# NOTIZIE DIGITALI

PID - Punto Impresa Digitale / #06 - 07.2024

*FOCUS 4.0*

## Cybersecurity: gestione delle password

**Quella di gestire le password è una pratica troppo spesso sottovalutata: vediamo come ottimizzarla**

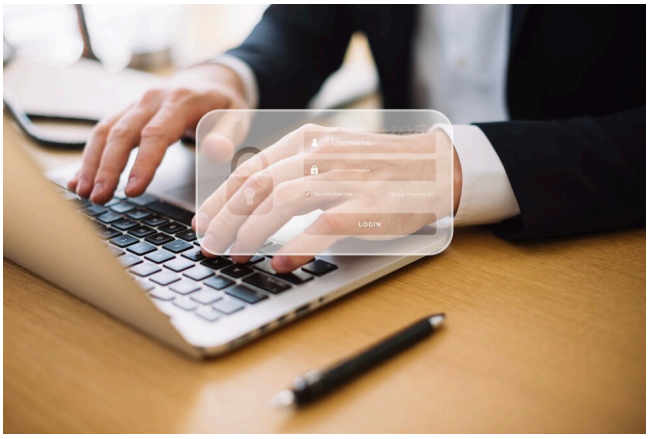

Immagine di Freepick su Freepik

L'idea di una **parola o una frase segreta** per l'accesso a luoghi protetti esiste da tempo (pensiamo alle parole d'ordine per identificare alleati e prevenire intrusioni nei campi militari nell'antica Roma). Uno dei primi usi moderni delle password risale agli **anni '60** e da lì, crescendo piattaforme e device, le password sono diventate un fondamentale strumento di protezione. Ciononostante, spesso assistiamo (o attuiamo) **pratiche scorrette**. Scopriamo il perché e quali sono le best practice più utili.

### ❌ PERCHÉ SBAGLIAMO NELLA GESTIONE DELLE PASSWORD?

**Pensiamo che tanto nessuno le indovinerà** L'idea che ci sia un umano intento a tirare a indovinare è radicata soprattutto tra le "generazioni meno digitali".

**Tra lavoro e vita privata, abbiamo troppe credenziali** Il burnout dovuto al dover ricordare tante password ci porta ad acquisire abitudini errate.

**Crediamo che, anche in caso di furto di credenziali, non ci siano conseguenze gravi** Spesso non conosciamo le possibili conseguenze e i meccanismi che a catena possono attivarsi dopo un furto di (anche solo) una password.

**Ci illudiamo di non essere vittime di interesse e/o di non avere nulla di "prezioso"** Potenzialmente chiunque può essere ricattato, e l'oggetto del ricatto è qualcosa di importante per noi, non per i ladri (quindi siamo disposti a riaverlo).

**Dal momento che non ci è mai capitato, abbassiamo le difese** Più passa il tempo in cui non subiamo nulla, più tendiamo erroneamente a credere che difficilmente ci succederà.

Dobbiamo accettare il fatto che i cybercriminali siano vere e proprie **organizzazioni criminali**, con un giro di affari più redditizio del traffico di droga (vedi Rapporti Clusit) e che tendono a sferrare attacchi di massa, consapevoli che una piccola percentuale cascherà sempre nelle loro trappole. Solitamente le credenziali vengono usate per introdursi negli account per delinquere, ricattare o vengono messe in vendita nel **Dark Web**, sicché altri criminali le acquistino per sferrare i loro attacchi.

**LA TUE CREDENZIALI SONO FINITE NEL DARK WEB?**

Vai sul sito Have I Been Pwned e inserisci la tua email personale: se compare il **colore rosso**, scoprirai anche dove e quando le tue credenziali sono finite nel Dark web.

### ✔️ A COSA PRESTARE ATTENZIONE ONLINE?

**Attenzione a qualsiasi richiesta di credenziali tramite email o telefono** I cybercriminali possono fingersi una banca e fare delle richieste via email (anche se dobbiamo ormai sapere che certe richieste non vengono mai fatte via email o telefono).

**Attenzione a quando ci registriamo su un sito** Prediligiamo siti conosciuti e sicuri (NB. Il protocollo "https" nell'URL non è sinonimo di sicurezza verso un cybercriminale: egli, infatti, potrebbe aver creato benissimo un sito con tale protocollo).

