La checklist di sicurezza definitiva per Windows: la guida da inviare (una volta per tutte) a genitori, parenti e amici

Gentiluomo Digitale

https://www.youtube.com/@gentiluomodigitale

Introduzione

Se in famiglia sei tu quello "bravo con i computer", probabilmente conosci bene la sensazione: un messaggio improvviso, magari alle nove di sera, con scritto "il PC fa una cosa strana" oppure "mi è arrivata una chiamata che dice che il mio computer ha un virus, cosa faccio?". Ogni volta si ricomincia da capo, si spiegano le stesse cose, si mettono le stesse pezze.

Questa guida nasce proprio per rompere questo circolo. L'idea è semplice: invece di intervenire ogni volta che qualcosa va storto, mettiamo mano una volta sola alle impostazioni di sicurezza fondamentali di Windows, spieghiamo bene *perché* servono, e costruiamo insieme qualche abitudine mentale che eviti la maggior parte dei problemi futuri.

Non serve essere esperti per seguirla: ogni passaggio è spiegato in modo semplice, con il percorso esatto da seguire nelle Impostazioni di Windows 11 (e le differenze rispetto a Windows 10, dove rilevanti). Alla fine di questa guida avrai:

- attivato le protezioni che riducono drasticamente il rischio di furto di dati o accessi indesiderati;
- sistemato una volta per tutte le impostazioni che, se lasciate come sono di default, espongono il PC a rischi inutili;
- imparato a riconoscere i tentativi di truffa più comuni, quelli che circolano per telefono, email e finti popup;
- capito quando è il caso di preoccuparsi davvero e quando invece si può ignorare un allarme.

Cominciamo dalle cose più urgenti.

Prima di iniziare: che sistema operativo hai?

Prima di mettere mano a qualsiasi impostazione, è importante sapere su quale versione di Windows stai lavorando, perché cambia sia il percorso dei menu sia l'urgenza di alcuni interventi.

Windows 10 ha raggiunto la fine del supporto ufficiale il 14 ottobre 2025: da quella data Microsoft non rilascia più aggiornamenti gratuiti di sicurezza per il grande pubblico, il che significa che un PC con Windows 10 non aggiornato diventa progressivamente più vulnerabile. Buona notizia: Microsoft ha successivamente prorogato il programma ESU (Extended Security Updates, aggiornamenti di sicurezza estesi), che ora copre gratuitamente gli utenti privati fino al 12 ottobre 2027 — in Europa l'iscrizione è gratuita e non richiede particolari condizioni, a differenza di quanto previsto inizialmente in altri Paesi. Se il tuo dispositivo o quello di un tuo familiare è ancora su Windows 10, il primo passo pratico è verificare che l'iscrizione a ESU sia attiva: si controlla da **Impostazioni > Windows Update**, dove dovrebbe comparire la dicitura "Il PC è registrato per ricevere gli Aggiornamenti della sicurezza estesi". Se non c'è, conviene iscriversi subito, oppure valutare l'aggiornamento a Windows 11 se il PC è compatibile.

Detto questo, tutte le indicazioni di questa guida valgono sia per Windows 11 sia per Windows 10, salvo dove specificato diversamente: i percorsi nei menu sono quasi identici, con qualche piccola differenza di nome o posizione che segnaleremo di volta in volta.

Parte 1 — Le cose da sistemare SUBITO

Questa prima sezione raccoglie gli interventi più urgenti: sono tutti gratuiti, richiedono pochi minuti e vanno fatti su ogni PC di famiglia, indipendentemente da quanto sia "vecchio" o usato di rado.

1. Attiva Windows Hello

Che cos'è. Windows Hello è il sistema di accesso "intelligente" di Windows: al posto di digitare una password ogni volta, puoi sbloccare il PC con un'impronta digitale, un riconoscimento del volto (se il PC ha una webcam compatibile) oppure un codice PIN numerico dedicato al dispositivo.

