



Proteggere dispositivi e reti

Aggiornamenti, Sicurezza di Windows, blocco schermo, cifratura e Wi-Fi

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



Indice

Come usare questa dispensa 3

1. Gli aggiornamenti: chiudere le falle note 3

1.1 Il caso che tutti ricordano: WannaCry 4

1.2 Come tenere tutto aggiornato 5

2. Sicurezza di Windows: antivirus e firewall già inclusi 6

2.1 Come aprirla 7

2.2 Le sezioni da conoscere 8

2.3 Serve un antivirus a pagamento? 8

3. Proteggere il computer quando non ci sei: blocco e cifratura 9

3.1 Il blocco dello schermo: un gesto da ripetere 10

3.2 Sguardi indiscreti e post-it 10

3.3 Un account normale per il lavoro di ogni giorno 11

3.4 La cifratura: se il computer viene perso o rubato 11

4. Wi-Fi pubbliche e reti di casa e d'ufficio 12

4.1 Che cosa è prudente fare, in pratica 13

4.2 Le buone abitudini quando sei fuori 14

4.3 E la rete del tuo ufficio? 14

5. Chiavette USB e supporti sconosciuti 15

5.1 Il caso della chiavetta in sala d'attesa 16

5.2 Quando devi usare le tue chiavette 16

Esercitazione pratica 18

Le domande che arrivano in aula 19

Glossario 20

Per approfondire 20

Come usare questa dispensa

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

> **OBIETTIVO**
>
> Imparare a mantenere aggiornato e protetto il computer con gli strumenti già inclusi in Windows 11, a proteggere i dati se il dispositivo viene lasciato incustodito o perso, e a comportarsi con prudenza su Wi-Fi pubbliche e chiavette USB.

Che cosa saprai fare alla fine

- Verificare che gli aggiornamenti di Windows e dei programmi siano attivi.
- Aprire Sicurezza di Windows e controllare antivirus e firewall.
- Bloccare lo schermo e impostare il computer in modo che non resti aperto per errore.
- Capire a cosa serve la cifratura del disco e come funziona BitLocker.
- Comportarsi con prudenza su reti Wi-Fi pubbliche e con chiavette USB sconosciute.

1. Gli aggiornamenti: chiudere le falle note

Le porte più usate dagli attaccanti non sono quelle nuove: sono quelle già note, che qualcuno non ha ancora chiuso.

Ogni programma, dal sistema operativo al lettore di PDF, è scritto da persone, quindi contiene errori. Alcuni sono **falle di sicurezza** (in inglese vulnerability): punti deboli che un attaccante può sfruttare per entrare nel computer. Quando una falla viene scoperta, chi produce il programma pubblica una correzione, che arriva a te sotto forma di **aggiornamento**.



Gli aggiornamenti chiudono le vulnerabilità conosciute.

Da quel momento succede una cosa inquietante: la falla diventa pubblica. Chi attacca sa dove guardare, e va a caccia dei computer che non hanno ancora installato la correzione. Il rischio non è tanto la falla in sé, quanto il tempo in cui resta aperta.



Il rischio sta nel tempo tra la correzione e il tuo aggiornamento

1.1 Il caso che tutti ricordano: WannaCry

Nel maggio del 2017 un ransomware chiamato WannaCry ha colpito centinaia di migliaia di computer nel mondo, bloccando anche ospedali e aziende. Sfruttava una falla di Windows per cui Microsoft aveva già pubblicato la correzione quasi due mesi prima

(marzo 2017). I computer colpiti erano, in larga parte, quelli che non erano stati aggiornati.

Lo stesso vale in piccolo. Immagina uno studio dove un vecchio computer della segreteria «non si tocca perché funziona». Funziona, certo. Ma ogni mese che passa senza aggiornamenti, la lista di falle note aumenta.

