Topic: Computer Viruses and Other Online Threats

When I am done this lesson, I will know:

- Some common online threats
- Some tips to avoid online threats
- What to do if my computer gets a virus

Pre and Post Self-Assessment

	Pre	Pre	Post	Post
	Yes, I know this	**No, I want to learn this**	**Yes, I know this**	**I still need more practice to learn this**
I know what some common online threats are				
I know how to avoid online threats				
I know what to do if my computer gets a virus				

New Words and Terms

malware
adware
trojan
spyware
ransomware
worm

There are many different kinds of online threats to computers. Some of the most common terms are:

- Malware
- Virus
- Adware
- Trojan
- Spyware
- Ransomware
- Worm

Type of Threat	Description
Malware	Malware is short for malicious software. This means that while most of us refer to these threats as viruses, the correct catch-all term should indeed be malware. Malicious software comes in many forms, but malware itself is a general term that could be used to describe any number of things, such as viruses, worms, trojans, spyware, and others. It's a program or file with bad intentions. Luckily, malware is what all the most popular antivirus programs are look for.
Virus	Viruses are malicious code that infect a computer after you install a software. This usually happens through USB drives, Internet downloads, or email attachments, but it can happen other ways as well. The infection doesn't occur just from having the infected files on your computer. The infection happens once the program runs for the first time, whether through Autorun, a manual install, or an executable file that the user opens. Once opened – or run – the infection happens. From that point, it can be very difficult to find and get rid of the virus. Unlike other threats, viruses have no other purpose than attempting to make your computer impossible to use.
Adware	Adware is usually harmless but it can be really annoying. Adware is often bundled with apps or software, which makes initial detection somewhat difficult. A common example is the checkbox at the bottom of a download link (often pre-checked) that asks if we want to "Include X for free" – "X" is often the program containing the adware. If you aren't sure what these additional programs are, or how they function, don't download them.

Trojan	Trojans were named after the Trojan Horse, which was a giant wooden horse used to conceal Greek soldiers as they entered Troy during the Trojan War. A trojan damages your computer the same way. It hides malicious code inside a program or file in order to gain access to your machine. Once inside, the program installs itself on your device and communicates with a server in the background without your knowledge. This gives an outside party access to your computer and information on your computer through what's called a backdoor.
Spyware	Spyware is the most common piece of malware on the Internet. While it's quite deceptive in nature and a major annoyance, most spyware is relatively harmless. Typically, spyware is used to monitor your browsing behaviour. This information is often used to send you ads based on your browsing behaviour. While typical spyware is mostly used for ad-serving purposes, there are other more malicious types of spyware that communicate sensitive data back to another user, or to a server. This data can include emails, photos, log files, credit card numbers, banking information, and/or online passwords. Spyware is most often downloaded by the user as part of an add-on to a legitimate download (such as a toolbar) or included as part of a freeware or shareware program.
Ransomware	The goal of ransomware is to collect money by manipulating the user into believing something that's often untrue. After the malicious software is installed, it'll lock down your system except for a window that allows you to pay the ransom in order to regain use of your system.
Worm	Worms are the most damaging form of malware. While a virus attacks one computer and relies on a user to share infected files in order for it to spread, a worm exploits security loopholes in a network and can bring the entire network down. Once the worm is in the network, it passes (often unnoticed) from computer to computer. As it passes from one device to another, the infection spreads until each machine is infected.

☑**Check Your Knowledge**

1. What is a trojan named after?

2. What is the most damaging type of malware?

3. What is the goal of ransomware?

Review this tutorial to learn what to do if your computer gets a virus. Source: GCFGlobal.org	https://edu.gcfglobal.org/en/internetsafety/what-to-do-if-your-computer-gets-a-virus/1/

Tips for Avoiding Online Threats

- Keep your operating system and each of your programs up to date by downloading updates as they become available.
- Install an antivirus program and keep it up to date.
- Use a firewall.
- Do not download apps or programs from unknown and untrusted sources.
- Use your antivirus program or a malware detection program to scan programs and links before opening them.
- Avoid pirated (stolen or illegal) software.
- Don't open email attachments from people you don't know.

💬**Discussion Questions**

Can you think of any other ways to avoid online threats?

ⓘ**Optional: I want to learn more**

▶	**Watch** this to learn three tips on how to spot malware. Source: Google Help	https://www.youtube.com/watch?v=nvIXGeB1WgE

Bridge Adult Literacy Curriculum Framework Connection	
Competency	**Task Group(s)**
Find and Use Information	• Read Continuous Text (L3) • Interpret Documents (L3 - compares virus types, unfamiliar vocabulary) • Extract Information from Films, Broadcasts and Presentations (not levelled)
Communicate Ideas and Information	• Complete and Create Documents (L2 – tables, ability to estimate, ability to evaluate)

www.bridgela.org 🌐

info@bridgela.org ✉

(310) 999-0001 📞