A cosa serve e perché conviene. Molti pensano che digitare una password lunga sia "più sicuro" di un PIN breve. In realtà è vero il contrario, per un motivo tecnico interessante: la password che usi per accedere a Windows viene spesso condivisa con il tuo account Microsoft online (quello che usi anche per Outlook, OneDrive, ecc.), quindi se qualcuno la intercetta può provare ad usarla anche altrove. Il PIN di Windows Hello, invece, è legato esclusivamente a quel dispositivo fisico: anche conoscendolo, non serve a nessuno per accedere al tuo account da un altro computer. In più, con impronta o volto l'accesso è più rapido e non c'è nulla da digitare (e quindi nulla che un malintenzionato possa "origliare" guardandoti le dita sulla tastiera).

Quando è utile. Sempre, su qualsiasi PC personale o condiviso in famiglia.

Quando non è strettamente necessario. Se il PC non lascia mai una stanza chiusa a chiave e non contiene dati sensibili, l'urgenza è minore, ma resta comunque una buona pratica da adottare.

Come attivarlo. Vai su **Impostazioni > Account > Opzioni di accesso**. Da qui puoi impostare PIN, impronta digitale (se il PC ha un lettore) o riconoscimento facciale (se la webcam lo supporta). Ti verrà chiesto di inserire prima la password dell'account per confermare l'identità, poi di configurare il nuovo metodo.

Errore comune: pensare che il PIN debba essere complicato come una password. Non serve: proprio perché è legato solo a quel PC, un PIN di 4-6 cifre è già efficace. L'importante è non usare sequenze ovvie come 1234 o la data di nascita.

2. Controlla che Windows Update sia davvero attivo

Che cos'è. Windows Update è il servizio che scarica automaticamente le correzioni di sicurezza (le cosiddette "patch") rilasciate periodicamente da Microsoft per chiudere le falle scoperte nel sistema operativo.

A cosa serve. Ogni mese vengono scoperte nuove vulnerabilità nei sistemi operativi, cioè "porte" non protette che i malintenzionati possono sfruttare per introdurre virus o rubare dati. Windows Update chiude queste porte automaticamente, ma solo se è effettivamente in funzione.

Perché è facile che sia disattivato senza saperlo. Windows permette di "mettere in pausa" gli aggiornamenti fino a 5 settimane, funzione comoda per chi ha bisogno di stabilità in un momento preciso, ma spesso viene attivata per errore (magari toccando un pulsante sbagliato) e poi dimenticata. Un PC con gli aggiornamenti in pausa da mesi è un PC vulnerabile.

Come controllare. Vai su **Impostazioni > Windows Update**. Se vedi la scritta "Aggiornamenti sospesi" con una data, premi su "Riprendi aggiornamenti". Approfitta della visita per premere anche su "Verifica disponibilità aggiornamenti", così ti assicuri che tutto sia allineato all'ultima versione disponibile.

Consiglio pratico: imposta il PC in modo che gli aggiornamenti vengano installati automaticamente durante la notte, così non interferiscono mai con l'uso quotidiano. Questa opzione si trova in **Windows Update > Impostazioni avanzate > Recapito ottimizzato / Ore di attività**, dove puoi specificare la fascia oraria in cui usi normalmente il PC, in modo che i riavvii per l'installazione avvengano fuori da quella fascia.

3. Verifica che Windows Defender (Sicurezza di Windows) sia attivo

Che cos'è. Windows Defender — oggi chiamato ufficialmente "Sicurezza di Windows" nell'interfaccia — è l'antivirus integrato in Windows, attivo di default e gratuito.

A cosa serve. Esegue una scansione continua in tempo reale di file, app e processi in esecuzione, bloccando malware, ransomware e altri software dannosi prima che possano causare danni.

Perché a volte risulta "mezzo disattivato". Se in passato è stato installato un antivirus di terze parti (per esempio Norton, McAfee o simili) e poi disinstallato, capita che Windows Defender resti in uno stato intermedio, non completamente riattivato. Anche un antivirus di terze parti tuttora installato può disattivare alcune funzioni di Defender per evitare conflitti: questo è normale e non è un problema, purché l'antivirus di terze parti sia effettivamente attivo e aggiornato.