1.2 Come tenere tutto aggiornato

- **Windows Update:** apri Impostazioni, scegli **Windows Update** e lascia gli aggiornamenti automatici attivi. Se vedi il pulsante «Controlla gli aggiornamenti» puoi cliccarlo per controllare subito;
- **riavvia davvero:** molti aggiornamenti si completano solo al riavvio. Un computer che resta acceso per settimane con un «riavvio in sospeso» non è ancora protetto;
- **i programmi:** browser, lettore di PDF, programmi di videoconferenza e di ufficio si aggiornano da soli, di solito. Lasciali fare, e non ignorare gli avvisi;
- **telefono e tablet:** valgono le stesse regole, dal menu delle impostazioni del sistema.



Aggiorna sistema e programmi; completa i riavvii richiesti.

QUANDO IL SISTEMA È TROPPO VECCHIO

Ogni versione di Windows ha una data oltre la quale non riceve più correzioni di sicurezza. Per Windows 10 questa data è passata (14 ottobre 2025): i computer che lo usano senza programmi di supporto aggiuntivi restano esposti alle nuove falle, a meno che non aderiscano al programma di aggiornamenti di sicurezza estesi (ESU) di Microsoft, che per i privati è disponibile fino al 12 ottobre 2027. È una soluzione temporanea: pianifica il passaggio a Windows 11. Se in ufficio ne hai ancora, parlane con chi si occupa di informatica e pianifica il passaggio a una versione supportata.

C'è anche un'abitudine collegata: installa solo programmi di cui hai bisogno, e togli quelli che non usi più. Ogni programma in più è una porta in più da tenere aggiornata.

2. Sicurezza di Windows: antivirus e firewall già inclusi

In Windows 11 ti serve meno di quanto pensi: la protezione di base è già dentro, e basta controllare che sia accesa.

Windows 11 include **Sicurezza di Windows**, che usa il motore chiamato Microsoft Defender. Contiene due strumenti fondamentali. L'**antivirus** controlla i file e i programmi alla ricerca di software dannoso (il malware della lezione due). Il **firewall** (letteralmente «muro tagliafuoco») controlla il traffico di rete in entrata e in uscita dal computer, e blocca i collegamenti non autorizzati.



Antivirus e firewall controllano rischi diversi.

2.1 Come aprirla

1. Apri il menu Start e scegli **Impostazioni**.
2. Vai su **Privacy e sicurezza** e poi su **Sicurezza di Windows**.
3. Clicca su **Apri Sicurezza di Windows**. In alternativa, scrivi «Sicurezza di Windows» nella casella di ricerca e apri il programma dal risultato.

La prima schermata mostra una panoramica, chiamata «Sicurezza in breve». Ogni area ha un'icona: una **spunta verde** significa che non devi fare nulla. Un punto esclamativo giallo o una croce rossa significa che qualcosa richiede la tua attenzione.



Le quattro aree principali di Sicurezza di Windows

2.2 Le sezioni da conoscere

Sezione	A cosa serve	Cosa controllare
Protezione da virus e minacce	Antivirus e scansioni	Che la protezione in tempo reale sia attiva; ogni tanto avvia una scansione
Protezione account	Accesso a Windows, Windows Hello, blocco dinamico	Che l'accesso sia protetto da PIN, impronta o volto
Protezione firewall e della rete	Il muro tra il computer e la rete	Che il firewall sia attivo su tutte le reti
Controllo app e browser	Protezione contro programmi e siti sospetti	Che i controlli di reputazione siano attivi
Sicurezza dei dispositivi	Funzioni di sicurezza dell'hardware	Che non compaiano avvisi in giallo

Le aree principali di Sicurezza di Windows.

L'antivirus lavora da solo in sottofondo: analizza i file mentre li scarichi o li apri. Puoi anche avviare a mano una **scansione rapida** dalla sezione «Protezione da virus e minacce», per esempio dopo aver aperto un allegato di cui non eri sicuro.



Controlla le protezioni e presta attenzione agli avvisi.

