Internet-based devices are present in every aspect of our lives. Constant connection provides opportunities for innovation and modernization, but also present opportunities for potential cybersecurity threats that can compromise your devices and information. Understand the threats to your devices, as well as built-in protection features to help keep your information and equipment safe and secure.

Malware

Malware, short for *malicious software*, is a term for viruses, worms, trojans and other harmful computer programs that scammers use to cause damage and gain access to sensitive information on a single computer, server, or computer network.

What to do if you have Malware

Removing malware can be extremely difficult. Malware, by design, will try to make itself almost impossible to remove. The only guaranteed way to remove malware is to reformat your computer and reinstall - which will delete all of your files. This is a reason why backing up your data is crucial. Hard drive reformatting is a stressful enterprise without a good backup, but a minor time annoyance otherwise. **In addition to restoring your computer or device to a previous state - you should change your passwords.**

Types of Malware

Adware

Adware is essentially abusive advertising software. This includes pop-up ads and "bundled" software such as browser toolbars. Some adware is innocuous advertising, but other instances of adware are highly manipulative and create an open door for other malicious programs. It is never a good idea to knowingly install or click on adware. When downloading software, be sure it is not also asking permission to download additional software on top of the desired product. When browsing be sure to use pop-up or script blockers.

Ransomware

Ransomware encrypts a computer's data so that it is inaccessible without a password. The ransomware distributor will then demand a certain amount of money, sent through an anonymous method such as bitcoin, in order to decrypt the computer data. There is oftentimes a time limitation for payment. After this time limit, the computer's files will be deleted. There is no way of knowing for sure if the criminal will decrypt your files after paying the "ransom". The best way to recover from ransomware is to recover your data from a backup. This is why it is essential to create strong backups of your data, especially the data that is crucial to your job.

Rootkit

Rootkits are designed to remain hidden on a victim’s computer while providing the scammer the ability to remotely control the computer and potentially steal sensitive information and cause significant damage. Rootkits can include viruses, worms, and Trojan horses and depending on the type, can perform remote modifications to the computer, steal personal information, execute malicious files, and potentially create bots.

Spyware

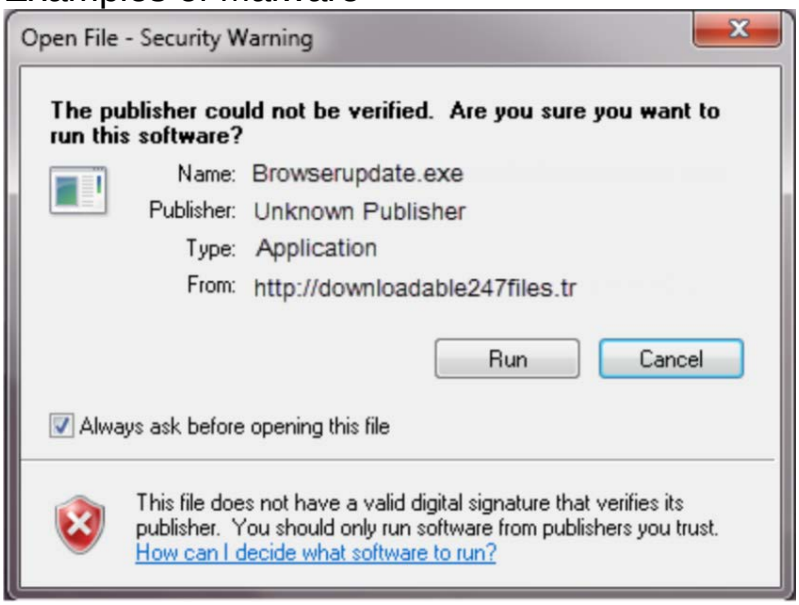
Spyware will record activity on a victim's computer and transmit the data elsewhere. This includes login information, browser history, and potentially other information. Spyware will try to remain hidden so that it won't be removed. It can also modify security and network settings.

Trojan Horse
A Trojan Horse malware will trick a user into downloading malicious software. A Trojan Horse will often disguise itself as an innocent file to download, but instead will provide someone else access to the computer where the scammer can steal information and/or install additional malware such as ransomware.

Virus
Viruses are malicious programs that will attempt to spread from machine to machine. They can attach themselves to files and programs shared between computers in order to infect as many machines as possible.

Worm
Worms are spread through networks, finding security vulnerabilities in programs and operating systems to infect machines. A computer worm has the ability to damage a computer, steal or delete information, and install bots.

Examples of Malware



In this example, the malicious file is seeking human permission to execute (.exe) or run. Analyzing the Publisher and the From can help to determine if the file is malicious. In this scenario, the file has an "Unknown Publisher" and the "From" address doesn't look legitimate.

