



Password e verifica in due passaggi

Come chiudere bene la porta dei tuoi account, senza impazzire a ricordare niente

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Indice

Come usare questa dispensa 3

1. Perché la password è il punto debole 3

1.1 Il caso di Marta e della scuola di danza 4

1.2 Come si rubano le password 5

2. Come si costruisce una password buona 6

2.1 La frase lunga 6

2.2 Cosa evitare 8

2.3 Cambiarla ogni tre mesi? Oggi non più 8

3. Una password per servizio: il gestore 9

3.1 Che cosa fa, in pratica 10

3.2 Quale scegliere 11

3.3 Il caso dello studio di Luca 11

4. La verifica in due passaggi 12

4.1 I metodi, dal più debole al più robusto 13

4.2 Quando arrivano richieste che non hai fatto 14

5. Dove attivarla per prima e come non restare fuori 15

5.1 Un ordine pratico 16

5.2 Il piano B: i codici di recupero 16

5.3 Il caso del telefono perso 17

Esercitazione pratica 19

Le domande che arrivano in aula 20

Glossario 21

Per approfondire 21

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Imparare a costruire password lunghe e diverse per ogni servizio, a custodirle in un gestore di password e ad attivare la verifica in due passaggi sugli account che contano davvero.

Che cosa saprai fare alla fine

- Riconoscere perché una password corta, prevedibile o riutilizzata è un rischio.
- Costruire una frase lunga facile da ricordare e difficile da indovinare.
- Usare un gestore di password per avere una password diversa per ogni servizio.
- Attivare la verifica in due passaggi scegliendo il metodo più adatto.
- Sapere come recuperare un account se si perde il telefono.

1. Perché la password è il punto debole

Puoi avere il computer più aggiornato del mondo: se la tua password è «segreteria2024», la porta è aperta.

Una **password** è la chiave con cui un servizio capisce che sei proprio tu. Posta elettronica, registro della scuola, gestionale delle fatture, banca online: ogni porta ha la sua chiave. E il problema, nella vita di tutti i giorni, è che le chiavi sono tante e la memoria è una sola.

Così facciamo quello che fanno quasi tutti: scegliamo una password facile e la usiamo ovunque. Magari con un numero in fondo, per rispettare la regola «almeno una cifra». È comodo. È anche il modo più veloce per farsi rubare l'account.



Una password riutilizzata collega la sicurezza di account diversi.

1.1 Il caso di Marta e della scuola di danza

Marta lavora in segreteria in una piccola scuola di danza. Anni fa si è iscritta a un sito di sconti per l'abbigliamento sportivo, usando la stessa e-mail e la stessa password che usa per la posta della scuola. Un giorno quel sito di sconti viene violato: i ladri portano via l'elenco di indirizzi e password degli iscritti.



Credenziali sottratte a un sito vengono provate su altri servizi.

Nessuno avvisa Marta. Pochi giorni dopo, però, un programma automatico prova quella coppia di dati su centinaia di altri servizi, uno dopo l'altro. Alla posta della scuola la password funziona. Da lì, i ladri leggono le mail, vedono gli elenchi degli iscritti e scrivono ai genitori fingendosi la segreteria.



Come una password riutilizzata apre account che non c'entrano

L'IDEA IN UNA RIGA

Una password riutilizzata vale quanto il **sito più fragile** su cui l'hai usata.

1.2 Come si rubano le password

Non serve un genio informatico. Esistono pochi metodi, tutti molto comuni:

- **furto da un sito violato:** gli elenchi di password finiscono in vendita o in rete, e vengono provati su altri servizi (si chiama *credential stuffing*, cioè «riempimento di credenziali»);
- **tentativi a raffica:** un programma prova le password più usate al mondo, e parole del dizionario con qualche cifra aggiunta;
- **phishing e siti trappola:** sei tu a digitare la password in una pagina falsa (le lezioni tre e quattro del corso);
- **programmi spia:** un keylogger registra i tasti che premi (lezione due);
- **sguardi e post-it:** la password scritta sul foglietto sotto la tastiera, che chiunque passi può leggere.

