Materia: INFORMATICA

Sicurezza informatica 2 - Password, account e identità digitale

Credenziali, passphrase, password manager, MFA, passkey, recupero account e identità online

Gli account digitali permettono di accedere a posta elettronica, social network, registro scolastico, cloud, videogiochi, servizi bancari e piattaforme di lavoro. Proteggere un account significa proteggere dati, identità, reputazione e, in alcuni casi, denaro. Una sola password debole oppure riutilizzata può trasformarsi in una porta d'ingresso per molti servizi.

IDEA FONDAMENTALE
Un account non è soltanto un accesso tecnico: rappresenta una parte della tua identità digitale. Proteggerlo significa proteggere ciò che fai, ciò che conservi e ciò che altri potrebbero fare fingendosi te.

1. L'account come identità digitale

Un account non è soltanto una coppia formata da nome utente e password. È una rappresentazione digitale della persona. Se qualcuno ottiene accesso alla casella email, può provare a reimpostare le password di altri servizi. Se entra in un social network, può pubblicare messaggi a nome della vittima. Se entra in un account scolastico, può leggere o modificare materiali non destinati a lui.

Per questo un account deve essere trattato con attenzione: non va prestato, non va condiviso e non deve rimanere aperto su computer condivisi. La comodità non deve diventare una porta aperta.

Figura 1 - Alcuni elementi che compongono e proteggono l'identità digitale.

2. Password deboli e riutilizzo delle credenziali

Le password più facili da ricordare sono spesso anche le più facili da indovinare. Nomi propri, date di nascita, sequenze come 123456 e parole comuni offrono una protezione molto ridotta. Un altro errore grave è riutilizzare la stessa password per servizi differenti: se un servizio subisce una violazione, la stessa credenziale può essere provata automaticamente su altri account.

ERRORE DA EVITARE
Usare la stessa password per email, social, giochi e servizi scolastici è comodo, ma rischioso. Se una sola credenziale viene rubata, l'attaccante può tentare di usarla ovunque.

3. Password lunghe e passphrase

Le linee guida moderne danno molta importanza alla lunghezza. Una passphrase è una sequenza di parole o elementi più lunga di una password tradizionale. Deve essere difficile da indovinare, non basata su informazioni personali facilmente conoscibili e diversa per ogni servizio importante. Gli esempi presenti nella dispensa servono soltanto per capire il concetto e non devono essere utilizzati realmente.

Una buona password o passphrase non deve contenere nome, cognome, data di nascita, squadra preferita o altri elementi facilmente ricavabili dai social network. La robustezza dipende anche dal fatto che venga conservata e usata correttamente.

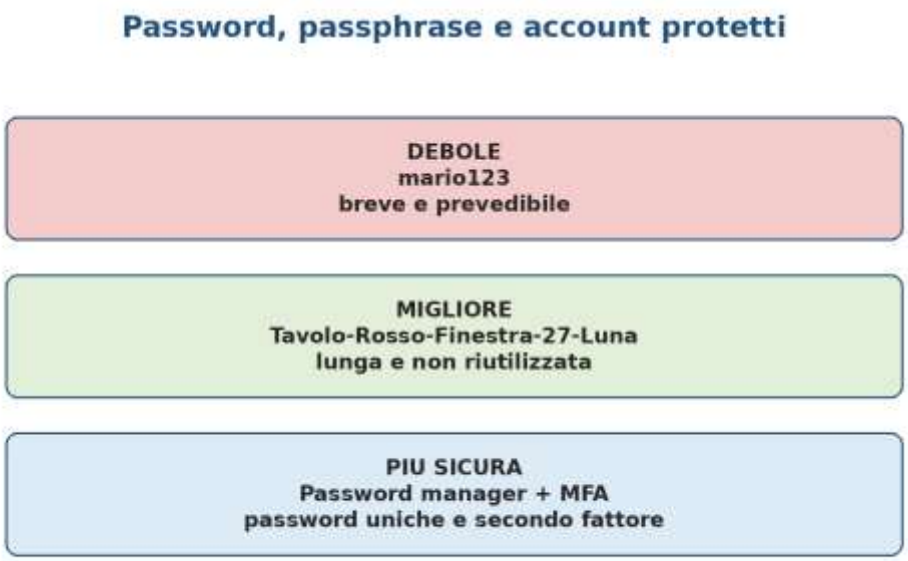

Figura 2 - Password debole, passphrase e protezione più robusta mediante password manager e MFA.

