Prevention - Malware Teachers Guide

Disclaimer – This was prepared as a guide to the slides. If it does not suit your students' learning style feel free to change it up. It is intended to help lead the discussion around password safety

Show: Slide 1: Malware Prevention Title Slide

Say: "Today we are going to go over Malware, what it is and what dangers it poses."

Show: Slide 2 – Learning Objectives

Say: By the end of this lesson, you will

Learn what malware and viruses are

Understand the dangers of being infected with malware.

Know how malware is able to infect computers

And Understand how to effectively stop malware.

Show: Slide 3 – What is Malware?

Say: Malware gets its name because it is a malicious piece of software, with mal being short for malicious.

Ask: Knowing what malicious means, what could Malware mean? Give the class a chance to respond on what they think malware might be.

Say: Malware is a program that is designed to be disruptive and cause damage to a computer. Often, malware hides on a device so it is more difficult to detect.

Show: Slide 4 – What is a Computer Virus?

(Play Video)

Say: Just like people, computers can become sick too, this is called a Computer Virus.

Ask: What do we think a computer virus is? Ask students what they think a computer virus is? It can be related back to being sick or catching a cold, analogies that can be helpful for visualizing what a computer virus is.

Say: Definition – A computer program that makes copies of itself to destroy information and take over a computer.

Show: Slide 5 – What does a computer virus do?

Say: A virus always has a negative impact on any device it's on. The 3 main goal of a virus are to: Steal and Corrupt Data – often to sell the information, Cause the computer to slow down – in this case using resources to spread itself through the computer and look for information, and finally to use the computer to replicate itself and spread itself to other computers.

Show: Slide 6 – What is the difference between a virus and malware?
Say: While both Malware and a computer virus sound similar in nature, they have a major difference.
Ask: What do you think the main difference between a normal piece of malware is and a computer virus?
Say: A virus is actually a type of malware, the main difference being that a virus creates copies of itself so it can spread to other computers.

Show: Slide 7 – What are some common types of Malware?
Say: There are many different types of Malware, these 3 are some of the most common types. Adware, Spyware and Ransomware are all dangerous forms of malware that can infect a device. These three while all being malware differ in what harm they do.

Show: Slide 8 – What is Adware?
Say: Similar to the prefix mal in Malware, the Ad in Adware is short for advertisement.
Ask: Knowing this, what do we think that Adware could mean?
Say: Adware is an unwanted program that collects personal information about you and then displays advertisements that are often disruptive to the computer. This information is often used to show you ads that may interest you and lead you to downloading other more dangerous programs. The information that is taken from adware is often sold.

Show: Slide 9 - What is Spyware?
Say: Spyware is the second type of malware we'll look at and is more harmful than Adware, this type of malware has the prefix of Spy.
Ask: Knowing what a Spy is and knowing what malware does, what do you think Spyware could do?
Say: Spyware is a malicious program that is designed to collect information from your computer without your knowledge. This is different from the information collected by adware, this information includes things like: passwords, bank details, and other personal information that can be used to steal from you.

Show: Slide 10 – What is Ransomware?

Say: Finally, Ransomware is a type of malware that is being used more in recent years and is by far some of the most dangerous and damaging malware. You may have even seen it mentioned on the news.

Ask: This malware has a prefix of "Ransom", what do we think ransomware could do?

Say: Ransomware is a program that is designed to block access to a computer or files on your computer. This program works by putting passwords on every file, so that you can no longer access them. Sometimes the program will completely lock you out of a device and will demand money to let you back in. It's important to never pay the ransom as you aren't guaranteed to get your files back.

Show: Slide 11 – What is an executable.

Say: A computer executable is simply a file or program that can be run by a computer.

Show: Slide 12 – How are we infected with a virus or malware?

Say:

Emails – Emails can become infected and be used to transmit a virus from one computer to another. Commonly an email address can be stolen and used to send a virus to friends to all that person's contacts. Emails will often send executables or programs that are disguised as email attachments such as pictures or videos. Upon trying to open them malware will be installed.

Executables and Programs – Executables can be infected with a virus or malware, when they are used it will infect the device. These can include programs that are found online that are not from the creators website, or even in a player made mod for a game.

Internet Links – Internet links can be infected and can download malware to your device without your knowledge. These links often run malicious programs automatically, install malware in your computer. Often they are also capable of recording information typed into the website, especially passwords.

Show: Slide 13 – What devices can be infected with malware?

Say: Almost all modern technology is susceptible to being infected by malware. Most commonly, apps downloaded on android smartphones and windows computers can contain viruses. While it may be uncommon for even devices like Mac computers and video game consoles can be infected with a virus or malware. Even refrigerators or other appliances that are connected to the internet are known to be attacked with malware.

Show: Slide 14 Class Discussion – How do we avoid malware?

Ask: Now that we know how malware spreads, how can we prevent being infected with malware? Challenge students to think of ways that malware can be avoided. Have them think of responses and record them inside of a notepad or on a whiteboard.

Show: Slide 15 – How can we prevent being infected with viruses and malware?

Say:

Malware is very important to avoid. We know that emails, internet links and corrupted programs are the main ways we get malware. Most importantly we should never click links we think are suspicious or are unsure of, especially if they visit sites that are unsafe.

Second, we should never open email or email attachments from anyone unless we know the person who sent them and we know that they meant to send the attachment.

Third We should install programs that prevent malware from infecting our computers and that detect existing malware to remove it.

You should always make sure that any programs you install on your computer are trusted programs on your computer. It is important to ensure that any program is installed by using the official website and never anywhere else.

Show: Slide 16 – What is an Anti-virus

Say: The best way to protect ourselves is by using programs that are called Anti-virus programs.

Say: An anti-virus is a program that is designed to detect and destroy computer viruses and malware.

Show: Slide 17 – Trusted Antivirus programs

Say: There are many different anti-virus programs, these are a few of the most popular. Many different anti-virus software cost money to use such as McAfee or Norton but provide increased protection. Some anti-virus software can be free, most notably Windows Defender which comes preinstalled on any Windows device. You can install antivirus software in the same way you would install any other program on a computer and often have very helpful guides to ensure they've been installed correctly.

Show: Slide 18 – Reflection

Say: What steps can you take to reduce your risk of being reduced by malware. Take this time to record student responses.