CAMBIARE IL PIN

Come metterne uno che ricordi facilmente **(ma sicuro)**

Guida pratica per chi parte da zero

Aprile 2026 • Circa 4.000 parole • Tempo di lettura: 18-22 minuti

Sommario

Introduzione – Il PIN nella nostra vita quotidiana

Pensa all'ultima volta che hai prelevato dei soldi al bancomat, hai sbloccato il tuo smartphone, oppure hai effettuato un pagamento con il telefono al supermercato. Cosa avevano in comune tutte queste azioni? In ognuna di esse hai usato un PIN.

Il PIN – acronimo di *Personal Identification Number*, cioè *Numero di Identificazione Personale* – è quella piccola sequenza di cifre (di solito da 4 a 6 numeri) che agisce come una chiave digitale. Come la chiave di casa tua, il PIN apre una porta: quella che ti dà accesso al tuo conto bancario, ai tuoi messaggi, alle tue fotografie, alla tua identità digitale.

Eppure, nonostante sia così importante, la maggior parte delle persone sceglie il proprio PIN in modo automatico, spesso usando date di nascita, sequenze banali come 1234, oppure lo stesso codice per tutto. È un po' come mettere la stessa serratura economica su tutte le porte di casa, della macchina e dell'ufficio.

Questa guida è stata scritta per te: che tu sia alle prime armi con la tecnologia o che voglia semplicemente capire come funziona davvero la sicurezza del PIN. Non troverai tecnicismi complicati, ma istruzioni chiare, esempi pratici e consigli che potrai applicare subito.

Alla fine di questa lettura saprai: come funziona un PIN, perché è importante sceglierlo con cura, come cambiarlo sui dispositivi più comuni e, soprattutto, come crearne uno che ricordi con facilità senza compromettere la tua sicurezza.

Cosa imparerai in questa guida

- Cos'è esattamente un PIN e dove viene usato
- Perché i PIN più comuni sono pericolosi
- Come cambiare il PIN su bancomat, smartphone e SIM
- Tecniche per creare un PIN sicuro E facile da ricordare
- Cosa fare se dimentichi il PIN
- Come funziona l'autenticazione a due fattori

Parte 1 – Che cos'è un PIN e come funziona

1.1 Origini e definizione

Il PIN nasce nel 1966, inventato dall'ingegnere scozzese James Goodfellow in concomitanza con l'arrivo dei primi sportelli bancari automatici. L'idea era semplice ma geniale: invece di richiedere la presenza fisica di un impiegato per verificare l'identità del cliente, bastava un codice segreto che solo il titolare doveva conoscere.

Tecnicamente, il PIN è una stringa di cifre numeriche (anche se alcune varianti moderne includono lettere) che viene confrontata con un valore memorizzato in modo cifrato nel sistema. Il concetto fondamentale è: **il sistema non conosce il tuo PIN in chiaro**, ma è in grado di verificare se quello che hai inserito corrisponde a quello registrato.

> 🕮 **Glossario – PIN**
> PIN (Personal Identification Number): Sequenza numerica (di solito 4-6 cifre) usata per identificarsi e accedere a un servizio o dispositivo. È personale e segreto.

1.2 Dove viene usato il PIN?

Il PIN è ovunque. Ecco i contesti principali in cui lo utilizziamo ogni giorno:

I principali utilizzi del PIN

Dispositivo / Servizio	Utilizzo tipico
Carta bancomat/credito	Prelievi ATM, pagamenti POS
Smartphone	Sblocco schermo, app di pagamento
SIM telefonica	Protezione della scheda SIM
App bancarie	Accesso rapido all'app della banca
Computer aziendale	Accesso Windows Hello, account aziendali
Decoder / Smart TV	Blocco canali, acquisti on demand
Sistemi d'allarme casa	Inserimento/disinserimento allarme
Servizi online	Verifica identità, pagamenti digitali

1.3 Come il PIN protegge i tuoi dati

Quando inserisci il PIN, il dispositivo o il sistema esegue una serie di verifiche. Questo processo avviene in frazioni di secondo e prevede diversi livelli di protezione:

- Il PIN viene confrontato con una versione cifrata memorizzata nel chip della carta o nel sistema.
- Dopo un numero limitato di tentativi sbagliati (di solito 3), il dispositivo o la carta si blocca automaticamente.
- Il PIN non viaggia mai in chiaro sulla rete: viene sempre protetto da algoritmi crittografici.
- In molti sistemi moderni, il PIN è abbinato a qualcosa che possiedi (la carta o il telefono), creando un doppio livello di sicurezza.