4. Password manager

Un password manager conserva le credenziali in un archivio protetto e può generare password lunghe, casuali e differenti per ogni servizio. L'utente deve proteggere con particolare attenzione la password principale del gestore. Salvare tutte le credenziali in un file di testo non protetto oppure su foglietti lasciati in vista non è una soluzione sicura.

BUONA PRATICA
Usa password uniche per gli account importanti. Proteggi con cura la password principale del password manager. Non comunicare credenziali tramite chat, email o telefonate.

5. Autenticazione multifattore

L'autenticazione multifattore, spesso abbreviata in MFA, aggiunge un secondo controllo oltre alla password. Il secondo fattore può essere una conferma su smartphone, un'app di autenticazione, una chiave fisica oppure un dato biometrico. Questo riduce il rischio, perché conoscere la password potrebbe non bastare per entrare.

Figura 3 - L'autenticazione multifattore aggiunge un controllo oltre alla password.

La MFA non funziona se l'utente approva qualsiasi notifica oppure comunica un codice temporaneo a chi lo chiede. Se ricevi una notifica di accesso inattesa, non approvarla: potrebbe indicare che qualcuno conosce già la password e sta cercando di completare l'accesso.

6. Passkey e sblocco biometrico

Le passkey sono un metodo moderno di accesso che riduce la dipendenza dalle password tradizionali. Possono usare il dispositivo e lo sblocco locale, per esempio PIN o biometria. È utile conoscere il concetto, ma la regola resta la stessa: proteggere il dispositivo e non approvare richieste inattese.

Impronte digitali e volto sono dati biometrici. Sono comodi, ma devono essere trattati con prudenza: una password può essere cambiata; un dato biometrico non può essere sostituito con la stessa facilità.

7. Recupero dell'account

Molti servizi permettono di recuperare l'accesso mediante email alternativa, numero di telefono o codici di recupero. Questi strumenti devono essere protetti quanto la password. Un codice di recupero non deve essere lasciato in vista né inviato a persone sconosciute. È importante mantenere aggiornati i recapiti associati all'account.

8. Furto di identità

Il furto di identità avviene quando qualcuno usa dati personali di un'altra persona per fingersi quella persona. Può riguardare nome, fotografie, email, numero di telefono, documenti e account social. Il danno non è soltanto tecnico: può colpire reputazione, relazioni personali e denaro.

- pubblica online soltanto le informazioni realmente necessarie;
- non inviare documenti a siti o persone non affidabili;
- controlla le impostazioni di privacy dei social network;
- avvisa subito un adulto se qualcuno crea un profilo falso;
- non lasciare lo smartphone sbloccato e incustodito.

9. Immagini, voce e deepfake

Gli strumenti di intelligenza artificiale possono generare immagini, voci e video realistici. Una richiesta urgente ricevuta in videochiamata oppure tramite messaggio vocale non deve essere considerata autentica soltanto perché la voce o il volto sembrano familiari. Prima di inviare denaro, documenti o codici, verifica mediante un secondo canale già noto.

Figura 4 - Una richiesta urgente deve essere verificata mediante un secondo canale.

10. Proteggere l'email e gli account principali

La casella email è spesso la chiave di molti altri account, perché viene usata per recuperare password e ricevere notifiche. Per questo merita una protezione particolarmente accurata: password unica, MFA, controllo periodico degli accessi e attenzione ai messaggi di recupero non richiesti.

11. Buone abitudini quotidiane

- blocca lo schermo quando ti allontani;
- non lasciare password visibili;
- non usare account condivisi se non espressamente previsti;
- esci dagli account sui computer condivisi;
- controlla periodicamente i dispositivi collegati;
- cambia subito la password se sospetti una compromissione;
- non approvare notifiche inattese.

12. Come vengono attaccate le password

Una password può essere scoperta in modi diversi: tentativi automatici su combinazioni comuni, riutilizzo di credenziali rubate in altri servizi, phishing, malware oppure osservazione diretta. Per questo la sicurezza non dipende soltanto dalla complessità della password, ma anche dal modo in cui viene conservata e utilizzata.

