Verifica in due passaggi

Perché quel messaggino col codice ti salva la vita

Guida Completa · Aprile 2026

⚠ Disclaimer

NOTA LEGALE — Limitazione di Responsabilità

Il presente articolo ha esclusivamente scopo informativo e divulgativo. Le informazioni contenute non costituiscono consulenza legale, tecnica o professionale di alcun tipo.

L'autore e il publisher declinano ogni responsabilità per eventuali danni diretti, indiretti o consequenziali derivanti dall'applicazione delle indicazioni riportate.

Il panorama della sicurezza informatica è in continua evoluzione: le procedure descritte potrebbero variare nel tempo o differire a seconda della piattaforma utilizzata.
Si raccomanda sempre di consultare la documentazione ufficiale del servizio di proprio interesse e, per questioni critiche, di rivolgersi a un professionista qualificato.

Tutti i marchi, i loghi e i nomi di prodotti citati appartengono ai rispettivi proprietari.

Sommario

1. Introduzione — Il ladro invisibile

Immagina di tornare a casa dopo una giornata di lavoro, aprire il tuo laptop e scoprire che qualcuno ha svuotato il tuo conto corrente online. Non hai perso il portafoglio. Non ti hanno rubato la borsa. Eppure i tuoi soldi sono spariti.

Oppure immagina di provare ad accedere alla tua email e scoprire che la password non funziona più. Qualcuno ha preso il controllo del tuo account, ha letto tutte le tue email, ha scritto ai tuoi amici fingendo di essere te, magari chiedendo denaro.

Questi scenari non appartengono ai film di fantascienza. Accadono ogni giorno, a milioni di persone in tutto il mondo. E nella maggior parte dei casi, la porta d'ingresso usata dal ladro è una sola: la password.

99,9%	degli attacchi automatici agli account vengono bloccati dall'attivazione della verifica in due passaggi (fonte: Microsoft, 2024).

La buona notizia è che esiste uno strumento semplicissimo — già disponibile su quasi tutti i servizi online — capace di rendere il tuo account praticamente inviolabile: si chiama verifica in due passaggi, o autenticazione a due fattori.

In questo articolo scoprirai cos'è, come funziona, perché è così importante e, soprattutto, come attivarla anche se non sei esperto di tecnologia. Ti basteranno pochi minuti per mettere al sicuro le cose più preziose che hai online.

2. Cos'è la verifica in due passaggi

Prima di tutto, un po' di chiarezza sui nomi. Questo sistema di sicurezza viene chiamato in modi diversi:

- Verifica in due passaggi (il termine più usato in italiano)
- Autenticazione a due fattori (2FA — dall'inglese Two-Factor Authentication)
- Autenticazione a più fattori (MFA — Multi-Factor Authentication)
- Doppio fattore di autenticazione

Tutti questi nomi descrivono la stessa idea: per accedere al tuo account, non basta inserire la password. Devi dimostrare la tua identità in due modi diversi.

Glossario rapido — Cos'è un "fattore"?	
In sicurezza informatica, un "fattore" è una categoria di prova della tua identità:	
Qualcosa che SAI	→ La tua password, un PIN, una risposta segreta
Qualcosa che HAI	→ Il tuo telefono, una chiavetta USB sicura

Qualcosa che SEI	→ La tua impronta digitale, il riconoscimento facciale
La verifica in due passaggi combina almeno due di questi fattori.	

Un esempio della vita reale: quando vai allo sportello bancomat, esegui automaticamente una verifica in due passaggi. Hai la carta (qualcosa che hai) e inserisci il PIN (qualcosa che sai). Se perdi la carta, chi la trova non può prelevare senza il PIN. Se qualcuno scopre il PIN, non può fare nulla senza la carta fisica. È esattamente lo stesso principio applicato al mondo digitale.

3. Come funziona — Spiegazione semplice

Vediamo passo dopo passo cosa succede quando provi ad accedere a un account protetto dalla verifica in due passaggi.

