Managing a Malware Attack
In This Module

- What are some signs of a malware attack?
- How do you manage a malware attack?
- What are some ways to deal with the aftermath of a malware attack?
Malware

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

Malware can take stealthy and hidden forms, or can be aggressive and obvious.
Activity

What are things that malware can do to a device?
Aggressive Types of Malware

Here are some common types of more aggressive malware:

- **Ransomware:** Malware that locks your device and holds it for ransom
- **Trojan viruses:** These can be more stealthy, but they can delete files and data or lock a device
- **Adware:** Often takes the form of out-of-control pop-up ads
Aggressive Types of Malware

Here are some common types of more aggressive malware:

- **Worms:** A type of virus that actually copies itself and sends itself to other users; can be used to send mass phishing scheme emails
- **Botnets:** Malware that can gain access to devices via malicious code and can take remote control of devices, among other things
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 to Do During an Attack

- 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 an Attack

● 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
Malware can often get onto devices without your knowledge and can engage in stealth activities.

However, some malware can engage in more aggressive and overt attacks that can cause you to lose control of your device.

Use strategies like Safe Start or, in extreme cases, an operating system reinstallation to regain control and rid your device of malware.

Remember to be careful with what you download and open to help you avoid malware in the first place!
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](#))

Safe Mode Directions for Windows ([link](#))

Safe Mode Directions for Mac ([link](#))
Questions?
NYC Digital Safety
Privacy & Security