Password robuste: perché servono e come crearle

Una password robusta oggi si misura soprattutto in lunghezza: almeno 15 caratteri, unica per ogni servizio e affiancata dall'autenticazione a due fattori. In questo articolo vediamo perché le vecchie regole non bastano più e come costruire password sicure ma facili da ricordare.

Perché la password conta ancora

Email, home banking, gestionale aziendale, PEC, cloud: dietro quasi ogni servizio c'è ancora una password. Se un malintenzionato la indovina o la ruba, entra con le nostre credenziali e il sistema lo tratta come se fossimo noi.

Per una piccola impresa le conseguenze sono concrete: fatture falsificate inviate dalla casella aziendale, dati dei clienti esposti, gestionale bloccato da un ransomware. Spesso tutto parte da una sola password debole o riutilizzata.

Come vengono violate le password

Capire gli attacchi aiuta a capire le regole. I più comuni sono quattro:

- **Forza bruta**: un programma prova tutte le combinazioni possibili. Con le schede grafiche moderne si testano miliardi di tentativi al secondo, e una password di 8 caratteri può cadere in tempi brevi.
- **Attacco a dizionario**: invece di provare tutto, si provano parole comuni, nomi, date e le varianti tipiche ("Password1!", "Roma2024", "P@ssw0rd"). Sostituire la "a" con "@" non inganna nessuno: i programmi lo fanno in automatico.
- **Credential stuffing**: quando un sito subisce un furto di dati, le coppie email/password finiscono in rete. Gli attaccanti le riprovano su centinaia di altri servizi. Se usi la stessa password ovunque, una sola violazione apre tutte le porte.
- **Phishing**: una falsa email della banca, del corriere o di Microsoft porta a una pagina identica all'originale. Qui nessuna password, per quanto complessa, ti protegge: serve l'autenticazione a due fattori.

Lunghezza batte complessità

Per anni ci hanno chiesto password con maiuscole, numeri e simboli, da cambiare ogni 90 giorni. Il risultato? Password come "Marzo2025!" diventate "Aprile2025!": complicate da ricordare, facili da indovinare.

Il NIST, l'ente americano di riferimento per gli standard di sicurezza, ha pubblicato a luglio 2025 la versione definitiva delle nuove linee guida (SP 800-63B-4). Il cambio di rotta è netto:

Vecchia regola	Indicazione attuale
Minimo 8 caratteri	Almeno 15 caratteri se la password è l'unico fattore (8 se c'è l'autenticazione a due fattori)
Obbligo di maiuscole, numeri e simboli	Nessuna regola di composizione imposta: conta la lunghezza
Cambio obbligatorio ogni 60-90 giorni	Si cambia solo se c'è sospetto di compromissione
Domande di sicurezza ("nome del tuo cane?")	Da non usare
Lunghezza massima bassa	Accettare almeno 64 caratteri, spazi compresi
Nessun controllo	Rifiutare password comuni o già trapelate in violazioni note

Il motivo è matematico: ogni carattere in più moltiplica le combinazioni da provare. Una frase lunga di parole comuni resiste molto più di una parola breve piena di simboli.

Come costruire una password robusta

Il metodo più efficace è la **passphrase**: una sequenza di 4-5 parole scollegate tra loro, facile da ricordare per te e lunghissima per un computer.

1. **Scegli 4 o 5 parole casuali, senza legame logico.** Evita frasi fatte, citazioni o titoli di canzoni: sono nei dizionari degli attaccanti.
2. **Uniscile con un separatore** a tua scelta: trattino, punto, spazio.
3. **Aggiungi un dettaglio personale**, se il servizio lo richiede: un numero o un simbolo in una posizione non ovvia, non sempre alla fine.
4. **Verifica la lunghezza**: punta ad almeno 20 caratteri.
5. **Usala per un solo servizio.** Mai riutilizzarla altrove.

Esempio (non usarlo, è ormai pubblico): **tegame-volpe-Lunedi-ombrello-47** — 31 caratteri, si ricorda con un'immagine mentale, ed è molto più robusta di "Xs!9k#Q2".

Errori da evitare

- Nomi di familiari, animali, squadre del cuore, date di nascita o anniversari

- Sequenze da tastiera come "qwerty", "123456", "asdfgh"
- Il nome dell'azienda o del servizio dentro la password ("Fatture2025")
- Varianti della stessa password su siti diversi ("Mario.Amazon", "Mario.Gmail")
- Password scritte su post-it attaccati al monitor o salvate in un file "password.txt" sul desktop
- Comunicare la password via email, WhatsApp o telefono, anche a chi sembra un tecnico

Password manager e autenticazione a due fattori

Nessuno può ricordare decine di passphrase diverse. La soluzione è un **password manager**: un archivio cifrato che genera, conserva e compila le password al posto tuo. Devi ricordarne una sola, la password principale, che sarà la tua passphrase migliore.