Nota una cosa: contro quattro di questi cinque metodi, una password più complicata non basta. È per questo che serve anche la seconda parte della lezione, la verifica in due passaggi.

2. Come si costruisce una password buona

Per anni ci hanno insegnato a scrivere password brutte e difficili. La buona notizia è che oggi si consiglia l'esatto contrario.

Una password come «Xk9#pL2!» è ostica per te e abbastanza facile per un programma, perché è corta. Quello che conta davvero è la **lunghezza**: ogni carattere in più moltiplica il lavoro che serve per indovinarla. Per questo la regola pratica è di arrivare ad almeno **dodici-quattordici caratteri**, meglio ancora se sono una frase.

2.1 La frase lunga

Una frase lunga è una password che riesci a ricordare perché ha un senso, ma che nessuno può indovinare perché è tua. Un esempio come «Il-giovedi-porto-il-caffe-in-ufficio!»: sette parole, sei trattini, un punto esclamativo. Facile da ricordare, lunga, non è una parola del dizionario.

> **NON COPIARE L'ESEMPIO**
>
> Una frase stampata su una dispensa, su un sito o su una slide è una frase che **tutti conoscono**. Usala solo per capire il metodo e inventane una tua, che non hai mai letto da nessuna parte.



Scegli una frase lunga e unica, senza copiare gli esempi.

Come inventarne una? Pensa a un'immagine vivida e un po' assurda, e scrivila con parole separate da trattini o spazi. Per esempio: «tre-gatti-mangiano-una-pizza-sul-tram». Non è un modo di dire, non è collegata a te, ma la visualizzi subito.

Debole e forte

Password debole	Frase lunga
Corta e prevedibile	Dodici-quattordici caratteri o più
Nome più numero finale	Parole non collegate
Uguale su più servizi	Una per servizio
Scritta su un foglietto	Custodita nel gestore

vs

Password debole e frase lunga a confronto

2.2 Cosa evitare

Scelta	Perché è un rischio	Cosa fare invece
Nome, data di nascita, nome del cane	Si trovano sui social o si indovinano con due domande	Una frase senza legami con la tua vita
Parola comune più un numero («Estate2026»)	È la prima cosa che i programmi provano	Più parole non collegate tra loro
Sostituzioni ovvie («p4ssw0rd»)	I programmi le conoscono e le provano	Lunghezza, non travestimenti
La stessa password dappertutto	Un solo sito violato apre tutti gli altri	Una password diversa per ogni servizio
Il foglietto sotto la tastiera	Lo legge chiunque passi dalla scrivania	Un gestore di password (vedi dopo)

Le scelte più comuni e perché non funzionano.



Nomi e date pubbliche sono scelte prevedibili.

2.3 Cambiarla ogni tre mesi? Oggi non più

Probabilmente in qualche ufficio ti obbligano a cambiare password di continuo. Le linee guida più recenti sull'identità digitale, quelle dell'ente americano NIST (National Institute of Standards and Technology, l'istituto che fissa gli standard tecnici negli Stati Uniti), non lo consigliano più come regola fissa: chi è costretto a cambiare spesso, tende a fare cambi minimi («Estate1», «Estate2») che non proteggono nulla.

La regola di buon senso è questa: **cambia la password subito** se hai il sospetto che sia stata rubata, se un servizio ti avvisa di una violazione, o se l'hai data a qualcuno. Altrimenti, una password lunga e unica può restare dov'è.



Cambiala se è compromessa o se il servizio segnala una violazione.

> **CONTROLLA SE SEI GIÀ IN UN ELENCO**
>
> Esiste un servizio gratuito e molto noto, *Have I Been Pwned* (haveibeenpwned.com), dove inserisci il tuo indirizzo e-mail e vedi se compare in violazioni di dati già pubbliche. Se compare, non è una tragedia: cambia la password di quel servizio e di ogni altro dove l'avevi riusata.

3. Una password per servizio: il gestore

Hai venti account e una memoria. Lascia fare il lavoro a chi non si dimentica niente.

Una password diversa per ogni servizio è l'unico modo per fermare la catena di Marta. Ma nessuno riesce a ricordare venti frasi lunghe e diverse. Qui entra in scena il **gestore di password** (in inglese *password manager*): un programma, o una funzione del browser, che conserva tutte le tue password in un archivio cifrato.

