# Encrypting Ransomware

*Recovering from Encrypting Ransomware*

Ransomware is a type of malicious software that either threatens to publish your information or encrypts data and blocks access until a ransom is paid. Most likely your device was infected after clicking a malicious link or opening an infected attachment.

Ransomware is popular with cyber criminals as many people are willing to pay to recover their photos and files and also because the crypto currencies (such as Bitcoin) used to take payment are difficult to trace.

Encrypting ransomware is the most common and most harmful type of ransomware. With this type you can browse the folders and applications on your device and see your files, but you can't open them. Often the name of the files have been altered and there is a new file or message which includes a ransom note. Ransomware may also involve data theft or double extortion, where attackers threaten to release stolen data. This data theft or extortion can also happen even when files are not encrypted.

## Encrypting ransomware - Do this First

Before trying to remove the ransomware and gain back access to your files it is important to do the following:

### Disconnect and Contain

- Immediately disconnect the infected device from Wi-Fi and all networks.
- Unplug any connected hard drives or USB devices.
- Turn off shared drives and network storage (NAS, mapped drives).
- Unplug ethernet cables and disable Bluetooth on infected machines.
- Isolate any backups that may be connected.
    - Use tested offline backups or immutable/cloud-versioned backups where possible.

### Preserve Evidence

- Use a camera or a smartphone to take a picture of the ransom note.
- Take screenshots of the ransom note and any suspicious behavior.
- Use tools like ID Ransomware or NoMoreRansom.org to identify which ransomware you're dealing with by uploading the ransom note or an encrypted file.
    - Only upload a ransom note or encrypted sample to reputable services if you are comfortable sharing it; do not upload sensitive files.
- Record timestamps, file names, file extensions changed, and ransom demands.
- Save system logs, firewall logs, and antivirus reports if available.
- Do NOT wipe the system before preserving evidence.

## Document the Attack

- When did it start?
- How was it discovered?
- What systems were impacted?
- What files or data were encrypted?
- Was any sensitive or regulated data potentially accessed?

## Report the Crime

Report immediately to the following agencies:

- For All Victims
  - FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov
  - CISA Incident Reporting Form (for public, private, gov): https://www.cisa.gov/report
  - FBI Cleveland Field Office: (216) 522-1400
- For Government Entities in Ohio
  - Ohio Cyber Reserve / Ohio Homeland Security: https://www.ohio.gov
  - Statewide Terrorism Analysis & Crime Center (STACC): 1-877-OHS-INTEL (647-4683)
- Legal and Compliance Reporting, If PII, health data, or education records were affected, report to:
  - Ohio Attorney General – Data Breach Reporting: https://www.ohioattorneygeneral.gov
  - HIPAA (if applicable): https://ocrportal.hhs.gov/ocr/breach
  - FERPA or student privacy contacts (for K-12 or higher ed)

## Should I Pay the Ransom?

Many victims are targeted again, so rebuilding safely matters.

Instead of paying, report the attack, isolate the system, preserve evidence, and seek professional help. Tools like NoMoreRansom.org may even offer free decryptors.

## Recovery - Removing Encrypting Ransomware and Restoring Files

Depending on the type of ransomware you have there are a number of different ways to try and get your files decrypted. Follow the steps below and stop once you have recovered your files. If you don't feel confident performing the steps below, get help from someone with more IT experience.

- Visit NoMoreRansom.org to see if a free decryptor exists for your ransomware strain.
- Use reputable antivirus or antimalware software to scan and remove the ransomware. Boot into Safe Mode if needed.
- If no decryptor is available, restore files from secure offline backups (e.g., external drives or cloud backups made before the attack).
- Do not pay the ransom. As noted by the FBI and CISA, paying does not guarantee recovery and encourages further attacks.

    - Paying may also encourage more demands. If you already paid, report the incident and ask payment providers about reversal options.
- Start again by reinstalling the operating system. If you have nothing of value on the device or you have given up on getting your files back, you can start again. Use the 'Factory Reset' feature if available or wipe the disk and reinstall the operating system.
    - A reinstall or factory reset may erase local evidence and files. Preserve evidence first if reporting, insurance, or legal follow-up may be needed.
    - Reinstall or factory reset before reconnecting to sensitive accounts when compromise is likely.
- Harden Systems to Prevent Re-infection. Patch all software, enable MFA, restrict admin access, and audit security controls.

## How do I avoid being infected with encrypting ransomware again?

- Back-Up – having a back-up copy of your files is the best way to beat ransomware. Get an external hard drive and do a regular back-up of your device. Make sure you disconnect the external drive after use to make sure it doesn't get infected too. It is also worth using a cloud service that automatically backs-up your files.
- Use a good antivirus solution – this will stop the majority of known versions of ransomware and may give you an option to remove if new ransomware does get onto your device.
- Update your devices when prompted – when software updates are available do them as quickly as possible. If possible turn on automatic updates. The majority of these updates include security fixes that may stop or limit ransomware.
- Trust no one – be extremely careful about clicking links or opening attachments in your email or any other messaging platform. Legitimate email accounts can be hacked and used to send malicious messages and emails can be designed to look exactly like they are from your bank, shop, account etc.