

WHY DEVICE ENCRYPTION?



The purpose of file and disk encryption is to protect data stored on a computer or network storage system.

All organizations, including small and midsize businesses (SMBs), that collect personally identifiable information (PII) like names, birthdates, Social Security numbers and financial information must secure that information. An organization can be sued if a computer containing PII is stolen and the information is leaked or shared.

If a laptop is lost or stolen and the files or disk aren't encrypted, a thief can easily steal the information, so it's a good practice to encrypt your sensitive data, if not your entire hard drive.

The thief doesn't even need to know the sign-on password to access the files – it's easy to boot a computer from a USB thumb drive and then access the disks within the computer.



Disk encryption doesn't protect a computer entirely. A hacker can still access the computer over an insecure network connection, or a user can click a malicious link in an email and infect the computer with malware that steals usernames and passwords.

Those types of attacks require additional security controls, like anti-malware software, firewalls and awareness training. However, encrypting a computer's files or the entire disk greatly reduces the risk of data theft.