GUIDA PRATICA ALLA DEMERDIFICAZIONE DALLE BIG-TECH COMPANIES

PASSWORD · BITWARDEN



Dal gestore di Google a *Bitwarden*

Perché le password non devono stare nel browser né nell'account Google, come creare una cassaforte cifrata e gratuita, e come traslocarci dentro tutto.

I Perché un gestore di password

II Perché Bitwarden

III Creare la cassaforte

IV Traslocare le password

I Perché un gestore di password

E perché non quello di Google, che molti usano senza saperlo.

Ognuno di noi ha decine di account: posta, banca, SPID, negozi, social, scuola, fascicolo sanitario. Nessuno può ricordare decine di password diverse e lunghe, e così si finisce per usare sempre la stessa, magari con una piccola variante. È l'errore più comune, e il più pericoloso.

SICUREZZA Una password per tutto

I siti vengono violati di continuo, e gli elenchi di email e password rubate circolano in rete. Chi li ottiene prova la stessa coppia su posta, banca e social: se la password è la stessa, entra ovunque. Per sapere se il tuo indirizzo compare in una violazione puoi controllare su **haveibeenpwned.com**, un servizio gratuito e indipendente.

Un **gestore di password** risolve il problema: ricorda per te una password diversa e lunga per ogni sito, la inserisce da solo, e a te ne resta da ricordare **una sola**, quella principale.

La password più sicura è quella che non devi ricordare: la genera e la custodisce la cassaforte.

GOOGLE Il gestore che hai già

Se usi Chrome o un telefono Android, probabilmente hai già un gestore di password: quello di Google, che salva tutto nel tuo account Google. È comodo, ma ha tre problemi.

- **Tutte le chiavi in un solo posto, che non controlli.** Se l'account Google viene bloccato, sospeso per errore o rubato, perdi l'accesso a tutte le password insieme, o le consegni tutte a chi te l'ha rubato.
- **Ti lega a Google.** Funziona bene solo dentro Chrome e Android: è uno dei fili che rendono difficile lasciare il resto dell'ecosistema.
- **La cifratura completa è facoltativa.** Per fare in modo che nemmeno Google possa leggere le password bisogna attivare a parte la "crittografia sul dispositivo", e pochi lo fanno.

E IL GESTORE DI BRAVE O DI FIREFOX?

È meglio di niente, ma resta chiuso nel browser: non ti aiuta sul telefono, sulle app, sugli altri browser. Un gestore indipendente funziona ovunque, e se un giorno cambi browser le password vengono con te.

II Perché Bitwarden

Gratuito, a codice aperto, cifrato in modo che nemmeno l'azienda possa leggere le tue password.

Bitwarden è un gestore di password nato nel 2015. Funziona su computer (Windows, Mac, Linux), telefono (Android e iPhone) e come estensione dei browser, Brave e Firefox compresi. Il piano gratuito non ha limiti di password né di dispositivi.

0 €
il piano gratuito, con password e dispositivi illimitati

UE
puoi scegliere che i tuoi dati stiano su server in Europa

100%
codice pubblico, verificato ogni anno da esperti esterni

1
sola password da ricordare: quella principale

SICUREZZA Cifrata prima di partire

Le password vengono cifrate **sul tuo dispositivo**, con una chiave che nasce dalla tua password principale, prima di essere inviate ai server. Bitwarden conserva solo un blocco di dati illeggibile: non può vedere le tue password, non può consegnarle a nessuno e, se i suoi server venissero violati, chi li ruba troverebbe solo dati cifrati. Lo stesso vale per le note sicure, le carte e i documenti che puoi aggiungere.

OPEN SOURCE Il codice è di tutti

Il codice delle app e dei server è pubblico, e ogni anno società di sicurezza indipendenti lo verificano e pubblicano i risultati. Chi vuole può perfino far girare un server Bitwarden a casa propria. E puoi **esportare** tutto in qualsiasi momento: se un giorno vuoi andartene, le tue password vengono con te.

	GOOGLE	BITWARDEN
Dove funziona	Chrome e Android	**ovunque: ogni browser, telefono, computer**
Cifratura completa	facoltativa	**sempre**
Legato a	tutto l'account Google	**un account solo per le password**
Codice	chiuso	**aperto e verificato**
Dati in Europa	no	**sì, se lo scegli**
Costo	gratis	**gratis (Premium 19,80 $ l'anno)**

PER ONESTÀ: I LIMITI

- Bitwarden è un'**azienda statunitense a scopo di lucro**; dal 2022 ha tra i soci un fondo di investimento (PSG), con una quota di minoranza;
- nel 2026 ha raddoppiato il prezzo del piano Premium, ha cambiato amministratore delegato senza annunciarlo e per qualche settimana la scritta “sempre gratis” è sparita dal sito, per poi tornare. Il nuovo amministratore ha confermato che il piano gratuito resta;
- la regione (USA o Europa) si sceglie all'iscrizione e non si può cambiare dopo, se non rifacendo l'account;
- se dimentichi la password principale, **nessuno può recuperarla**, nemmeno Bitwarden: è il prezzo della cifratura. Per questo c'è il foglio della parte III.

