ONLINE SAFETY BASICS

Malware and Botnets

The internet is a powerful and useful tool, but in the same way that you shouldn't drive without buckling your seat belt or ride a bike without a helmet, you shouldn't venture online without taking some basic precautions.

Viruses

Viruses are harmful programs that can be transmitted to computers and other connected devices in a number of ways. Although viruses differ in many ways, all are designed to spread themselves from one device to another and cause havoc. Most commonly, viruses are designed to give the criminals who create them some sort of access to the infected devices.

Spyware

The terms "spyware" and "adware" apply to several different technologies. The two important things to know about them are that:

- They can download themselves onto your device without your permission (typically when you visit an unsafe website or via an attachment).
- They can make your computer do things you don't want it to do, such as as opening an advertisement you didn't want to see. In the worst cases, spyware can track your online movements, steal your passwords and/or compromise your accounts.

Botnets

Botnets are networks of computers infected by malware (such as computer viruses, key loggers and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on websites or networks.

If your computer is infected with this malware and part of a botnet, it communicates and receives instructions about what it's supposed to do from "command and control" computers located anywhere around the globe. What your computer does depends on what the cybercriminals are trying to accomplish.

Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, addresses, telephone numbers and other personal information. The data is then used for nefarious purposes, such as identity theft, credit card fraud, spamming (sending junk email), website attacks and malware distribution.

Ransomware

Ransomware is a type of malware that accesses a victim's files, locks and encrypts them and then demands the victim to pay a ransom to get them back. Cybercriminals use these attacks to try to get users to click on attachments or links that appear legitimate but actually contain malicious code. Ransomware is like the "digital kidnapping" of valuable data – from personal photos and memories to client information, financial records and intellectual property. Any individual or organization could be a potential ransomware target.

Protect Yourself With These STOP. THINK. CONNECT.™ Tips:

- **Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- **When in doubt, throw it out:** Links in email, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- **Protect all devices that connect to the internet:** Along with computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Find more information at https://www.staysafeonline.org