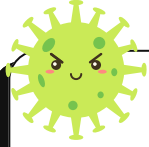
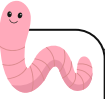


# MALWARE MANSION



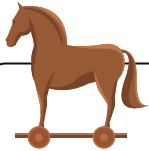
## Virus

A virus is a type of malware that spreads from the infected file to other machines via the network or your router. It then makes copies of itself on the other device. Some ways to prevent viruses are to use a trusted antivirus, avoid clicking on pop-ups, scan your email attachments, and scan the files you download.



## Worms

Worms are a type of virus that can replicate and spread through a network automatically. Worms consume large amounts of memory machines or networks to slow down. Worms can spread through links primarily. Some ways to tell if you have a worm on your computer is to check your hard drive space. Some ways to avoid getting a computer worm include updating your Operating Systems (OS) and having some strong internet security software.



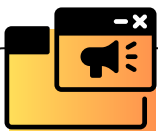
## Trojan

A Trojan (Trojan horse) is a type of malware that appears non malicious at first but houses a virus or other damaging program. Trojans are a delivery method for computer viruses. Some ways to protect yourself against malware found is to keep your OS up to date and scan devices often on an anti virus software. Be mindful of phishing attacks and to try to avoid downloading software from suspicious sources.



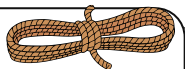
## Spyware

Spyware is a type of malware that sits on your computer and tracks your personal data to be sold to advertisers or other malicious parties. Some ways to accidentally get spyware on your computer is accepting cookies without reading the terms of service, getting phishing attacked, clicking malicious links on accident, and downloading things from suspicious websites.



## Adware

Adware is like spyware that sits on your computer and tracks your personal data. Adware uses your data to show pop up ads on your device. Some ways to avoid this type of malware is to read the terms and conditions on websites and to double check and scan files you download onto your device.



## Ransomware

Ransomware is a type of malware that holds a machine hostage until it is unlocked. If you are the victim of a ransomware attack, it is recommended to not to pay the malicious group that locked your device. Paying them does not guarantee your device will be unlocked. Some ways to avoid ransomware is to keep your OS up to date, back up your files, and to run regular scans with your antivirus software on your machine.

## Resources:

- [cisa.gov/news-events/news/virus-basics](https://cisa.gov/news-events/news/virus-basics)
- [fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams](https://fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams)
- [cyberhouserock.info](https://cyberhouserock.info)