Il processo in 4 mosse

1. Inserisci il tuo nome utente e la tua password come al solito. Il sistema li controlla e li trova corretti.
2. A questo punto, invece di farti entrare subito, il sistema ti chiede un secondo elemento di verifica.
3. Ricevi un codice numeroso sul tuo telefono (via SMS, tramite un'app o in altro modo).
4. Inserisci quel codice nella pagina web o nell'app. Solo ora potrai accedere al tuo account.

Perché il codice cambia ogni volta?
I codici inviati via SMS o generati da un'app sono temporanei: scadono di solito
entro 30-60 secondi (per le app) oppure dopo pochi minuti (per gli SMS).
Questo è fondamentale per la sicurezza: anche se un malintenzionato intercettasse
il codice, non potrebbe usarlo poco dopo perché sarebbe già scaduto.

Il grande vantaggio di questo sistema è che un criminale informatico, anche se riesce a scoprire la tua password (per esempio perché è stata rubata in una violazione di dati di un altro sito), non può comunque entrare nel tuo account. Gli manca il secondo elemento: il tuo telefono.

Un esempio pratico: accedere a Gmail

Marco usa Gmail con la verifica in due passaggi attivata. Un giorno, un hacker in un altro continente ottiene la sua password da una lista di credenziali rubate. Prova ad accedere al

suo account. Inserisce l'email e la password: corrette. Ma il sistema gli chiede un codice di verifica. Il codice arriva sul telefono di Marco, in Italia. L'hacker, dall'altra parte del mondo, non ha il telefono di Marco e non può andare avanti. Account salvato.

4. I diversi metodi di 2FA

Non tutti i sistemi di verifica in due passaggi sono uguali. Esistono vari metodi, ognuno con i suoi vantaggi e svantaggi. Vediamoli dal più comune al più sicuro.

4.1 SMS — Il messaggino con il codice

È il metodo più diffuso e quello con cui la maggior parte delle persone ha il primo contatto con il 2FA. Funziona così: dopo aver inserito la password, ricevi un SMS con un codice numerico (di solito 6 cifre). Lo inserisci e accedi.

☑ Vantaggi e ✕ Svantaggi degli SMS
☑ Facilissimo da usare, non richiede app aggiuntive
☑ Funziona su qualsiasi telefono, anche i più vecchi
☑ Universalmente supportato dai servizi online
✕ Può essere intercettato da attacchi tecnici avanzati (SIM swapping)
✕ Non funziona senza campo telefonico
✕ Ritardi nell'arrivo dell'SMS in alcune zone

Nonostante i limiti tecnici, gli SMS rimangono nettamente superiori all'avere solo una password. Per l'utente medio, attivare il 2FA via SMS è già un grandissimo passo avanti nella sicurezza.

4.2 App di autenticazione — Il generatore di codici

Le app di autenticazione (come Google Authenticator, Microsoft Authenticator o Authy) generano codici temporanei direttamente sul tuo smartphone, senza bisogno di connessione internet o campo telefonico. Ogni 30 secondi viene generato un nuovo codice a 6 cifre.

Come funziona in pratica? La prima volta che configuri il 2FA, inquadri un codice QR con l'app. Da quel momento, l'app e il server condividono un "segreto" e possono generare indipendentemente gli stessi codici nello stesso momento.

Le app di autenticazione più popolari
• Google Authenticator — Semplice, gratuita, disponibile per iOS e Android
• Microsoft Authenticator — Ottima per chi usa servizi Microsoft
• Authy — Ha il backup su cloud: utile se si perde il telefono
• 1Password, Bitwarden — App password manager con 2FA integrato

4.3 Chiave di sicurezza fisica (Token hardware)

È un piccolo dispositivo USB o NFC (simile a una chiavetta USB) che si collega al computer o si avvicina al telefono per autenticarsi. Il livello di sicurezza è il più alto possibile perché il fattore fisico è completamente separato dal telefono.

