

# Cybersecurity VI: Storia ed evoluzione della Password

14/07/2025

CYBERSECURITY

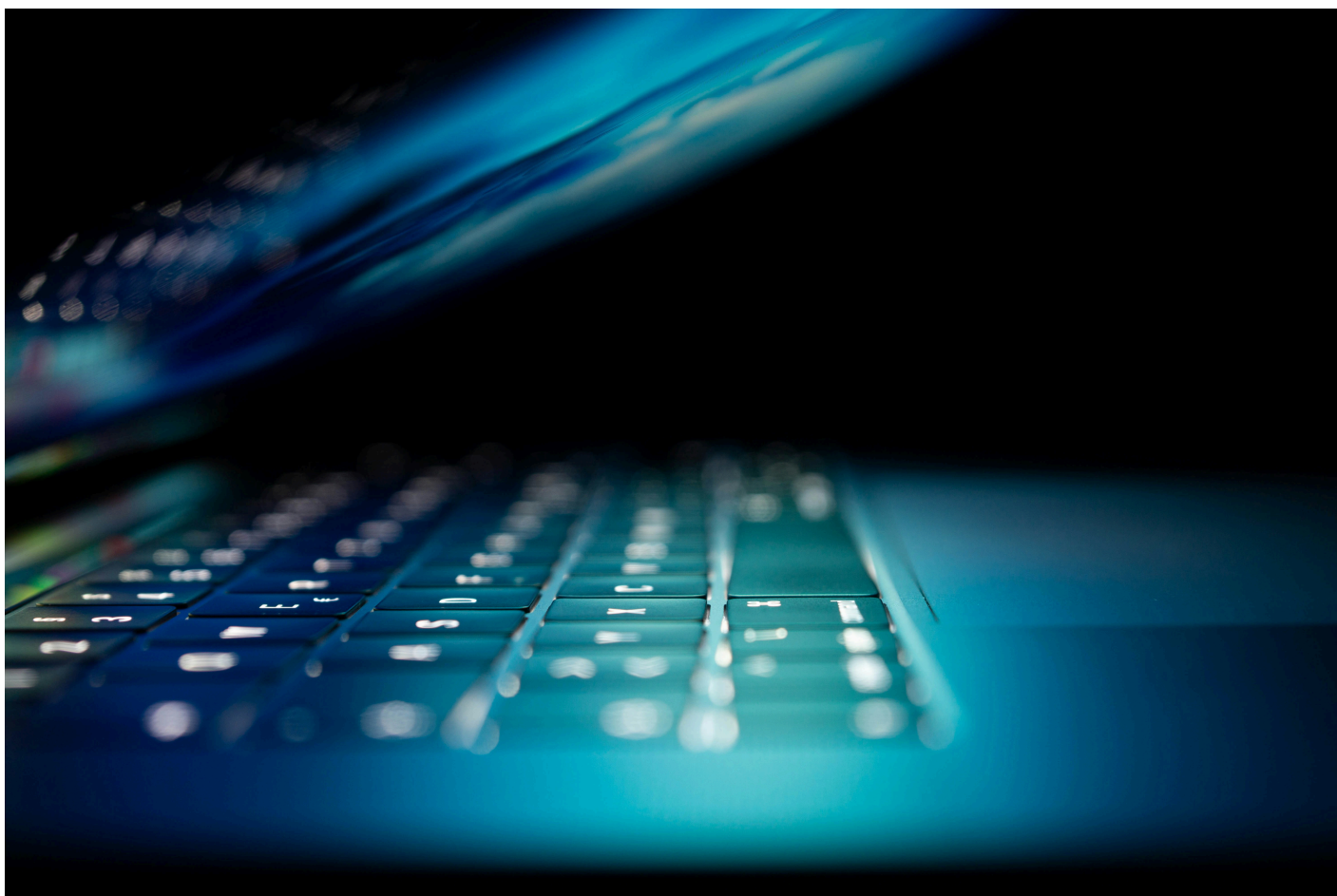
PASSWORD

PRIMO BIENNIO

QUINTO ANNO

SECONDO BIENNIO

LICEO , PROFESSIONALE , TECNICO



Le **password**, nate negli anni '60 con i primi sistemi informatici condivisi, sono rimaste a lungo il principale **strumento di autenticazione**. Nel tempo, le linee guida si sono evolute: dagli anni '90, con l'introduzione di criteri di lunghezza e complessità, fino all'uso di password manager e dell'autenticazione a due fattori per contrastare le crescenti minacce informatiche.