2.3 Serve un antivirus a pagamento?

Per un uso normale in ufficio o a casa, la protezione inclusa in Windows 11 è una base solida, a patto di tenerla attiva e aggiornata. Prodotti a pagamento possono aggiungere

funzioni (gestione centralizzata, protezione di più dispositivi), e in aziende più grandi si scelgono per questo. Non è un obbligo, e non risolve gli errori umani: nessun antivirus ferma chi inserisce la password in una pagina falsa.

UN SOLO ANTIVIRUS ALLA VOLTA

Se installi un antivirus di un altro produttore, Windows di solito disattiva automaticamente il suo. Non installarne due insieme: si ostacolano a vicenda. E diffida dei finti avvisi che compaiono nel browser dicendo «Il tuo computer è infetto, scarica questo programma»: sono truffe, non allarmi di Windows.



Un avviso in una pagina web può essere un'esca.

3. Proteggere il computer quando non ci sei: blocco e cifratura

Il computer più sicuro del mondo, lasciato acceso e sbloccato, è un computer aperto a chiunque passi.

Fino a qui abbiamo parlato di attacchi dalla rete. Ma in una segreteria un buon numero di rischi è molto più fisico: un cliente che passa dietro la scrivania, una collega delle pulizie, un fornitore lasciato un attimo da solo, un portatile dimenticato sul treno.

3.1 Il blocco dello schermo: un gesto da ripetere

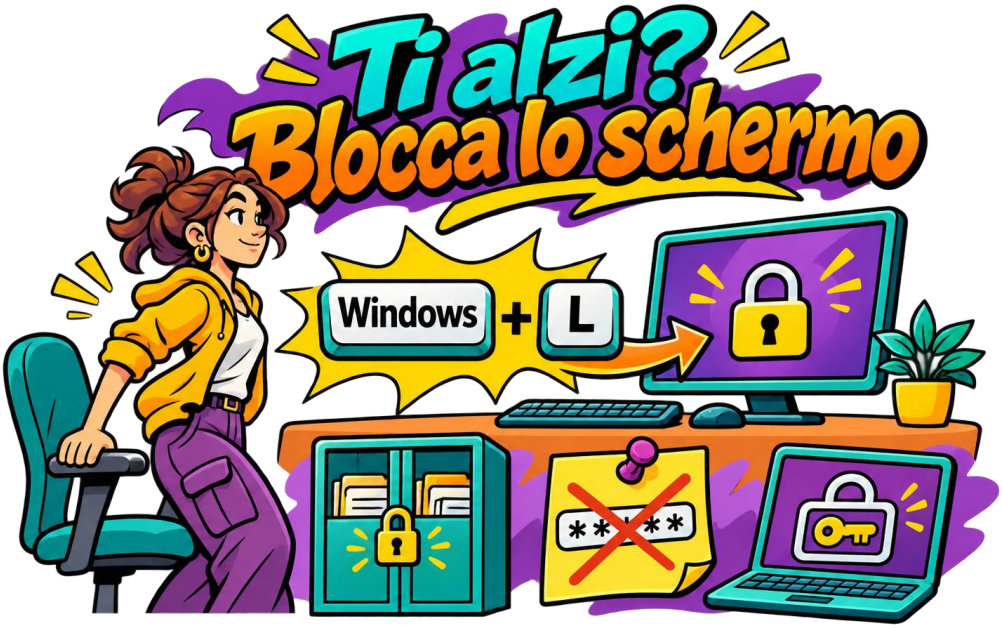
Ogni volta che ti alzi dalla scrivania, premi insieme il tasto **Windows** e il tasto **L**. Lo schermo si blocca e per rientrare serve la tua password, il PIN o l'impronta. È un gesto di un secondo. Fallo anche se esci per due passi, perché due passi bastano per leggere uno schermo.

Aiutati con l'automatismo: nelle impostazioni di accesso di Windows puoi far sì che il computer richieda di nuovo la password dopo un periodo di inattività, e puoi impostare lo screensaver in modo che chieda l'accesso al ritorno. Windows Hello offre anche il **blocco dinamico**: il computer si blocca quando il telefono collegato via Bluetooth si allontana.

