

6.4 Device Incidents

Ransomware Infection

Signs of ransomware

- Files suddenly encrypted with unfamiliar extensions (.locked, .cerber, etc.)
- Ransom note demanding payment for decryption
- Desktop wallpaper changed to ransom message
- Unable to open files (photos, documents, etc.)
- Pop-up demanding Bitcoin payment

Step 1: Isolate the Infection (IMMEDIATELY)

- Disconnect from network
 - Do NOT shut down the computer (some ransomware encrypts more on reboot)
- Unplug ethernet cable
- Turn off WiFi
- Disconnect external and network drives
 - Unplug any external hard drives, thumb drives, etc
 - Log out of any cloud accounts you have connected on your computer
- Identify the ransomware variant
 - Take a photo of ransom note with phone
 - Note the file extensions (.locky, .cerber, etc.)
 - Visit ID Ransomware <https://id-ransomware.malwarehunterteam.com> to identify variant

Step 2: Assess and Report (Within 1 Hour)

Do NOT pay the ransom, there is no guarantee of file recovery and this funds criminal activity

- Report to law enforcement (FBI) <https://ic3.gov>
- Check if free decryption is available from ID Ransomware
- Check what protections and warranties your antivirus solution offers
- Additional potentially free options:
 - <https://nomoreransom.org>
 - <https://kaspersky.com>

Step 3: Recovery Options

If decryption is available from your assessment, follow the instructions. This differs by type of ransomware and who is providing instruction, so I cannot be more specific than that.

If no decryption is available AND you have backups then performing a clean reinstall of your operating system is the way to go. Again, I cannot be more specific as there are too many variables. If you aren't sure how to do this, ask a technical friend or visit somewhere that services computers (Microcenter, Best Buy, Apple Store, etc).

If no decryption is available and you DON'T have backups, I'm sorry, you're pretty screwed. From a clean computer, go through all your accounts and remove that computer as an authorized device. Under no circumstances should you boot this computer and connect to anything until it is clean. Keep an eye on the decryption assistance sites above, there may be something in the future that can help, or seek assistance from a professional service.

Malware or Virus Infection (Not Ransomware)

Signs of malware infection:

- Computer running extremely slowly
- Unexpected pop-ups or ads
- Browser homepage changed without permission
- Programs opening automatically
- Antivirus disabled or won't update
- Strange network activity
- New toolbars in browser
- Files disappearing or appearing
- Excessive hard drive activity when idle

Step 1: Isolate The Infection (IMMEDIATELY)

- Disconnect from internet (unplug ethernet, disable WiFi), and log out of cloud accounts

Step 2: Scan and Remove (Within 1 Hour)

- Run a full scan using your installed antivirus software
- If this fixes the issue, reconnect to the internet and continue to step 3
 - Note that removing the virus will not restore settings which the virus changed, so you may need to follow steps 1 through 3 multiple times until the malware is removed and settings "stick"
- If this does not fix the issue, boot the computer into safe mode
 - For Windows: Restart, hold Shift, select Troubleshoot > Advanced > Startup Settings > Safe Mode
 - For Mac: Restart, hold Shift key

- Run full antivirus scan with your installed antivirus
- If you do not have an antivirus and are running Windows, use Windows Defender Offline Scan
 - Settings > search for “virus and threat protection” > click “scan options” > choose “Microsoft Defender Anti-Virus (offline scan)” > click “Scan now”
- If you do not have an antivirus and are using a Mac, you can look for a free scanner from Sophos, Kaspersky, Malwarebytes, or BitDefender
 - The options to run these vary, so follow the instructions
- If this fixes the issue, reconnect your cloud accounts and continue to step 3
- If this does not fix the issue it is probably time to seek help from a technical friend or professional services

Step 3: Check for Damage (Within 24 Hours)

