Ransomware is on the rise in 2025: Here are 6 quick tips to protect your data!

Ransomware attacks often make headlines, and the worst part is that they target ordinary people, not just large corporations.

Ransomware attacks often make headlines, and the worst part is that they target ordinary people, not just large corporations. Cybercriminals are evolving their tactics, but protection doesn't have to be complicated or expensive. These simple tips can help prevent ransomware.

6. Use a reliable antivirus solution

A reliable antivirus solution is the first line of defense against ransomware. While Windows Defender offers good protection, third-party options from Bitdefender, Kaspersky, or Norton offer advanced ransomware protection with real-time monitoring. It's important to choose software that proactively scans for suspicious file behavior, not just known malware signatures.

More importantly, keep your antivirus software up to date. Ransomware evolves every day, and outdated virus definitions leave you vulnerable to new threats. Most antivirus programs update automatically, but double-check those settings. If you realize you've downloaded a virus, up-to-date antivirus software can still help stop the damage before ransomware encrypts your files.

Despite these benefits, performance concerns shouldn't stop you from using antivirus protection. Some security software can slow down your system, but if your PC is running slow after installing antivirus software, check out our guide on how to optimize your PC's performance. Protection is more important than small speed gains, especially when ransomware can destroy everything you've worked on.

You can also use online tools like VirusTotal to scan downloaded files before opening them. This free service checks files with multiple antivirus engines at once. Be especially wary of file types like PDFs and compressed files, which are often used to hide viruses. Executables, scripts, and macro-enabled documents are also popular targets for ransomware distribution.

5. Create regular data backups

Creating regular backups may seem tedious, but it's the best defense against ransomware. The 3-2-1 rule remains the gold standard: Keep three copies of your important data, store them on two different types of media, and keep one copy offline. This strategy works; even if ransomware strikes, you'll have a clean copy to restore from.

Ransomware can't encrypt what it can't access, so you'll need to unplug your external hard drive after the backup is complete. Cloud storage works well for off-site backups, but consider using a service that has versioning to recover data from ransomware that can encrypt files. Fortunately, there are simple, inexpensive ways to back up your data securely.

Automation makes it easier to keep things consistent. Set up a backup schedule so you can back up your entire digital life without having to think about it. Windows File History, Time Machine for Mac, or other third-party solutions can handle this automatically.

Tip: Don't just back up, test. Regular recovery tests ensure that your backups actually work when you need them most.

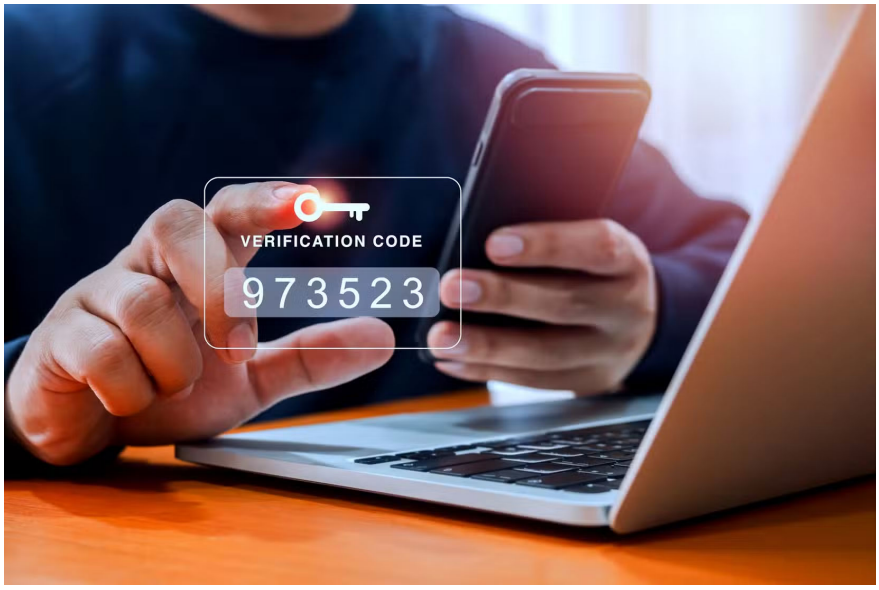
4. Be careful with email attachments and links!

Email is one of the favorite delivery methods for ransomware, and cybercriminals get creative with their tactics. An urgent invoice or shipping notice from an unfamiliar email address can be a cleverly disguised attack. Always verify the sender's address carefully. Hovering over email addresses and links often reveals suspicious domains that don't match the supposed sender.