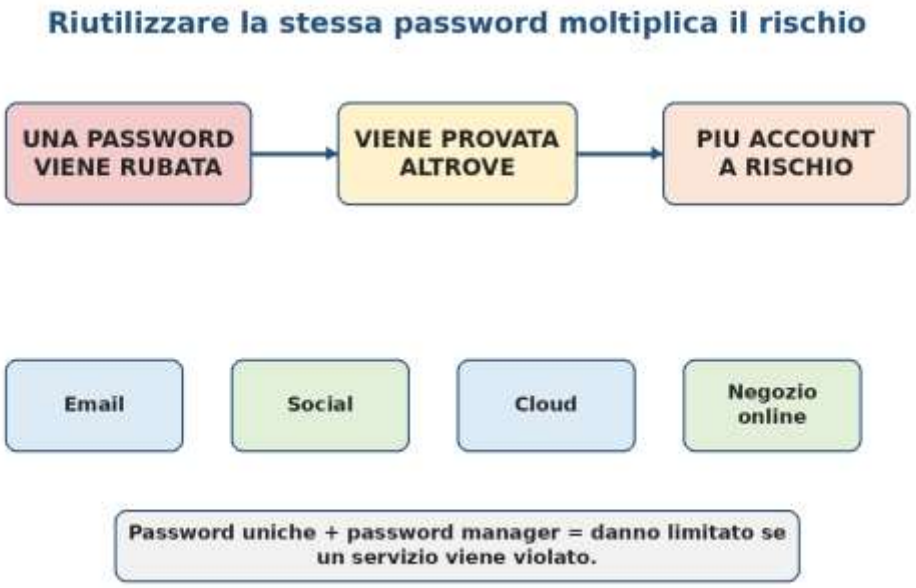

Figura 5 - Riutilizzare la stessa password espone più account.

13. Computer condivisi e dispositivi personali

Su un computer condiviso evita di salvare credenziali personali se non è previsto. Al termine del lavoro disconnettiti, chiudi il browser e verifica di non avere lasciato file scaricati oppure sessioni aperte. Sullo smartphone usa blocco schermo, aggiornamenti e copia di sicurezza. Se il dispositivo viene smarrito, la protezione locale riduce il rischio di accesso immediato ai dati.

14. Social network e informazioni pubblicate

Anche informazioni apparentemente innocue possono essere combinate: data di nascita, scuola frequentata, nomi dei familiari, fotografie e luoghi visitati. Pubblicare meno dati riduce le possibilità di furto di identità e rende più difficile costruire richieste ingannevoli molto personalizzate.

15. Piano di recupero personale

Per gli account importanti conviene sapere in anticipo come recuperare l'accesso: mantenere aggiornati email e telefono di recupero, conservare in modo sicuro eventuali codici, conoscere il canale ufficiale di assistenza e controllare periodicamente i dispositivi collegati. Prepararsi prima evita decisioni affrettate durante un problema.

16. Glossario essenziale

Termine	Significato
Account	identità usata per accedere a un servizio;
Credenziale	informazione usata per dimostrare l'identità;
Passphrase	sequenza lunga di parole o elementi;
Password manager	programma che conserva credenziali in modo protetto;
MFA	autenticazione con più fattori;
Passkey	metodo moderno di accesso basato sul dispositivo;
Biometria	dati come volto o impronta digitale;
Credential stuffing	tentativo automatico di riutilizzare credenziali rubate su servizi diversi;
Deepfake	contenuto audio, video o visivo manipolato o generato con IA.

17. Sintesi operativa

Proteggere l'identità digitale significa usare password uniche, attivare MFA, difendere la casella email, non comunicare codici temporanei, limitare le informazioni pubblicate e verificare le richieste urgenti mediante un secondo canale. La comodità è importante, ma non deve trasformarsi in fiducia automatica.

18. Checklist periodica per gli account importanti

Ogni tanto è utile controllare gli account principali, soprattutto la casella email. Non serve diventare ossessivi: basta dedicare qualche minuto a una verifica ordinata. Controllare prima evita di accorgersi troppo tardi di una modifica non autorizzata.

- verifica quali dispositivi risultano collegati;
- controlla se sono presenti accessi recenti che non riconosci;
- verifica che email e numero di recupero siano corretti;
- attiva l'autenticazione multifattore quando disponibile;
- rimuovi applicazioni o collegamenti che non usi più;
- aggiorna la password se sospetti che qualcuno possa conoscerla;
- conserva i codici di recupero in una posizione protetta.

19. Tre situazioni da riconoscere

Situazione	Comportamento corretto
Ricevi una notifica di accesso mentre non stai usando il servizio.	Non approvarla e cambia la password da un dispositivo affidabile.
Un amico ti chiede in chat un codice ricevuto sul telefono.	Non inviarlo e contattalo con un altro canale.
Un computer condiviso propone di salvare la password personale.	Verifica le regole del laboratorio o evita il salvataggio.

20. Sintesi operativa conclusiva

La protezione dell'identità digitale richiede continuità: password uniche, MFA, dispositivo bloccato, email protetta, dati personali pubblicati con prudenza e verifiche periodiche. Non bisogna fidarsi automaticamente di richieste urgenti, notifiche inattese o voci apparentemente familiari. Quando qualcosa non torna, il comportamento più intelligente è fermarsi e controllare.

