

Reinstallazione di Windows 10

Vi consigliamo di utilizzare Windows 11!

Se cercate le indicazioni per Windows 11, trovate tutto l'elenco [qui \(https://www.ebas.ch/it/reinstallazione-di-windows-11/\)](https://www.ebas.ch/it/reinstallazione-di-windows-11/)

Il vostro computer è stato infettato dal malware? Non sapete bene come reinstallare il sistema nel modo giusto? Queste istruzioni vi mostrano passo dopo passo come rimettere in sesto il PC limitando al contempo il rischio di una nuova infezione.

Queste istruzioni si rivolgono agli utenti privati e sono scritte in termini semplici e generali. Alcuni passaggi, tuttavia, presuppongono un certo grado di competenza tecnica. In caso di dubbi, rivolgetevi a uno specialista per ricevere un supporto competente.

Per reinstallare correttamente il sistema operativo secondo queste istruzioni, avrete bisogno di una **licenza valida** e di un **supporto di installazione di Windows 10** (su unità USB o DVD).

NOTA: se non avete a disposizione un supporto di installazione del sistema operativo, potete crearlo su un computer che esegue Windows 10. Assicuratevi tuttavia di farlo su un PC privo di malware e non sul sistema infetto. Per creare il supporto di installazione, è necessario scaricare ed eseguire l'apposito strumento messo a disposizione da Microsoft (Media Creation Tool). [Qui \(https://www.microsoft.com/it-it/software-download/windows10\)](https://www.microsoft.com/it-it/software-download/windows10) trovate maggiori informazioni su come usarlo.

Fase 1: Scollegare il PC dalla rete

- Se il vostro PC è collegato alla rete tramite cavo, è sufficiente scollegare il cavo di rete.
- Se utilizzate una rete senza fili (WLAN), attivate la modalità aereo (clic sull'icona di rete in basso a destra nella barra delle applicazioni → clic sul pulsante della modalità aereo).

Fase 2: Salvataggio dei dati personali e della licenza

- Collegate un supporto di memorizzazione esterno (un disco rigido esterno) tenendo premuto il tasto «Maiusc» e [salvate tutti i vostri dati personali \(https://www.ebas.ch/it/1-salvare-i-dati/\)](https://www.ebas.ch/it/1-salvare-i-dati/). Non utilizzate il vostro supporto di backup «solito», ma se possibile procuratevene uno nuovo, completamente vuoto.

NOTA: il malware presente sul PC potrebbe infettare anche il supporto di memorizzazione esterno e i dati che contiene. In particolare, i malware sfruttano la funzione di esecuzione automatica per diffondersi sui supporti esterni (unità USB ecc.). Disattivare temporaneamente la funzione di esecuzione automatica è relativamente semplice: è sufficiente tenere premuto il tasto «Maiusc» della tastiera mentre si collega al PC il supporto di memorizzazione esterno, e rilasciarlo solo dopo alcuni secondi. In questo modo si impedisce che Windows esegua automaticamente i programmi e i file contenuti sul supporto esterno.

Se proseguirete formattando il PC – come è caldamente consigliato in caso di attacco di malware – potrebbe andare persa anche la vostra licenza. Quindi è importante metterla prima al sicuro.

- Fate clic sul logo di Windows in basso a sinistra sulla barra delle applicazioni.
- Aprite una finestra del prompt dei comandi digitando «cmd» e premendo il tasto Invio (Enter).
- Digitate il comando «wmic path softwarelicensing get OA3xOriginalProductKey» e premete Invio (Enter). Verrà visualizzata sullo schermo la vostra licenza.
- Annotatela in un programma di elaborazione testi e salvatela sul supporto di memorizzazione esterno.

NOTA: se il comando indicato non visualizza nulla, significa che nell'UEFI/BIOS non è salvata nessuna licenza. In tal caso la licenza deve essere stata inserita manualmente ed è molto probabile che sia riportata su un adesivo apposto sul PC. In caso contrario, potete estrarla dal file di registro (Registry) del PC utilizzando un programma come [Magical Jelly Bean Keyfinder](https://www.magicaljellybean.com/keyfinder/) (<https://www.magicaljellybean.com/keyfinder/>) o [Windows Product Key Viewer](https://www.heise.de/download/product/WindowsProductKeyViewer) (<https://www.heise.de/download/product/WindowsProductKeyViewer>).

Fase 3: Pulizia della GPT o dell'MBR

Alcuni programmi dannosi si insediano nella GPT (tabella delle partizioni GUID) o nell'MBR (Master Boot Record) del computer. Per questo motivo è consigliabile ripulirle sovrascrivendo i dati che contengono.

NOTA: l'MBR (Master Boot Record) è uno stile di partizione datato ma comunque utilizzato ancora frequentemente. La GPT (tabella delle partizioni GUID) è il nuovo stile di partizione, sempre più diffuso.