3.2 Sguardi indiscreti e post-it

Il post-it con la password attaccato al monitor è un classico. Ma anche l'elenco delle iscrizioni lasciato accanto alla tastiera, o lo schermo orientato verso la sala d'attesa, sono falle di sicurezza. Alcuni accorgimenti semplici:

- orienta lo schermo in modo che non sia visibile da chi entra o da chi aspetta;
- metti sotto chiave i documenti con dati personali quando non servono;
- usa un gestore di password al posto dei foglietti (lezione cinque);
- se lavori in treno o al bar, valuta una pellicola «privacy» per lo schermo, che restringe l'angolo di visione.



Blocca lo schermo e custodisci fogli e credenziali.

3.3 Un account normale per il lavoro di ogni giorno

Windows distingue tra account **amministratore** (può installare programmi e cambiare impostazioni di sistema) e account **standard**. Per il lavoro quotidiano conviene un account standard: se un malware si insinua, ha meno poteri per fare danni. Quando devi installare qualcosa, Windows ti chiede la conferma con la password di amministratore, ed è proprio quel momento di pausa il vantaggio.

3.4 La cifratura: se il computer viene perso o rubato

Immagina che il portatile di una collaboratrice, con gli elenchi dei partecipanti a un corso, venga rubato dall'auto. Se il disco **non è cifrato**, chi lo ruba può estrarlo, collegarlo a un altro computer e leggere tutto, anche se Windows aveva una password. Il codice di accesso protegge Windows, non i file sul disco.

La **cifratura** trasforma i dati in un codice illeggibile, che si sblocca solo con la chiave giusta. Chi non ha la chiave vede soltanto caratteri senza senso. In Windows lo strumento si chiama **BitLocker** ed è disponibile nelle edizioni **Windows Pro** (e superiori). Le edizioni Home hanno una funzione simile, chiamata crittografia del dispositivo, che dipende dall'hardware del computer.



La cifratura protegge i dati sul disco sottratto.

LA CHIAVE DI RIPRISTINO NON VA PERSA

Quando attivi la cifratura, Windows ti dà una **chiave di ripristino**: serve per sbloccare il disco se qualcosa va storto. Salvala in un posto sicuro **fuori dal computer** (per esempio nel tuo account o stampata e custodita). Senza chiave e senza accesso, i dati cifrati sono persi anche per te. Per questo il backup (lezione sette) resta indispensabile.



Conserva la chiave di ripristino separatamente dal computer.

Per sapere se il tuo computer è già cifrato, cerca nelle impostazioni la voce dedicata (per Windows Pro, scrivi «BitLocker» nella ricerca; per Home, controlla la sezione sulla crittografia dei dispositivi in Privacy e sicurezza). Se non sei sicuro, chiedi a chi segue l'informatica: è una scelta da fare con calma, perché cambia l'organizzazione dei dati.

4. Wi-Fi pubbliche e reti di casa e d'ufficio

Una rete Wi-Fi gratuita in stazione è comodissima. È anche una sala d'attesa dove non sai chi siede accanto a te.

Quando ti colleghi a una rete Wi-Fi pubblica, i tuoi dati viaggiano nella stessa rete di sconosciuti. Se la rete è aperta, o gestita male, chi è collegato può tentare di intercettare il traffico o di farti collegare a una rete falsa con un nome quasi uguale a quella vera: per esempio «Stazione_Free_WiFi» al posto di quella ufficiale.

4.1 Che cosa è prudente fare, in pratica

Situazione	Cosa è ragionevole	Cosa evitare
Leggere notizie, cercare un orario	Va bene	Niente di particolare
Accedere alla posta o al gestionale	Meglio il telefono come punto di accesso (hotspot personale)	Entrare con password su una rete sconosciuta
Operazioni bancarie o pagamenti	Rete dati del telefono o rete fidata	Qualunque Wi-Fi pubblica
Scaricare o inviare documenti con dati di persone	Solo da rete fidata, con VPN se la tua organizzazione la fornisce	Farlo dal bar con il Wi-Fi gratuito

Un criterio semplice: più il dato è delicato, meno ti fidi della rete.