If you receive a suspicious Pop-up Warning on your computer, prompting you to register for a computer scan, it may mean that you already have a form of malware on your device. You can use the Task Bar to force quit this pop-up and immediately run a computer scan using your trusted antivirus software.

If your computer screen suddenly shows an official looking message from a government agency suggesting that your system is in violation of a federal law and requires a form of payment to unlock the device, it is most likely a form of ransomware. If you receive this message on your device, disconnect from the network and contact the NOC IT Help Desk.

Public Wi-Fi Safety

Coffee shops, hotels, shopping malls, airports, and many other locations offer their customers free access to open public Wi-Fi. It's a convenient way to check email, catch up on social networking, or surf the web when you're out and about. These "open" networks also involve un-encrypted connections, leaving users at great risk. Cybercriminals can infiltrate unsecured Wi-Fi networks and intercept data such as banking credentials, account passwords, and other sensitive information that is transferred across the web.

Here are some useful tips on staying safe when using public Wi-Fi:

- *Treat all Wi-Fi networks with suspicion*: Don't assume that any Wi-Fi network is legitimate. It could be a bogus network that has been set up by a cybercriminal trying to capture sensitive information from unsuspecting users.
- *Verify it's a legitimate wireless connection*: Speak to an employee at the location that's providing the public Wi-Fi connection and ask for information about their legitimate Wi-Fi access point — such as the connection's name and IP address.
- *Avoid entering personal or sensitive information*: It's a good idea to avoid logging into websites that store or require the input of any sensitive information — such as online banking services or any websites that store your credit card information.
- *Consider using your mobile phone's network*: If you need to access a website that stores or requires the input of any sensitive or financial information, it is more secure to use your mobile phone wireless network to access the site instead of the public Wi-Fi.
- *Use a Virtual Private Network (VPN)*: The most effective way to stay safe on public Wi-Fi is to install a VPN on your devices. A VPN makes it difficult for criminals lurking on the network to steal your data and spy on your activities.
- *Keep software up to date*: Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent cybercriminals from being able to take advantage of known vulnerabilities.
- *Disable auto-connect features and always log out*: Turn off features on your computer or mobile devices that allow you to connect automatically to Wi-Fi. Once you've finished using a network or account, be sure to log out.
- *Ensure your websites are encrypted*: When entering personal information over the Internet, make sure the website is encrypted. Encrypted websites use https://. Look for https:// on every page, not just the login or welcome page. Where an encrypted option is available, you can add an "s" to the "http" address prefix and force the website to display the encrypted version.

Physical Device Security

Sometimes, our information doesn't get stolen by cyber criminals but rather by common thieves as we go about our day. Other times, we may accidentally lose a device. We store nearly everything on our phones, tablets, laptops, and desktops. Whichever the reason, we need to ensure that our devices and information on them are protected if we should lose access to them.

Below are a few ways you can assure your devices will remain secure:

Track and Protect Your Device

Each of your devices should have a strong, unique password or a unique PIN number with at least 6-digits. You can configure your mobile devices to erase data on the device automatically after multiple failed login attempts. If your device has a biometrics authentication factor, be sure to turn it on.

- iPhone, iPad, or iPod touch Passcode Settings
- Android Device Lock & Unlock Settings

If you have an iPhone (or most other Apple devices) you can track them through their GPS location using Apple's Find My iPhone. If you are on an Android device, and you've added a Google Account

to the device, you can track your phone through the Android Device Manager. These services will allow you to get an exact location, lock your device, and even wipe your device clean.

If you have your computer with you in the car and need to leave the vehicle for any reason, the computer should be placed in a locked trunk.

Use a Lockout Mechanism

Every time you leave you are not actively using your device it should be locked. This means locking your computer screen when you are stepping away from your workstation.

Be Aware of Your Surroundings

Tailgating

Tailgating, also referred to as piggy-backing, is when an unauthorized person follows an authorized person into a restricted building or area. Once inside of a restricted area, a tailgater could physically destroy computing equipment, steal valuable property, or access sensitive data.

Dumpster Diving

Criminals will often search through trash receptacles searching for items of value such as personal information or old tax documents. If you have physical documentation that contains sensitive information, it should be cross-shredded or placed in a blue or gray locked receptacle located around campus to be incinerated.

Shoulder Surfing

Shoulder surfing refers to spying on other users of a device in order to obtain personal access information. Shoulder surfing involves looking over a person's shoulder to gather pertinent information while the victim is oblivious. This is especially effective in crowded places where a person uses a computer, smartphone or ATM. The most commonly stolen data through shoulder surfing includes passwords, credit card numbers, and personal identification numbers (PIN).