Chi lo usa? Principalmente aziende, professionisti con dati sensibili e utenti avanzati. I modelli più famosi sono YubiKey e Google Titan Key. Per l'utente comune non è indispensabile, ma è bene sapere che esiste.

4.4 Notifica push — Il tocco sull'app

Invece di un codice, ricevi una notifica push sul telefono con un semplice pulsante "Approva" o "Rifiuta". È il sistema usato, ad esempio, da Microsoft Authenticator per accedere agli account aziendali Microsoft 365.

Vantaggio: è velocissimo e intuitivo. Svantaggio: se qualcuno ti inonda di notifiche di accesso sperando che tu ne approvi una per errore (attacco MFA fatigue), potresti essere ingannato.

4.5 Biometria

Su molti smartphone moderni, il secondo fattore può essere la tua impronta digitale o il riconoscimento del viso. È comodo e sicuro, ma dipende dalle capacità del tuo dispositivo.

Metodo	Livello di sicurezza e note
Solo password	★ Minimo — vulnerabile a furto e indovinazione
Password + SMS	★★★ Buono — già molto efficace per uso quotidiano
Password + App auth.	★★★★ Molto buono — resistente agli attacchi via SMS
Password + Chiave fisica	★★★★★ Eccellente — lo standard per la massima sicurezza
Password + Biometria	★★★★ Molto buono — comodo e sicuro

5. Perché la password da sola non basta

Molte persone pensano: «Ho una password complicata, sono al sicuro». Purtroppo non è così. Le password, per quanto complesse, sono vulnerabili in modi che non possiamo controllare direttamente.

5.1 Le violazioni dei dati (Data Breach)

Ogni anno, centinaia di aziende e servizi online vengono hackerati. Gli hacker rubano milioni di combinazioni email-password e le vendono o le pubblicano sul dark web. Se hai usato quella password su altri siti — cosa che quasi tutti facciamo — il tuo account su quei siti è in pericolo.

24 mld	di combinazioni email-password rubate erano disponibili sul dark web già nel 2022 (fonte: Digital Shadows). Il numero è cresciuto ogni anno.

5.2 Il phishing — La truffa della pagina falsa

Ricevi un'email che sembra provenire dalla tua banca, da Amazon o da Netflix. Ti dice che c'è un problema con il tuo account e ti chiede di cliccare su un link per risolvere. Il link porta a una pagina identica a quella vera, ma è falsa. Inserisci la tua email e la password: un criminale le ha appena rubate.

Il phishing è la tecnica di furto di credenziali più usata al mondo. Anche gli utenti più attenti possono cascarci, perché le pagine false sono sempre più convincenti.

Come riconoscere il phishing — Segnali d'allarme

- L'email crea urgenza: «Il tuo account sarà chiuso entro 24 ore!»
- L'indirizzo email del mittente è strano (es. noreply@amaz0n-secure.com)
- Il link non porta al sito ufficiale (controlla sempre l'URL nella barra del browser)
- Ti chiedono la password via email (nessun servizio legittimo lo fa mai)
- Errori grammaticali o di ortografia nel testo

5.3 Il riutilizzo delle password

Uno studio di Google del 2023 ha rivelato che il 65% degli utenti utilizza la stessa password per più account. Questo significa che rubare le credenziali di un sito poco sicuro (per esempio, un forum di hobby) può aprire le porte a siti ben più importanti come l'email principale o il conto bancario.

5.4 Gli attacchi a forza bruta

I programmi automatici provano milioni di combinazioni al secondo. Le password corte o comuni (come "123456", "password" o il proprio nome) vengono violate in pochi secondi. Anche password più lunghe possono essere violate se un hacker dispone di abbastanza tempo e potenza di calcolo.

< 1 sec	Il tempo necessario a un moderno programma di hacking per violare la password "password123" (fonte: Security.org, 2024).