Se le cose dovessero peggiorare, l'esportazione ti permette di passare in pochi minuti a un'alternativa, come **KeePassXC** (gratuito, a codice aperto, tutto sul tuo computer) o **Proton Pass** (svizzero).

III Creare la cassaforte

Un quarto d'ora, con calma. È l'unico momento in cui serve concentrazione.

Ti servono il computer, il telefono, la tua email, un foglio di carta e una penna. Se stai aiutando un genitore o un nonno, fatelo insieme e la password principale fatela scegliere a lui: deve essere sua e la deve ricordare lui.

FACILE Creare l'account in 5 passi

1. **Vai su bitwarden.eu** dal computer (il sito europeo) e scegli `Crea account`. Se arrivi da bitwarden.com, nella pagina di accesso cambia la regione in `bitwarden.eu`.
2. **Scrivi email e nome** e conferma l'indirizzo dal messaggio che ti arriva.
3. **Scegli la password principale** (vedi il riquadro qui sotto) e scrivila due volte. Il “suggerimento” lascialo vuoto o scrivi qualcosa che capisci solo tu.
4. **Scrivila sul foglio**, insieme all'email usata. Rileggi il foglio e controlla che sia giusta, lettera per lettera.
5. **Entra nella cassaforte** (“vault”). È vuota: la riempiremo nella parte IV.

COME SCEGLIERE LA PASSWORD PRINCIPALE

La regola più semplice: **quattro o cinque parole a caso**, unite da un trattino, con un numero. Per esempio `tavolo-ciliegia-vento-faro-82` (non usare questa!). È lunga, quindi difficilissima da indovinare, ma si ricorda con un'immagine. Evita frasi famose, nomi di familiari, date e animali di casa. Se non ti viene in mente niente, il generatore di Bitwarden sa creare frasi così: **Generatore → Passphrase**.

SICUREZZA La verifica in due passaggi

Così, anche se qualcuno scoprisse la password principale, senza il tuo telefono non potrebbe entrare.

1. Sul telefono installa un'app di autenticazione a codice aperto: **Bitwarden Authenticator** (gratuita) va benissimo.
2. Nella cassaforte, dal computer: **Impostazioni → Sicurezza → Accesso in due passaggi**, poi **App di autenticazione → Gestisci**.
3. Inquadra il codice QR con l'app, scrivi il codice di sei cifre che compare e salva.
4. Nella stessa pagina scegli **Visualizza codice di recupero** e **copialo sul foglio**: serve se perdi il telefono.

IL FOGLIO DA CONSERVARE

Sul foglio scrivi: "Bitwarden (bitwarden.eu) – email: ..... – password principale: ..... – codice di recupero: .....". Tienilo con i documenti importanti, non nel portafoglio e non in una foto sul telefono. Puoi darne una copia in busta chiusa a una persona di fiducia.

COMPUTER L'estensione nel browser

1. Da **bitwarden.com/download** installa l'estensione per il tuo browser: per Brave si prende dal Chrome Web Store, per Firefox dal sito dei componenti aggiuntivi.
2. Fissala nella barra (l'icona dello scudo blu) e accedi: come regione scegli **bitwarden.eu**.
3. Nelle impostazioni dell'estensione attiva lo **sblocco con PIN** o con impronta: così non devi scrivere ogni volta la password principale.

TELEFONO L'app e il riempimento automatico

1. Installa **Bitwarden Password Manager** (di Bitwarden Inc.) dal Play Store o dall'App Store e accedi, regione **bitwarden.eu**.
2. Attiva lo sblocco con impronta o volto.
3. **Android:** **Impostazioni del telefono → Password e account → Servizio preferito** (o **Servizio di compilazione automatica**) e scegli Bitwarden al posto di Google.
   iPhone: **Impostazioni → Generali → Riempimento automatico e password**, attiva Bitwarden.

IV Traslocare le password

Esportare da Google, importare in Bitwarden, cancellare le tracce.

GOOGLE Esportare le password

1. Dal computer, in Chrome, scrivi nella barra degli indirizzi `chrome://password-manager/settings`. Senza Chrome: vai su **passwords.google.com** e apri le impostazioni (la rotella).
2. Alla voce **Esporta password** scegli **Scarica file**. Il computer o Google ti chiedono la password per conferma.
3. Salva il file sulla Scrivania: si chiama più o meno `Chrome Passwords.csv`.

Se avevi password salvate anche in Brave (`brave://password-manager/settings`) o in Firefox (`about:logins`, poi i tre puntini e **Esporta credenziali**), esportale allo stesso modo.



Il file in chiaro: pochi minuti e poi via

Per spostare le password si passa da un file **.csv**: un semplice elenco con sito, nome utente e password **in chiaro**, leggibile da chiunque apra il file. Fai il trasloco sul tuo computer, in un momento tranquillo, tutto di seguito: esporta, importa, e **cancella subito il file**, svuotando anche il Cestino.