Come funziona il blocco dopo 3 tentativi

Questo meccanismo si chiama 'blocco per tentativi errati' ed è una protezione fondamentale.
Serve a scoraggiare chi tenta di indovinare il tuo PIN per tentativi.
Sul bancomat: la carta viene inghiottita o bloccata.
Sullo smartphone: dopo alcuni tentativi richiede password lunga, poi può cancellare i dati.
Sulla SIM: si blocca e richiede il PUK (vedi Glossario).

Parte 2 – I PIN più usati (e perché sono pericolosi)

2.1 La classifica dei PIN più comuni

Ogni anno, ricercatori di sicurezza analizzano milioni di PIN rubati o esposti in violazioni di dati. I risultati sono sempre gli stessi e abbastanza preoccupanti. Ecco una classifica dei codici più usati al mondo:

I 10 PIN più comuni al mondo (fonte: ricerche di sicurezza 2023-2025)

Pos.	PIN	Problema
1°	1234	⚠ Facilissimo da indovinare
2°	0000	⚠ Quattro zeri uguale a nessuna protezione
3°	1111	⚠ Quattro uni: usato da milioni di persone
4°	1212	⚠ Schema ripetuto prevedibile
5°	7777	⚠ Cifra fortunata, ma nota
6°	1004	⚠ Comune in alcune nazioni asiatiche
7°	2000	⚠ Anno tondo, facile da pensare

8°	4444	⚠ Quattro cifre uguali
9°	2222	⚠ Stesso problema
10°	6969	⚠ Molto comune, facile da ricordare

Questi 10 PIN coprono, da soli, circa il **26% di tutti i codici a 4 cifre usati**. Significa che se qualcuno prova solo questi 10 codici, ha quasi 1 possibilità su 4 di indovinare il tuo PIN. Spaventoso, vero?

Attenzione alle date di nascita!

Il tuo PIN è 0585? Significa '05/85', cioè maggio 1985?
Oppure 2310 per il 23 ottobre?
I ladri e gli hacker sanno che le persone usano date. È la prima cosa che provano.
Qualcuno che ti conosce (o che ha trovato il tuo documento) può indovinare facilmente.
Lo stesso vale per: anno di nascita dei figli, anniversari, compleanni del partner.

2.2 Quanto tempo ci vuole a indovinare un PIN?

Capire 'quanto è facile' indovinare un PIN ci aiuta a capire quanto è importante sceglierlo bene.

Tempo necessario per indovinare un PIN (attacco a forza bruta)

Tipo PIN	Combinazioni	Con computer	Manualmente
4 cifre	10.000	Pochi secondi (computer)	Minuti (umano con fortuna)
5 cifre	100.000	Qualche secondo	Ore (molto improbabile)
6 cifre	1.000.000	Qualche minuto	Praticamente impossibile
6 cifre + lettere	Miliardi	Ore/giorni	Impossibile

La buona notizia: grazie al blocco dopo 3 tentativi, gli attacchi automatici sono molto più difficili sui dispositivi reali. Ma questo non significa che possiamo rilassarci: i PIN semplici rimangono pericolosi, specialmente se qualcuno ti osserva mentre lo digiti (attacco chiamato 'shoulder surfing', cioè 'sbirciare dalla spalla').

Parte 3 – Come cambiare il PIN: guida pratica

Vediamo ora, passo dopo passo, come cambiare il PIN nei quattro scenari più comuni. Segui le istruzioni nell'ordine e, se incontri qualcosa di diverso sullo schermo, non preoccuparti: i menu possono variare leggermente da modello a modello.

3.1 Cambiare il PIN del bancomat (carta di debito o credito)

Prima di iniziare

Avrai bisogno di: la tua carta bancaria + il PIN attuale.

Se non ricordi il PIN attuale, dovrai contattare la banca (non è possibile cambiarlo senza conoscerlo).

