or opening e-mails from unknown e-mail addresses. So of course, the easiest way to protect yourself: do not do those things. However, even with the most meticulous cyber hygiene practices you can still get malware onto your system.

The next option would be to utilize a third-party program to protect your systems, and there are several good anti-virus software or anti-malware programs to choose from such as Bitdefender, Norton, McAfee, BullGuard, or Kaspersky. Each has different capabilities and features than the other, but all are a good frontline defense to prevent a system from getting infected. It would be best to stick with a well-known program with good reviews that offers a full-protection suite. This would include antivirus, anti-malware, web browser, and phishing prevention on multiple devices.

The last option is to perform regular system backups. As stated in an earlier section, with certain malware you will be unable to remove them from the system. You will either have to do a clean install and lose everything or load a backup of your system from a point before it was infected. Backing up your system retains all of your information, programs, files, and settings. So, aside from the hassle of loading a backup and wasting your time in the process, you do not lose anything on the system.

#BeCyberSmart

MALWARE

How to identify it and remove it from your devices

Wanda T. Jones-Heath
Chief Information Security Officer
(CISO), DAF
Twitter: @SAF_DCIO
@SAF_CISO
https://www.safcn.af.mil/ciso/

Air Force Cybersecurity
To assure the effectiveness of
Air Force's core
missions by increasing the
cybersecurity and resiliency
of systems and information

SDC
AIR FORCE CYBERSECURITY
DEFENDING THE DOMAIN
NATIONAL CYBERSECURITY AWARENESS MONTH
UNITED STATES SPACE FORCE
NATIONAL CYBERSECURITY AWARENESS MONTH
UNITED STATES AIR FORCE

What is malware?

Malicious software, or Malware, refers to any program, script, or code that is harmful to electronic devices (computers, cell phones, tablets, etc.). Malware is utilized by criminal actors primarily to take personal information or make money off their victims through scams and advertisements. Once malware has entered your devices, it can take control of a system's processes to steal, encrypt, or delete any information stored there. Malware can also be used to gain unauthorized access to a network or alter permissions on the infected device to spy on the user's activity without their knowledge.

Types of malware

Malware can come in several different varieties and can have several purposes. In this section we will be covering some of the more common types of malware, a few of their characteristics, and known file names.

- **Virus:** *Probably the most common malware. Its specific purpose is to infect a system rapidly and cause damage to the core functions. It can also corrupt files and lock you out of the systems. Viruses are normally hidden within an executable file awaiting activation by the system or the user.*
  Examples: MyDoom, Storm Worm, Slammer

- **Trojan:***Just as the Greeks used a Trojan horse to enter the city of Troy, a Trojan is a type of malware that hides itself within a seemingly harmless file. Once the file is opened, it goes to work circumventing a systems security and creating backdoors that give access to other malicious files or criminal actors.*
  Examples: Backdoor, Exploit Rootkit

- **Worm:** *Just as worms tunnel through the earth, this malware tunnels through networks. These don't need a file to attach to and they replicate themselves from one system to the next. After executing on the new system, it can drop off additional malware, copy itself to devices physically attached to the system, delete files, and consume a lot of your bandwidth.*
  Examples:ILOVEYOU, Michelangelo, MSBlast

- **Adware:** *This malware is a type of software that can be very annoying. Its purpose is to infect a system, automatically download advertising content banners, and display pop-ups repeatedly when a user is active on their system.*
  Examples: Altnet, Ads by Gamevance, Virtumundo

- **Spyware:** *Criminal actors utilize this malware, as the name suggests, to spy on your activities on a system. From sites you visit, to user names and passwords, and even to banking information, this program sits in the background (unknowingly) and transmits the information back to the criminal actors.*
  Examples: Gator, Internet Optimizer, TIBS Dialer, Zlob

- **Hijacker:** *Hijacker is also a bit self-explanatory. It is utilized to hijack your internet browsers and alter settings, or it is configured to redirect you to advertisements, scam sites, or other malicious files.*
  Examples: GoSave, RocketTab, CoolWebSearch

- **Ransomware:** *This is one of the more recent malwares to be created and utilized. Its purpose is to gather important documents, files, programs, or your entire system and lock them until you meet the demands of the criminal actor. Normally paying them a substantial fee to get your items back.*
  Examples: WannaCry, Troldesh, NotPetya

How do I know if my system is infected?

Each malware acts in a very specific way and some are easily identified by their characteristics (e.g., adware or ransomware). However, there are several that you may not notice unless you are paying attention to your system. Here are a few items to watch out for:

- *Computer slows down.*
- *System crashes, freezes, or blue screens.*
- *Pop-ups or aggressively displaying ads.*
- *Increase in system's internet activities.*
- *Browser settings or homepage changes.*
- *New extensions or add-ons in your browsers.*
- *New programs or processes.*
- *Programs or applications close, function differently, or do not work at all.*

How do I remove malware?

Removing any malware is a very tricky process, and most of the time it may be easier and safer to do a new system install which is basically a factory reset for your computer. However, if you know what program contains malware specifically, you can normally find a YouTube video or instructions from several online sources with a simple web search. There is also the option of paying a third party (program or company) to remove the malware for you.

How do I protect myself from malware?

The most common ways you would get malware onto your system are by downloading files from unknown sources, surfing the internet and going to hacked/unknown websites,