BITWARDEN Importare

1. Apri la cassaforte dal sito **vault.bitwarden.eu**.
2. Vai in **Strumenti → Importa dati**.
3. In **Formato file** scegli **Chrome (csv)**; per il file di Firefox, **Firefox (csv)**.
4. Seleziona il file con **Scegli file** e premi **Importa dati**.
5. Controlla che il numero di elementi importati corrisponda, e apri qualche voce a caso per verificare.

Non importare due volte lo stesso file: Bitwarden non controlla i doppioni.

> **SUBITO DOPO: CANCELLA IL FILE**
>
> Elimina il file .csv (e le eventuali copie nella cartella Download) e **svuota il Cestino**. Se l'avevi messo su una chiavetta o in una cartella sincronizzata nel cloud, cancellalo anche da lì.

GOOGLE Cancellare le password da Google

Solo dopo aver controllato che in Bitwarden c'è tutto:

1. Torna in `chrome://password-manager/settings` (o su passwords.google.com, impostazioni).
2. In fondo alla pagina scegli **Elimina i dati di Gestore delle password di Google** e conferma.
3. Fai lo stesso con le password salvate in Brave o Firefox.

BROWSER Smettere di salvarle nel browser

DOVE	CHE COSA SPEGNERE
Brave	**Impostazioni → Compilazione automatica e password → Gestore delle password**: disattiva **Offri di salvare le password** e **Accesso automatico**
Firefox	**Impostazioni → Privacy e sicurezza**: togli la spunta da **Chiedi se salvare le credenziali**
Android	Bitwarden come servizio di compilazione automatica, al posto di Google (parte III)

DOPO Rinforzare, un po' alla volta

Ora puoi sostituire le password deboli o ripetute, un po' alla volta, cominciando dagli account che contano di più.

1. **La posta elettronica**, perché da lì si recuperano tutte le altre password.
2. **Banca, SPID, servizi pubblici e sanitari.**
3. **I social e i negozi** dove hai salvato una carta di pagamento.

Per ognuno: “cambia password”, fai generare a Bitwarden quella nuova e salva. Dove si può, attiva la verifica in due passaggi.

> **LE PASSKEY**
> Sempre più siti offrono le **passkey**, chiavi d'accesso che sostituiscono la password e non si possono rubare con un finto sito. Bitwarden le salva e le sincronizza su tutti i tuoi dispositivi: quando un sito propone di crearne una, scegli di salvarla in Bitwarden e non nell'account Google.

Le domande più comuni

«E se dimentico la password principale?»

Non si può recuperare. Per questo c'è il foglio, e per questo conviene usare Bitwarden ogni giorno: la password principale si ricorda scrivendola.

«Posso condividere le password con la famiglia?»

Sì: il piano gratuito permette di creare un'organizzazione per condividere password tra due persone (per esempio il conto di casa con il partner). Per tutta la famiglia c'è il piano Families, a pagamento.

«Una voce di menu ha un nome diverso»

Bitwarden, Google e i browser aggiornano spesso i menu. Se non trovi una voce esattamente come è scritta qui, cerca quella più simile.

Lista di controllo

- [ ] Account creato su bitwarden.eu
- [ ] Password principale scelta e scritta sul foglio
- [ ] Verifica in due passaggi attiva, codice di recupero sul foglio
- [ ] Estensione installata in Brave o Firefox
- [ ] App sul telefono, riempimento automatico attivo
- [ ] Password esportate da Google (e dai browser)
- [ ] Password importate e controllate in Bitwarden
- [ ] File .csv cancellato, Cestino svuotato
- [ ] Password eliminate da Google e dai browser
- [ ] Browser non salvano più le password
- [ ] Password della posta cambiata con il generatore
- [ ] Banca, SPID e servizi importanti rinforzati

§

Fonti

Le referenze principali dei fatti citati in questa guida, verificate il 27 novembre 2026.

GOOGLE

Google, Centro assistenza del Gestore delle password: crittografia sul dispositivo ed esportazione delle password.

Have I Been Pwned (haveibeenpwned.com), servizio di verifica delle violazioni.

BITWARDEN

Bitwarden, pagine su sicurezza, audit indipendenti e conformità; centro assistenza su regioni dei server (USA/UE), esportazione e importazione.

Bitwarden, comunicato sull'investimento guidato da PSG, settembre 2022.

Bitwarden, «Bitwarden launches enhanced Premium plan», gennaio 2026 (19,80 $ l'anno); Fast Company, 2026.

It's FOSS, 19 maggio 2026, e Linuxiac sul cambio di amministratore delegato e sulla scritta «Always free».

ALTERNATIVE

KeePassXC (keepassxc.org) e Proton Pass (proton.me/pass): documentazione ufficiale.

ALTRE GUIDE DI QUESTA SERIE

Perché lasciare le Big Tech · Da Gmail a Infomaniak · Da Chrome a Brave · Da Chrome a Firefox · Da WhatsApp a Signal · Dai social di Meta e X a Mastodon e Bluesky · Da Facebook, Instagram e WhatsApp a un diario ricordo · La musica dopo Spotify · Film e serie, con criterio · E se passassi tutto ad Apple? · L'intelligenza artificiale, con coscienza