ARTICOLO DI ELEARNINGNEWS

Year 6 - number 188 Wednesday 2 february 2022

Cybersecurity: come impostare una password sicura

A livello mondiale, i dati sulla vulnerabilità delle password sono peggiorati dal 2020 al 2021. Messe al bando le parole chiave facili che risultano le più scelte del 2021

Abbiamo parlato spesso dell'importanza della **sicurezza informatica** e di quanto essa dipenda dal **fattore umano** e possa passare anche dalle **password**.

Password: viene scelta la meno sicura

La pigrizia e la smemoratezza sono due nemici potenti, anche in ambito sicurezza informatica e password. 123456 sarà giudicata dalla maggioranza di noi una password non sicura, eppure, nel 2021 è stata la password più scelta secondo un **report di Nordpass**, insieme a sequenze numeriche come 111111 oppure 123123. Tra le password non numeriche, a seconda dell'argomento, vediamo come nel mondo le più scelte siano "Ferrari", "Porsche" (in ambito automobilistico), "Michael" (nei nomi propri). In Italia anche le squadre di calcio si posizionano nella classifica delle password e svetta tra tutte "Juventus" e "Napoli". Emblematica, nonchè paradossale, anche la scelta della password "cambiami" o "password".

A livello mondiale, i dati sulla **vulnerabilità delle password** sono peggiorati dal 2020 al 2021: se nel 2020 il 73% delle password poteva essere decifrato in meno di un secondo (con appositi applicativi usati dagli hacker, sebbene la misura del "tempo di decifrazione" sia indicativa e dipenda da vari aspetti tecnologici), nel 2021 la percentuale si attesta a 84,5%. Già nel 2020, il 55% dei data breaches a livello worldwide era dovuto nel 55% a password vulnerabili. **Qui** un calcolatore virtuale e gratuito che determina in pochi secondi quanto sono vulnerabili le nostre password.

A detta di Jonas Karklys, CEO di NordPass, "le password continuano a indebolirsi e le persone continuano a non occuparsene correttamente.È importante capire che le password rappresentano la porta d'accesso alle nostre vite digitali, e con l'aumento del tempo trascorso online, sta diventando estremamente importante prestare più attenzione alla sicurezza informatica".

Sulla gestione della cybersecurity in azienda e la forte correlazione col fattore umano, talvolta erroneamente presa con leggerezza, si fonda il **corso online di un'ora "Cyber Security - Tutela dei dati e delle informazioni aziendali"** creato da Mega Italia Media S.p.A., eLearning company molto attenta al fattore tecnologico e leader in Italia. Il corso spazia su varie tipologie di attacco e le best practices attraverso cui il dipendente o il collaboratore può gestire la situazione ed evitare rischi per i dati aziendali o personali.

In ambito eLearning, inoltre, il tema password è molto importante anche per la protezione dei dati di formazione e i dati personali dei dipendenti e tocca in maggior misura gli amministratori di piattaforma.

Password robuste: come gestirle

Lo stesso Garante della Privacy, per arginare gli alti rischi connessi alla scelta di una password non sicura (data da disinformazione, atteggiamento lassista o sottovalutante) ha steso un **vademecum**.

La scelta della password dovrebbe seguire alcuni precisi criteri:

- lunghezza: minimo 8 caratteri (meglio 15)
- tipologia di caratteri: almeno 4 (lettere maisucole, lettere minuscole, numeri, caratteri speciali, ad esempio asterischi, punti esclamativi ...)
- non usare riferimenti personali (nome, data di nascita ...)
- non usare riferimenti allo username
- evitare parole di uso comune (meglio parole di fantasia o camuffate, ad esempio "computer" potrebbe diventare "c0mpu!3r") per evitare il facile successo dell'azione di software che provano sistematicamente tutte le parole di uso

comune in diverse lingue
- cambiare periodicamente la password
- utilizzare password diverse per account diversi (per evitare che rubando una sola password, il criminale informatico abbia accesso a tutti gli account della vittima)
- non utilizzare password utilizzate in passato
- cambiare immediatamente le password temporanee rilasciate al primo accesso da un sistema o servizio informatico
- utilizzare, se disponibili, meccanismi di autenticazione multi fattore
- conservare le password senza scriverle (su un bigliettino, file non protetti su PC, smartphone o tablet o nel corpo di email e messaggi) o comunicarle ad alcuno