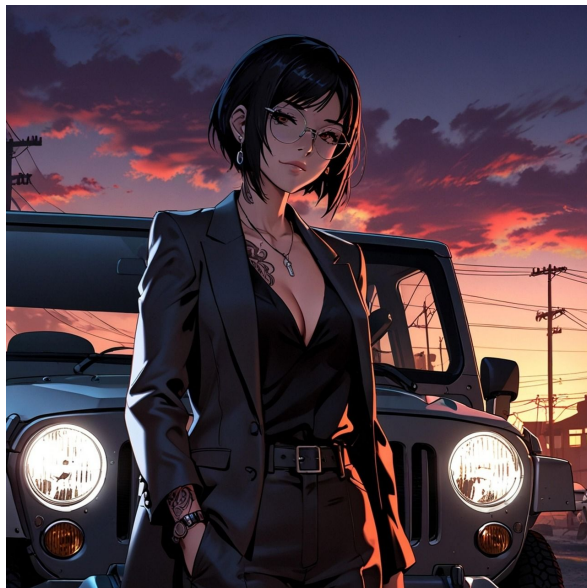




Cifrare i dispositivi



Perché cifrare i dispositivi

Immagina di perdere il tuo laptop con tutti i dati dei clienti, oppure che ti rubino lo smartphone con le foto personali e le email di lavoro.

La crittografia è l'unica vera protezione che **rende i tuoi dati illeggibili a chiunque non abbia la password.**

In troppe occasioni professionisti e piccole aziende devono affrontare violazioni evitabili semplicemente perché "non ci avevano pensato".

La crittografia non è più roba da esperti: oggi è semplice come attivare un interruttore.

5 vantaggi immediati

- **Protezione** totale in caso di furto o smarrimento: anche se qualcuno ruba il tuo dispositivo, i dati rimangono inaccessibili senza la password
- **Conformità normativa**: rispetti automaticamente molti requisiti del GDPR sulla protezione dei dati personali
- **Tranquillità** negli spostamenti: puoi viaggiare e lavorare ovunque senza preoccuparti di controlli o verifiche sui tuoi dispositivi
- **Protezione dalle riparazioni**: anche portando il dispositivo in assistenza, i tecnici non possono accedere ai tuoi file personali
- **Valore legale**: in caso di incidenti, dimostrare di aver adottato misure di sicurezza adeguate può fare la differenza