Scegli una rete fidata per le attività di lavoro delicate.

Due precisazioni oneste. Oggi la maggior parte dei siti usa una connessione cifrata (il lucchetto accanto all'indirizzo, *HTTPS*), che rende molto più difficile leggere il traffico anche sulle reti pubbliche. Non è però una garanzia contro le reti false o i siti trappola. E una **VPN** (*virtual private network*, rete privata virtuale: un tunnel cifrato tra il tuo dispositivo e un server di fiducia) aiuta, ma solo se è di un fornitore serio e se la usi davvero.



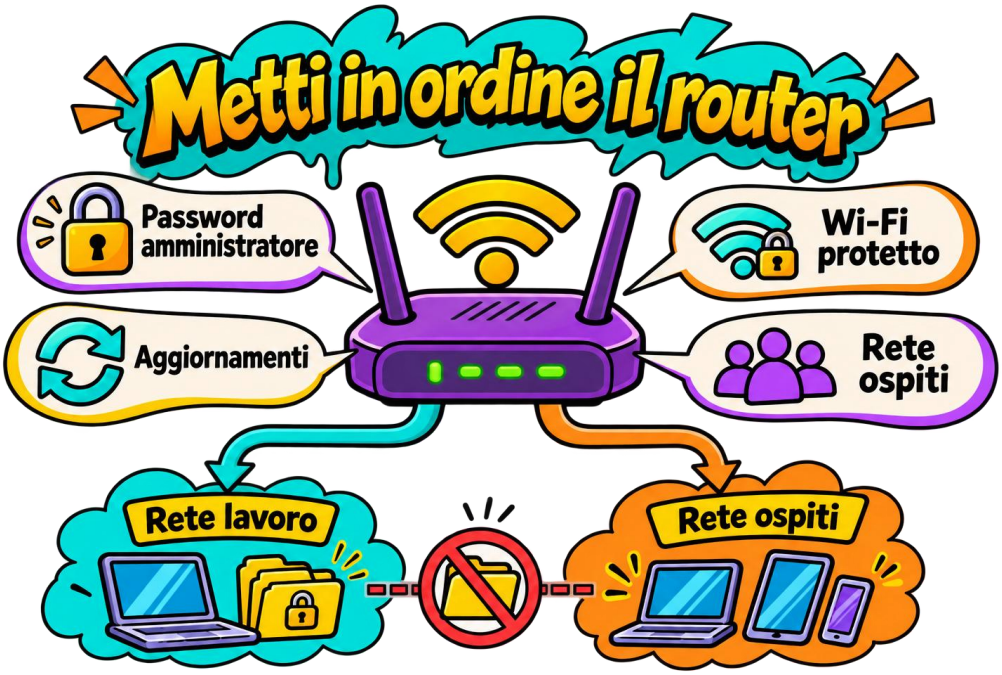
La cifratura aiuta, ma resta necessario verificare rete e destinazione.

4.2 Le buone abitudini quando sei fuori

- se Windows ti chiede che tipo di rete è, scegli **pubblica** per ogni rete che non è casa tua o il tuo ufficio: il firewall sarà più rigoroso;
- disattiva la condivisione automatica di file e stampanti sulle reti pubbliche;
- chiedi al personale il nome **esatto** della rete e non fidarti dei nomi simili;
- dopo l'uso, scollegati e fai «dimentica rete», per non riconnetterti da solo in futuro;
- preferisci i dati del telefono quando devi lavorare su cose riservate.

4.3 E la rete del tuo ufficio?

Il router, la scatola che porta internet in ufficio, è la porta d'ingresso della tua rete. Tre controlli che valgono per studio e casa: cambia la password di amministrazione predefinita (quella stampata sull'etichetta); imposta il Wi-Fi con la cifratura più recente disponibile (WPA3, oppure WPA2 se il dispositivo non supporta altro) e una password lunga; tieni aggiornato il software del router, ricorrendo al tuo fornitore di connessione se non sai come fare.