Tieni la carta in un posto sicuro mentre segui i passaggi.

Ecco come fare:

1. Vai a uno sportello ATM (bancomat) della tua banca o di qualsiasi banca convenzionata.
2. Inserisci la carta nello sportello. Lo slot è solitamente nella parte frontale centrale della macchina.
3. Inserisci il tuo PIN attuale quando richiesto.
4. Dal menu principale, cerca la voce 'Servizi', 'Altre operazioni' o 'Gestione carta'. I termini variano.
5. Seleziona 'Cambio PIN' o 'Modifica PIN'.
6. Inserisci il nuovo PIN che hai scelto (vedremo come sceglierlo nella Parte 4).
7. Conferma il nuovo PIN inserendolo una seconda volta.
8. Attendi il messaggio di conferma. La macchina ti dirà se l'operazione è andata a buon fine.
9. Ritira la carta e ricorda il nuovo PIN prima di allontanarti.

Puoi farlo anche online o in filiale

Molte banche permettono di cambiare il PIN tramite l'app bancaria o il sito internet della banca.

In alternativa, puoi recarti in filiale con un documento d'identità e chiedere al personale.

Se hai una carta prepagata (es. Postepay), controlla l'app dedicata: spesso c'è l'opzione diretta.

3.2 Cambiare il PIN sugli smartphone Android

Le istruzioni seguenti sono valide per la maggior parte degli smartphone Android (Samsung, Xiaomi, Huawei, Motorola, ecc.). I nomi dei menu potrebbero variare leggermente.

10. Apri 'Impostazioni' (l'icona a forma di ingranaggio ⚙).
11. Scorri verso il basso e cerca 'Sicurezza' oppure 'Sicurezza e privacy' oppure 'Blocco schermo'.
12. Tocca 'Blocco schermo' o 'Tipo di blocco schermo'.
13. Il telefono ti chiederà di inserire il PIN attuale. Fallo.
14. Seleziona 'PIN' dall'elenco delle opzioni (le altre sono: nessuno, scorrimento, sequenza, password, impronta, volto).
15. Inserisci il nuovo PIN (di solito minimo 4 cifre, consigliati 6).
16. Inserisci il PIN una seconda volta per confermarlo.
17. Tocca 'OK' o 'Conferma'.

Consiglio per Samsung Galaxy

Su alcuni modelli Samsung, vai in: Impostazioni → Schermata di blocco → Tipo di blocco schermo → PIN.

Per cambiare il PIN delle app (come Samsung Pay), vai in: Impostazioni → Dati biometrici e sicurezza → Samsung Pay.

3.3 Cambiare il PIN sugli iPhone (iOS)

Apple chiama il PIN 'Codice'. Ecco come cambiarlo:

18. Apri 'Impostazioni' (l'icona a forma di ingranaggio grigio ⚙).
19. Tocca il tuo nome in alto (profilo Apple ID), oppure scorri direttamente a 'Face ID e codice' o 'Touch ID e codice'.
20. Inserisci il codice attuale.
21. Scorri verso il basso fino a 'Cambia codice'.
22. Inserisci ancora una volta il codice attuale per sicurezza.
23. Inserisci il nuovo codice.
24. Conferma il nuovo codice inserendolo di nuovo.

Opzioni di codice su iPhone

iPhone offre diversi tipi di codice: numerico a 6 cifre (predefinito), numerico a 4 cifre, alfanumerico (mix di lettere e numeri).

Per cambiare il tipo: al passaggio 6, tocca 'Opzioni codice' e scegli quello che preferisci.

Consigliamo il codice a 6 cifre numerico: è più sicuro di 4 cifre ma più facile da inserire rispetto a una password lunga.

3.4 Cambiare il PIN della SIM telefonica

Il PIN della SIM è diverso dal PIN del telefono: serve a proteggere la scheda SIM stessa. Se qualcuno toglie la SIM e la mette in un altro telefono senza conoscere il PIN SIM, non può usarla.

Su Android:

25. Impostazioni → Sicurezza → Blocco SIM → Cambia PIN SIM.

Su iPhone:

26. Impostazioni → Dati cellulare → PIN SIM → Modifica PIN.

Attenzione al PIN SIM!

Il PIN SIM predefinito del tuo operatore è spesso 0000 o 1234. Cambialo subito!

