# Strategie per prevenire il phishing nelle piccole imprese: un approccio sistematico alla sicurezza informatica

Le piccole imprese rappresentano un obiettivo privilegiato per gli attacchi di phishing, manifestando una probabilità tre volte superiore di essere vittime di attacchi mirati rispetto alle grandi aziende. Il phishing rappresenta l'utilizzo di comunicazioni elettroniche convincenti per indurre gli utenti ad aprire collegamenti dannosi o scaricare software malevolo, spesso mascherandosi come fonte fidata quale la propria banca, compagnia di carte di credito o un dirigente aziendale.

Le piccole imprese sono bersagli comuni degli attacchi informatici, avendo registrato nel 2023 un numero superiore di violazioni di dati confermate rispetto alle grandi imprese, con l'82% degli attacchi ransomware del 2021 che ha preso di mira specificamente le piccole e medie imprese. Questo preoccupante scenario richiede l'implementazione di strategie difensive articolate e scientificamente validate.

## Riconoscere e bloccare email di phishing

### Meccanismi di autenticazione basati su dominio

L'implementazione di protocolli di autenticazione domini rappresenta la prima linea di difesa contro la compromissione delle comunicazioni elettroniche. Il **Sender Policy Framework (SPF)** costituisce il meccanismo standardizzato attraverso cui

il dominio mittente identifica e asserisce i server di posta autorizzati per un determinato dominio.

Il **DomainKeys Identified Mail (DKIM)** permette al Mail Transfer Agent mittente di apporre una firma digitale crittografica sui header selezionati e sul corpo del messaggio utilizzando una firma RSA, includendo tale firma in un header DKIM che viene allegato al messaggio prima della trasmissione. La validazione della firma assicura al destinatario che il messaggio non abbia subìto modifiche durante il transito.

Il **Domain-based Message Authentication, Reporting and Conformance (DMARC)** rappresenta l'evoluzione più sofisticata, consentendo ai proprietari di domini mittenti di specificare le politiche relative alla verifica dell'autenticità delle proprie comunicazioni elettroniche e le modalità di gestione delle email che falliscono la verifica.

## Implementazione di filtri email avanzati

L'utilizzo di filtri email configurabili può prevenire la maggior parte dei messaggi di phishing dal raggiungere le caselle di posta dei dipendenti. Le tecnologie di sicurezza email possono inoltre implementare meccanismi di autenticazione che verificano l'origine dei messaggi e possono configurare filtri per bloccare comunicazioni non autorizzate.

I filtri avanzati dovrebbero incorporare:

- **Analisi euristica dei contenuti**: Identificazione di pattern linguistici e strutturali caratteristici del phishing
- **Blacklist dinamiche**: Utilizzo di servizi terzi quali Spamhaus Project e SORBS per mantenere elenchi aggiornati di mittenti malevoli
- **Verifica della reputazione dei domini**: Controllo incrociato con database di reputazione per identificare domini compromessi o recentemente registrati

### Tecnologie di sandboxing

L’impiego di “detonation chambers” per aprire collegamenti/allegati ai fini della scansione malware, igienizzazione degli allegati, rappresenta una misura essenziale prima della consegna. Questi ambienti isolati permettono l’esecuzione sicura di codice potenzialmente malevolo senza compromettere l’infrastruttura aziendale.

## Formazione dei dipendenti sulla sicurezza del phishing

### Approcci pedagogici evidence-based

Una forza lavoro adeguatamente formata può imparare a identificare i segni comuni del phishing e prevenire gli attacchi. La ricerca NIST sviluppa la NIST Phish Scale, che consente ai Chief Information Security Officer (CISO) e agli implementatori di training di phishing di valutare più facilmente la difficoltà dei loro esercizi di phishing e spiegare i tassi di click associati.

Con la formazione appropriata e la consapevolezza, la maggior parte degli attacchi di phishing di base possono essere facilmente riconosciuti. Come parte del corso di formazione, è utile utilizzare una varietà di email di phishing note per aiutare le persone a individuare caratteristiche comuni e identificare la truffa.

### Metodologie formative diversificate

La ricerca accademica evidenzia l’efficacia di approcci formativi multipli:

**Gamification:** Gli studi hanno trovato che questo tipo di formazione fa un lavoro fantastico nell’aumentare la partecipazione dei dipendenti e la ritenzione delle informazioni.