Tu ricordi **una sola** password, la principale (in inglese *master password*), che apre l'archivio. Tutte le altre le sceglie e le compila lui, e possono essere lunghe e casuali, perché non devi impararle.



Un archivio cifrato conserva credenziali diverse per ogni servizio.

3.1 Che cosa fa, in pratica

- **crea** password lunghe e casuali quando ti iscrivi a un servizio;
- **le ricorda** e le compila al posto tuo sul sito giusto, sul computer e sul telefono;
- **ti avvisa** se una password è debole, se è riusata o se compare in una violazione nota;
- **conserva anche** altre informazioni riservate: codici di recupero, note, a volte i dati della carta.

C'è un bonus meno evidente e molto utile: il gestore compila la password **solo sul sito giusto**. Se finisci su www.ente-esempio.it, un sito trappola come quelli visti nella lezione quattro, il gestore non riconosce l'indirizzo e non ti propone niente. Quel silenzio è un campanello d'allarme.



Se la compilazione attesa non compare, verifica il dominio.

3.2 Quale scegliere

Tipo	Pregi	Limiti
Gestore del browser (Edge, Chrome, Firefox)	Già installato, comodo, gratuito	Funziona al meglio dentro quel browser; conta molto chi protegge l'accesso al profilo
Gestore dedicato (applicazione o estensione)	Funziona ovunque, condivisione in famiglia o in ufficio, controlli più completi	Va installato e spesso ha un costo, soprattutto per i team
Gestore del sistema (telefono, computer)	Integrato con impronta e volto	Può legarti a un solo produttore di dispositivi

Tre strade possibili: la migliore è quella che userai davvero.

Non ti do un nome di prodotto, perché le offerte cambiano di continuo. Ti do il **criterio**: cerca un gestore di un fornitore noto, con archivio cifrato, che funzioni sui dispositivi che usi e che sappia attivare la verifica in due passaggi sul suo stesso accesso.

3.3 Il caso dello studio di Luca

In un piccolo studio di commercialisti, quattro persone condividevano le credenziali del portale delle scadenze con un foglio incollato sul monitor. Quando una collaboratrice ha lasciato lo studio, nessuno ha cambiato nulla: lei aveva ancora l'accesso, e nessuno poteva dire chi avesse fatto cosa.

Con un gestore di password che prevede condivisione, ogni persona ha il suo accesso. Si decide chi vede quali credenziali, e quando qualcuno se ne va si cambia la password condivisa in un attimo. Per un ufficio con più persone, è molto meglio di qualsiasi foglio.

I LIMITI DEL GESTORE

Se perdi la password principale, nella maggior parte dei gestori **nessuno può recuperarla per te**: è una conseguenza della cifratura. Scrivi un promemoria e custodiscilo in un posto sicuro, per esempio in una busta chiusa in cassaforte. E proteggi l'accesso al gestore con la verifica in due passaggi.