Come controllare. Vai su **Impostazioni > Privacy e sicurezza > Sicurezza di Windows > Protezione da virus e minacce**. Dovresti vedere tutte le voci con un segno di spunta verde e nessuna azione richiesta, in particolare la voce "Protezione in tempo reale" deve risultare attiva.

Consiglio pratico: se non usi un antivirus di terze parti a pagamento, Windows Defender da solo è più che sufficiente per un utente domestico: i test indipendenti di laboratori come AV-Test e AV-Comparatives lo collocano costantemente tra i prodotti più efficaci sul mercato. Non è necessario, né consigliabile, installare due antivirus contemporaneamente: entrano in conflitto e possono rallentare il PC senza aumentare realmente la protezione.

4. Attiva "Trova il mio dispositivo"

Che cos'è. È la funzione che permette di localizzare un PC Windows smarrito o rubato attraverso il tuo account Microsoft, in modo simile a "Dov'è" su iPhone o "Trova il mio dispositivo" su Android.

A cosa serve. Se il portatile viene dimenticato al bar, perso in viaggio o rubato, questa funzione ti permette di vederne l'ultima posizione nota su una mappa e, soprattutto, di bloccarlo da remoto per impedire che chi lo trova possa accedere ai tuoi dati.

Requisito indispensabile: funziona solo se il PC è collegato a un account Microsoft (non a un account locale) e se è connesso a Internet nel momento in cui provi a localizzarlo. Se il ladro spegne subito il Wi-Fi, la localizzazione in tempo reale non sarà possibile, ma resterà comunque visibile l'ultima posizione registrata.

Come attivarla. Vai su **Impostazioni > Privacy e sicurezza > Trova il mio dispositivo** e assicurati che l'interruttore sia su "Attivo". Da questa stessa pagina puoi anche vedere l'elenco di tutti i PC collegati al tuo account Microsoft.

Consiglio pratico: per localizzare un PC smarrito, vai sul sito account.microsoft.com/devices da un altro dispositivo (telefono, tablet o altro PC), accedi con lo stesso account Microsoft e cerca la sezione dedicata ai dispositivi.

Parte 2 — Le impostazioni da sistemare una volta per tutte

A differenza della sezione precedente, questi interventi richiedono qualche minuto in più, ma vanno fatti una sola volta: dopo la configurazione iniziale non richiedono più manutenzione.

5. Passa da un account locale a un account Microsoft con verifica in due passaggi

Che cos'è un account locale e perché è un problema. Quando configuri un PC Windows senza collegarlo a Internet o scegliendo esplicitamente "accesso offline", viene creato un account locale: esiste solo su quel PC, non è collegato a nessun servizio online e, soprattutto, non ha alcun modo di recupero se dimentichi la password. Se questo accade, l'unica soluzione realistica è reinstallare Windows da zero, perdendo tutti i dati non salvati altrove.

A cosa serve un account Microsoft. Collegando Windows a un account Microsoft (lo stesso che usi per Outlook.com, Xbox o Office) ottieni diversi vantaggi concreti:

- puoi reimpostare la password online, da qualsiasi dispositivo, se la dimentichi;
- le impostazioni, alcuni file e le password salvate nel browser possono sincronizzarsi tra più PC;
- le licenze digitali di app e giochi acquistati restano associate al tuo account, non al singolo PC;
- diventano disponibili funzioni come "Trova il mio dispositivo" e il backup automatico della chiave di ripristino di BitLocker/crittografia dispositivo (ne parliamo al punto successivo).

Il passaggio più importante: l'autenticazione a due fattori (2FA). Una volta collegato l'account Microsoft, attiva la verifica in due passaggi. In pratica, oltre alla password, per accedere da un dispositivo nuovo o non riconosciuto verrà richiesto un secondo elemento di conferma: un codice inviato via SMS, una notifica sull'app Microsoft Authenticator, o un codice generato da un'app di autenticazione. Questo significa che, anche se qualcuno riuscisse a scoprire la password (per esempio a causa di una fuga di dati da un sito terzo), non potrebbe comunque accedere all'account senza avere anche il telefono o il dispositivo di conferma.

