Dealing With Malware and Viruses

In This Module

- What are some examples of viruses, and malware more generally?
- How do you deal with a virus or malware infection?

Malware and Viruses

Malware is a type of software that is designed to deliberately infect devices, causing disruptions or gaining unauthorized access to information

Viruses are a type of malware that can infect devices and replicate themselves

Activity

What are some computer viruses that you have seen or heard about before?

Types of Malware

- **Ransomware:** Malware that locks your device and holds it for ransom
- **Adware:** Often takes the form of out-of-control pop-up ads
- **Spyware:** Malware that gathers information about a user

Types of Viruses

- **Trojan virus:** A famous kind of computer virus that gets onto a machine by being disguised as a legitimate program. Users are tricked into installing or downloading something that contains a trojan virus
- **Browser hijacker:** Viruses that can infect a browser and change settings or redirect users to malicious sites

Types of Viruses

- **Macro virus:** Viruses that can infect macros in Microsoft Word
- **File infector virus:** A virus that can infect and spread among critical computer files

Signs You Have a Malware Infection

- Your device is slow or keeps freezing or crashing
- Programs are opening, closing, and changing on their own
- Your device is running out of storage space unexpectedly
- You're bombarded with pop-ups
- Emails are being sent without your knowledge

What other signs come to mind for you?

What to Do if You Have Malware

- Stop using accounts or entering in passwords
- If your device is part of a network of devices, disconnect it until you have removed the malware
- Reboot your device in Safe Mode
- Run a scan using an antivirus security software to identify and remove the problem
- For a severe attack, you might need to reinstall your entire operating system

What to Do After a Malware Infection

- Reset passwords and update security settings for your device
- Update your device software
- Make sure you keep any security software you use up to date
- If you haven’t already, get on a schedule for backing up your data
- Be on the alert for signs of fraud or identity theft after a malware attack

What to Do After a Malware Infection

- Check your credit scores since attackers might have stolen your identity
- Be on the alert for signs of fraud or identity theft after a malware attack

Checking Your Credit Report

There are three major credit reporting agencies where you can keep an eye on your credit and watch for signs of fraud, suspicious account activity, and strange charges:

- **Experian:** https://www.experian.com/
- **Equifax:** https://www.equifax.com/
- **TransUnion:** https://www.transunion.com/

Takeaways

- Malware and viruses can often get onto devices without your knowledge and can compromise your personal security
- Remember to be careful with what you download and open to help you avoid malware in the first place!
- If your device has been infected, take steps to remove the malware or virus and to secure and monitor your accounts
- Remember, malware and virus infections can lead to identity theft, so check your credit reports and personal financial accounts for suspicious activity

Resources

“The Best Antivirus Software” from *PC Mag* (link)

“The best antivirus software: Free and paid options” from *Tom’s Guide* (link)

Antivirus Software Guide from *The New York Times’ Wirecutter* (link)

Questions?

NYC Digital Safety

Privacy & Security