Reading 3

Skills:

- Details

Getting started: What kind of antivirus do you use? Do you think it is effective? Do you use any other type of protection?

WHAT IS A COMPUTER VIRUS?

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Once a virus has successfully attached to a program, file, or document, the virus won't be active until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be

executed. This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, corrupting files, spamming your email contacts, and even giving orders to your machine are just some of the devastating consequences of a virus. Some viruses can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk.

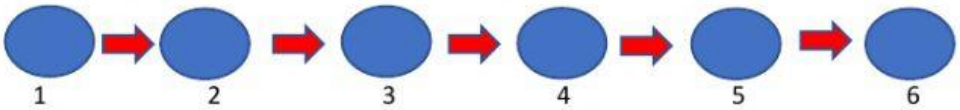
In a constantly connected world, you can contract a computer virus in many ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Your mobile devices and smartphones can become infected with mobile viruses through app downloads. Viruses can be disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

To avoid contact with a virus, it's important to exercise caution when surfing the web, downloading files, and opening links or attachments. To help stay safe, never download text or email attachments that you're not expecting, or files from websites you don't trust.

There are some other things you can do to help keep your computer safe. For example, use a trusted antivirus product, keep it updated with the latest virus definitions, and run it every now and then. Also, avoid clicking on any pop-up advertisements if you are not in a trusted site. Always scan your email attachments before opening them as well as the files that you download using file sharing programs.

**Adapted from https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html*

Complete the chart that represents a computer virus process using the situations below:



a. Code is executed.
b. Virus attaches to a file.
c. The virus is now on your computer.
d. User downloads a file/program.

e. Your information is stolen, or your computer is running slow.
f. Infected file/program is executed.

What do you think?

What kind of precautions do you take when you surf the internet?