ARTICOLO DI ELEARNINGNEWS

Year 4 - number 101 Wednesday 26 february 2020

Cybersecurity: l'eLearning può contribuire alla sicurezza informatica aziendale?

In che modo l'eLearning può migliorare la sicurezza informatica dell'azienda?

Il protocollo di **sicurezza informatica** aziendale appartiene davvero in modo esclusivo al solo reparto IT? Certo, il team IT è responsabile dell'installazione e della manutenzione dei sistemi di sicurezza in azienda, ma il mondo digitale è in continua crescita ed espansione e tocca tutti i reparti aziendali. E qui entra in gioco l'**eLearning**.

Secondo uno studio del 2016, pubblicato su Information and Knowledge Management, la costante crescita di Internet ha riformulato l'inclinazione pedagogica dell'eLearning. L'obiettivo primario della formazione online è proprio quello di rendere il più accessibile possibile l'apprendimento.

I corsi online, i tutorial e i file digitali possono essere ottimi canali di comunicazione interna e di aggiornamento dello staff. Inoltre, l'eLearning è cresciuto in popolarità, il che lo rende il veicolo perfetto per formare i dipendenti sulla sicurezza informatica.

Coinvolgimento

Il tema " **cyber security**" non è largamente trattato da tutti perchè porta alla mente immagini di complessità, tecnicità e gergo informatico inaccessibile ai più. L'eLearning consente di affrontare l'argomento in modo coinvolgente. C'è anche la possibilità di basare le lezioni su casi pratici e calarli in **scenari** di vita reale (come segnalato dal rapporto di ZDNet.

La sicurezza informatica ha una natura fortemente interdisciplinare, tanto che, nel Congresso sulla sicurezza ISC2, è stata paragonata alle arti.

Come diffondere **formazione** e aggiornamento circa la **sicurezza informatica** in azienda?

- le app di messaggistica possono essere utilizzate per informare rapidamente sulle potenziali violazioni dei dati e su come evitarli;
- i file utili e i video formativi possono essere archiviati in cloud e aggiornati facilmente;
- attraverso la piattaforma eLearning aziendale si può offrire formazione online sull'argomento a tutti i dipendenti aziendali;
- i brevi video tutorial possono essere molto utili a coloro che vogliono creare protocolli di protezione con password e simili.

La sicurezza informatica è in continua evoluzione

Il protocollo di sicurezza informatica richiede molto più della creazione di password complesse, ma riguarda in generale tutti i sistemi di prevenzione di furto dei dati e di preservazione dell'integrità dei dati stessi. L'importanza della sicurezza informatica è un concetto che può essere oggetto di formazione efficace, anche perchè le minacce informatiche sono in rapida evoluzione. Questo offre ai manager l'opportunità di coinvolgere i propri dipendenti in modo più approfondito.

Chiaramente, i tipi di protocolli di sicurezza informatica necessari dipenderanno dalle operazioni che la tua azienda svolge. I dipendenti delle aziende tecnologiche, ad esempio, necessitano di una formazione molto più intensa che copra sia software che hardware: i **corsi eLearning** possono essere personalizzati e aggiornati in quest'ottica, per soddisfare le specifiche esigenze.

I prossimi passi

I dipendenti rappresentano una grossa minaccia per la sicurezza informatica aziendale, soprattutto nei casi di lavoratori da remoto, in quanto è difficile monitorare l'utilizzo del computer e la sicurezza dei propri device. Gulf Business News consiglia di istruire in anticipo i dipendenti in modo che possano comprendere i rischi.

È importante valutare rapidamente la conoscenza della cyber security dei tuoi dipendenti in modo che tu possa sapere da dove iniziare con la formazione. Gli **LMS** tengono traccia dei livelli delle date di completamento della formazione e ciò può aiutare a ad avere report precisi circa la formazione dei dipendenti. Queste metriche possono quindi essere utilizzate per stabilire una solida cultura della sicurezza all'interno dell'azienda; monitorando ciò che i dipendenti già sanno, i manager possono aggiungere nuovi moduli che si basano su altri dati e colmare le lacune o (prevenendo attacchi futuri).

Articolo tratto da InfoSecurity Manager