Removing Malicious Software

Recovering from Malware Infections

Malware (malicious software) is any software designed to harm your device, steal information, spy on activity, or give criminals remote access. Malware often installs without your knowledge after clicking a malicious link, opening an attachment, installing fake software updates, or visiting compromised websites.

Common Signs of a Malware Infection:

- Device is unusually slow or frequently freezes
- Device won't start properly or crashes repeatedly
- Mouse moves or programs open without your input
- Pop-ups with warnings, fake alerts, or urgent messages
- Homepage or search engine redirects unexpectedly
- Ads appear in unusual places (including inside apps or system screens)
- Security software is disabled or cannot update

Some infections are obvious. Others are silent and designed to remain hidden.

Before You Begin – Important Warning

Before attempting removal, honestly assess your level of IT confidence.

If you are not a confident IT user, strongly consider seeking professional help.

Improper removal attempts can:

- Permanently delete data
- Corrupt the operating system
- Allow malware to spread to other devices
- Make forensic recovery impossible

If the device is used for work, healthcare, finances, or school, professional assistance is strongly recommended.

Malware Infection – Do This First

Disconnect and Contain

Immediately reduce the malware's ability to spread or communicate.

- Disconnect from Wi-Fi and wired networks
- Turn off Bluetooth
- Unplug:
    - External hard drives
    - USB devices
    - Memory cards
- Do not log into email, banking, or work accounts from the infected device

Preserve Evidence (If Needed)

If you may need help from IT support, law enforcement, or an organization:

- Take photos or screenshots of:
    - Error messages
    - Fake warnings
    - Pop-ups
    - Unusual behavior
- Note:
    - When the issue started
    - What you were doing before it began
    - Any recent downloads or links clicked
- Do not wipe or reset the device before preserving evidence if professional help may be required.

Decide: Self-Help or Expert Help

- Seek expert help immediately if:
    - You see signs of remote control
    - The device contains financial, medical, or work data
    - You are unsure how to safely proceed
    - The device belongs to a child or senior
    - Multiple devices appear affected

Removing Malware (For Confident Users Only)

Boot Into Safe Mode (If Possible)

Safe Mode limits what runs on startup and can prevent malware from activating.

- Restart the device
- Enter Safe Mode using your operating system's instructions

Run Reputable Security Scans

Use well-known antivirus or antimalware software

- Update definitions if possible
- Run a full system scan
- Follow removal instructions carefully
- Avoid pop-ups claiming to be "security tools" many are malware themselves.

Remove Suspicious Programs and Extensions

- Uninstall unfamiliar software
- Remove unknown browser extensions
- Reset browser settings if redirected or hijacked

Change Passwords (From a Clean Device)

Once the infected device is secured:

- Change passwords for:
  - Email
  - Banking
  - Social media
  - Work or school accounts
- Enable additional protections where available

If Removal Fails or You're Unsure

- Reinstall the Operating System
- If malware persists or system integrity is uncertain:
  - Back up only essential files (documents, photos—not programs)
  - Perform a factory reset or OS reinstall
  - Restore files carefully after reinstalling security software
- If unsure, stop and seek help.

Report the Incident (If Appropriate)

Reporting helps track criminal activity and protect others.

- FBI Internet Crime Complaint Center (IC3)
  - https://www.ic3.gov
  - (Recommended if financial loss, data theft, or extortion occurred)
- Ohio Resources
  - Ohio Attorney General – Consumer Protection & Cybercrime
  - https://www.ohioattorneygeneral.gov
  - Hotline: 800-282-0515

- Geauga County
  - Geauga County Sheriff's Office
  - https://www.geaugasheriff.org
  - Local police non-emergency line if device compromise led to fraud or threats

Recovery – After Malware Removal

- Monitor accounts for unusual activity
- Review bank and credit card statements
- Consider credit monitoring if personal data may have been exposed
- Reconnect devices to the network one at a time and observe behavior

How to Reduce Risk of Future Malware Infections

- Be skeptical of urgent pop-ups and scare tactics
- Avoid clicking links or attachments you weren't expecting
- Only install software from trusted sources
- Don't ignore early warning signs, slowdowns and pop-ups are signals
- Ask for help early instead of "clicking through" warnings