Proteggi il router e separa gli ospiti dalla rete di lavoro.

Se ospiti clienti o fornitori, usa la **rete ospiti** del router: dà loro internet senza aprire la porta ai computer dello studio.

5. Chiavette USB e supporti sconosciuti

Una chiavetta trovata nel parcheggio è un regalo. Il problema è che nessuno sa da chi.

Una **chiavetta USB** è un piccolo supporto di memoria che colleghi al computer. Proprio perché è comodissima, è anche un classico veicolo di malware. Chi vuole colpire un'organizzazione a volte lascia chiavette in giro, con etichette invitanti («Stipendi», «Foto della festa»), contando sulla curiosità.

Alcuni dispositivi, inoltre, sembrano chiavette ma si comportano da tastiera: appena li colleghi, **digitano da soli** comandi veloci sul computer. Non c'è nulla da cliccare. Per questo l'unica regola sicura è non collegare supporti di origine ignota.



Che cosa fare se trovi una chiavetta sconosciuta

5.1 Il caso della chiavetta in sala d'attesa

In una piccola clinica, un'infermiera trova una chiavetta nella sala d'attesa. Sul portachiavi c'è scritto «Referti». Con le migliori intenzioni (restituirla al proprietario!) la infila nel computer della reception, per capire di chi sia. È esattamente ciò che l'attaccante sperava.

Il comportamento giusto è semplice: non la collega, la consegna al responsabile, che la mette da parte o la fa analizzare da chi sa come, in un computer separato dalla rete e senza dati.

5.2 Quando devi usare le tue chiavette

- usa solo chiavette che conosci, comprate da te o fornite dall'organizzazione, non regali di fiere o promozioni;
- se ci metti dati di persone, **cifra la chiavetta** (BitLocker To Go, in Windows Pro, protegge anche i supporti USB) e usa una password lunga;
- non lasciarle in giro, e non usare la stessa chiavetta tra il computer di casa e quello dell'ufficio senza una buona ragione;
- una chiavetta non è un backup: si perde e si rompe facilmente (lezione sette);
- per scambiare un file con un cliente, preferisci un servizio di condivisione protetto da password.



Non collegare supporti ignoti; proteggi quelli autorizzati.

IN SINTESI

Aggiorna, controlla Sicurezza di Windows, blocca lo schermo con Windows più L, cifra il disco, diffida del Wi-Fi pubblico e delle chiavette trovate.

Esercitazione pratica

Una breve esercitazione da fare sul computer che usi di più: un piccolo «tagliando» di sicurezza, con quello che Windows 11 ti mette già a disposizione.

1. Apri Impostazioni, vai su Windows Update e controlla che non ci siano aggiornamenti in attesa. Se serve, riavvia il computer.
2. Vai su Privacy e sicurezza, poi su Sicurezza di Windows, e apri il programma.
3. Guarda la schermata «Sicurezza in breve»: annota quali aree hanno la spunta verde e quali no.
4. Nella sezione «Protezione da virus e minacce» verifica che la protezione in tempo reale sia attiva e avvia una scansione rapida.
5. Nella sezione «Protezione firewall e della rete» controlla che il firewall sia attivo.
6. Prova la scorciatoia Windows più L: blocca lo schermo, poi rientra con il tuo PIN o la tua password.
7. Cerca «BitLocker» o la crittografia del dispositivo e annota se il tuo disco risulta cifrato o no, senza cambiare nulla prima di aver sentito chi segue l'informatica.
8. Scrivi tre righe di regole per la tua postazione: dove metti i documenti, quando blocchi lo schermo, cosa fai con una chiavetta sconosciuta.

CONTROLLA DI AVER FATTO COSÌ

Windows Update non ha aggiornamenti in attesa?

