PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4898 di Mercoledì 24 marzo 2021

Come e perché formare i dipendenti sulla cyber security?

Come creare programmi di formazione efficaci che contribuiscano a ridurre le violazioni alla sicurezza informatica delle aziende?

Secondo uno studio di IBM, il 95% delle **violazioni alla sicurezza informatica** delle aziende dipende dalle azioni dei propri dipendenti.Ciò significa che, anche implementando i più sofisticati sistemi di sicurezza, la mancata formazione dei dipendenti rischia comunque di esporre l'azienda a rischi e minacce informatiche.Un'**adeguata formazione sui temi della cybersecurity** costituisce pertanto la prima linea di difesa contro il cyber crime che, nella maggior parte dei casi, è favorito proprio dall'errore o dalla negligenza delle persone.Un dipendente non formato potrebbe, ad esempio, aprire email sospette o non proteggere adeguatamente informazioni sensibili adottando comportamenti non conformi alla sicurezza.

Quali dipendenti dovrebbero frequentare corsi sulla sicurezza informatica?

La risposta a questa domanda è molto semplice: se un dipendente utilizza il computer, ha bisogno di una **formazione sulla sicurezza informatica**. La tecnologia, infatti, offre ai dipendenti infinite opportunità di mettere inconsapevolmente a rischio i dati aziendali.Gli attacchi alla sicurezza informatica sono aumentati notevolmente durante la pandemia da coronavirus, in conseguenza della rapida diffusione del **lavoro da remoto**. L'uso di computer personali e di reti Internet non adeguate aumenta infatti la vulnerabilità delle aziende.La formazione sulla **cyber security** può aiutare a mitigare questa esposizione e contribuire a formare una forza lavoro sicura. Ma come creare un efficace programma di formazione sulla sicurezza informatica?

Consigli per un'efficace formazione sulla sicurezza informatica

1. Includi la formazione sulla cybersecurity nei programmi di onboarding

La creazione di consapevolezza sulle minacce alla sicurezza online deve iniziare il primo giorno. Rendi obbligatoria la formazione online sulla sicurezza informatica per i nuovi dipendenti. Incorpora la formazione sulla sicurezza informatica nel tuo **programma di onboarding** e assicurati che copra tutti gli argomenti più importanti.In questo modo, farai in modo che capiscano l'importanza di un comportamento online attento sin dalla prima settimana di lavoro.

2. Valuta i punti deboli della tua azienda

Prima di progettare corsi di formazione sulla sicurezza informatica per la propria azienda, occorre esaminare la sicurezza complessiva già in atto e individuare i punti deboli. Ci sono **lacune nella sicurezza** quando si tratta di elaborazione dei pagamenti? E-mail tra uffici? Allegati e sicurezza dei documenti? Individua l'anello più debole e focalizza lì l'inizio della progettazione del corso.

3. Aggiorna continuamente i tuoi dipendenti sulle nuove minacce

Uno dei concetti più importanti da comprendere è che, proprio come la tecnologia, la sicurezza informatica è in continua evoluzione e rimanere aggiornati potrebbe fare la differenza tra mantenere la tua azienda al sicuro o meno.Fai quindi in modo che la formazione non sia un'azione sporadica, ma prevedi **aggiornamenti continui** (ad esempio, trimestralmente) e invia ai tuoi dipendenti promemoria costanti sui nuovi attacchi che si sono sviluppati.

4. Utilizza i principi del microlearning

Sfrutta le potenzialità del **microlearning** per fornire piccoli frammenti di informazioni essenziali. Questa modalità formativa richiede uno sforzo minore in termini di tempo rispetto alla formazione tradizionale (sia per la creazione dei contenuti, sia per la loro fruizione), garantendo un tasso di completamento dei corsi più alto e un **aggiornamento immediato della forza lavoro**. Ad esempio, puoi creare contenuti microlearning per aggiornare i dipendenti su nuove tipologie di attacchi informatici.

5. Crea un senso di responsabilità condivisa

Ricorda che è meglio conoscere una potenziale violazione non appena si verifica, quindi assicurati di creare un ambiente in cui la condivisione è incoraggiata ed evita una situazione in cui qualcuno cerca di nascondere i propri errori aggravando ulteriormente la situazione.Quando una minaccia viene identificata, invia un'e-mail a tutta l'azienda per informare i dipendenti. Essere aggiornati li aiuterà a tenere sempre alto il livello di allerta.

Corsi online sulla cyber security e la protezione dei dati

Quando si parla di formazione continua dei lavoratori, una delle soluzioni al tempo stesso più efficaci ed economiche è quella della **formazione online**. Eccoti quindi un paio di corsi eLearning in materia di cyber security e protezione dei dati:

- **Corso online "Cyber Security: tutela dei dati e delle informazioni aziendali"**: per offrire ai tuoi dipendenti una formazione specifica sui rischi e le responsabilità nel trattamento di dati e informazioni tramite l'utilizzo di dispositivi informatici
- **Corso online "Privacy GDPR: Tutela dei dati personali"**: per illustrare ai tuoi dipendenti come applicare le disposizioni della normativa sulla tutela dei dati personali, garantendo un trattamento dei dati efficiente e garantendone al tempo stesso la tutela

---