21. Domande di verifica

Rispondi con parole tue. Le domande servono a verificare la comprensione, non a ripetere meccanicamente il testo.

1. Perché un account rappresenta una parte dell'identità digitale?
2. Perché riutilizzare una password è rischioso?
3. Che cos'è una passphrase?
4. Quali caratteristiche deve avere una password efficace?
5. A che cosa serve un password manager?
6. Perché la password principale del password manager è importante?
7. Che cos'è l'autenticazione multifattore?
8. Quali esempi di secondo fattore conosci?
9. Perché non devi approvare una notifica di accesso inattesa?
10. Che cosa sono le passkey?
11. Che cosa sono i dati biometrici?
12. Perché un dato biometrico richiede attenzione?
13. A che cosa servono i codici di recupero?
14. Che cos'è il furto di identità?
15. Quali dati possono essere usati per rubare identità?
16. Perché la casella email merita particolare protezione?
17. Che cos'è un deepfake?

18. Come devi verificare una richiesta urgente ricevuta in videochiamata?
19. Perché devi bloccare lo schermo quando ti allontani?
20. Quali controlli periodici conviene fare sugli account principali?

22. Risposte ragionate

1. Perché permette di agire online a nome della persona e può contenere dati, messaggi e autorizzazioni.
2. Perché una credenziale rubata in un servizio può essere provata automaticamente su altri servizi.
3. È una sequenza lunga di parole o elementi pensata per essere più robusta e gestibile.
4. Deve essere lunga, non ovvia, diversa per ogni servizio importante e non basata su informazioni personali facili da conoscere.
5. Serve a conservare credenziali in modo protetto e a generare password uniche.
6. Perché protegge l'accesso all'archivio che contiene molte altre credenziali.
7. È un metodo che richiede almeno un controllo aggiuntivo oltre alla password.
8. Notifica su smartphone, app di autenticazione, chiave fisica, SMS in alcuni casi oppure biometria.
9. Perché potrebbe essere il tentativo di un attaccante che possiede già la password.
10. Sono un metodo moderno di accesso basato sul dispositivo e sullo sblocco locale, riducendo la dipendenza dalle password.
11. Sono informazioni legate al corpo, come volto e impronta digitale.
12. Perché non può essere cambiato facilmente come una password.
13. Servono a recuperare l'accesso quando il metodo principale non è disponibile.
14. È l'uso non autorizzato dei dati di una persona per fingersi quella persona.
15. Nome, immagini, documenti, email, telefono, account social e altre informazioni personali.
16. Perché spesso viene usata per recuperare le password di altri account.
17. È un contenuto audio, video o visivo manipolato o generato con IA per sembrare reale.
18. Usando un secondo canale già noto, come un numero salvato, e facendo controlli indipendenti.
19. Per impedire ad altre persone di usare l'account lasciato aperto.
20. Controllare dispositivi collegati, accessi recenti, recapiti di recupero e notifiche di sicurezza.

23. Esercizi pratici e attività

Svolgi gli esercizi senza usare password reali e senza inserire dati personali. Gli esempi devono essere inventati o preparati dal docente.

1. Confronta cinque password inventate e classificale come deboli o migliori, motivando la scelta.
2. Costruisci tre passphrase inventate senza usare informazioni personali reali.
3. Elenca i servizi per i quali sarebbe particolarmente importante usare password uniche.
4. Disegna uno schema che mostri password manager e password principale.
5. Simula l'attivazione della MFA su un account di prova, se il docente lo consente.
6. Scrivi come reagiresti a una notifica di accesso inattesa.
7. Prepara una checklist per proteggere la casella email.
8. Elenca cinque dati personali da non condividere inutilmente.
9. Analizza un profilo social simulato e individua informazioni eccessive.
10. Descrivi un caso di furto di identità e le possibili conseguenze.
11. Scrivi un breve dialogo in cui verifichi una richiesta urgente ricevuta in videochiamata.
12. Prepara un cartello: "I codici temporanei non si comunicano".
13. Controlla su un account di prova quali dispositivi risultano collegati.
14. Spiega la differenza tra password, PIN, MFA e biometria.
15. Scrivi cinque regole per l'uso sicuro di un computer condiviso.

24. Checklist finale

CHECKLIST ACCOUNT SICURO
Password unica e lunga. MFA attiva dove possibile. Email protetta. Codici di recupero conservati con cura. Schermo bloccato quando ti allontani. Nessun codice temporaneo comunicato ad altri. Richieste urgenti verificate con un secondo canale.