Come procedere. Per collegare l'account: **Impostazioni > Account > Le tue informazioni**, poi "Accedi con un account Microsoft" e segui la procedura guidata. Per attivare la verifica in due passaggi, bisogna andare sul sito account.microsoft.com, sezione "Sicurezza", e cercare l'opzione relativa alla verifica in due passaggi.

Attenzione: conserva sempre un metodo di recupero alternativo (un numero di telefono e un indirizzo email secondario aggiornati) collegato all'account Microsoft. Sono la rete di sicurezza che ti permette di rientrare nell'account anche se perdi l'accesso al metodo di verifica principale.

6. Attiva la crittografia del disco

Che cos'è. La crittografia trasforma tutti i dati salvati sul disco in un codice illeggibile senza la chiave corretta (che, in pratica, coincide con l'accesso al tuo account Windows). Senza crittografia, chi ruba un portatile può semplicemente estrarre il disco, collegarlo a un altro PC come disco esterno e leggere tutti i file senza dover superare alcuna schermata di accesso.

Le due versioni disponibili in Windows: qual è la differenza.

Windows offre due strumenti che usano la stessa tecnologia di fondo ma con un livello di controllo diverso:

- **Crittografia dispositivo (Device Encryption):** è la versione semplificata, pensata per chi non vuole configurare nulla. È disponibile su tutte le edizioni di Windows, incluse le versioni Home, ma richiede alcuni requisiti hardware (un chip di sicurezza TPM presente e attivo, principalmente). Quando è disponibile, si attiva spesso in automatico durante l'accesso con un account Microsoft, e la chiave di ripristino viene salvata automaticamente nel tuo account Microsoft online.
- **BitLocker:** è la versione completa e configurabile, disponibile solo su Windows Pro, Enterprise ed Education (non su Windows Home). Permette di scegliere quali unità cifrare, di richiedere un PIN aggiuntivo all'avvio e di scegliere dove conservare la chiave di ripristino (account Microsoft, file locale, stampa su carta).

Nella pratica, per un utente domestico con Windows Home, la Crittografia dispositivo è più che sufficiente: fa lo stesso lavoro di fondo di BitLocker, solo con meno opzioni da gestire.

Come verificare/attivare. Vai su **Impostazioni > Privacy e sicurezza**, cerca la voce "Crittografia dispositivo" (oppure "BitLocker" se hai Windows Pro) e attivala se non lo è già. Se il PC non mostra questa voce, significa che l'hardware non soddisfa i requisiti minimi (in genere l'assenza del chip TPM), e in quel caso la funzione semplicemente non è disponibile.

Il punto più importante di tutta questa sezione: la chiave di ripristino. Quando attivi la crittografia, ti verrà chiesto dove salvare la chiave di ripristino: è un lungo codice numerico che serve per sbloccare il disco in situazioni particolari, ad esempio dopo una sostituzione della scheda madre o un aggiornamento importante del firmware. **Verifica sempre che venga effettivamente salvata nel tuo account Microsoft** (è l'opzione predefinita e più semplice): senza quella chiave, in caso di blocco, i tuoi dati diventano irrecuperabili, nemmeno da un tecnico specializzato. Puoi controllare in qualsiasi momento se la chiave è salvata visitando aka.ms/myrecoverykey da un browser, con lo stesso account Microsoft collegato al PC.

7. Passa da un account Amministratore a un account Standard per l'uso quotidiano

Che cos'è la differenza. Quando configuri un PC Windows per la prima volta, il primo account creato diventa automaticamente "Amministratore": ha pieno controllo sul sistema e può installare software, modificare impostazioni protette e accedere a ogni parte del sistema operativo senza restrizioni. Un account "Standard", invece, può usare il PC normalmente (navigare, scrivere documenti, guardare video) ma non può installare programmi o modificare impostazioni di sistema senza l'autorizzazione (tramite password) di un account Amministratore.

