Protecting Against Malware

VIGITRUST

Malware is an umbrella term used to describe malicious software, including computer viruses, spyware, and ransomware. Malware infection can have serious consequences for you and your company. In this short course. we look at the dangers posed by malware, and what you can do to prevent malware infection.

Protecting Against Malware

Protecting Against Malware

Consider this...

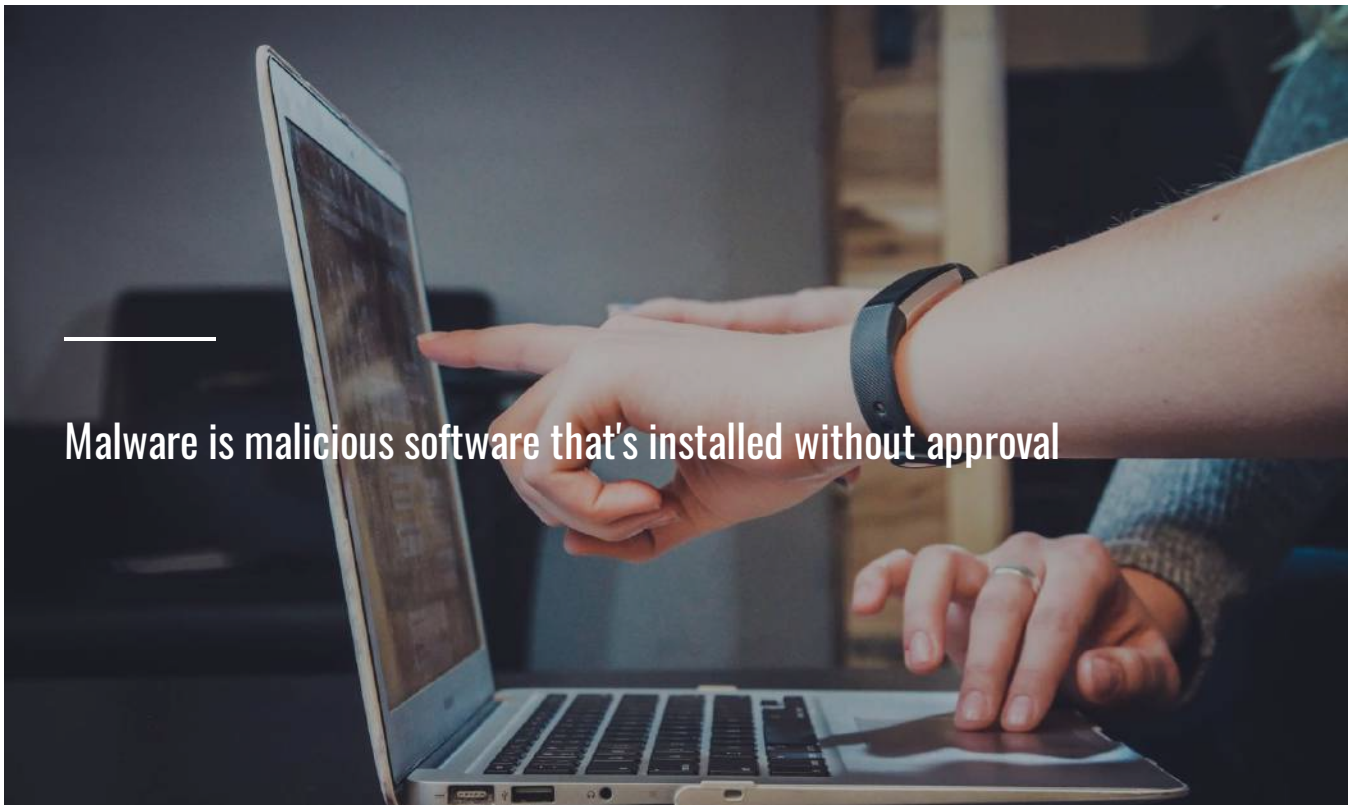
You are the receptionist at a medium sized hotel in London. One day, a guest presents you with a USB key containing a copy of an airline boarding pass and requests that you print it out. What should you do in this case?

- ○ Plug the USB key into your computer and print the pass
- ○ Politely refuse and direct the guest to the nearest Internet cafe

SUBMIT

What Is Malware?