Se inserisci il PIN SIM sbagliato 3 volte, la SIM si blocca.

Per sbloccarla serve il PUK (codice di sblocco). Lo trovi nel documento che accompagnava la SIM o chiamando il tuo operatore.

Se inserisci il PUK sbagliato 10 volte, la SIM viene DISTRUTTA definitivamente. Fai molta attenzione.

Parte 4 – Come scegliere un PIN sicuro e memorabile

Questa è la parte più importante della guida. Scegliere un PIN sicuro NON significa necessariamente scegliere uno impossibile da ricordare. Con le giuste tecniche, puoi avere entrambe le cose.

4.1 Le regole d'oro

Le 7 Regole d'Oro per un PIN Sicuro

1. NON usare sequenze ovvie: 1234, 0000, 1111, 9876.
2. NON usare la tua data di nascita, né quella di familiari.
3. NON usare lo stesso PIN per tutto (bancomat, telefono, SIM).
4. NON scrivere il PIN su foglietti o tenerlo nel portafoglio.
5. USA almeno 6 cifre quando possibile.
6. USA un PIN diverso per ogni servizio importante.
7. CAMBIA il PIN almeno una volta all'anno, o subito se sospetti che qualcuno lo conosca.

4.2 Tecniche mnemoniche per ricordare il PIN

Una tecnica mnemonica è un trucco mentale che ci aiuta a memorizzare qualcosa collegandolo a qualcosa che già conosciamo bene. Ecco le più efficaci per i PIN:

Tecnica 1 – La Frase Segreta

Pensa a una frase che conosci bene e usa le iniziali o le ultime cifre di ogni parola.

Esempio pratico – Tecnica della Frase

Frase: 'Ho 3 gatti e 5 pesci rossi nel mio giardino'

Usa il numero di lettere di alcune parole: HO(2) GATTI(6) PESCI(5) GIARDINO(8)

Risultato: PIN → 2658

Oppure: usa solo le parole che contengono numeri: '3 gatti' e '5 pesci' → PIN → 3 5 → aggiungi qualcosa → 3542

Il trucco: la frase la conosci solo tu, e il PIN non ha nulla a che vedere con la tua vita personale.

Tecnica 2 – Il Metodo delle Posizioni sulla Tastiera

Pensa a una forma geometrica sulla tastiera numerica e usa le cifre che attraversa.

Esempio pratico – Metodo delle Posizioni

Tastiera numerica standard: 1-2-3 / 4-5-6 / 7-8-9 / *-0-#
Disegna mentalmente una 'L' capovolta: 7-4-1-2-3 → PIN: 74123
Disegna una 'Z': 1-2-3-6-4-7-8-9 → troppo lungo, prendi solo le prime 4: 1236
Vantaggio: puoi ricordare la forma invece delle cifre. Prova a disegnarla nel palmo della mano.

Tecnica 3 – Il Numero Mascherato

Prendi un numero che conosci bene (es. la tua via, il tuo numero di scarpe, un anno importante) e trasformalo con una regola personale.

Esempio pratico – Numero Mascherato

Il tuo numero civico è 47 e sei nato nel 1978.
Prendi 47 e aggiungi 1978 → 4719 (prendo solo alcune cifre).
Oppure: numero civico invertito (74) + ultime due cifre dell'anno (78) → PIN: 7478.
La regola che usi per la trasformazione la conosci solo tu.

Tecnica 4 – Il PIN a Blocchi

Divide il PIN in 'blocchi' con significati separati che solo tu puoi collegare.

Esempio pratico – PIN a Blocchi

Blocco 1: quanti fratelli hai? Diciamo 2.
Blocco 2: quanti anni aveva il tuo cane preferito quando è morto? Diciamo 13.
Blocco 3: il tuo numero fortunato? Diciamo 7.
PIN: 21 + 37 = 2137 (o 213 + 7 = 2137)
Questo PIN non ha nessun senso per chiunque altro, ma per te è una storia.

