DEVICE *INFECTED?*

Warning signs that your device is infected:

- Your web browser freezes or becomes unresponsive.
- You get redirected to web pages other than the ones you are trying to visit.
- You are bombarded with pop-up messages.
- Your device or internet runs slower than usual.
- You see new icons on your desktop that you don't recognize.
- Your device's cooling fan spins suspiciously louder or harder than usual.

Follow these ten steps to nurse your device back to health:

1. Disconnect your device from the internet immediately.
2. Remove any CDs or DVDs, and unplug USB drives from your computer.
3. Shut down your device and restart it in Safe Mode.
4. Back up files like documents, photos, and videos. Do not back up program files, as those are where infections like to hide.
5. Use another computer to download a malware scanning program or purchase a program disc at a store. If you don't have another computer, ask a good friend or family member to use their computer to download the malware scanning software.
6. Use an empty flash drive to transport the malware scanning program from the clean computer to the infected one.
7. Run the scan. A list of scan results will tell you what malware was found and removed.
8. After scanning and removing any malware, restart your computer and confirm the results of your anti-malware scan by running a full scan with another malware detection program. Restart your device again if the program found additional infections.
9. Update your operating system, browser, and applications.
10. Change and create new strong passwords for all of your accounts. Learn how from ConnectSafely.org.

** If you still believe you have problems after following these steps or don't feel comfortable completing these steps, take your device to a professional.*

For more recovery help, visit FraudSupport.org

Updated March 2020