# Screen Locking Ransomware

*Recovering from Screen-Locking Ransomware*

Screen-locking ransomware is a type of malware that prevents access to your device by displaying a full-screen message or ransom note that blocks you from using your operating system. It may claim to be from law enforcement or simply demand money to unlock your computer.

Real law enforcement also will not demand crypto, gift cards, or payment apps to unlock a device.

Unlike encrypting ransomware, this type may not encrypt your files; it blocks access to the device. The good news is that recovery is often possible without paying the ransom, especially if caught early.

## Screen-Locking Ransomware – Do This First

### Disconnect and Contain

- Disconnect the device from the internet (unplug ethernet or turn off Wi-Fi).
- Disable Bluetooth.
- Remove any connected external drives or USBs.
- Do not plug in backup drives or devices.
- If you're on a network (home or work), disconnect the affected device from the network; if multiple devices show symptoms, isolate them too.

### Preserve Evidence

- Take a photo of the ransom screen using your phone.
- If possible, take a screenshot and save system logs.
- Note any visible file names, ransom amounts, or deadlines.
- Use ID Ransomware to help identify the strain if the screen displays a message.

### Document the Attack

- What message is shown on the screen?
- When did it start?
- What software or attachment was opened before the lock?
- Does it impersonate law enforcement or display your IP/address?

## 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?

No. The FBI and CISA strongly discourage paying any ransom. Paying does not guarantee access will be restored and often leads to further targeting. Paying may also support criminal or sanctioned organizations. Instead, isolate the device, preserve evidence, and follow recovery steps or seek expert help.

Paying may also encourage more demands. If you already paid, report it and ask the payment provider about reversal options.

## Recovery – Removing Screen-Locking Ransomware

If you don't feel confident with these steps, ask a trusted IT professional for help.

### Option 1: Use Windows Recovery Environment / Safe Mode

- Reboot your computer.
- Use Windows Recovery Environment or Shift+Restart to access recovery mode; Windows Recovery Environment or Shift+Restart is unreliable on modern Windows.
- Choose Safe Mode without networking unless a trusted professional directs otherwise.
- Use antivirus software to scan and remove the malware.
- Restart normally and check if the lock screen is gone.

### Option 2: Use System Restore

- Reboot into Safe Mode with Command Prompt.
- Type: rstrui.exe and hit Enter.
- Follow the prompts to restore the system to a point before the lock screen appeared.

### Option 3: Use Bootable Antivirus Rescue Disk

- Download a bootable antivirus rescue tool from a reputable vendor (like Bitdefender Rescue CD or a reputable, currently supported rescue tool from a trusted security vendor) on another clean device.
- Create a bootable USB.
- Plug it into the infected device and boot from it.
- Let the tool scan and remove the malware.

### Option 4: Factory Reset (Last Resort)

If the ransomware can't be removed and no important files are stored locally:

- Use the PC's built-in recovery function to reset the system.
- Or perform a clean install of the operating system using a bootable USB.

## How to Avoid Screen-Locking Ransomware Again

- Back Up Your Data - Use external drives or cloud backup services. Keep backups offline and disconnected when not in use.
- Install Strong Antivirus Software - Keep it updated and run regular scans.
- Update Your Operating System - Turn on automatic updates to patch security holes quickly.
- Be Wary of Phishing & Attachments - Don't click unknown links or download unsolicited files. Always verify unexpected emails, even from people you know.
- Don't Trust "Police Ransomware" - If the screen lock claims to be from the FBI or police, don't panic, real law enforcement does not lock your screen or ask for payment via gift cards or crypto.