4. La verifica in due passaggi

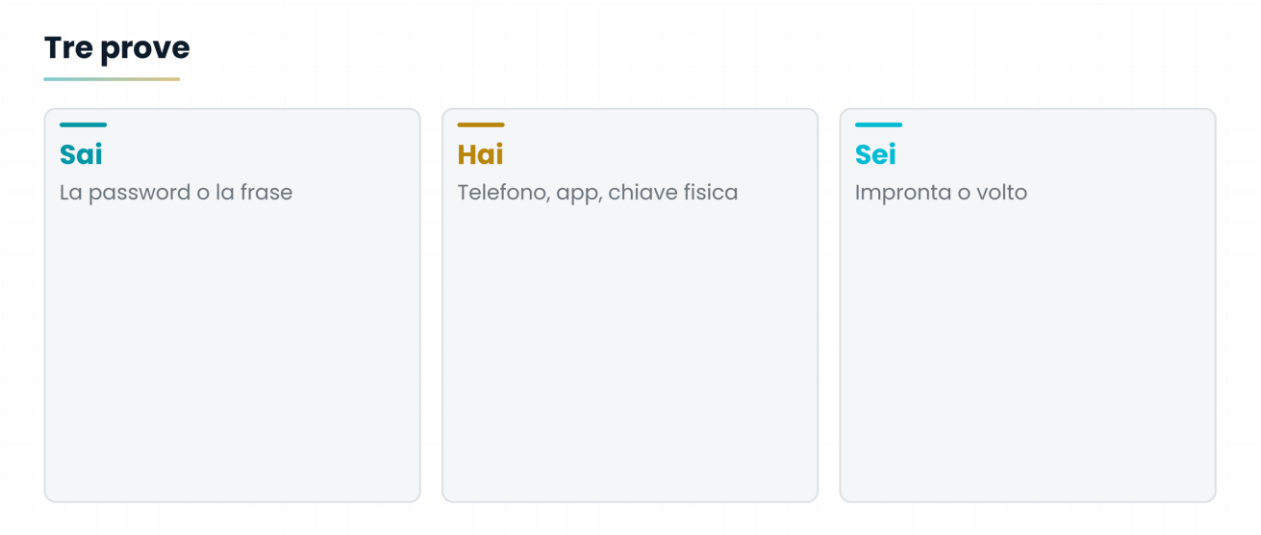
La password può essere rubata. Il secondo passaggio la rende molto meno utile a chi l'ha rubata.

La **verifica in due passaggi** (in inglese *multi-factor authentication*, abbreviata MFA, cioè autenticazione a più fattori) significa che per entrare non basta la password: serve un secondo elemento, diverso dal primo. Anche se un ladro conosce la tua password, senza il secondo elemento non entra.



Qualcosa che sai, che hai e che sei.

In pratica combini due cose di famiglie diverse, tra queste tre: qualcosa che **sai** (la password), qualcosa che **hai** (il telefono, una chiave fisica), qualcosa che **sei** (l'impronta, il volto).



I tre tipi di prova che dimostrano chi sei

4.1 I metodi, dal più debole al più robusto

Metodo	Come funziona	Punti di forza e di debolezza
Codice per SMS	Ricevi un codice sul telefono e lo digiti	Meglio di niente. Ma l'SMS può essere intercettato, e un truffatore può convincerti a dettargli il codice
App di autenticazione	Un'app sul telefono genera un codice che cambia continuamente	Più sicura dell'SMS, funziona anche senza rete. Se cambi telefono va trasferita con cura
Notifica «approva»	Il telefono ti chiede di confermare l'accesso	Comodissima. Attenzione a non premere «approva» se non sei stato tu
Impronta o volto	Il dispositivo ti riconosce	Veloce. Sblocca di solito un solo dispositivo, non l'account ovunque
Chiave fisica o passkey	Una piccola chiavetta, o un'identità salvata sul dispositivo, dimostra che sei tu	Il metodo più robusto, perché non si lascia ingannare da siti falsi. Richiede un po' di abitudine

Scegli il più robusto tra quelli che il servizio offre.

Una **passkey** è una credenziale che sostituisce la password: invece di digitare qualcosa, confermi con l'impronta, il volto o il codice di sblocco del dispositivo. Un sito falso non può rubarla, perché funziona solo con il sito vero. Sempre più servizi la offrono: se la trovi, provala.



I metodi non offrono tutti la stessa resistenza al phishing.

NESSUNO TI CHIEDERÀ MAI IL CODICE

Un operatore della banca, un collega dell'assistenza, un corriere: **nessuno** ha bisogno del codice che ricevi sul telefono. Se qualcuno te lo chiede, anche con voce gentile, è un truffatore (il *vishing*, la truffa telefonica della lezione tre). Il codice non si detta, non si inoltra, non si fotografa.

4.2 Quando arrivano richieste che non hai fatto

Se ti arriva sul telefono una richiesta di approvazione senza che tu abbia fatto nulla, vuol dire che qualcuno ha la tua password e sta provando a entrare. A volte i truffatori ne mandano a raffica, sperando che tu prema «approva» per sfinimento. **Rifiuta**, e cambia subito la password di quell'account.

