

SICUREZZA INFORMATICA: 6 CONSIGLI PER CREARE UNA PASSWORD A PROVA DI HACKER

7 Marzo 2019



Con l'entrata in vigore del Regolamento UE sulla protezione dei Dati (GDPR Reg. UE 2016/679), il tema della sicurezza informatica è più che mai attuale.

È fondamentale lavorare al riparo da attacchi informatici ma non è semplice creare password "sicure", a prova di hacker. Inoltre, manca ancora la consapevolezza di quanto sia importante questo tema: basti pensare che nel 2017 quella più utilizzata è stata "123456" e, a seguire, "password".

Bastano pochi accorgimenti per creare un login a prova di pirati informatici e far sì che i nostri dati siano al sicuro.

Di seguito, alcune linee guida per creare una password sicura:

1. Cercare on line: se proprio siamo indecisi e dobbiamo cambiarla urgentemente, possiamo utilizzare diversi siti generatori di password, che saranno sicuramente inviolabili.
2. Cambiare frequentemente password: per essere sempre "protetti", è bene cambiare periodicamente la password, in modo che gli hacker non abbiano il tempo di decriptare quella precedentemente creata.

3. Scrivere le password al contrario: una password “imprevedibile” può essere quella scritta al contrario, in modo che risulti una parola apparentemente senza senso. Deve essere “lunga” ed è consigliato aggiungere numeri e caratteri.

4. Utilizzare il metodo passphrase: spesso capita di creare password “difficili”, può essere utile ma allo stesso tempo, si possono facilmente dimenticare. Si può, quindi, utilizzare il passphrase, ossia trasformare un insieme di parole in stringhe alfanumeriche. Ad esempio, un’intera frase, può diventare una combinazione di lettere se si uniscono le iniziali di ciascuna parola. Altra soluzione, è quella di trasformare i caratteri, come la “o” con lo “zero”, la “S”, con il simbolo del \$; altra idea è quella di utilizzare il titolo di un film, di una canzone che vi piace e sia che sia facilmente memorizzabile.

5. Diversificare le password: è necessario utilizzare password diverse per account diversi e soprattutto cambiarle completamente al rinnovo. Se avete utilizzato “ufficio”, quella successiva non deve essere “ufficio1”, “ufficio2” e così via.

6. Utilizzare il metodo del padding: il termine inglese significa letteralmente “imbottire” una frase, ossia aggiungere simboli all’inizio e alla fine. La password facilmente intuibile “ufficio”, lo sarà molto meno se diventerà “!!!!!!ufficio111111”

Seguire questi piccoli accorgimenti, è fondamentale per rispondere alla questione della sicurezza aziendale, tema sempre più stringente visti i ripetuti e ben noti attacchi informatici subiti su larga scala. Basta prendersi qualche minuto per creare una password imprevedibile e a prova di hacker.

[HUMANGEST](#)