4.3 PIN sicuri: esempi e controesempi

Confronto tra PIN deboli e PIN forti

PIN	Valutazione	Motivazione
1234	✗ Debolissimo	Il più usato al mondo, primo tentativo di qualsiasi hacker
0804	✗ Debole	Sembra una data (8 aprile), facile da indovinare

1111	✕ Debolissimo	Quattro cifre uguali, blocca in 1 secondo
847263	☑ Buono	6 cifre casuali, nessun pattern evidente
291847	☑ Buono	6 cifre, nessuna sequenza, difficile da indovinare
736291	☑ Ottimo	Creato con tecnica mnemonica, sicuro e memorabile
K4m2r9	☑ Eccellente	Alfanumerico (se disponibile): massima sicurezza

Parte 5 – Errori comuni da evitare

Anche chi pensa di avere un PIN sicuro spesso commette errori che ne riducono l'efficacia. Ecco i più frequenti:

I 10 errori più comuni con i PIN

1. Usare lo stesso PIN per bancomat, telefono e SIM.
2. Scrivere il PIN sul telefono (nei contatti, nelle note o nelle foto).
3. Dire il PIN ad amici o parenti 'solo per questa volta'.
4. Non coprire la tastiera quando si digita il PIN in pubblico.
5. Non cambiare il PIN dopo aver perso il portafoglio o la carta.
6. Usare l'anno di nascita o la data del matrimonio.
7. Scegliere un PIN basato sul nome (A=1, B=2... quindi 'ANNA' = 1441).
8. Non cambiare il PIN predefinito della SIM (spesso 0000 o 1234).
9. Usare lo stesso PIN da anni senza mai cambiarlo.
10. Inserire il PIN quando qualcuno è vicino senza coprire la tastiera.

Uno degli errori più sottovalutati è il **'shoulder surfing'**, cioè quando qualcuno ti spia mentre inserisci il PIN. Può succedere:

- Alla cassa del supermercato, mentre paghi con il POS.
- Al bancomat, se c'è qualcuno vicino a te.
- Sul tram o autobus, mentre sblocchi il telefono.
- Nei negozi, mentre usi l'app di pagamento.

La soluzione è semplice: **copri sempre la tastiera con l'altra mano** mentre digiti il PIN. È un gesto piccolo che fa una grande differenza.

Parte 6 – Cosa fare se dimentichi il PIN

Succede a tutti. Hai dimenticato il PIN e ora non sai come fare. Ecco cosa fare in base al dispositivo:

Hai dimenticato il PIN del bancomat

- Non tentare per tentativi! Dopo 3 errori la carta si blocca.
- Contatta la tua banca (numero sul retro della carta o sul sito ufficiale).
- Puoi richiedere un nuovo PIN allo sportello in filiale con un documento d'identità.
- Alcune banche inviano il nuovo PIN per posta o permettono di reimpostarlo dall'app.

Hai dimenticato il PIN dello smartphone Android

- Dopo troppi tentativi sbagliati, Android propone di sbloccare con l'account Google.
- Inserisci email e password del tuo account Google associato al telefono.
- Se non ricordi nemmeno le credenziali Google, potrebbe essere necessario un ripristino di fabbrica (attenzione: cancella tutti i dati!).

Hai dimenticato il codice di iPhone

- Dopo i tentativi errati, iPhone mostra 'iPhone disabilitato'.
- Devi collegare l'iPhone al computer e usare iTunes (Windows) o il Finder (Mac).
- Oppure usa la funzione 'Cancella iPhone' dalla pagina di blocco (disponibile da iOS 15.2).
- Attenzione: il ripristino cancella tutti i dati se non hai un backup su iCloud.

Hai dimenticato il PIN della SIM

- La SIM si blocca dopo 3 tentativi errati.
- Hai bisogno del codice PUK (Personal Unblocking Key).
- Lo trovi: nel documento originale della SIM, sull'app del tuo operatore, chiamando il servizio clienti.
- Hai 10 tentativi per il PUK. Dopo il 10° tentativo errato, la SIM è definitivamente inutilizzabile.

Consiglio Pro: Conserva i codici di recupero in modo sicuro

Stampa o annota i codici PUK e i codici di recupero dei tuoi account.
Conservali in un posto fisico sicuro (cassaforte, cassetto chiuso a chiave).
NON salvarli sul telefono o su foglietti nel portafoglio.
Considera un password manager (app sicura per conservare password e PIN).