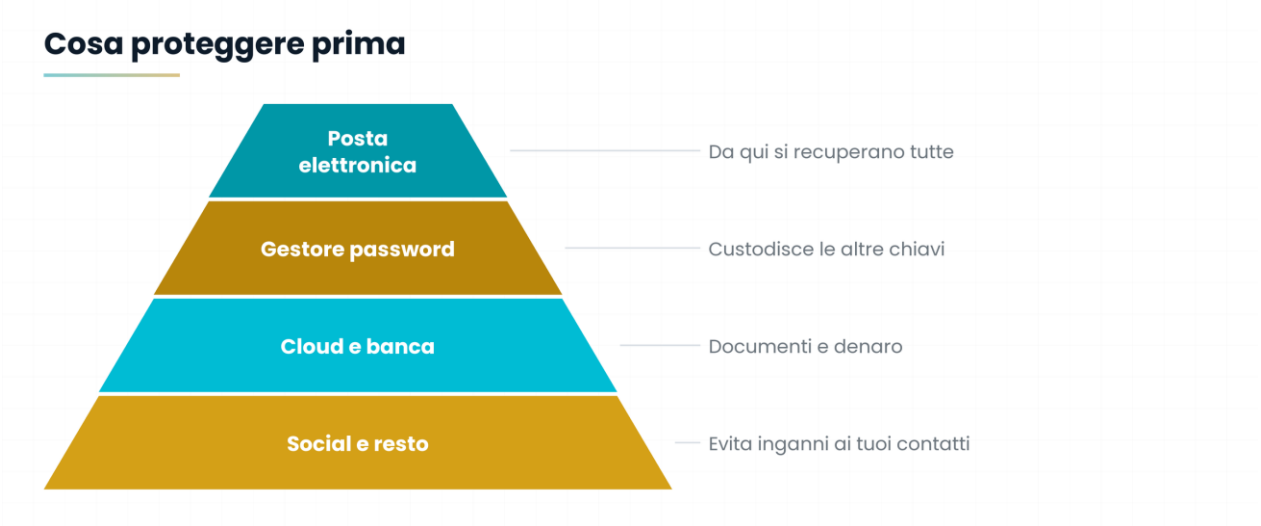


Non condividere i codici e non approvare richieste inattese.

5. Dove attivarla per prima e come non restare fuori

Non devi attivare tutto oggi. Devi attivare le cose giuste, nell'ordine giusto.

Il primo bersaglio dei truffatori è la **posta elettronica**. Il motivo è semplice: quasi ogni servizio, quando dimentichi la password, ti manda il link per reimpostarla all'indirizzo di posta. Chi controlla la tua posta controlla, a cascata, tutto il resto.



In che ordine proteggere i tuoi account

5.1 Un ordine pratico

1. **La posta elettronica,** quella personale e quella dell'ufficio.
2. **Il gestore di password.** Se lui è protetto bene, tutto il resto lo è.
3. **Il cloud e i documenti** (gli archivi online dove tieni file e cartelle).
4. **La banca, i pagamenti e i portali pubblici,** come l'area riservata dell'Agenzia delle Entrate (l'ente fiscale italiano) o i servizi che usi con la tua identità digitale.
5. **I social e tutto il resto.** Anche un profilo social rubato serve ai truffatori per ingannare i tuoi contatti.



Comincia dalla posta, poi proteggi gli altri accessi importanti.

Di solito l'opzione si trova nelle impostazioni dell'account, in una voce che si chiama «Sicurezza», «Verifica in due passaggi» o «Autenticazione a più fattori». I nomi variano da servizio a servizio, ma il percorso è sempre simile: scegli il metodo, scansioni un codice con l'app o confermi con il telefono, e il gioco è fatto.

5.2 Il piano B: i codici di recupero

Quando attivi la verifica in due passaggi, il servizio ti dà quasi sempre dei **codici di recupero**: una breve serie di codici monouso, da usare se perdi il telefono. Sono più importanti di quanto sembrino.

- stampali o scrivili a mano e **custodiscili lontano dal computer** (una cassaforte, un cassetto chiuso a chiave);

- oppure salvali **nel gestore di password**, se lo proteggi con una verifica robusta;
- non lasciarli in un file qualsiasi sul desktop e non fotografarli sul telefono, dove finiscono nel backup automatico di tutto il resto.