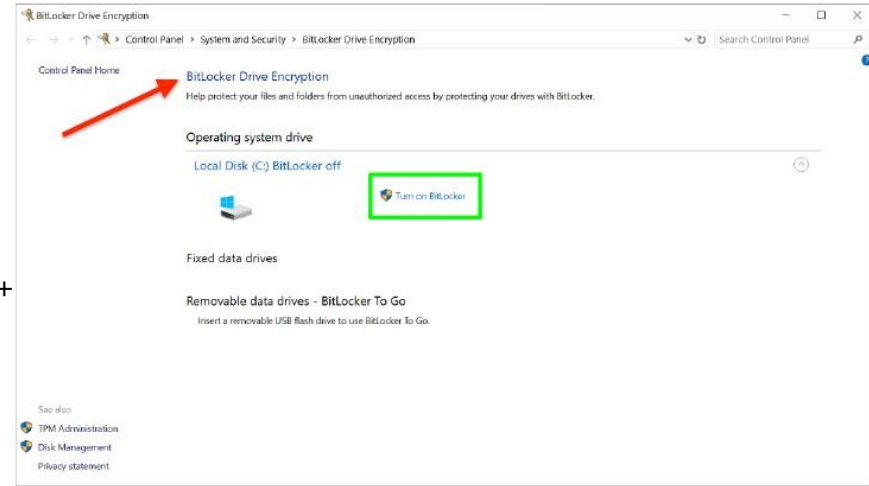
Computer: Windows e bitlocker

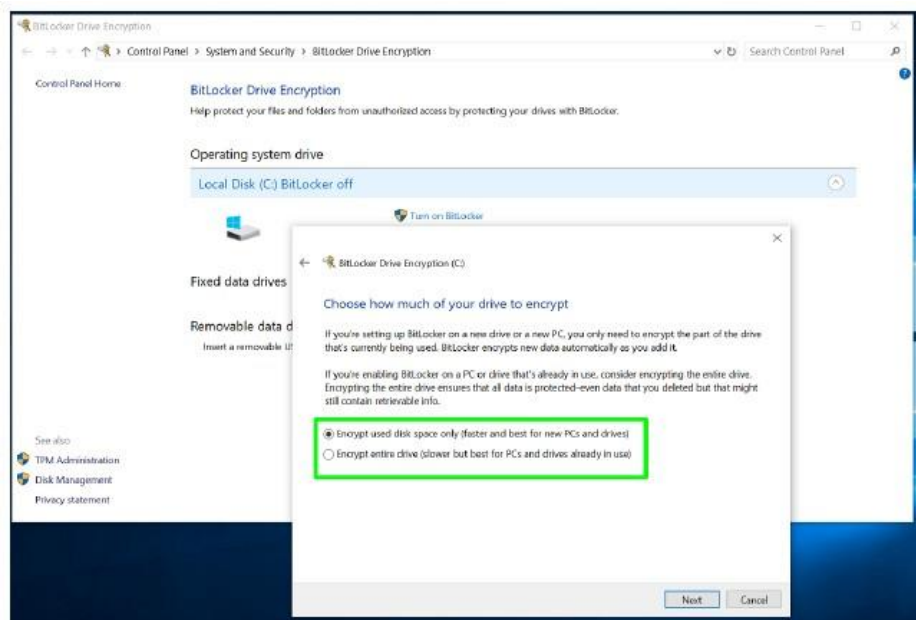
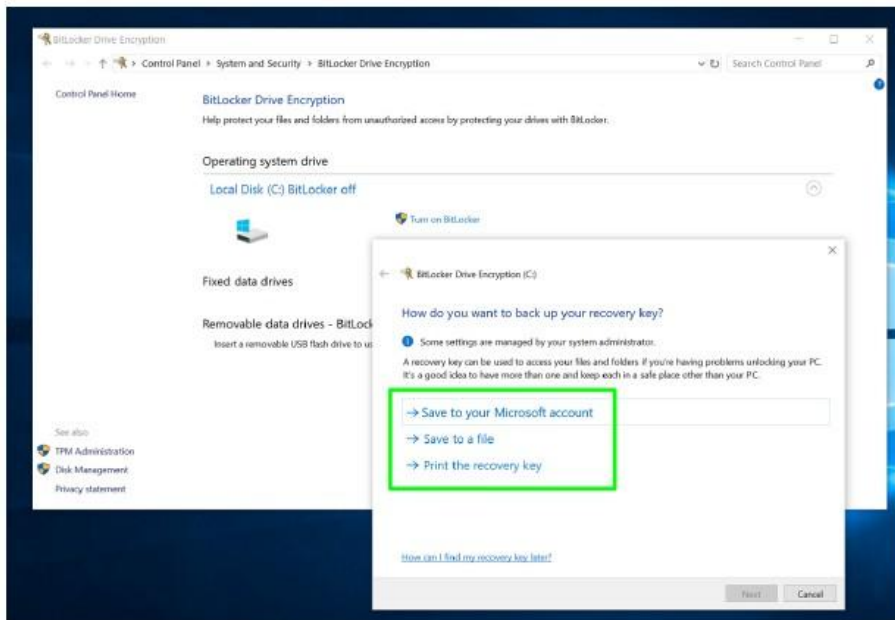
BitLocker è già incluso in Windows (versioni Pro, Enterprise ed Education)



Procedura:

- Vai su Pannello di controllo → Sistema e sicurezza → Crittografia unità BitLocker
- Clicca su Attiva BitLocker accanto al disco che vuoi proteggere
- Scegli come eseguire il backup della chiave di ripristino (raccomando: salva su account Microsoft + stampa su carta)
- Seleziona "Crittografia solo lo spazio utilizzato" per installazioni nuove, "Crittografia l'intera unità" per computer già in uso
- Avvia la crittografia - il processo può durare da 30 minuti a diverse ore





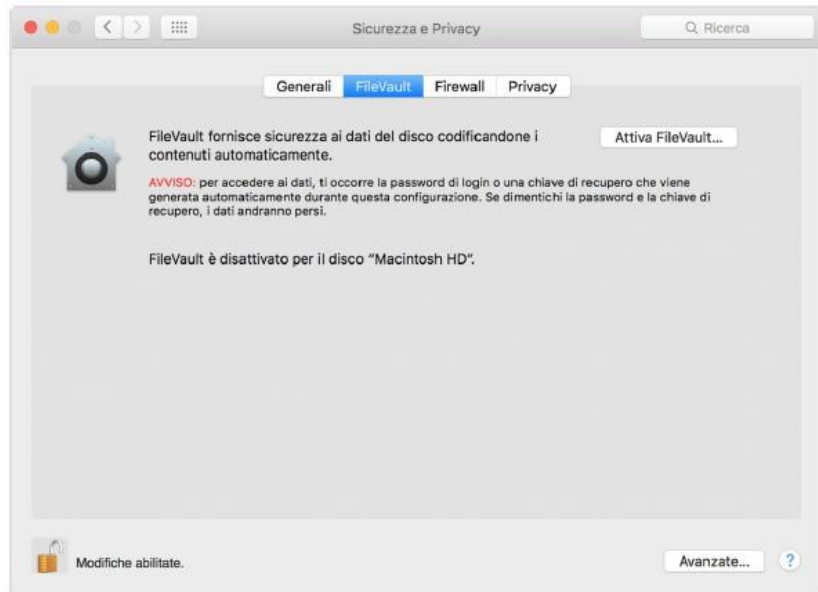
Nota importante : conserva sempre la chiave di ripristino in un posto sicuro.
Senza quella, se dimentichi la password, i dati sono persi per sempre.

