How to protect your computer/device

against viruses & malware

Things to do with your computer if you are the victim of fraud

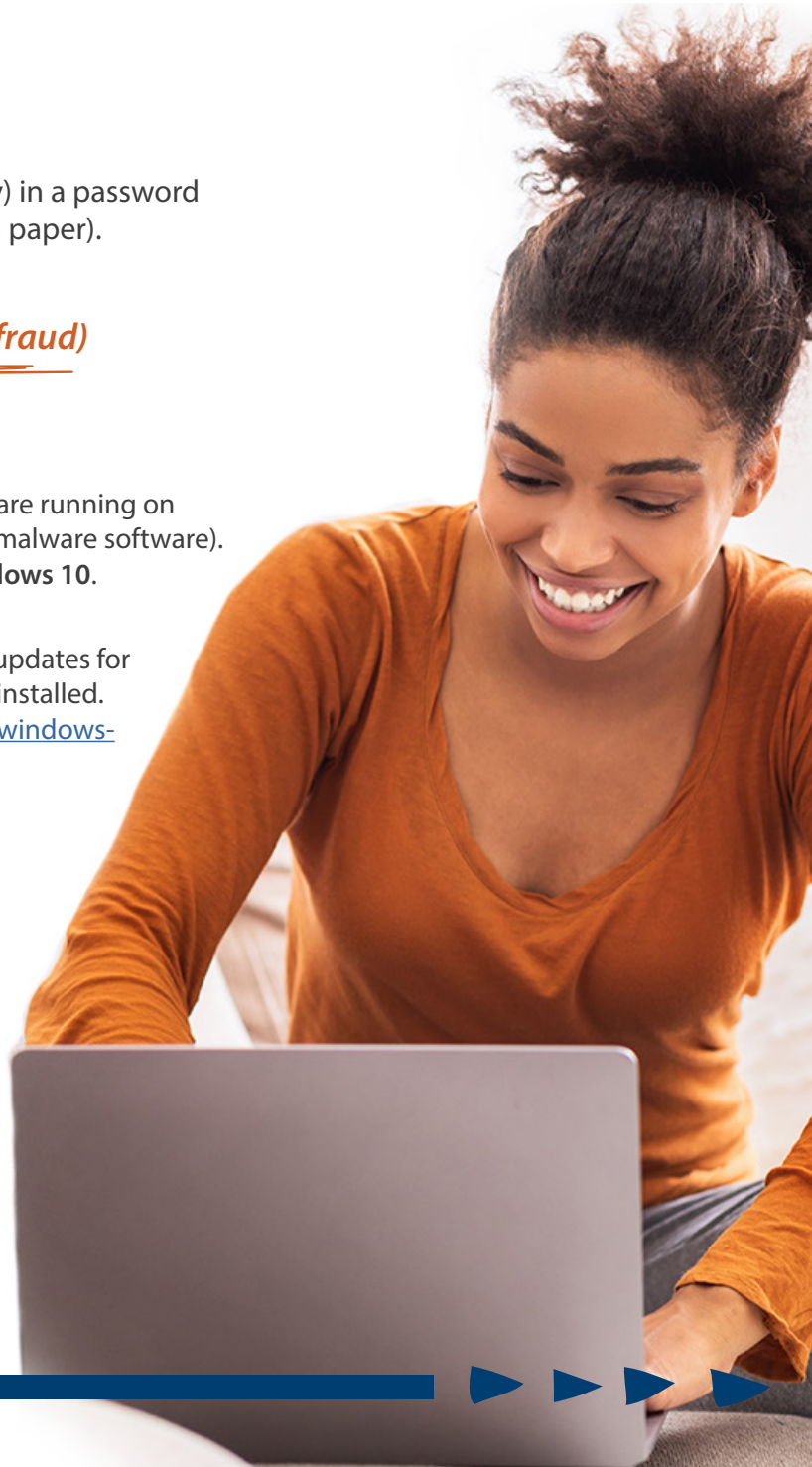
Your Online Banking

- ☑ Setup alerts for your mobile/online banking
- ☑ Store your password in a secure place: (preferably) in a password manager (example: KeePass) or in a lockbox (if on paper).

Things to do right now (before you experience fraud)

Your Computer

- ☑ Make sure you have active endpoint protection software running on your computer (commonly known as antivirus or antimalware software). **Windows Defender comes (free/included) with Windows 10**.
- ☑ Keep your computer secure by turning on automatic updates for Windows and by making sure that updates are being installed. (https://www.zdnet.com/article/faq-how-to-manage-windows-10-updates/)
- ☑ Make sure your computer is running an operating system that is currently supported. (Those members with computers running Windows 7 should consider moving to Windows 10 – the end of life for Windows 7 was January 14, 2020.)
- ☑ Setup regular backups for your computer, to a portable (USB) hard drive using Windows Backup; backup to your hard drive and keep your backups, through a rotation (ideal: one week of daily backups, 4 weekly backups and 1 backup per month) (https://www.windowscentral.com/how-backup-windows-10-automatically)



If you experience fraud or suspect that your computer has been infected by a virus or malware

Your Computer

- Disconnect your computer from the internet by unplugging the network cable from the back of your computer or (in the case of wireless connections) by disabling the network connection (do not just disconnect from the wireless network; malware has the potential to reconnect without you being aware)

- Perform a deep/full scan of your computer:
  (NOTE: If you are unsure or uncomfortable attempting this yourself, take your computer or device to a professional computer services company to be scanned and cleaned.)

  - If the scan results show that malware was found, record the name of the malware (it could be useful, later in the process.)
  - Once the scan results come back clean, restart the computer then run another full/deep/complete scan. If the second scan shows that no malware was found, your computer should be free of malware.
  - If additional scans continue to come back showing malware is found, then take your computer to a computer services shop to be professionally cleaned of malware.

How does malware get on your computer?

Malware is often hidden in free software or shareware that you download from the internet (for example, a multimedia program or file, such as music or a video, or a peer-to-peer transfer system):

- When visiting a website, you get a pop-up that states that it has found a virus on your computer; You can install a free trial of a virus scanner or run an online scan of your computer;
- You get an e-mail that appears to be from your bank with the request to install the attached update to plug a hole in their internet banking security;
- You find a video on the internet. In order to play it, you have to install a special plug-in;
- You get an e-mail with a really great offer. If you open the photos, your computer gets infected with malware;
- You get a message from someone you know via social media that there are photos of this person on the internet, including a link to these photos. If you click the link, your computer gets infected with malware.

CORNERSTONE Credit Union