Perché conviene usare un account Standard per il giorno per giorno. Il rischio principale è questo: se un virus o un malware riesce a introdursi nel PC mentre sei collegato con un account Amministratore, quel software ottiene automaticamente gli stessi identici permessi che hai tu, cioè pieno accesso al sistema. Se

invece sei collegato con un account Standard, anche in caso di infezione il danno potenziale è molto più limitato, perché il malware si scontra con le stesse restrizioni che limitano te.

Come funziona in pratica. Non è scomodo come sembra: quando serve installare un programma legittimo o modificare un'impostazione avanzata, Windows chiederà semplicemente la password dell'account Amministratore in una finestra di conferma (il cosiddetto "Controllo account utente"). Con un account Standard, tutte le attività quotidiane — email, browser, videochiamate, ufficio, streaming — funzionano esattamente allo stesso modo.

Come impostarlo. Vai su **Impostazioni > Account > Famiglia** (oppure "Altri utenti" se non è un account familiare collegato). Da qui puoi creare un nuovo account e assegnargli il tipo "Standard", oppure modificare il tipo di un account già esistente selezionandolo e scegliendo "Cambia tipo di account".

Attenzione pratica: ti consigliamo di mantenere comunque un account Amministratore separato (magari usato solo tu, o solo occasionalmente) per le operazioni di manutenzione, e di usare l'account Standard come account "principale" per l'uso quotidiano di ogni membro della famiglia.

8. Usa un gestore di password

Che cos'è. Un gestore di password (in inglese "password manager") è un'applicazione che crea, memorizza e inserisce automaticamente password complesse e diverse per ogni sito, custodendole in un "caveau" digitale protetto da un'unica password principale che sei tu a dover ricordare.

Perché è quasi indispensabile oggi. Il problema più comune, e più pericoloso, è il riutilizzo della stessa password su più siti. Quando un sito subisce una violazione dei dati (evento purtroppo frequente, anche per servizi molto noti), le combinazioni email/password rubate finiscono spesso in circolazione online, e i malintenzionati le testano automaticamente su altri servizi popolari (banche, email, social). Se usi sempre la stessa password, basta una sola violazione altrove per mettere a rischio anche il tuo conto in banca. Un gestore di password risolve il problema alla radice, permettendoti di usare una password unica, lunga e casuale per ogni servizio, senza doverle memorizzare tutte.

Vantaggi concreti:

- password generate automaticamente, molto più complesse di quelle che una persona inventerebbe;
- compilazione automatica dei moduli di accesso, con protezione aggiuntiva contro i siti-truffa (un gestore di password non compila i campi su un sito con indirizzo diverso da quello memorizzato, anche se la pagina sembra identica all'originale — un ottimo scudo automatico contro il phishing);
- possibilità di condividere in modo sicuro alcune credenziali con altri membri della famiglia (per esempio l'account Netflix), senza dover comunicare la password a voce o per messaggio.

Quali scegliere. Tra le opzioni più diffuse e affidabili ci sono 1Password, Bitwarden, Proton Pass e NordPass; tutte offrono un piano gratuito o un periodo di prova, con funzioni a pagamento più avanzate (condivisione familiare, monitoraggio delle violazioni dei dati, ecc.). Anche i browser più diffusi, come Microsoft Edge, Google Chrome e Firefox, includono un gestore di password integrato: è un'opzione "meglio di niente" molto valida per chi vuole iniziare senza installare nulla di nuovo, anche se i gestori dedicati offrono generalmente più funzioni e una sicurezza più solida per i dati davvero critici (banca, email principale).

Consiglio pratico per iniziare: non serve cambiare tutte le password in un giorno solo. Inizia dai servizi più critici — email principale, home banking, account Microsoft o Google, social — e prosegui gradualmente man mano che accedi agli altri siti.

Parte 3 — Le abitudini da imparare (e da insegnare)

Anche con tutte le impostazioni sistemate alla perfezione, la difesa più importante resta il buonsenso davanti a situazioni sospette. Queste tre abitudini coprono la stragrande maggioranza delle truffe informatiche che colpiscono utenti non esperti.