**Attenzione ai login** Spesso riceviamo finte email che spingono a loggarci su piattaforme fasulle ma simili alle originali.

**QUALI SONO LE PASSWORD PIÙ USATE?**
Vai sul sito Nord Pass e scopri le password più comuni nei vari Paesi del mondo e il tempo medio che impiega un cybercriminale per intercettarle.

Molti pensano che qualcuno trascorra le giornate cercando di **indovinare manualmente** le password, ma ciò è raro e avviene solo in casi mirati (dove la vittima è ben designata e l'attaccante tenta di trovare informazioni personali, come hobby, nomi di familiari, etc. - potenzialmente usate nella password). Tuttavia, la maggior parte dei furti di password avviene o per cause più comuni, come **negligenza o cattive abitudini** (tra le quali scrivere le password su fogli o agende, essere spiati mentre si digita, cadere vittime di falsi login o scaricare inconsapevolmente malware che installano sul pc dei programmi che "leggono" i tasti digitati sulla tastiera) ma, soprattutto, **attacchi di "brute force"**, in cui potenti computer, sfruttando software avanzati che superano le protezioni di blocco, eseguono migliaia di tentativi al secondo per indovinare le password: così, molte password che usiamo, sono indovinate in pochissimi secondi.

**LE PASSWORD CHE USI SONO SICURE?**
Vai sul sito Kaspersky e scopri quanto sono sicure le password che stai utilizzando.

## COME SI CREA UNA PASSWORD ROBUSTA E QUANTO INCIDE?

Oggi esistono device e piattaforme che, al momento della registrazione, creano in automatico password ottimizzate e sicure.

| | | | |
|---|---|---|---|
| 💬 Lunghezza di almeno 12 caratteri | 🔠 Presenza di lettere maiuscole, minuscole, numeri e caratteri speciali | 🚫 Nessun riferimento personale | 🔇 Nessuna parola o frase di senso compiuto |

Al crescere del numero di caratteri con una combinazione di maiuscole, minuscole, numeri e caratteri speciali, cresce in maniera esponenziale il tempo per un computer di indovinare la password: si passa così da una password di **8 caratteri**, solo numeri o solo lettere, indovinata in un decimo di secondo, ad una password di **12 caratteri** con tutti gli elementi, indovinata in 3mila anni, che, se portata a **18 caratteri**, viene indovinata in 438 miliardi di anni.

Molte persone, per semplificare la gestione delle password, commettono l'errore di **usare la stessa password** per diversi account: pratica molto rischiosa perché, se una password viene rubata, tutti gli account che utilizzano la stessa combinazione di "email e password" sono vulnerabili. I cybercriminali conoscono bene questa debolezza e la sfruttano.

**I SALVATAGGI AUTOMATICI SONO SICURI?**
Samsung, Google, Huawei: oggi device e browser ci chiedono se "devono salvare la password". Questo non è un modo sicuro di salvare, perché non c'è una crittografia avanzata e perché i browser non sono così sicuri (sono aziende il cui core business non è salvaguardare le vostre password). Fa eccezione Apple, che fa della sicurezza una sua value proposition.

Ciò dimostra che non sempre la compromissione di credenziali è dovuta a un nostro errore: aziende a cui affidiamo i dati possono subire furti, esponendoci a seri rischi. La soluzione più sicura ed efficace per gestire le password sono i **password manager** (come LastPass o NordVPN): delle casseforti virtuali dove vengono salvate tutte le password con una **crittografia molto avanzata**. Il consiglio è di scegliere i più famosi (un cybercriminale potrebbe creare un password manager con molte funzionalità gratuite per spingere gli utenti ad usarlo: a quel punto, saremmo direttamente noi a dargli le credenziali).