Antivirus e firewall risultano attivi?

Sai bloccare lo schermo con una sola mano, senza pensarci?

Hai annotato lo stato della cifratura, senza toccare nulla di non necessario?

Le domande che arrivano in aula

Basta Microsoft Defender o devo comprare un altro antivirus?

Per un uso normale la protezione inclusa in Windows 11 è una base valida, se resta attiva e aggiornata. Un prodotto a pagamento può aggiungere funzioni (gestione centrale, più dispositivi) utili soprattutto alle organizzazioni più grandi. Nessun antivirus, in ogni caso, sostituisce la prudenza con link e allegati.

Gli aggiornamenti rallentano il computer: posso rimandarli?

Puoi sceglierne il momento, per esempio lasciando che il riavvio avvenga a fine giornata. Rimandarli a lungo è però rischioso, perché ogni falla non corretta resta aperta. Meglio un riavvio programmato che settimane di esposizione.

Windows Home ha BitLocker?

BitLocker nella sua forma completa è in Windows Pro e superiori. Molti computer con Home hanno la crittografia del dispositivo, se l'hardware lo permette. Controlla nelle impostazioni o chiedi a chi segue l'informatica: dipende dal modello.

Posso usare il Wi-Fi dell'hotel per la posta di lavoro?

Meglio evitarlo, o usare la rete dati del telefono. Se non hai alternative, accedi solo a siti con il lucchetto (HTTPS), attiva la verifica in due passaggi e, se la tua organizzazione te la fornisce, usa la VPN.

Ho inserito una chiavetta sconosciuta: che cosa faccio?

Non farti prendere dal panico, ma agisci subito: scollega il computer dalla rete (togli il cavo o disattiva il Wi-Fi), avvisa il responsabile informatico e non continuare a lavorare. Vedi la lezione nove per i passi da fare.

Basta il blocco dello schermo, perché cifrare il disco?

Sono due protezioni diverse. Il blocco ferma chi si siede alla tua scrivania. La cifratura ferma chi porta via il computer o il disco. Per i portatili, che si perdono e si rubano, sono tutte e due consigliate.

Glossario

Termine	Che cosa significa
Aggiornamento	Una versione corretta di un programma che chiude le falle note.
Antivirus	Programma che cerca e blocca il software dannoso (malware).
BitLocker	Lo strumento di cifratura del disco incluso in Windows Pro e superiori.
Cifratura	La trasformazione dei dati in un codice illeggibile, sbloccabile solo con la chiave giusta.
Falla di sicurezza	Un errore in un programma che un attaccante può sfruttare per entrare nel computer.
Firewall	Il «muro» che controlla il traffico di rete in entrata e in uscita dal computer.
Sicurezza di Windows	L'applicazione di Windows 11 che raccoglie antivirus, firewall e altri controlli, basata su Microsoft Defender.
VPN	Rete privata virtuale: un tunnel cifrato tra il tuo dispositivo e un server di fiducia.
Wi-Fi pubblica	Rete senza fili aperta a chiunque, come quelle di stazioni, bar e alberghi.

Per approfondire

Microsoft, documentazione su Sicurezza di Windows e Microsoft Defender - funzioni e aree dell'applicazione

Microsoft, documentazione su BitLocker e sulla crittografia del dispositivo - edizioni di Windows e chiave di ripristino

Microsoft, ciclo di vita di Windows 10 - data di fine supporto del 14 ottobre 2025

Agenzia per la cybersicurezza nazionale (acn.gov.it) - materiali di sensibilizzazione su aggiornamenti e uso sicuro dei dispositivi

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. I nomi dei menu sono quelli di Windows 11 in italiano e possono cambiare leggermente con gli aggiornamenti: se non trovi una voce, usa la casella di ricerca di Windows. Le funzioni (BitLocker, crittografia del dispositivo) dipendono dall'edizione di Windows e dal computer. L'Agenzia per la cybersicurezza nazionale è l'autorità italiana per la sicurezza informatica.