9. Impara a riconoscere il phishing

Che cos'è. Il phishing è una tecnica di truffa in cui il malintenzionato si finge un mittente affidabile — una banca, un corriere, un servizio online, persino un collega o un familiare — per convincerti a cliccare un link, inserire le tue credenziali su un sito-truffa, oppure aprire un allegato dannoso.

Come si presenta. Può arrivare via email, SMS ("smishing"), messaggi su WhatsApp o social, oppure tramite pagine web compromesse. Windows include un sistema chiamato SmartScreen che blocca automaticamente molti siti di phishing noti, mostrando un avviso rosso a schermo intero prima di farti accedere: se lo vedi, non ignorarlo e torna indietro. Tuttavia SmartScreen non intercetta tutto, soprattutto i siti-truffa creati di recente, quindi non bisogna fare affidamento solo su di esso.

Segnali d'allarme a cui prestare attenzione:

- un senso di urgenza innaturale ("il tuo account verrà chiuso entro 24 ore", "pacco bloccato in dogana, paga subito");
- l'indirizzo email del mittente che, guardato con attenzione, non corrisponde all'azienda dichiarata (per esempio dominio leggermente diverso o con caratteri strani);
- richieste di inserire password, dati della carta di credito o codici di accesso cliccando su un link ricevuto via email o SMS — le aziende serie non lo chiedono mai in questo modo;
- link che, passandoci sopra con il mouse senza cliccare, mostrano un indirizzo diverso da quello visualizzato nel testo.

Cosa fare in caso di dubbio. Non cliccare sul link presente nel messaggio. Se pensi possa trattarsi di una comunicazione legittima (per esempio dalla tua banca), apri il browser e digita tu stesso l'indirizzo ufficiale del sito, oppure usa l'app ufficiale, per verificare direttamente se c'è davvero qualcosa che ti riguarda.

10. Non credere mai a chi ti chiama "per il tuo computer"

Il principio di base, semplice ma efficacissimo: nessuna azienda seria — non Microsoft, non la tua banca, non il tuo fornitore di internet — ti chiamerà mai al telefono in modo spontaneo per dirti che il tuo computer ha un problema. Questo tipo di chiamata, se ricevuta, è quasi sempre una truffa, nota come "truffa del finto supporto tecnico" (tech support scam).

Come funziona tipicamente questa truffa:

- Ricevi una telefonata (o vedi comparire un numero di telefono su un popup a schermo intero, spesso accompagnato da suoni di allarme) che ti avvisa di un presunto virus o problema critico sul tuo PC.
- L'interlocutore, molto professionale nei modi, ti guida a scaricare un software di assistenza remota per "risolvere il problema insieme".
- Una volta ottenuto l'accesso remoto al tuo PC, il truffatore può rubare dati, installare malware, oppure convincerti a effettuare pagamenti fasulli per un "servizio" mai richiesto.

Cosa fare se succede a te (o a un tuo familiare):

- Se ricevi una telefonata di questo tipo: riaggancia, senza discutere e senza fornire alcuna informazione.

- Se compare un popup con un numero da chiamare: non chiamare quel numero. Chiudi il browser (se non si chiude normalmente, usa **Ctrl+Alt+Canc** per aprire Task Manager e chiudere il processo del browser da lì).
- **Non condividere mai le tue password**, né per telefono, né via email, né tramite messaggi, con nessuno che dichiari di rappresentare un servizio di assistenza.

11. Non installare mai software su richiesta di uno sconosciuto al telefono

Il collegamento con il punto precedente. Il passaggio finale delle truffe di finto supporto tecnico spesso consiste nel convincere la vittima a installare un programma di accesso remoto — strumenti come AnyDesk o TeamViewer, che di per sé sono software legittimi e ampiamente usati anche in ambito lavorativo per assistenza tecnica reale — per permettere al "tecnico" di "vedere lo schermo e risolvere il problema".

Perché è pericoloso. Una volta installato e autorizzato, questo tipo di software dà il controllo completo del PC alla persona dall'altra parte, esattamente come se fosse seduta davanti alla tastiera. Da quel momento può fare praticamente qualsiasi cosa: accedere a file personali, home banking già collegato, password salvate nel browser, oppure installare ulteriore malware.

