How to Prevent and Recover from Ransomware

Ransomware is a hack with teeth, an attack aimed to cause extreme financial pain to its victims.

While the idea of getting held up for cryptocurrency in the digital wild west is scary, there are some steps you can take to significantly reduce the likelihood of an attack. We'll also explain what to do if your data is currently being held for ransom.

Essentially, ransomware is malicious software that encrypts a victim's data, and the criminals who infected the victim's device demand a ransom for the data's release. Typically, ransomware (like other forms of malware) infiltrate systems through deceptive emails (i.e., phishing attacks) or software vulnerabilities, causing devastating consequences for individuals and businesses. Individuals can face emotional distress and data loss, while businesses suffer operational disruptions, financial damages, and reputational harm.

Ransomware attacks are, unfortunately, common news headlines. Huge corporations, large school districts, and governments have dealt with sickingly effective ransomware operations. The WannaCry ransomware attack in 2017 infected an estimated 200,000 computers around the world and ended up costing a total of $4 billion, according to recent analysis. According to Verizon's 2023 Data Breach Investigations Report, ransomware is now the second-most common cybersecurity incident and is now being present in almost 16% of all incidents (Verizon found that most common is a Denial of Service attack).

We'll explain how you can mitigate your risk by adopting some simple-to-learn cybersecurity behaviors. Early detection through antivirus and intrusion systems is vital, and you can back up your data effectively to facilitate recovery without paying any ransom. Following these guidelines strengthens defenses and safeguards against the dire consequences of ransomware.

How to prevent ransomware attacks

As you might suspect, preventing a ransomware attack is easier than dealing with the frustrating fallout after it has happened. By practicing some good cyber hygiene behaviors, you exponentially increase your chances of staying off the ransomware radar.

- Lock down your login with strong passwords, a password manager, and multi-factor authentication
- Back up your data regularly to the cloud or an external drive (or both!)
- Use up to date antivirus software
- Update your software regularly (turning on automatic updates is easiest!)
- Avoid the phishing bait

- Most ransomware attacks start as a phishing message, which is when a cybercriminal sends you an email, message, social media post, or text that includes a malicious download or link. Here are some common signs of a phishing message:
    - Does it contain an offer that's too good to be true?
    - Does it include language that's urgent, alarming, or threatening?
    - Is it poorly crafted writing riddled with misspellings and bad grammar?
    - Is the greeting ambiguous or very generic?
    - Does it include requests to send personal information?
    - Does it stress an urgency to click on unfamiliar hyperlinks or attachments?
    - Is it a strange or abrupt business request?
    - Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.

How to detect ransomware

Generally, the people behind a ransomware attack want to get your attention, but ransomware might not be so obvious at first. Look out for:

- A ransom note or message on your screen demanding payment to unlock your data or device
- An inability to access your files, folders, software, or apps
- A change in the file extensions or names of your encrypted files
- A noticeable slowdown or malfunction of your device or network
- An increase in network traffic or CPU usage

How to recover from a ransomware attack

If you suspect a device is infected with ransomware, you want to act fast but remain collected. If at work, contact the Metro ITS Help Desk ASAP. Don't start talking to the digital hostage-takers but reach out for help from the cybersecurity experts in Metro ITS, law enforcement, and others. Here are some techniques to take on ransomware and get your data back in your personal life:

1. **Stay calm and focused.** Hackers want to send you into a state of panic – don't let them! By maintaining your cool, you can make more informed decisions. Even if the situation is dire, a calm approach will ensure you are taking stock of all your options.
2. **Take a photo of the ransomware message for evidence.**
3. **Quarantine your device by disconnecting from Wi-Fi and unplugging any ethernet cables.** Remove any external hard drives or thumb drives ASAP because many ransomware programs will try to corrupt your backups.
4. **Check your antivirus software to see if it has decryption tools to remove the ransomware.** Depending on the malware, your antivirus software might be able to decrypt your data without requiring you to pay a ransom to anyone. Even if you can't undo the encryption, the software might be able to identify the strain of ransomware which will help with the investigation.
5. **Wipe your hard drive and reinstall your operating system.** Ideally, you will have backed up your files on the cloud or an external hard drive. Wiping your hard drive will eliminate everything you saved on your computer, but it might also eliminate the ransomware program, too.
6. **Report the ransomware attack to your local police department, the FBI, CISA, and the U.S. Secret Service.**

7. **Should you pay the ransom?** We recommend never paying out during a ransomware attack because it only fuels more cybercrime. If you have exhausted every option and you believe the files being held hostage are worth the ransom, consider that there is no guarantee that the cybercriminals will decrypt your files even if you pay. Consult with law enforcement, cybersecurity professionals, and legal advisors to assess the situation and make an informed decision.

8. **Once you have control of your device again, change all your passwords because the hackers could've looked through passwords saved on your web browser or elsewhere.**

You have the power to prevent & beat ransomware

While ransomware can seem like one of the scariest things that can happen to you online, you can work to prevent it with some simple cybersecurity habits. Now that you know what to do, you can work fast to mitigate any attack if ransomware turns its ugly eye your way. Most importantly, remember that you are not alone when dealing with an attack – reach out to experts and law enforcement.

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

STOP | THINK
CONNECT™

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.