- Collegate il supporto di installazione di Windows 10 (unità USB o DVD) al PC e riavviate.
- Se in seguito al riavvio il PC non si avvia dal supporto di installazione di Windows 10, impostate l'unità desiderata come prima periferica nell'UEFI/BIOS (la procedura è descritta nel manuale della scheda madre). In alternativa, subito dopo aver avviato il PC si può premere il tasto funzione «F8». Si aprirà il Boot Manager, che consente di selezionare l'unità di avvio desiderata.
- Premete un tasto qualsiasi quando viene chiesto di farlo.
- Nella procedura di installazione di Windows premete la combinazione di tasti «Maiusc» e «F10» per aprire una finestra del prompt dei comandi.
- Aprite lo strumento diskpart digitando il comando «diskpart» e premendo il tasto Invio (Enter).
- Digitate il comando «list disk» e premete Invio (Enter).
- Digitate il comando «select disk <disk number>» e premete Invio (Enter).

NOTA: sostituite l'indicazione con il numero del disco in cui verrà installato Windows. Attenzione: se si seleziona l'unità USB con il supporto di installazione di Windows 10, verrà cancellato tutto il contenuto!

- Ripulite la GPT o l'MBR digitando il comando «clean [-all]» e premendo il tasto Invio (Enter).

ATTENZIONE: la cancellazione del contenuto della GPT o dell'MBR eliminerà tutti i dati presenti sul sistema!

- Chiudete la finestra del prompt dei comandi e spegnete il PC. Lasciate il supporto di installazione di Windows 10 (unità USB o DVD) connesso al PC.

NOTA: [qui](https://docs.microsoft.com/de-de/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style) (<https://docs.microsoft.com/de-de/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style>) trovate ulteriori informazioni sull'eliminazione di GPT e MBR e sulla reinstallazione di Windows 10.

Fase 4: Reinstallazione di Windows 10

- Avviate il PC.
- Se in seguito al riavvio il PC non si avvia dal supporto di installazione di Windows 10, impostate l'unità desiderata come prima periferica nell'UEFI/BIOS (la procedura è descritta nel manuale della scheda madre). In alternativa, subito dopo aver avviato il PC si può premere il tasto funzione «F8». Si aprirà il Boot Manager, che consente di selezionare l'unità desiderata.
- Premete un tasto qualsiasi quando viene chiesto di farlo.
- Installate Windows 10 con le impostazioni desiderate.

NOTA: la cancellazione della GPT o dell'MBR ha eliminato anche le partizioni. Createle da zero secondo le vostre preferenze.

ATTENZIONE: durante l'installazione di Windows 10 potete già decidere come configurare alcuni aspetti della protezione dei dati. Vi viene chiesto, per esempio, in che misura desiderate trasmettere a Microsoft i dati di diagnostica. In questa fase potete scegliere soltanto tra «Dati di diagnostica facoltativi» e il profilo «Dati di diagnostica obbligatori». Per impedire che il sistema operativo invii a Microsoft molti dati che preferite non condividere, scegliete l'opzione «Dati di diagnostica obbligatori». Dopo l'installazione di Windows 10 potrete personalizzare alcune impostazioni. Attendete il completamento dell'installazione del sistema operativo e definite le opzioni in seguito. Le nostre istruzioni, contenenti ulteriori informazioni utili sulla protezione dei dati in Windows 10, è disponibile [qui \(https://www.ebas.ch/it/protezione-dei-dati-in-windows-10/\)](https://www.ebas.ch/it/protezione-dei-dati-in-windows-10/).

- Completate l'installazione di Windows 10 con le impostazioni desiderate.
- Collegate quindi il PC a Internet (reinserite il cavo di rete).
- Aggiornate il sistema operativo: fate clic sul logo di Windows in basso a sinistra sulla barra delle applicazioni, digitate «Windows Update» e confermate premendo il tasto Invio (Enter). Fate quindi clic su «Verifica disponibilità aggiornamenti». Ora gli aggiornamenti verranno installati automaticamente.

Fase 5: Installazione e aggiornamento dei programmi

- Installate i programmi desiderati. Aggiornate tutti i programmi e dove possibile attivate la funzione di aggiornamento automatico.

NOTA: prestate attenzione a installare soltanto programmi provenienti da fonti affidabili (come le pagine di Download dei produttori o archivi software come PCtipp, Heise ecc.).

Fase 6: Analisi dei dati

- Tenete premuto il tasto «Maiusc» e collegate al PC il supporto di memorizzazione esterno (disco rigido esterno) contenente i dati salvati in precedenza.

NOTA: se durante il backup dei dati è stato copiato sul supporto di memorizzazione esterno del malware, il PC potrebbe infettarsi di nuovo! Per prevenire questo problema, è indispensabile tenere premuto il tasto «Maiusc» quando si collega il supporto esterno.

- Eseguite un'analisi dell'intero sistema e del supporto di memorizzazione esterno con Microsoft Defender. Se vengono individuati dei file infetti, occorre pulirli o eliminarli!

NOTA: un'alternativa migliore ma più impegnativa rispetto all'analisi del sistema appena installato sarebbe quella di controllare il supporto di memorizzazione esterno con un Live-CD avviabile o un sistema operativo diverso (p. es. Linux, macOS).

Fase 7: Ripristino dei dati

- Copiate i dati del vostro backup dal supporto di memorizzazione esterno al PC.

Fase 8: Che cosa rimane da fare!

- Poiché il malware si impossessa molto frequentemente di nomi utente e password, è assolutamente necessario modificare tutte le password del sistema stesso, come pure tutte le password dei siti Internet (p. es. e-banking, accesso all'e-mail, Facebook ecc.).
- Oltre a questo, controllate attentamente i vostri estratti conto dell'e-banking e delle carte di credito.