- Esistono soluzioni affidabili gratuite e a pagamento, come Bitwarden, 1Password, KeePass o il gestore integrato di Apple e Google.
- Lascia che sia il password manager a generare password casuali di 20 o più caratteri per tutti i siti.
- Per i team aziendali, le versioni business permettono di condividere accessi in modo controllato, senza girarli in chiaro.

Il secondo pilastro è l'**autenticazione a due fattori (2FA)**: oltre alla password serve un codice dallo smartphone o una chiave fisica. Anche se la password viene rubata, l'attaccante resta fuori.

- Attivala subito su email, PEC, home banking, cloud e social aziendali.
- Preferisci un'app di autenticazione (Microsoft Authenticator, Google Authenticator) o una chiave di sicurezza agli SMS, che sono meno sicuri.
- Dove disponibili, valuta le **passkey**: sostituiscono la password con il riconoscimento del dispositivo e sono resistenti al phishing.

Per le aziende: regole chiare e conservazione sicura

La sicurezza delle password in azienda non può dipendere dalla buona volontà del singolo. Servono regole scritte e strumenti adeguati:

- **Una policy aggiornata**: lunghezza minima di 15 caratteri, niente scadenze arbitrarie, cambio immediato in caso di sospetta violazione.
- **Password manager aziendale** per tutti i collaboratori, con accessi condivisi gestiti centralmente.
- **2FA obbligatoria** su posta, VPN, accessi remoti e account amministrativi.

- **Account separati**: niente utenze condivise tipo "ufficio" o "admin" usate da più persone.
- **Formazione periodica** sul phishing: è l'attacco che aggira anche la password migliore.

C'è poi il lato di chi gestisce siti, gestionali e servizi online. L'Agenzia per la Cybersicurezza Nazionale e il Garante Privacy hanno pubblicato le Linee guida sulla conservazione delle password (provvedimento del 7 dicembre 2023): le password non vanno mai salvate in chiaro, ma protette con funzioni di *password hashing* robuste. Per chi tratta dati di molti utenti o dati particolari, adeguarsi è parte degli obblighi di sicurezza previsti dal GDPR.

E se l'accesso remoto passa da una VPN?

Molte aziende raggiungono il server dall'esterno tramite VPN, ad esempio WireGuard, invece di esporre il desktop remoto su Internet. È una scelta che consigliamo: per arrivare alla schermata di login serve una chiave crittografica installata sul dispositivo, che funziona come un secondo fattore. In questo caso la password può essere meno lunga, ma non banale: una passphrase unica di 12-15 caratteri è un buon equilibrio.

Abbassare troppo la guardia sarebbe un errore, per tre motivi:

- **La VPN riconosce il dispositivo, non la persona.** Se il portatile viene rubato o infettato, chi lo controlla ha già il tunnel aperto: a fermarlo resta la password.
- **Il server è raggiungibile anche dalla rete interna.** Un ransomware entrato da un PC dell'ufficio prova le credenziali dall'interno, dove la VPN non conta.
- **Le password tendono a essere riutilizzate.** Una password debole usata anche altrove resta debole ovunque.

Per completare la protezione: consentire il desktop remoto solo dalla rete VPN, assegnare una chiave diversa a ogni utente o dispositivo (così se ne perdi uno lo revochi senza toccare gli altri), cifrare i dischi dei portatili e mantenere attivo il blocco dell'account dopo troppi tentativi falliti.

Checklist in 6 punti

- [ ] Password di almeno 15 caratteri, meglio una passphrase di 4-5 parole
- [ ] Una password diversa per ogni servizio
- [ ] Password manager per generarle e conservarle
- [ ] Autenticazione a due fattori su email, banca, PEC e cloud
- [ ] Cambio immediato se un servizio che usi subisce una violazione (verificalo su haveibeenpwned.com)
- [ ] Mai comunicare le password via email, chat o telefono

Ti aiutiamo a mettere in sicurezza la tua azienda

Sistemi Informatici Italia affianca professionisti e piccole imprese di Roma nella sicurezza informatica di tutti i giorni: definizione delle policy sulle password, installazione di password manager aziendali, attivazione dell'autenticazione a due fattori e formazione del personale. Contattaci per una verifica della tua situazione.

Fonti

- NIST SP 800-63B-4, Digital Identity Guidelines — Authentication
- Garante Privacy — Linee guida funzioni crittografiche, conservazione delle password