La regola pratica da seguire e da insegnare: se una persona che non conosci, contattata per telefono o arrivata tramite un popup, ti chiede di installare un software — qualunque software, non solo quelli di assistenza remota — la risposta corretta è sempre no, e la conversazione va interrotta immediatamente.

L'unica eccezione legittima: installare un software di assistenza remota va bene solo quando sei stato tu a contattare per primo un servizio di assistenza di cui ti fidi (per esempio il supporto tecnico ufficiale del produttore del tuo PC, o un tecnico di fiducia che conosci personalmente), non quando è qualcun altro a contattarti per primo proponendosi spontaneamente.

Conclusioni

Se hai seguito questa guida dall'inizio alla fine, il PC che avevi davanti — o quello di un tuo familiare — è ora significativamente più sicuro di prima, e con un investimento di tempo che, in totale, richiede meno di un'ora.

Vale la pena però ricordare la logica complessiva di quello che hai fatto, perché aiuta a capire perché ogni passaggio conta:

- **Le impostazioni della Parte 1** (Windows Hello, Windows Update, Windows Defender, Trova il mio dispositivo) sono la manutenzione di base: vanno controllate periodicamente, perché possono essere disattivate per errore o da un aggiornamento futuro.
- **Le impostazioni della Parte 2** (account Microsoft con 2FA, crittografia del disco, account Standard, gestore di password) sono strutturali: una volta configurate correttamente restano attive senza bisogno di ulteriore intervento, e costituiscono la vera differenza tra un PC vulnerabile e uno solido.
- **Le abitudini della Parte 3** sono la parte più importante di tutte, perché nessuna impostazione tecnica può proteggerti da una decisione presa sotto pressione o per fiducia mal riposta. La regola d'oro da ricordare, e da far ricordare a chi assisti, è semplicissima: **nella fretta e nella pressione si nascondono quasi tutte le truffe.** Se qualcosa ti chiede di agire "subito", prenditi invece un minuto per fermarti e verificare.

Un ultimo consiglio pratico: rivedi questa checklist una volta all'anno, magari in un momento fisso (ad esempio a inizio anno, o quando cambi la password del gestore principale), perché Windows evolve, nuove funzioni vengono introdotte, e vale la pena controllare che tutto sia ancora impostato correttamente.

Disclaimer

Le informazioni contenute in questa guida sono accurate alla data di pubblicazione e sono state verificate tramite fonti ufficiali Microsoft e testate tecniche indipendenti. Sistemi operativi, applicazioni, servizi online e normative sono soggetti a modifiche nel tempo: percorsi di menu, nomi di funzioni e requisiti tecnici possono cambiare con i futuri aggiornamenti di Windows. Si consiglia di verificare sempre la documentazione ufficiale Microsoft più recente prima di applicare modifiche importanti alle impostazioni di sicurezza del proprio dispositivo.

Fonti consultate

- Windows Central – "How I stopped being my parents' emergency IT hotline": https://www.windowscentral.com/microsoft/windows/windows-security-cheat-sheet-family-it
- Microsoft Learn – BitLocker Overview: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
- Microsoft – Aggiornamenti della sicurezza estesi di Windows 10: https://www.microsoft.com/it-it/windows/extended-security-updates
- Microsoft – Fine del supporto per Windows 10: https://www.microsoft.com/it-it/windows/end-of-support
- Microsoft Learn – Programma ESU per Windows 10: https://learn.microsoft.com/it-it/windows/whats-new/extended-security-updates
- TurboLab.it – Windows 10, supporto esteso fino al 2027: https://turbolab.it/windows-update-280/windows-10-supporto-esteso-fino-2027-come-iscriversi-programma-esu-quanto-costa-4802
- IlSoftware.it – Windows 10 continua a resuscitare: https://www.ilsoftware.it/focus/windows-10-continua-a-resuscitare-tutte-le-scadenze-rinviate-da-microsoft/
- Technipages – What's the Difference Between BitLocker and Device Encryption: https://www.technipages.com/whats-the-difference-between-bitlocker-and-device-encryption-in-windows-11/