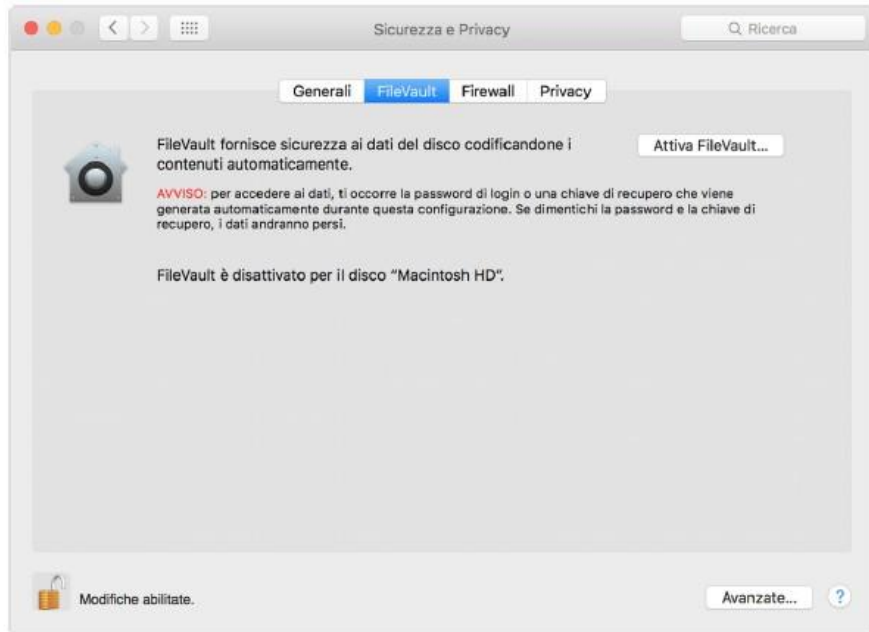
Computer: Mac e filevault

FileVault è integrato in macOS ed è molto semplice da attivare.

Procedura:

- Vai su Preferenze di Sistema → Sicurezza e Privacy → FileVault
- Clicca su Attiva FileVault
- Scegli se consentire il reset della password tramite account iCloud oppure creare una chiave di ripristino
- Attendi che la crittografia sia completata (può richiedere diverse ore, ma puoi continuare a usare il Mac)





La gestione degli utenti è fondamentale: ogni utente del Mac deve inserire la propria password per sbloccare il disco.

iPhone e iPad - Crittografia automatica

Su dispositivi Apple moderni, **la crittografia è attiva di default** quando imposti un codice di sblocco.

Verifica che sia attiva:

1. **Impostazioni** → **Face ID e codice** (o **Touch ID e codice**)
2. Scorri verso il basso: dovresti vedere "**La protezione dati è abilitata**"
3. Se non c'è, attiva un codice di sblocco di almeno 10 cifre

Per massima sicurezza:

- Usa un codice di almeno 10 cifre (meglio se alfanumerico)
- Attiva "**Cancella dati dopo 10 tentativi errati**" nelle impostazioni Face ID/Touch ID



Smartphone e Tablet Android

La procedura varia leggermente tra i produttori, ma il principio è sempre lo stesso.

Procedura generale:

1. **Impostazioni** → **Sicurezza** (o **Biometria e sicurezza**)
2. Cerca "**Crittografia**" o "**Crittografia dispositivo**"
3. Assicurati che il dispositivo sia carico almeno all'80% e collegato alla corrente
4. Avvia il processo (può durare da 1 a 4 ore)

Su Samsung: Impostazioni → Biometria e sicurezza → Altre impostazioni di sicurezza → Crittografia dispositivo

Su Google Pixel: la crittografia è attiva di default sui dispositivi recenti

Nota: una volta attivata la crittografia su Android, è molto difficile disattivarla senza perdere tutti i dati.





Consigli pratici

Password e codici di accesso

Mai usare password banali.

La crittografia più forte del mondo è inutile se usi "123456" come password.

Quindi:

- Password di almeno 12 caratteri con lettere, numeri e simboli
- Codici di sblocco di almeno 10 cifre sui dispositivi mobili
- Considera l'uso di un gestore di password per generare e ricordare password complesse



Backup delle chiavi di ripristino

Fondamentale:

stampa le chiavi di ripristino e conservale in un posto sicuro fisico (cassetta di sicurezza, cassaforte).