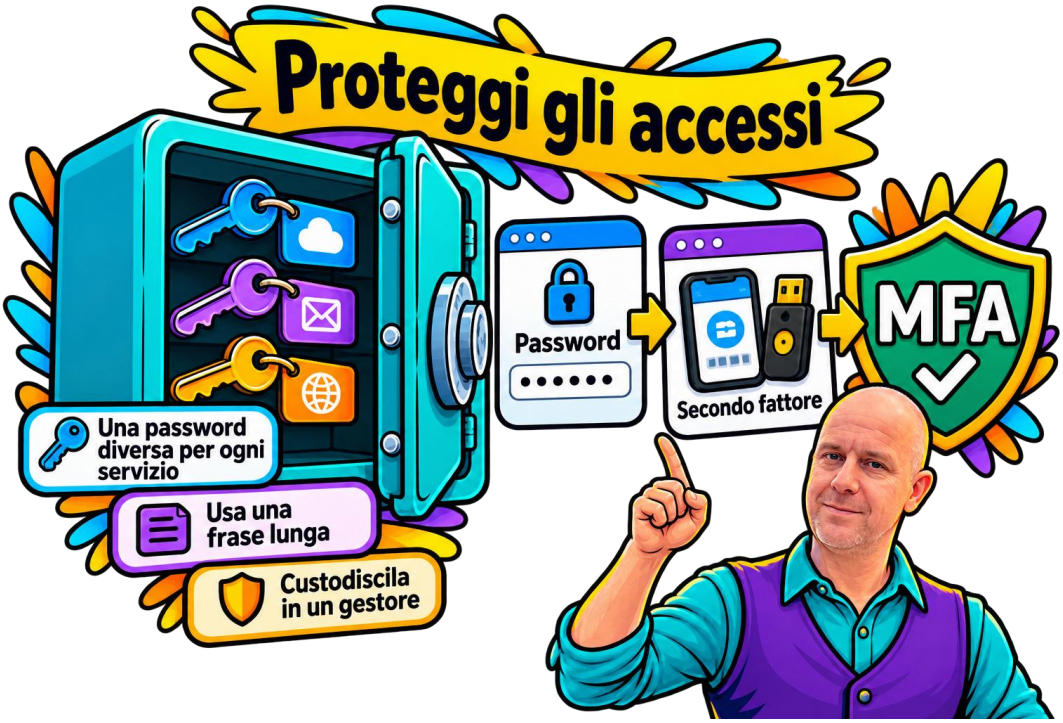
5.3 Il caso del telefono perso

Giulia, segretaria di una scuola media, perde il telefono in autobus. Dentro c'è l'app che genera i codici per la posta dell'istituto. Se Giulia ha conservato i codici di recupero, accede con quelli, toglie il telefono perso dall'elenco dei dispositivi di fiducia e ne collega uno nuovo. Se non li ha conservati, deve passare dall'assistenza, con tempi e documenti da presentare.



Conserva i codici di recupero in un luogo sicuro.

Morale: la verifica in due passaggi protegge, ma richiede di preparare **prima** il piano B. Dieci secondi di organizzazione oggi, giornate di lavoro risparmiate domani.



Proteggi gli accessi

IN SINTESI

Password lunga, una per servizio, in un gestore; verifica in due passaggi su posta, cloud e banca; codici di recupero in un posto sicuro.

Esercitazione pratica

Una breve esercitazione da fare davanti al tuo computer, con quello che hai già: la posta elettronica e il telefono.

1. Elenca su un foglio (solo i nomi dei servizi, **mai le password**) i cinque account più importanti che usi: posta, cloud, banca, gestionale, social.
2. Apri il servizio di haveibeenpwned.com e controlla il tuo indirizzo di posta. Annota se compare in qualche violazione.
3. Inventa una frase lunga, nuova e tua, di almeno quattro parole, e usala per la password principale di un gestore (quello del browser va benissimo per cominciare).
4. Entra nelle impostazioni della tua posta elettronica, cerca «Sicurezza» e attiva la verifica in due passaggi, scegliendo l'app di autenticazione se disponibile.
5. Quando il servizio ti propone i codici di recupero, salvali in un posto sicuro e fuori dal computer.
6. Scegli un secondo account dell'elenco e ripeti: cambia la password con una lunga e attiva il secondo passaggio.