Parte 7 – PIN e autenticazione a due fattori

Negli ultimi anni, la sicurezza digitale si è evoluta. Il solo PIN non è sempre sufficiente. Entra in scena l'autenticazione a due fattori (2FA), che aggiunge un secondo strato di protezione.

Che cos'è l'autenticazione a due fattori?

È un sistema che richiede DUE prove di identità invece di una sola.

Il concetto: qualcosa che SAI (il PIN) + qualcosa che HAI (il telefono) o che SEI (impronta digitale).

Esempio: accedi al sito della banca con PIN → la banca ti manda un SMS con un codice temporaneo → inserisci anche quello.

Anche se qualcuno scopre il tuo PIN, non può accedere senza il secondo fattore.

Domande Frequenti (FAQ)

D: Posso usare lo stesso PIN per il bancomat e per il telefono?

R: Tecnicamente sì, ma è fortemente sconsigliato. Se qualcuno scopre il PIN del telefono (magari sbirciando mentre lo inserisci), avrebbe anche accesso al tuo bancomat. Usa PIN diversi per ogni servizio importante.

D: Ogni quanto devo cambiare il PIN?

R: Almeno una volta all'anno per i PIN principali (bancomat, telefono). Cambialo immediatamente se sospetti che qualcuno lo conosca, se hai perso il portafoglio, o se hai usato il PIN su un dispositivo non tuo.

D: È sicuro salvare il PIN sul telefono nelle note?

R: No, è molto pericoloso. Se qualcuno accede al tuo telefono (rubato, smarrito, o prestato), troverebbe il PIN immediatamente. Se devi conservarlo digitalmente, usa un'app password manager dedicata e sicura.

D: Cosa significa quando il bancomat 'mangia' la carta?

R: La carta viene trattenuta (non distrutta) dal bancomat quando: hai inserito il PIN sbagliato troppe volte, la carta è scaduta o bloccata, c'è un problema tecnico. Contatta la tua banca per recuperarla.

D: Un PIN a 6 cifre è davvero molto più sicuro di uno a 4 cifre?

R: Sì, enormemente. Un PIN a 4 cifre ha 10.000 combinazioni possibili. Uno a 6 cifre ne ha 1.000.000 — cento volte di più. Il tempo per indovinarlo cresce esponenzialmente.

D: Posso usare lettere nel PIN?

R: Dipende dal sistema. Molti bancomat accettano solo numeri. Alcuni smartphone e servizi online accettano PIN alfanumerici (mix di lettere e numeri). Se disponibile, è un'ottima scelta per maggiore sicurezza.

D: Il mio operatore telefonico conosce il mio PIN SIM?

R: No. Il PIN SIM è cifrato nella scheda e nemmeno il tuo operatore lo conosce. L'operatore conosce solo il PUK, che serve per sbloccare la SIM in caso di emergenza.

D: Cosa fa un 'password manager' esattamente?

R: È un'applicazione che conserva tutti i tuoi PIN, password e codici in modo sicuro e cifrato. Li protegge con una sola 'password master' che solo tu conosci. Alcuni sono gratuiti (Bitwarden), altri a pagamento (1Password). È la soluzione migliore per chi ha molti account.

D: Se qualcuno conosce il mio PIN ma non ha la mia carta fisica, può usarlo?

R: Per il bancomat fisico, no: servono sia la carta che il PIN. Per i pagamenti online con carta, il PIN da solo non basta: di solito serve anche il numero della carta, la scadenza e il codice CVV. Tuttavia, è sempre bene cambiare il PIN se pensi che qualcuno lo conosca.

D: Come faccio a sapere se il mio PIN attuale è sicuro?

R: Fai queste domande: è tra i 10 PIN più comuni? È una data di nascita? È una sequenza (1234, 4321)? È lo stesso per più servizi? Hai più di 3 anni che non lo cambi? Se hai risposto sì a una di queste domande, è il momento di cambiarlo.