Le pratiche più recenti hanno superato l'obbligo del cambio periodico, privilegiando passphrase robuste e sistemi multifattore. Oggi si guarda al **futuro** con **soluzioni passwordless**, basate su **chiavi crittografiche** e **autenticazione biometrica**. Queste

innovazioni promettono maggiore sicurezza e un'esperienza più semplice, riducendo la dipendenza dalla memoria degli utenti.

#### LE ORIGINI DELLE PASSWORD

L'idea di utilizzare una parola d'ordine segreta si può far risalire fino all'antichità, quando potevano già essere impiegate per identificare amici e nemici. Tuttavia, l'utilizzo moderno delle password inizia negli anni '60 con i primi sistemi informatici ad accesso condiviso, ovvero che potevano essere usati da diversi utenti. Uno dei primi esempi significativi fu il sistema CTSS (Compatible Time-Sharing System) del MIT, che nel 1961 consentiva agli utenti di accedere a sessioni personali protette da password.

#### GLI ANNI '90: LE PRIME LINEE GUIDA SULLA SICUREZZA DELLE PASSWORD

Negli anni '90, con la diffusione di Internet e dei servizi digitali l'autenticazione tramite username e password divenne rapidamente lo standard per accedere a servizi online e le password deboli e ripetute iniziarono fin da subito a rappresentare una vulnerabilità comune e diffusa; emerse quindi la necessità di definire criteri per la creazione di password sicure.

Le prime best practice suggerivano:

- Lunghezza minima della password (almeno 8 caratteri)
- Utilizzo di caratteri speciali, numeri e lettere maiuscole
- Cambi frequenti delle password, spesso ogni 30 o 90 giorni

L'obiettivo era mitigare il rischio di attacchi "brute force", ovvero in cui l'attaccante cerca di indovinare la password attraverso numerosi tentativi (spesso usando tool automatici), e limitare i danni in caso di compromissione delle credenziali.

#### GLI ANNI 2000: L'INTRODUZIONE DEL CRITERIO DI COMPLESSITÀ

Con l'aumento degli attacchi automatizzati, le linee guida si fecero via via più rigide:

- Password più complesse, con requisiti obbligatori di simboli e lettere miste
- Divieto di utilizzare parole comuni o informazioni personali facilmente reperibili
- Politiche per il blocco degli account dopo un certo numero di tentativi falliti
- Divieto di riutilizzo di una password già utilizzata in passato

Sebbene in teoria l'aumento della lunghezza e complessità delle password costituisca un valido ostacolo contro gli attacchi alle credenziali, ci si rese ben presto conto di come queste regole portassero gli utenti ad adottare pratiche scorrette e rischiose quali:

- il riutilizzo di password uguali per servizi diversi
- il riutilizzo di password molto simili tra loro per lo stesso servizio (magari postponendo un numero progressivo alla stessa parola chiave)
- il salvataggio delle password su documenti non protetti

#### GLI ANNI 2010: PASSWORD MANAGER E AUTENTICAZIONE A DUE FATTORI (2FA)

La necessità di adottare password di crescente complessità e la difficoltà degli utenti nel ricordare diverse password complesse e da aggiornare nel tempo, portò all'adozione di strumenti come i password manager, in grado di generare, memorizzare e proteggere credenziali complesse.

In parallelo, emerse l'autenticazione a due fattori come best practice per aggiungere un ulteriore livello di sicurezza. L'autenticazione a due fattori implica che per accedere ad un servizio gli utenti debbano fornire non solo una password, ma anche un secondo fattore di verifica, come un codice inviato via SMS o una notifica su un'app dedicata.

#### CAMBIAMENTI RECENTI: L'ADDIO AL CAMBIO PERIODICO DELLE PASSWORD

Uno dei cambiamenti più significativi nelle best practice è avvenuto con l'abbandono del requisito di cambiare frequentemente le password. Le nuove linee guida, supportate da enti come il National Institute of Standards and Technology (NIST) e la Direttiva NIS2 dell'Unione Europea, suggeriscono che il cambio frequente delle password non aumenta necessariamente la sicurezza, in quanto ha come effetto anche la promozione di comportamenti utente a rischio.

Le raccomandazioni attuali si concentrano invece su:

- La creazione di password uniche e robuste
- L'utilizzo di passphrase (lunghe combinazioni di parole facilmente memorizzabili)
- L'adozione, quando possibile, di autenticazione multifattore (MFA)

#### VERSO UN FUTURO SENZA PASSWORD

Con l'avanzare della tecnologia, molte organizzazioni stanno abbracciando soluzioni di autenticazione senza password (passwordless). Sistemi come quelli promossi dalla FIDO

Alliance utilizzano chiavi crittografiche sicure basate su hardware o autenticazione biometrica.

Le nuove tecnologie promettono di eliminare le vulnerabilità associate alle password tradizionali, migliorando sia la sicurezza che l'esperienza utente.