**Simulazioni di ingegneria sociale**: La simulazione di ingegneria sociale è un metodo per testare la consapevolezza di sicurezza degli utenti e la preparazione creando una storia di sfondo fittizia che viene utilizzata per influenzare il comportamento o manipolare qualcuno per fornire informazioni private.

**Formazione just-in-time**: Se i dipendenti cliccano sui test di phishing, vengono reindirizzati a una pagina di destinazione con una rapida esperienza di formazione, incluso un video breve, divertente ma educativo insieme a suggerimenti su come individuare ed evitare email di phishing in futuro.

### Metriche di efficacia

Le simulazioni di phishing ripetute hanno dimostrato di essere un modo utile per aiutare i dipendenti a individuare email malevole e quindi ridurre la loro suscettibilità. Dopo aver completato un anno di formazione di consapevolezza del phishing, la percentuale media di propensione al phish è precipitata dal 37,9% al 4,7%, registrando un incredibile tasso di miglioramento dell'87%.

## Autenticazione a più fattori per una maggiore protezione

### Limitazioni dell'MFA tradizionale

L'autenticazione a più fattori (MFA) è richiesta e utilizzata su tutti gli account che la offrono? Specialmente gli account che accedono a informazioni sensibili? Stiamo utilizzando MFA resistente al phishing?

Non tutti i tipi di autenticazione a più fattori (MFA) sono creati uguali. L'autenticazione legacy come nomi utente e password può essere facilmente violata, e l'autenticazione basata su mobile come SMS, codici OTP e notifiche push è altamente suscettibile agli attacchi di phishing moderni,

malware, SIM swap e attacchi man-in-the-middle (MiTM).

## MFA resistente al phishing

L'MFA resistente al phishing è definita dal NIST Special Publication DRAFT 800-63-B4 come "la capacità del protocollo di autenticazione di rilevare e prevenire la divulgazione di segreti di autenticazione e output di autenticatori validi a una parte facente capo a un impostore senza fare affidamento sulla vigilanza dell'abbonato".

La strategia Zero Trust M-22-09 dell'OMB dalla Casa Bianca descrive specificamente due tecnologie resistenti al phishing: lo standard FIDO2 WebAuthn e le smart card PIV.

## Implementazione FIDO2/WebAuthn

FIDO è un insieme di protocolli di autenticazione che utilizza chiavi crittografiche sui dispositivi degli utenti per offrire un modo sicuro e resistente al phishing per autenticare le identità degli utenti – tutto senza password. Questa tecnologia ha consentito a circa 40.000 utenti registrati, alcuni dei quali storicamente richiedevano esenzioni PIV, di accedere alla rete USDA senza introdurre i rischi associati a nomi utente e password.

**Vantaggi chiave del FIDO2**:

- Eliminazione di segreti condivisi
- Binding crittografico al dominio specifico
- Resistenza agli attacchi di replay
- Supporto per autenticazione senza password

## Certificati PIV e PKI

I certificati X.509 possono essere utilizzati per autenticare una (o entrambe) le estremità di una connessione TLS quando SMTP viene eseguito su TLS. S/MIME utilizza anche certificati X.509 per certificare e memorizzare chiavi pubbliche utilizzate per validare firme digitali e crittografare email.

# Simulazioni di phishing per testare la consapevolezza

## Progettazione efficace delle simulazioni

Le simulazioni di phishing forniscono un metodo pratico e hands-on per i dipendenti per imparare come rilevare i tentativi di phishing. Questa esperienza pratica è spesso più efficace della formazione teorica.

Le simulazioni di phishing dovrebbero essere eseguite ogni trimestre per massimizzare l'impatto dei metodi di formazione di consapevolezza della sicurezza nuovi o migliorati. È importante seguire un approccio non punitivo quando i dipendenti sbagliano; coloro che inavvertitamente cliccano su un collegamento malevolo non dovrebbero essere puniti, ma incoraggiati a segnalare il loro errore.

