti come “IL TUO ACCOUNT SARÀ CANCELLATO ORA”, “Azione urgente richiesta” o “Hai vinto 10.000 Euro” sono progettati per attivare una risposta emotiva immediata — paura o avidità — prima che il pensiero razionale possa intervenire.

> *Attenzione anche agli errori grammaticali: molte campagne di phishing sono tradotte automaticamente e contengono imprecisioni che un mittente legittimo non commetterebbe.*

RIFERIMENTI

1 FBI Internet Crime Report (2023): il phishing è il tipo di crimine informatico più segnalato a livello globale.

04 3. Link e allegati: non cliccare, prima verificare

Prima di cliccare su qualsiasi link, passare il cursore sopra senza cliccare: l'URL reale appare nella barra inferiore del browser o in un tooltip. Se il testo visibile dice 'www.miabanca.it' ma il link punta a 'www.miabanca.it.uklogin.sicuro.com', è un attacco.

Allegati con estensioni **.exe**, **.zip**, **.docm**, **.xlsm** possono contenere malware. Anche i PDF possono nascondere link o script malevoli. La regola d'oro: in caso di dubbio, non aprire — e contattare direttamente il mittente tramite un canale ufficiale.

> *Regola d'oro: se hai il minimo dubbio, non aprire allegati, non cliccare su link e non rispondere. Contatta direttamente l'azienda tramite i canali ufficiali.*

4. Cosa fare se si cade in un attacco

Cambiare immediatamente la password di tutti gli account coinvolti. Attivare l'autenticazione a due fattori se non già presente. Segnalare l'e-mail come phishing al proprio provider. Se sono stati forniti dati bancari, avvisare immediatamente la banca. Seguire la procedura di segnalazione aziendale per gli incidenti di sicurezza.

In caso di malware, segnalare all'indirizzo ufficiale CERT-AGID: **malware@cert-agid.gov.it**.

RIFERIMENTI

1 FBI Internet Crime Report (2023): il phishing è il tipo di crimine informatico più segnalato a livello globale.

GPI PHISHING — CYBERSECURITY PLATFORM

Insegna al tuo team a riconoscere le e-mail di phishing in tempo reale

Simulazioni, feedback immediato e formazione continua per ridurre drasticamente i click su e-mail malevole.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com