

## Protecting Yourself from Ransomware

Keeping all of your files secure and backing them up may not be something you think of on a daily basis. But with scammers and hackers diligently working to corrupt files and make a quick buck, maintaining your computer's security is vital in today's world. One way your information could be at risk is through ransomware.

### How does ransomware work?

Just like many other viruses and malware, ransomware typically comes from opening infected files on a website or in your email inbox through phishing techniques. For example, you may receive a notice that seems official, stating that you are required to pay an invoice. Once you open the attachment in that email, the ransomware gets to work.

As soon as the ransomware is on your computer, it locks your files and prevents you from accessing them. If you use cloud services or external hard drives, the ransomware could even delete or encrypt files you have stored there. The only thing you'll likely be able to see is a screen telling you to pay a specific amount of money and how to do so. Most cyber criminals prefer to use Bitcoin as their preferred currency, as it allows for anonymity through its transactions, no matter how large they are.

### Know your risk factors

While this devious tech can be found on both PCs and Macs, a majority of the programs are found on PCs, according to technology journalist Dave Johnson, when writing for Business Insider. Additionally, if your email inbox is filled to the brim with spam emails or unknown contacts, you're more likely to unintentionally click on something malicious. If possible, clean your inbox by unsubscribing from mailing lists and check it regularly. If it becomes too overwhelming, you may want to create a new email address entirely and start from scratch.

### How to avoid ransomware

The best method for protecting your files from ransomware is through preventative steps. One of the safest ways to store and backup data is through the use of external hard drives. Because they can be disconnected from the main CPU and used with almost any computer, you can have your files available even if your PC stops working. And if you do fall victim to ransomware, Johnson notes that you can "rollback" your computer to a previous version with the external hard drive, allowing you to avoid losing everything and not having to pay the ransom. Just be sure to disconnect the device when you're done adding files so it can't be infected via something on your PC.

Along with backing up your files regularly, you'll want to be sure your computer has up-to-date, trusted anti-malware software installed. Apple has included its XProtect antivirus software on all Macs since 2009 and it is updated daily with potential threats. If you have a PC, you will likely

need to install antivirus software on your own. Johnson recommends specific anti-ransomware tools like Check Point ZoneAlarm Anti-Ransomware, Malwarebytes 4, and Acronis Ransomware Protection. Stay on top of patches and updates that become available, as cybercriminals are constantly working to get around antivirus software.

As always, the top tip for avoiding viruses is to not click on unknown links or emails. By abiding by that and the rest of these methods, you should be well on your way to avoiding paying a fee to access your own files.