FBI unlocks BitLocker thanks to Microsoft: Is Windows encryption still secure?

Microsoft has confirmed it will provide BitLocker keys to the FBI when ordered by a court. The incident in Guam has raised concerns about privacy and data security on Windows.

Microsoft recently confirmed that it continues **to cooperate with law enforcement agencies** when it receives a valid warrant or subpoena – including **providing BitLocker recovery keys** . This information was revealed by Forbes following a federal fraud investigation in Guam, where the FBI used keys provided by Microsoft to unlock **three encrypted laptops** linked to a COVID-19 unemployment benefits scam.

According to Microsoft, the company receives approximately 20 requests for BitLocker keys each year . Microsoft's compliance with legal government requests is nothing new, especially with data stored in its cloud infrastructure. However, this is **the first time Microsoft has publicly confirmed** that it has handed over encryption keys to federal investigators.

For those unfamiliar, **BitLocker** is encryption technology enabled by default on most modern Windows PCs to protect data on the hard drive. During use, Windows often requires users **to back up the 48-digit recovery key** to a Microsoft account. This means Microsoft still has **technical access** to those keys – and may provide them when requested by authorities.

In the Guam case, the FBI stated that they used keys received from Microsoft to **bypass encryption** that federal forensic experts had previously deemed "unbreakable." Court documents also clarified that agencies like Homeland Security Investigations (HSI) **lacked the tools** to crack BitLocker without the specific recovery key.

Microsoft's approach contrasts sharply with competitors like **Apple or Meta** . These companies employ a **zero-knowledge** architecture , where recovery keys are end-to-end encrypted or stored only on the user's device. Therefore, even with a warrant, the company itself **cannot provide the data** .

Following the release of this information, legal experts predict that **the number of requests for BitLocker keys from authorities will increase** . For users who do not want Microsoft to store their keys, you can check at **account.microsoft.com/devices/recoverykey** to see if the key is currently in the cloud.

If security is a higher priority, users are recommended **to switch to storing keys locally** , such as saving them to a physical USB drive or printing them out on paper. This gives you **full control over your encrypted data** , instead of relying on a cloud service.

You finished reading the article "**FBI unlocks BitLocker thanks to Microsoft: Is Windows encryption still secure?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.