## I VANTAGGI DEI PASSWORD MANAGER

- 🤝 **Facilità di utilizzo** Sono piattaforme estremamente semplici da usare
- 💰 **Costi ridotti** Solitamente sono Freemium: hanno una parte gratuita e una a pagamento, ma dal costo molto accessibile.
- 🔤 **Generazione automatica di password ottimizzate** Possiamo anche personalizzare la lunghezza.
- 💭 **Da ricordare una sola password** Potremo avere tutte password difficili e diverse: dovremo ricordare una sola password.
- 📲 **Multidevice** Sono strumenti utilizzabili e sincronizzabili in sicurezza su diversi dispositivi
- 🆘 **Identificazione intelligente di tentativi sospetti** In caso di tentativi sospetti (altri device, altre città, altri Paesi, etc.), anche con l'inserimento di password corretta, il password manager effettuerà una verifica tramite altri canali (come l'e-mail).

*di Nicolò Mora e Giulia Bernini*

*Vuoi approfondire la questione password e, più in generale, le best practice in ambito cybersecurity? Vuoi vedere come funziona un password manager? Guarda il webinar gratuito "Cybersecurity in pratica: strumenti e tecniche per riconoscere le minacce informatiche"*

# *I servizi del PID - Punto Impresa Digitale*

| | | |
|---|---|---|
|  **FORMAZIONE** | **Eventi e Seminari** | Appuntamenti gratuiti e aperti a tutti su digitale, tecnologie 4.0, digital marketing e contributi per investimenti tecnologici e green |
| | **EID - Eccellenze in Digitale** | Cicli formativi online e in presenza con focus sul marketing e sulle nuove tecnologie a supporto della trasformazione digitale continua delle imprese |
| | **Notizie Digitali** | Ogni mese nuovi articoli di approfondimento sul mondo 4.0 e sul marketing digitale |
| | **PID Academy** | Piattaforma di formazione gratuita e di livello con possibilità di acquisire badge |
|  **ORIENTAMENTO, ASSISTENZA E PREMI** | **Follow Up** | Appuntamenti individuali per suggerire implementazioni digitali e strategie aziendali |
| | **Atlante I4.0** | Network Nazionale Impresa 4.0 che offre servizi e strumenti a supporto della trasformazione digitale e dell'innovazione tecnologica 4.0 |
| | **Mentoring** | Accompagnamento individuale con esperti digitali per assistere le PMI nell'adozione delle tecnologie, nella digitalizzazione dei processi e nelle strategie aziendali |
| | **Way To Solution** | Ricerca di esperti del settore sulla base dei bisogni aziendali, dentro una banca dati proprietaria contenente oltre 70mila brevetti pubblicati dall'EPO |
| | **MIR - Matching Impresa Ricerca** | Collaborazione con i ricercatori del CNR e dell'ENEA per individuare nuove soluzioni tecnologiche integrando la ricerca pubblica ed il sistema produttivo |
| | **TOP of the PID** | Premia i progetti delle PMI che innovano prodotti o modelli di business grazie all'utilizzo delle tecnologie digitali |
|  **ASSESSMENT** | **SELFI4.0** | Autovalutazione della maturità digitale aziendale con benchmark di settore |
| | **ZOOM4.0** | Assessment guidato con i Digital Promoter con implementazioni e orientamenti |
| | **Digital Skill Voyager** | Autovalutazione della maturità digitale personale con punteggio finale in hard/soft skills e possibilità di attestato |
| | **Pid Cyber Check** | Autovalutazione per sapere il livello di rischio di un attacco hacker al quale l'impresa può essere esposta, con stima del danno economico derivante dai possibili attacchi |
| | **CEI - Cyber Exposure Index** | Analisi passiva (costo 55€+iva) su sito web ed email con dominio aziendale. Due report a distanza di 6 mesi contenenti la quantità dei servizi esposti, l'elenco delle vulnerabilità potenzialmente sfruttabili e data leakage (fughe di dati delle e-mail) |
| | **Sustainability** | Autovalutazione delle principali dimensioni della sostenibilità aziendale (ambientale, di governance, sociale) con spunti operativi per migliorare le performance aziendali |
|  **BANDI** | **Innovazione Digitale e Transizione Ecologica** | Voucher per spese sostenute per l'acquisto di beni e servizi, consulenze/formazione nel campo dell'utilizzo delle tecnologie I4.0. e per servizi finalizzati a favorire l'adozione di criteri ESG, per interventi di efficienza energetica e sistemi di autoproduzione FER |