Ecco perché, anche se hai una password forte, la verifica in due passaggi aggiunge uno scudo fondamentale: anche se la password viene scoperta, il malintenzionato non può andare avanti senza il secondo fattore.

6. Come attivare il 2FA passo dopo passo

Vediamo concretamente come attivare la verifica in due passaggi sui servizi più usati. La procedura è diversa da sito a sito, ma il concetto è sempre lo stesso: cerca "Sicurezza" o "Privacy" nelle impostazioni del tuo account.

6.1 Google / Gmail

5. Vai su myaccount.google.com dal tuo browser.
6. Clicca su "Sicurezza" nel menu a sinistra.
7. Scorri fino a trovare "Verifica in due passaggi" e clicca.
8. Clicca su "Inizia" e segui la procedura guidata.
9. Scegli come ricevere il secondo fattore: SMS, app Authenticator o altro.
10. Google ti chiederà di verificare che tutto funzioni prima di attivare.

6.2 Apple ID (iPhone, iPad, Mac)

11. Su iPhone/iPad: vai in Impostazioni → [tuo nome] → Password e sicurezza.
12. Tocca "Attiva autenticazione a due fattori".
13. Inserisci un numero di telefono affidabile.
14. Riceverai i codici di verifica via SMS o chiamata su quel numero.
15. Su Mac: vai in Preferenze di Sistema → ID Apple → Password e sicurezza.

6.3 Facebook / Instagram / WhatsApp

Su Facebook: Impostazioni → Sicurezza e accesso → Autenticazione a due fattori.

Su Instagram: Profilo → Menu (≡) → Impostazioni → Sicurezza → Autenticazione a due fattori.

Su WhatsApp: Impostazioni → Account → Verifica in due passaggi → Attiva. (Nota: WhatsApp usa un PIN di 6 cifre, non un codice via SMS.)

6.4 Banche e servizi finanziari

Le banche italiane sono obbligate per legge (normativa PSD2) a utilizzare la Strong Customer Authentication — una forma di autenticazione a due fattori — per qualsiasi operazione online. Molto probabilmente il tuo conto bancario usa già il 2FA. Controlla nell'app della tua banca nelle impostazioni di sicurezza per verificare che sia attivo.

La normativa PSD2 e il tuo conto
Dal 2019 è in vigore in Europa la direttiva PSD2 (Payment Services Directive 2),
che obbliga le banche a richiedere la Strong Customer Authentication (SCA)
per tutte le operazioni di pagamento online sopra una certa soglia.

In pratica: le banche DEVONO già proteggere i tuoi pagamenti con il 2FA.
Approva le operazioni solo attraverso i canali ufficiali della tua banca.

6.5 I codici di backup — Non dimenticarli mai!

Quando attivi il 2FA, la maggior parte dei servizi ti fornisce dei codici di backup (o codici di ripristino): una lista di codici numerici da usare nel caso in cui tu non abbia accesso al tuo secondo fattore (per esempio, se perdi il telefono).

⚠ IMPORTANTE — Salva i codici di backup
I codici di backup sono la tua ancora di salvezza se perdi il telefono.
☑ Stampali e tienili in un posto sicuro (non sul telefono!)
☑ Salvali in un gestore di password
☑ Tienine una copia in un posto diverso dalla tua abitazione
✗ Non salvarli solo sul telefono che usi per il 2FA
✗ Non condividerli con nessuno
✗ Non perderli: senza di essi, potresti perdere l'accesso all'account

7. I vantaggi concreti

I dati parlano chiaro: la verifica in due passaggi è una delle misure di sicurezza più efficaci in assoluto. Vediamo nel dettaglio cosa ottieni attivandola.