Glossario dei Termini Tecnici

Ecco tutti i termini tecnici usati in questa guida, spiegati con parole semplici:

2FA / Autenticazione a due fattori	Sistema di sicurezza che richiede due prove di identità: qualcosa che sai (PIN/password) + qualcosa che hai (telefono) o che sei (impronta). Molto più sicuro della sola password.
ATM / Bancomat	Sportello bancario automatico (Automated Teller Machine). La macchina in strada o in banca dove puoi prelevare denaro, controllare il saldo e fare operazioni. 'Bancomat' in Italia si riferisce sia allo sportello che alla carta.
Brute Force (Forza Bruta)	Tecnica di attacco informatico che prova tutte le combinazioni possibili finché non trova quella giusta. Per un PIN a 4 cifre ci sono 10.000 combinazioni possibili.
Cifratura / Crittografia	Processo matematico che trasforma un'informazione in un formato illeggibile (cifrato) per chi non ha la 'chiave'. Il tuo PIN viene conservato nei sistemi in forma cifrata, non in chiaro.
Codice OTP	One Time Password: codice temporaneo valido per un solo utilizzo (di solito 30-60 secondi). Usato nella 2FA. La banca ti manda un SMS con un OTP quando fai operazioni online.
Password Manager	Applicazione sicura che conserva tutte le tue password e PIN in un unico posto protetto da una sola password 'master'. Esempi: Bitwarden (gratuito), 1Password, LastPass.
PIN (Personal Identification Number)	Numero di identificazione personale. Sequenza di cifre (di solito 4-6) usata per verificare la tua identità e accedere a servizi o dispositivi. È personale e non va mai condiviso.
POS (Point of Sale)	Il terminale del negozio dove si striscia o avvicina la carta per pagare. 'Point of Sale' significa letteralmente 'punto vendita'. Qui si inserisce il PIN per i pagamenti con carta.
PUK (Personal Unblocking Key)	Codice di sblocco della SIM telefonica. Serve a sbloccare la SIM quando il PIN SIM viene inserito 3 volte in modo errato. Si hanno solo 10 tentativi prima che la SIM venga distrutta definitivamente.
Ripristino di fabbrica	Operazione che cancella tutti i dati di un dispositivo e lo riporta alle impostazioni originali di fabbrica. Usato come ultima risorsa quando si dimentica il PIN dello smartphone. Cancella foto, app e dati.

Shoulder Surfing	Letteralmente 'sbirciare dalla spalla'. Tecnica con cui un malintenzionato osserva di nascosto mentre inserisci il PIN, per poi usarlo senza il tuo permesso.
SIM (Subscriber Identity Module)	La piccola scheda che si inserisce nel telefono e contiene il tuo numero di telefono e i tuoi dati di abbonamento. Può essere protetta da un PIN SIM separato dal PIN del telefono.
Tecnica Mnemonica	Trucco mentale che aiuta a ricordare informazioni collegandole a qualcosa di già noto. Usata in questa guida per creare PIN sicuri ma facili da ricordare.

Conclusioni

Siamo arrivati alla fine di questa guida. Facciamo un riepilogo di tutto quello che hai imparato:

Quello che hai imparato oggi

- Il PIN è la tua chiave digitale: piccola ma importantissima.
- La maggior parte delle persone usa PIN facilmente indovinabili (1234, date di nascita).
- Cambiare il PIN su bancomat, smartphone e SIM è semplice: bastano pochi minuti.
- Con le tecniche mnemoniche puoi creare un PIN sicuro E facile da ricordare.
- Non usare mai lo stesso PIN per tutti i servizi.
- Copri sempre la tastiera quando inserisci il PIN in pubblico.
- L'autenticazione a due fattori ti protegge anche se qualcuno scopre il PIN.
- In caso di PIN dimenticato, non tentare per tentativi: contatta il servizio.

La sicurezza digitale non è qualcosa di complicato o riservato agli esperti. È fatta di piccole abitudini quotidiane: scegliere un PIN migliore, coprire la tastiera, non condividere il codice con nessuno.

Ogni passo che fai verso una migliore sicurezza è un passo verso la **protezione della tua identità, del tuo denaro e della tua privacy**. E spesso basta davvero poco.

Inizia oggi: prendi cinque minuti per cambiare il PIN della tua carta o del tuo telefono. Usa una delle tecniche che hai imparato. Ti sembrerà una piccola cosa, ma potrebbe fare una grande differenza.

Hai trovato utile questa guida? Condividila con amici e familiari — la sicurezza digitale è più forte quando la pratichiamo insieme.