> **CONTROLLA DI AVER FATTO COSÌ**
>
> La password principale è una frase che non hai mai letto altrove?
>
> I codici di recupero sono lontani dal computer?
>
> Hai attivato il secondo passaggio almeno sulla posta?
>
> Sai dire cosa fai se perdi il telefono?

Le domande che arrivano in aula

Un gestore di password non è come mettere tutte le uova in un solo paniere?

In parte sì, ed è per questo che l'archivio è cifrato e va protetto con una password principale lunga e con la verifica in due passaggi. Ma il paragone giusto è con l'alternativa reale: password deboli, riusate o scritte su un foglio. Per la grande maggioranza delle persone, un gestore è molto più sicuro di quello che fa oggi.

L'SMS come secondo passaggio è inutile?

No, è molto meglio di niente. È il metodo più debole tra quelli disponibili, perché si può intercettare o farsi dettare. Se il servizio offre un'app di autenticazione o una passkey, scegli quelle. Se c'è solo l'SMS, attivalo comunque.

Quanto deve essere lunga la mia password?

Come minimo dodici-quattordici caratteri; meglio una frase di quattro o cinque parole. Le password generate dal gestore possono essere ancora più lunghe, perché non devi ricordarle.

Posso usare la stessa frase con una piccola variazione per ogni sito?

È una cattiva idea: se un ladro vede la variazione su un sito, la indovina sugli altri. Ogni servizio merita una password diversa e indipendente, ed è proprio il lavoro del gestore.

Ho perso il telefono con l'app dei codici: sono fuori da tutto?

Se hai salvato i codici di recupero no: li usi per entrare e colleghi il nuovo telefono. Se non li hai, devi passare dalla procedura di recupero del singolo servizio, che può richiedere tempo e verifiche. Per questo conviene prepararli subito.

Posso condividere la password con una collega quando sono in ferie?

Meglio di no: un accesso condiviso non dice più chi ha fatto cosa. Se serve, usa la condivisione prevista dal gestore, oppure chiedi al responsabile di creare un accesso apposta per lei.

Glossario

Termine	Che cosa significa
Codici di recupero	Codici monouso forniti dal servizio per rientrare nell'account se perdi il telefono.
Credential stuffing	Tentativo automatico di usare su molti servizi le password rubate da un altro sito.
Frase lunga	Una password fatta da più parole, facile da ricordare e difficile da indovinare.
Gestore di password	Un programma che conserva in un archivio cifrato tutte le tue password e le compila al posto tuo.
Keylogger	Programma spia che registra i tasti premuti per rubare password e numeri di carta.
MFA (verifica in due passaggi)	Oltre alla password serve un secondo elemento: un codice nell'app, un'impronta, una chiave fisica.
Passkey	Credenziale che sostituisce la password: confermi con impronta, volto o sblocco del dispositivo.
Password	La chiave segreta con cui un servizio capisce che sei proprio tu.

Per approfondire

NIST, Digital Identity Guidelines (Special Publication 800-63B) - indicazioni su lunghezza minima (almeno 15 caratteri se la password è l'unico fattore) e sul cambio solo in caso di necessità

Have I Been Pwned (haveibeenpwned.com) - servizio gratuito per verificare se un indirizzo compare in violazioni note

FIDO Alliance, informazioni sulle passkey - descrizione del funzionamento e dei vantaggi

Agenzia per la cybersicurezza nazionale (acn.gov.it) - materiali di sensibilizzazione sull'uso sicuro degli account

ATTENZIONE

Informazioni aggiornate a ottobre 2026. I nomi dei menu e delle voci di sicurezza dei servizi online cambiano spesso: se non trovi una voce, cerca «sicurezza» nelle impostazioni dell'account. Riferimenti italiani: l'Agenzia delle Entrate è l'ente fiscale; l'Agenzia per la cybersicurezza nazionale è l'autorità italiana per la sicurezza informatica.