7.1 Protezione quasi totale contro le password rubate

Come abbiamo visto, le violazioni dei dati sono all'ordine del giorno. Milioni di password vengono rubate ogni anno. Con il 2FA attivo, anche se la tua password finisce in una lista di credenziali rubate, il tuo account rimane al sicuro. L'hacker ha la chiave, ma non può aprire la porta perché manca il secondo lucchetto.

7.2 Avviso immediato di tentativi di accesso non autorizzati

Ogni volta che qualcuno prova ad accedere al tuo account, ricevi un codice sul telefono. Se ricevi un codice senza aver fatto nulla, sai immediatamente che qualcuno sta cercando di entrare. Puoi così cambiare la password immediatamente, prima che riescano a fare danni.

7.3 Protezione contro il phishing

Anche se cadi nella trappola di una pagina di phishing e inserisci la tua password su un sito falso, il criminale non può accedere al tuo vero account perché gli manca il codice temporaneo che arriva sul tuo telefono.

7.4 Conformità legale e aziendale

In molti contesti professionali, il 2FA non è più facoltativo: è obbligatorio. Le normative sulla protezione dei dati (come il GDPR europeo) e le policy aziendali di sicurezza spesso richiedono l'autenticazione a più fattori per accedere a sistemi che contengono dati sensibili.

3x	Le aziende che adottano il 2FA riducono il rischio di violazioni degli account di oltre tre volte rispetto a quelle che usano solo password (fonte: Verizon Data Breach Report, 2024).

8. Possibili inconvenienti e come gestirli

Il 2FA non è perfetto. Esistono alcuni inconvenienti che è importante conoscere, insieme alle soluzioni per affrontarli.

8.1 «Ho perso il telefono — sono bloccato fuori!»

È la preoccupazione più comune. La risposta è: dipende da quanto sei preparato. Se hai salvato i codici di backup (come spiegato nel capitolo 6.5), puoi usarli per accedere all'account e poi configurare un nuovo secondo fattore. Se non li hai salvati, il recupero dell'account può essere lungo e complicato.

Soluzione preventiva: salva sempre i codici di backup e usa un'app di autenticazione (come Authy) che permette il backup su cloud. Puoi anche registrare un numero di telefono secondario come metodo di recupero.

8.2 «Il segnale telefonico non c'è — non ricevo l'SMS»

Gli SMS dipendono dalla rete telefonica. Se sei in zona senza copertura, in aereo o all'estero con il roaming disattivato, potresti non ricevere l'SMS. Soluzione: usa un'app di autenticazione, che funziona anche offline perché non ha bisogno di internet o di rete telefonica per generare i codici.

8.3 «Ci vuole troppo tempo per accedere»

In realtà, una volta abituati, il processo aggiunge solo 10-15 secondi all'accesso. Inoltre, la maggior parte dei servizi offre l'opzione «Non chiedere di nuovo su questo dispositivo per X giorni»: dopo aver verificato la tua identità, non ti verrà chiesto il secondo fattore ogni volta sullo stesso telefono o computer.

8.4 Il SIM Swapping — quando rubano il tuo numero

È un attacco avanzato in cui un criminale convince il gestore telefonico a trasferire il tuo numero su una nuova SIM in suo possesso. Da quel momento, riceve i tuoi SMS. Questo attacco colpisce principalmente persone con profili ad alto valore (come persone famose o

ricche). Per la maggior parte degli utenti, la protezione via SMS è comunque molto efficace. Chi vuole proteggersi ulteriormente può passare a un'app di autenticazione o a una chiave fisica.

Consigli pratici per il 2FA sicuro
1. Usa un'app di autenticazione invece degli SMS, se possibile
2. Salva SEMPRE i codici di backup in un posto sicuro
3. Non approvare notifiche push che non hai richiesto tu
4. Attiva il 2FA almeno su: email principale, conto bancario, social media
5. Se usi Authy, attiva la password di protezione del backup
6. Aggiorna periodicamente il numero di telefono associato ai tuoi account

9. Domande Frequenti (FAQ)

? Il 2FA è davvero necessario se ho già una password complicata?

