How to Survive a Ransomware Attack

Unlike white-water rafting, ransomware is an adrenaline rush no one wants to have.

Picture this: you savor your morning cup of coffee and fire up your computer only to discover you can't access any of your precious files. Then you receive a taunting message from nasty hackers saying your data will be toast unless you pay a ransom. You've been struck by ransomware, a serious crime that is on the rise. Here are some techniques to take on digital hostage-takers.

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. 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.**

If you cannot gain control of your device even though you are working with law enforcement and IT professionals, use another device (like a smartphone, tablet, or laptop) to change the passwords of any account that the compromised device accessed.