Before clicking any link or downloading an attachment, pause and think about it. Legitimate companies rarely send unexpected attachments or ask for immediate action via email links. When in doubt, contact the sender through another channel to verify. You can also block phishing emails from your inbox with built-in email filters and security features.

The same caution applies to downloading software. Ransomware often hides in pirated programs, so don't download cracked software — "free" versions could end up losing all your data. Stick to official sources and verified publishers. If an email attachment looks suspicious, delete it. Safety first.

3. Use strong authentication for all accounts



Strong authentication can be a good barrier against ransomware attacks that start with compromised accounts. Using complex, unique passwords for each service will prevent attackers from switching between accounts if one is compromised. Password managers help you manage this because they generate and store strong credentials.

Two-factor authentication (2FA) adds essential protection, but not all methods are created equal. While any 2FA is better than none, relying on SMS 2FA can be risky due to SIM swapping attacks.

Authentication apps like Google Authenticator or Authy offer more secure alternatives, and hardware security keys provide the strongest defense against account takeover attempts.

Just as importantly, don't forget about recovery options. You should guard your backup keys and recovery email with the same vigilance as you do your primary accounts. Ransomware operators often target email accounts first, then use them to reset passwords and gain broader access. Regular security audits to review active sessions and connected applications can help detect unauthorized access early.

2. Segment the network to limit the spread of attacks

Network segmentation may seem technical, but it simply divides your network into separate zones. Think of it as creating compartments – if ransomware infects one area, it can't easily spread to others. This containment

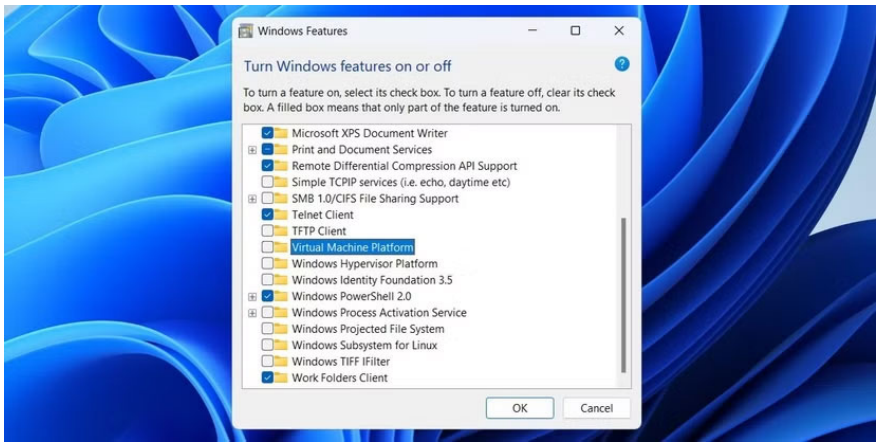
strategy greatly limits damage, especially in home networks with many devices.

Basic network segmentation starts with guest networks. Most modern routers offer this feature, allowing you to create separate networks for visitors or less trusted devices. Put smart home gadgets, security cameras, and IoT devices on separate networks from your computers and phones. That way, a compromised smart light bulb can't gain access to your work laptop.

For even stronger protection, consider using VLANs (Virtual Local Area Networks) to segment your home network. Although a bit more complicated, VLANs create truly separate network segments. You can separate work devices, PCs, and entertainment systems. Some advanced routers and managed switches support this feature without requiring enterprise-grade equipment.

Note: Segmentation works best when combined with strong passwords for each network segment. Change your router's default login credentials, use WPA3 encryption when possible, and keep your router's firmware up to date. These layers make it much harder for ransomware to move laterally.

1. Turn off unnecessary features and services



Every unnecessary service running on your computer is a potential entry point for ransomware. The more features you enable, the larger the attack surface. Reducing this surface by disabling unused services reduces the vulnerabilities that ransomware can exploit to gain initial access.

Remote Desktop Protocol (RDP) is a prime target for ransomware attacks. Turn it off completely unless you really need remote access. File and printer sharing services also pose a risk if left open unnecessarily. Turn off network discovery and public folder sharing if you don't use them, as these features are often enabled by default.

Windows comes with unnecessary Windows programs that can create security vulnerabilities. Services like Windows Script Host, PowerShell remoting, and SMBv1 are often exploited by ransomware. Disable these services through Windows Features or Group Policy unless your job requires them.

Regular checks help maintain security by keeping your system lean. Check your startup programs, background services, and browser extensions regularly. Delete anything you don't recognize or use. The rule is simple: Turn it off if you don't need it. A minimal system provides fewer opportunities for ransomware to establish a foothold.

regularly.