Sì, assolutamente. Una password complicata protegge dagli attacchi a forza bruta, ma non da furti di credenziali tramite violazioni di database o phishing. Il 2FA aggiunge una protezione che non dipende dalla forza della password, ma da un elemento fisico (il tuo telefono) che solo tu possiedi.

? Il 2FA mi protegge anche se clicco su un link di phishing?

Parzialmente. Il 2FA ti protegge dal fatto che il criminale non possa usare la tua password rubata per accedere all'account. Non ti protegge, però, se sei su una pagina falsa che in tempo reale ti chiede anche il codice OTP e lo invia al sito vero (attacco man-in-the-middle in tempo reale). Per questo motivo è fondamentale anche controllare sempre l'URL del sito prima di inserire qualsiasi credenziale.

? Cosa succede se cambio numero di telefono?

Devi aggiornare il numero sui servizi che usano il 2FA via SMS PRIMA di dismettere il vecchio numero. Accedi alle impostazioni di sicurezza di ogni servizio e sostituisci il vecchio numero con quello nuovo. Se hai già dismesso il vecchio numero, usa i codici di backup per accedere e poi aggiorna il numero.

? Il 2FA funziona anche senza connessione internet?

Dipende dal metodo. Gli SMS richiedono la rete telefonica (ma non internet). Le app di autenticazione come Google Authenticator generano codici offline e non hanno bisogno né di internet né di rete telefonica. Le chiavi fisiche USB funzionano sempre offline. Le notifiche push richiedono internet.

? È sicuro usare la stessa app di autenticazione per tutti gli account?

Sì, è normale e pratico. Un'app come Google Authenticator o Authy può gestire decine di account diversi. Ogni account ha il proprio codice indipendente. L'importante è proteggere l'app stessa con un PIN o la biometria del telefono, e fare il backup dei codici nel caso in cui si perda il dispositivo.

? Il 2FA costa qualcosa?

No, è completamente gratuito per gli utenti. I servizi online lo offrono senza costi aggiuntivi. Le app di autenticazione più diffuse (Google Authenticator, Microsoft Authenticator, Authy) sono gratuite. L'unica eccezione sono le chiavi fisiche di sicurezza (come YubiKey), che costano tra i 25 e i 70 euro, ma non sono necessarie per l'utente comune.

? Devo attivarlo su tutti i siti?

Idealmente sì, ma se vuoi iniziare con un approccio graduale, dai la priorità ai conti più importanti: la tua email principale (perché attraverso di essa si può resettare quasi ogni altra password), i conti bancari, i social media principali, e qualsiasi servizio che contiene dati sensibili o metodi di pagamento.

? Cosa faccio se ricevo un codice 2FA che non ho richiesto?

Significa che qualcuno sta cercando di accedere al tuo account con la tua password. Non fare nulla con il codice ricevuto (non condividerlo). Cambia immediatamente la password di quell'account, anche da un dispositivo diverso per precauzione. Poi controlla se ci sono stati accessi non autorizzati nelle impostazioni dell'account.

10. Glossario dei termini tecnici

Raccolta dei termini tecnici usati in questo articolo, spiegati in modo semplice.