The term “Malware” is used to describe malicious computer programs designed to infiltrate and damage computers without the users consent.



Why is Malware Dangerous?

Malware can have **serious consequences** for individual users and businesses.

If your home computer is infected your data could be deleted or sensitive information compromised – this could include passwords or personal banking information.

If your work computer is infected, not only could you lose sensitive or company information, the virus could spread throughout the company network and cause major disruption to the business.

1. Impairs device performance. Malware can have a detrimental effect on your computer's performance.

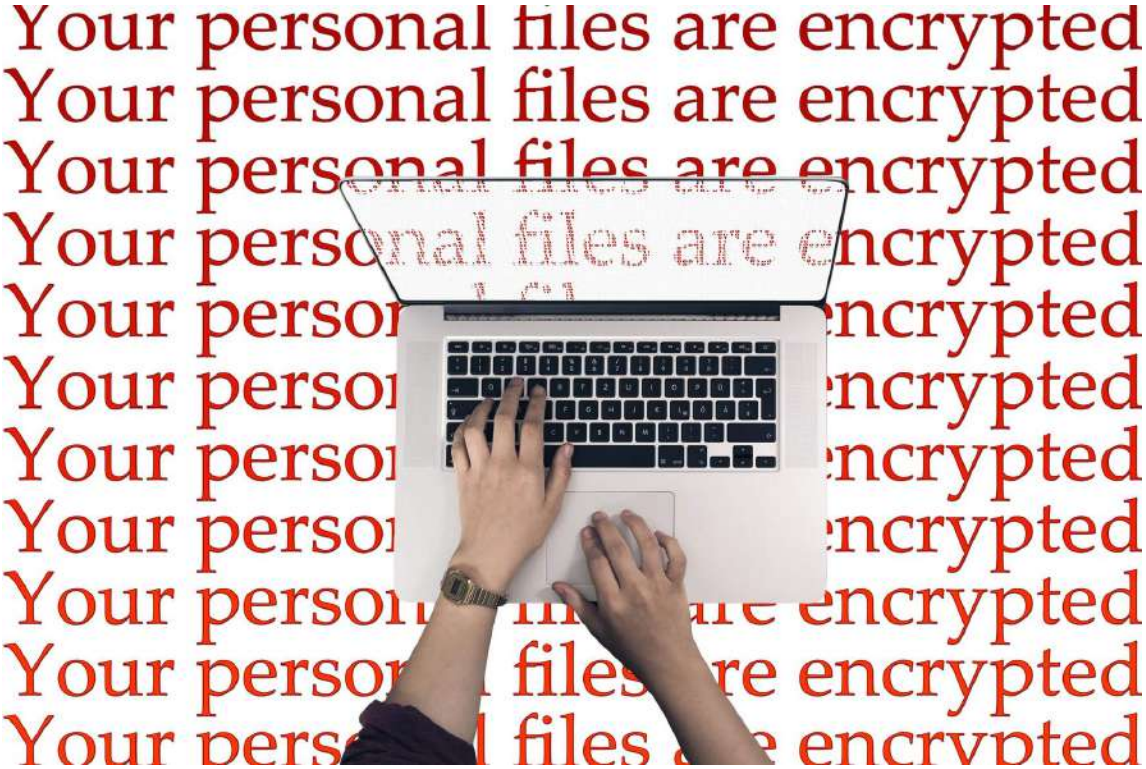
2. Steals or compromise personal or sensitive information such as passwords or banking details
3. Some malware programs can maliciously erase company or personal data.
4. May adversely affect computer hardware performance.
5. May completely take down company networks.

Types of Malware

Malware comes in a variety of shapes and sizes, from the merely annoying (Adware) to much more serious threats such as ransomware and spyware.

Ransomware

Ransomware is malicious software that blocks users from accessing their own files. Criminals encrypt the files on the victims system hold it “hostage” until the demanded ransom is paid, usually via Bitcoin.



Spyware

Spyware is malicious software that infiltrates your device, stealing your internet usage data and sensitive or personal information .