## Metodologie di testing avanzate

Le soluzioni di simulazione di phishing offrono tipicamente le seguenti capacità: minacce cyber realistiche che mirano a replicare vari tipi di minacce di sicurezza informatica che rispecchiano scenari di vita reale, scenari di phishing personalizzabili che le aziende possono adattare per assomigliare a quegli attacchi più probabili di colpire la loro industria o dipartimento.

**Componenti essenziali**:

- **Targeting intelligente**: Invio di simulazioni a tutti i dipendenti, dipartimenti specifici, dirigenti o individui frequentemente presi di mira
- **Contenuto adattivo**: Invio automatico di simulazioni personalizzate ai dipendenti che non sono mai stati testati o che hanno fallito il loro ultimo test
- **Misurazione delle prestazioni basata sui dati**: Analisi di come individui e gruppi si comportano durante le

simulazioni

### Reporting e analisi

I report completi con statistiche dettagliate, grafici e risultati dovrebbero includere riassunti a livello esecutivo con panoramiche di alto livello personalizzate per la leadership. L'efficacia organizzativa nelle impostazioni reali su larga scala, in particolare riguardo alla formulazione degli attacchi di phishing (personalizzata versus generale) e come diverse unità aziendali sono state colpite nel tempo, rappresenta un fattore critico.

### Integrazione con programmi formativi

L'integrazione del programma di formazione: il software di simulazione di phishing spesso si integra perfettamente in programmi di formazione di sicurezza informatica più ampi. Questo consente un approccio olistico all'apprendimento, dove i dipendenti possono immediatamente praticare le lezioni apprese da altri moduli di formazione in scenari realistici.

## Raccomandazioni implementative

### Framework di sicurezza strutturato

Il Cybersecurity Framework (CSF) del NIST fornisce una struttura flessibile che si adatta alle esigenze specifiche di ogni organizzazione, indipendentemente dalle dimensioni, dal settore o dal livello di maturità. La guida CSF 2.0: Small Business Quick Start è strutturata in base alle sei funzioni principali del CSF: Governare, Identificare, Proteggere, Rilevare, Rispondere e Recuperare.

### Approccio layered alla sicurezza

La protezione efficace contro il phishing richiede un approccio multi-livello che integri:

- **Controlli tecnici:** Filtri email, autenticazione domini,

MFA resistente al phishing
- **Controlli amministrativi:** Politiche di sicurezza, procedure di risposta agli incidenti
- **Controlli fisici:** Formazione del personale, simulazioni, consapevolezza organizzativa

### Monitoraggio e miglioramento continuo

Secondo USENIX, i dipendenti inizieranno a dimenticare la loro formazione dopo quattro mesi, quindi fornire sessioni di consapevolezza regolari è fondamentale per assicurarsi che le informazioni rimangano fresche nelle loro menti.

L'implementazione di un programma di monitoraggio continuo dovrebbe includere:

- Valutazioni trimestrali delle simulazioni di phishing
- Revisione mensile delle metriche di sicurezza email
- Aggiornamento annuale delle politiche e delle procedure

## Innovazioni emergenti e tendenze 2025

### Minacce potenziate dall'Intelligenza Artificiale

Il panorama del phishing ha subìto una trasformazione radicale con l'avvento dell'Intelligenza Artificiale generativa. Gli attacchi di phishing potenziati dall'AI utilizzano algoritmi di intelligenza artificiale generativa per creare messaggi di phishing altamente personalizzati e convincenti, analizzando vaste quantità di dati provenienti da social media, siti web aziendali e altre fonti pubbliche per imitare stili e contenuti di comunicazione legittimi.

La ricerca di Hoxhunt ha documentato che nel marzo 2025, gli agenti AI per il phishing mirato sono diventati il 24% più efficaci degli esperti umani, con un miglioramento del 55% nelle prestazioni relative rispetto ai team red umani dal 2023

al 2025. Le statistiche del 2024 rivelano che il 67,4% di tutti gli attacchi di phishing ha utilizzato qualche forma di AI, con un aumento del 4.151% del volume totale di phishing dall'avvento di ChatGPT nel 2022.