2FA	Two-Factor Authentication — verifica in due passaggi. Sistema che richiede due prove di identità distinte per accedere a un account.
MFA	Multi-Factor Authentication — autenticazione a più fattori. Come il 2FA, ma con la possibilità di usare più di due fattori.
OTP	One-Time Password — codice monouso. Un codice numerico valido per un solo utilizzo e per un tempo limitato (di solito 30-60 secondi).
Phishing	Truffa informatica che imita comunicazioni ufficiali (email, SMS, siti web) per ingannare l'utente e rubargli credenziali o dati.
SIM Swapping	Attacco in cui un criminale convince il gestore telefonico a trasferire il numero di telefono della vittima su una SIM in suo possesso.
Dark Web	Parte di internet non indicizzata dai motori di ricerca, accessibile solo con software specifici. Spesso usata per commercio illegale di dati rubati.
Data Breach	Violazione dei dati. Incidente di sicurezza in cui dati riservati (come password) vengono sottratti illegalmente da un sistema informatico.
Codici di backup	Codici di recupero forniti al momento dell'attivazione del 2FA. Da usare in emergenza se non si ha accesso al secondo fattore normale.
TOTP	Time-Based One-Time Password — codice monouso basato sul tempo. Il tipo di codice generato dalle app di autenticazione, che cambia ogni 30 secondi.
Password Manager	Gestore di password. Applicazione che memorizza in modo sicuro tutte le password, permettendo di usarne una diversa e complessa per ogni sito.
GDPR	General Data Protection Regulation — Regolamento Generale sulla Protezione dei Dati. Legge europea sulla privacy dei dati personali.
PSD2	Payment Services Directive 2. Normativa europea che obbliga le banche a usare l'autenticazione forte (2FA) per le operazioni di pagamento online.

Token hardware	Dispositivo fisico (simile a una chiavetta USB) usato come secondo fattore di autenticazione. Offre il massimo livello di sicurezza.

Autenticazione biometrica	Verifica dell'identità tramite caratteristiche fisiche uniche come impronta digitale, riconoscimento facciale o vocale.

Man-in-the-middle	Tipo di attacco informatico in cui un criminale si interpone tra l'utente e il sito web, intercettando in tempo reale le comunicazioni.

11. Conclusioni

Siamo arrivati alla fine di questo percorso nella verifica in due passaggi. Facciamo un riepilogo di ciò che abbiamo imparato.

Il messaggio più importante

Quel messaggino con il codice che a volte ti sembra una seccatura non è un capriccio tecnologico. È un guardiano. È il motivo per cui il criminale che ha trovato la tua password — in una delle tante violazioni di dati che accadono ogni giorno — non riesce comunque ad entrare nel tuo account. È una porta in più, un lucchetto aggiuntivo, uno scudo invisibile.

Cosa fare subito

Se dopo aver letto questo articolo vuoi fare qualcosa di concreto, ecco la tua lista d'azione:

- Attiva il 2FA sulla tua email principale OGGI. È il passo più importante.
- Poi attiva il 2FA sulla tua banca (se non è già obbligatorio).
- Poi i social media principali: Facebook, Instagram, LinkedIn.
- Scarica un'app di autenticazione (Authy è la scelta più comoda per principianti).
- Salva i codici di backup in un posto sicuro — stampa e metti in un cassetto.
- Se vuoi fare il salto di qualità, considera un gestore di password.

🎯 Il tuo piano d'azione in 3 livelli
LIVELLO BASE (15 minuti):
→ Attiva il 2FA via SMS su email e banca
LIVELLO INTERMEDIO (30 minuti):
→ Scarica un'app di autenticazione e usala al posto degli SMS
→ Attiva il 2FA su tutti i social media
→ Salva i codici di backup
LIVELLO AVANZATO (1-2 ore):
→ Installa un gestore di password
→ Considera una chiave fisica YubiKey per gli account più critici
→ Verifica su haveibeenpwned.com se la tua email è stata coinvolta in violazioni

La sicurezza digitale non è solo una questione per esperti informatici. È una responsabilità di ognuno di noi, così come chiudere la porta di casa a chiave. La verifica in due passaggi è la serratura aggiuntiva più efficace e più facile da installare che esista nel mondo digitale.

Non aspettare che ti capiti qualcosa di brutto. Agisci oggi, dedica quindici minuti alla tua sicurezza online, e domani potrai dormire sonni molto più tranquilli.

Articolo redatto nell'aprile 2026. Le informazioni sono soggette ad aggiornamento man mano che le tecnologie e le normative evolvono.