Salvale anche digitalmente in un servizio cloud affidabile, ma sempre in un file protetto da password.



I dati dei clienti sono una responsabilità seria

La crittografia non è solo una buona pratica, è spesso un obbligo contrattuale e normativo.

Coordina con l'IT aziendale se hai qualsiasi dubbio.

Documenta le misure adottate

Tenere traccia delle misure di sicurezza implementate può essere utile per dimostrare la dovuta diligenza in caso di audit o verifiche.



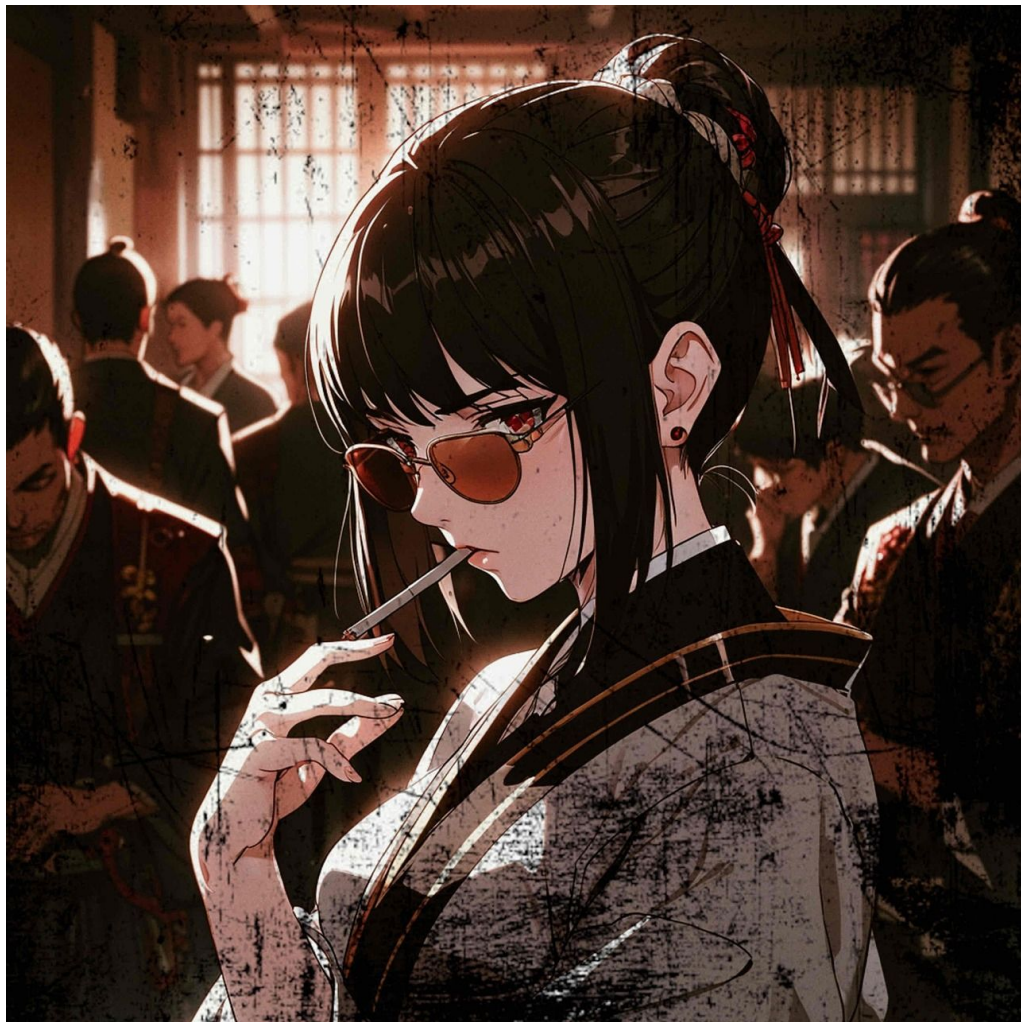
Domande e risoluzione problemi

La crittografia rallenta il dispositivo? Sui dispositivi moderni (ultimi 5-6 anni) l'impatto sulle prestazioni è trascurabile. Su dispositivi molto vecchi potrebbe esserci un leggero rallentamento.

Posso disattivare la crittografia se cambio idea? Su Windows e Mac sì, ma il processo richiede tempo. Su molti dispositivi Android è più complicato e può richiedere un reset completo.

Cosa succede se dimentico la password? Con la chiave di ripristino puoi recuperare l'accesso. Senza quella, i dati sono persi definitivamente. Per questo il backup della chiave è fondamentale.

La crittografia protegge anche da virus e malware? No, la crittografia *protegge solo dall'accesso fisico non autorizzato*. Serve comunque un buon antivirus e buone pratiche di sicurezza informatica.





| BROGL | Δ
_STUDIO LEGALE | SL3