Adware

Adware is malware that attempts to expose users to unwanted, advertising. Adware may redirect a user's browser searches to look-alike web pages that contain other product promotions

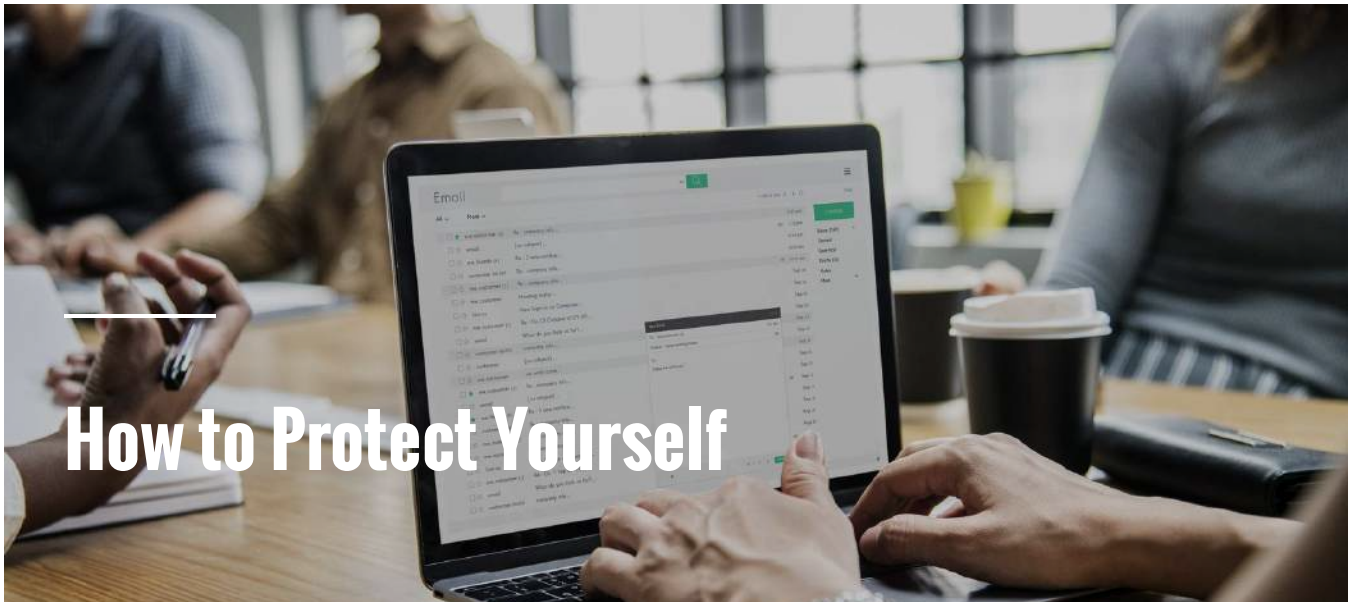
Viruses

A computer virus modifies other legitimate files such that when a victim's file is executed, the virus is also executed. Viruses comprise of 10% of all malware infections.

Trojans

A Trojan masquerades as a legitimate program, but in fact contains malicious instructions. Trojans usually propagate via email or infected websites. They often masquerade as anti-virus programs.

Regardless of the type, malware is dangerous software that threatens a user's information security.



How to Protect Yourself

Here are some tips to help prevent malware infection.

1. DON'T open emails or their attachments or embedded links from senders you don't know or that may look suspicious**.**
2. Be careful about visiting suspicious websites, such as those advertised in those annoying spam emails. This sites often act as a launchpad for adware or more serious virus.
3. Don't insert unknown USB drives in your computer. Viruses are often hidden on USB keys or other mobile devices.
4. Apply security updates**.** When your computer prompts you to update your system software, do it as soon as possible.
5. Use anti-virus software. Never go online without your computer's anti-virus software up-to-date and running.
6. Be aware that social media sites, such as Facebook, Instagram and Twitter are commonly used to distribute malware in the form of malicious advertising and rogue applications.

How do I know when my computer is infected?

The first step is to recognize that your computer has been infected. Here are the vital signs:

- You notice unusual activity when you start your computer or open your browser.

- You see new or suspicious programs in your list of programs or suspicious files in your files list.
- Your computer's performance is slower than usual and this problem persists when you reboot.
- Your anti-virus software is disabled for no particular reason, and you can't re-enable it.
- Your computer crashes unexpectedly.
- You notice an increase in the number of popup adverts.

Be suspicious if your computer exhibits ANY unusual behavior. Contact your IT department if you are unsure!

CONTINUE