## Quishing: la minaccia dei codici QR

Il **QR Code Phishing** o "Quishing" rappresenta una delle evoluzioni più insidiose degli attacchi di phishing. Nel 2025, gli attacchi quishing sono aumentati del 25% anno su anno, rappresentando ora 1 su ogni 8 campagne di raccolta credenziali. Il 90% degli attacchi con codici QR rilevati sono attacchi di phishing per credenziali, spesso collegati a siti web che appaiono legittimi (frequentemente emulazioni di pagine di login Google o Microsoft).

I dati dell'Action Fraud mostrano che le truffe con codici QR sono aumentate di quattordici volte negli ultimi cinque anni, con 1.386 segnalazioni ricevute nel 2024 rispetto a sole 100 nel 2019. La natura particolarmente pericolosa del quishing deriva dalla sua capacità di aggirare i tradizionali sistemi di difesa informatica, operando completamente al di fuori dei perimetri di sicurezza digitali.

## Deepfake e Voice Phishing (Vishing)

Il report Global Threat di CrowdStrike del 2025 evidenzia un aumento del 442% negli attacchi di voice phishing (vishing) tra la prima e la seconda metà del 2024, alimentati da tattiche di phishing e impersonificazione generate dall'AI. Nel 2024, un'azienda multinazionale è stata vittima di una truffa deepfake che è costata all'impresa 25 milioni di dollari, dove tutti i partecipanti a una videoconferenza erano deepfake creati utilizzando dati pubblicamente disponibili dai social media.

## Biometria comportamentale: la nuova frontiera

## difensiva

La **biometria comportamentale** emerge come soluzione innovativa per contrastare le minacce AI-powered. Questa tecnologia utilizza l'intelligenza artificiale per analizzare come gli utenti interagiscono con i sistemi, inclusi pattern di digitazione, movimenti del mouse e modalità di utilizzo del dispositivo, creando un profilo unico per ogni utente e segnalando qualsiasi deviazione che potrebbe indicare una violazione della sicurezza.

La biometria comportamentale può essere compresa come "linguaggio corporeo digitale", catturando e analizzando distinzioni sottili per stabilire un'impronta digitale unica che i fraudster e le loro macchinazioni trovano quasi impossibile da replicare. Il mercato della biometria comportamentale è previsto raggiungere i 14,00 miliardi di USD entro il 2032, con una crescita guidata dalla crescente domanda di verificazione dell'identità basata sull'AI e rilevamento delle frodi.

## Tecnologie di rilevamento AI-powered

Il report di External Threat Intelligence del 2025 di CybelAngel evidenzia che gli strumenti di rilevamento AI integrati sono il modo più efficace per identificare e segnalare tentativi di phishing potenziati dall'AI. Queste soluzioni incorporano:

- **Rilevamento di anomalie basato su AI**: Monitoraggio continuo dei pattern di comunicazione email per identificare deviazioni sottili
- **Algoritmi avanzati di rilevamento dell'offuscamento**: Superamento dei limiti dei filtri tradizionali basati su testo
- **Analisi comportamentale in tempo reale:** Identificazione di pattern non umani nelle interazioni digitali

# Conclusioni

La prevenzione del phishing nelle piccole imprese richiede un approccio sistematico e scientificamente fondato che integri tecnologie avanzate, formazione continua del personale e strategie di testing proattive. Con l'emergere di minacce AI-powered, quishing e deepfake, le organizzazioni devono evolvere le proprie strategie difensive incorporando biometria comportamentale, rilevamento di anomalie basato su AI e protocolli di risposta specializzati per minacce correlate all'intelligenza artificiale.

L'implementazione coordinata di autenticazione domini, MFA resistente al phishing, programmi formativi evidence-based, simulazioni regolari e tecnologie di rilevamento AI rappresenta la strategia più efficace per mitigare significativamente il rischio di compromissione nel panorama delle minacce del 2025.

Le evidenze scientifiche dimostrano che un approccio integrato può ridurre la suscettibilità al phishing dall'87% iniziale fino al 4,7%, rappresentando un miglioramento dell'efficacia difensiva di oltre l'87%. Tuttavia, il successo di tali iniziative dipende dall'impegno organizzativo verso l'implementazione sistematica, l'adozione di tecnologie emergenti e il miglioramento continuo delle misure di sicurezza informatica in risposta all'evoluzione del panorama delle minacce.

# Bibliografia e fonti utilizzate

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/phishing-imprese/