Per battere il phishing serve formazione

27 MAGGIO 2025 - **Parte II**

Nella Parte I abbiamo visto i motivi che rendono la formazione di tutto il personale interno su awareness e phishing investimento non rinviabile.
In questa Parte II vediamo le caratteristiche di un buon programma formativo e diamo alcune indicazioni su come implementarlo.

LA FORMAZIONE DEVE innanzitutto essere efficace. Programmi noiosi, ripetitivi, basati sul semplice trasferimento di nozioni risultano poco interessanti e non raggiungono lo scopo. I programmi che funzionano tendono invece a rispettare alcuni principi generali, che trasformano il training da semplice strumento di compliance a efficace misura di sicurezza.

- **Scienze comportamentali.** Le "scienze comportamentali" studiano i processi cognitivi che inducono le persone a comportarsi in un determinato modo. I buoni programmi applicano, per esempio, il principio della ripetizione dilazionata, brevi momenti formativi ripetuti a intervalli di tempo sempre più lunghi invece di una singola corposa lezione.
- **Simulazioni realistiche.** Le simulazioni phishing replicano le tattiche dei malfattori. Esporvi in piena sicurezza gli impiegati vuol dire far loro acquisire la capacità di riconoscere gli attacchi e respingerli senza mettere a rischio l'organizzazione.
- **Adattamento.** Il panorama delle minacce cambia ogni giorno e un buon programma formativo deve quindi essere un processo continuo, con frequenti interazioni tra studente e programma stesso.
- **Personalizzazione.** Nessun training generico e noioso può avere successo. È fondamentale poter definire ruoli aziendali specifici e coinvolgere il personale con tecniche di *gamification*, promuovendo per esempio la formazione di team in competizione tra loro.
- **Report e metriche utili.** Essenziale è l'analisi dei risultati della formazione per identificare i punti di forza e le aree di miglioramento del programma.

Le basi di un piano di formazione efficace

Un percorso di formazione non può essere improvvisato. Deve essere pianificato, strutturato e monitorato nel tempo. Ecco i passaggi fondamentali per implementare un piano efficace:

- **Analisi dei rischi e dei bisogni.** Prima di tutto occorre identificare le principali minacce per l’azienda e valutare il livello di consapevolezza del personale. Una verifica iniziale aiuta a personalizzare i contenuti.

- **Definizione degli obiettivi.** Chiarire che cosa si vuole ottenere: riduzione degli incidenti, miglioramento della procedura di segnalazione degli attacchi, maggiore aderenza alle policy interne.
- **Scelta dei contenuti e dei formati.** Alternare sessioni teoriche, simulazioni pratiche (di attacchi phishing), contenuti brevi, video e quiz per mantenere alta l'attenzione e l'efficacia.
- **Formazione continuativa.** Non basta un corso una tantum: la formazione deve essere permanente, con aggiornamenti periodici su nuove minacce e tecniche di attacco.
- **Misurazione e miglioramento.** Monitorare i risultati attraverso test, valutazioni e feedback dei partecipanti, adattando il piano in base ai dati raccolti.

Perché scegliere un percorso strutturato

Affidarsi a soluzioni professionali come il percorso di Cybertraining permette di trasformare la formazione in un processo continuo e misurabile. Il servizio integra:

- Moduli personalizzati per le esigenze della tua azienda
- Simulazioni di attacco reali per testare la prontezza degli utenti
- Report periodici sulle performance e sulle aree di miglioramento
- Supporto costante per aggiornamenti normativi e tecnologici

La formazione così strutturata non solo riduce il rischio di incidenti, ma crea una vera cultura della sicurezza: il personale diventa parte attiva della difesa aziendale, riconoscendo e segnalando tempestivamente comportamenti sospetti.

Un piano formativo continuo è il modo più efficace per rispondere all'evoluzione delle minacce. Le nostre soluzioni di **Cybersecurity Training** sono pensate per le PMI che vogliono investire nella prevenzione, con il supporto di specialisti e strumenti all'avanguardia.

E se pensi nonostante tutto di non poterti comunque permettere l'investimento, scopri quanto abbordabili siano invece i costi chiedendo un preventivo online in tempo reale.

PS - Se hai perso la ***Parte I*** e desideri riceverla contattami all'indirizzo in calce.

Marcello Fontana
commerciale@gotech.it
+39 351 4272010