- Review your installed software and remove anything you didn’t install (Windows will show you the date installed so you can use that as a guide for when the malware behavior started)
 - Start > add or remove programs
- Review browser extensions and remove anything suspicious
 - Browser settings > Extensions (varies by browser)
- Check browser homepage and search engine settings, restore as needed
 - Browser settings > Homepage (varies by browser)
 - Browser settings > Search engine (varies by browser)
- Check startup programs for unfamiliar entries
 - Windows: Settings > Apps > Startup
 - Mac: System settings > General > Login Items & Extensions

Step 4: Additional Actions

- Update operating system and all software
- Determine how infection occurred:
 - Downloaded software from untrusted source?
 - Opened email attachment?
 - Clicked suspicious link?
- Monitor accounts for any suspicious activity for a couple weeks

If infection cannot be cleaned, contact your antivirus provider. Even if you don’t pay for the service they may still offer help.

The worst-case scenario, make sure your backups are working and perform a clean reinstall of your operating system. If unsure how to do this, talk to a technical friend or seek professional services.

Gave Remote Access to Your Computer

Common scenarios:

- Tech support scammer asked you to install remote access software
- Downloaded and ran software that gave attacker control
- Allowed access via TeamViewer, AnyDesk, LogMeIn, etc.

Step 1: Cut Off Access (IMMEDIATELY)

- Disconnect from internet (unplug ethernet cable or turn off WiFi) to stop access
- Close remote access software, force close if necessary
 - Windows: Ctrl+Alt+Delete > Task Manager > End suspicious processes
 - Mac: Command+Option+Esc > Force Quit suspicious apps
- Close any software they installed or opened
- Uninstall any software they installed, booting into safe mode if necessary (safe mode prevents most malware from running)
 - For Windows: Restart, hold Shift, select Troubleshoot > Advanced > Startup Settings > Safe Mode
 - For Mac: Restart, hold Shift key
- Uninstall remote access software:
 - Windows: Settings > Apps > Find TeamViewer/AnyDesk/etc. > Uninstall
 - Mac: Drag application to Trash, empty Trash

Step 2: Scan for Malware (Within 30 minutes)

- See Malware or Virus Infection playbook above
- If you see anything that looks like it may be encrypting your files refer to Ransomware Infection playbook

Step 3: Additional Actions

- Consider what the attacker accessed
- Follow the appropriate playbook if any sensitive information was accessed
- Monitor accounts daily for a week

What To Do If Your Phone or Computer Is Lost or Stolen

Act quickly, the sooner you respond, the better your chances of recovery or protecting your data.

Step 1: Protect Your Data (IMMEDIATELY)

Use Find My Device (see Mobile Device Hardening or Physical Security section) to:

- Locate your device
- Play a sound (if nearby)
- Lock it remotely with a message to call you at another number

Suspend services and force logouts:

If you had an authenticator app on your phone, you may lose MFA access, so you may need to use another device where the authenticator app is install or the recovery codes form your password manager.

- Call your carrier (for phones) to suspend service (prevents calls and data charges)
- Disable payment methods on device
 - Apple Pay: iCloud > Devices > remove the lost device from the list
 - Google Pay: pay.google.com
 - Samsung Pay: <https://v3.account.samsung.com/dashboard/> > Devices
- Force active device logout for all accounts (prevents someone who gains access from accessing any of your data)

Step 2: Erase and File Reports (Within 12 Hours)

If stolen or otherwise not recoverable:

- Erase it remotely (see Mobile Device Hardening or Physical Security section)
- File a police report (needed for insurance claims)
- File insurance claim (if insured against theft) with the insurer (your mobile carrier, Apple, etc)

Step 3: Recovery

If device is recovered, before using:

- Inspect for physical tampering (opened, different SIM)
- Check for new apps you didn't install
- Review recently accessed files and folders
- Check settings for changes:
 - New accounts logged in
 - Developer options enabled (Android)
 - Unknown device profiles (iPhone)
 - New email forwarding rules
 - VPN or proxy configurations
 - Accessibility permissions changes

If suspicious changes found, factory reset the device and proceed as if setting up a new device.

Revision #1

Created 2026-07-12 22:28:32 UTC by Chris Landis

Updated 2026-07-12 22:29:39 UTC by Chris Landis