MALWARE TIP CARD

Malware, short for “malicious software,” includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.

TYPES OF MALWARE

There are many unique types of malware that can infect your computer. Below is more information about a few of the more common types, according to the Department of Homeland Security’s United States Computer Emergency Readiness Team (US-CERT):

- **Adware:** a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites.
- **Botnets:** networks of computers infected by malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information.
- **Ransomware**: a type of malware that infects a computer and restricts access to it until a ransom is paid by the user to unlock it. Even when a victim pays the ransom amount, the stolen files could remain locked or be deleted by the cybercriminal.
- **Rootkit**: a type of malware that opens a permanent “back door” into a computer system. Once installed, a rootkit will allow additional viruses to infect a computer as various hackers find the vulnerable computer exposed and compromise it.
- **Spyware:** a type of malware that quietly gathers a user’s sensitive information (including browsing and computing habits) and reports it to unauthorized third parties.
- **Trojan**: a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer.
- **Virus:** a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely.
- **Worm**: a type of malware that replicates itself over and over within a computer.

WHY SHOULD WE CARE?

- Most cybercrime starts with malware. Cybercriminals use it to access your computer

or mobile device to steal your personal information like your Social Security number, passwords, credit card information, or bank account information, to commit fraud.

- Once cybercriminals have your personal information, they use the data for illegal purposes, such as identity theft, credit card fraud, spamming, and spreading malware to other machines.

SIMPLE TIPS

- **Keep a clean machine:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Keeping the software on your device up-to-date will prevent attackers from being able to take advantage of known vulnerabilities.
- **When in doubt, throw it out:** Links in emails and online posts are often the way criminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it.
- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- **Use strong passwords.** Make your password eight characters or longer and use a mix of upper and lower case letters, numbers, and symbols.
- **Use stronger authentication.** Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username. Visit www.lockdownyourlogin.com for more information on stronger authentication.
- **Back up your system.** By regularly backing up your important files, you minimize the risk of a complete system failure caused by malware.

IF YOU'VE BEEN COMPROMISED

Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist. If your computer has been compromised by malware, you can either consult with a reputable security expert to assist in removing the malware or use a legitimate program to help eliminate the infection[1]. Some legitimate programs are:

- F-Secure: http://www.f-secure.com/en/web/home_global/online-scanner
- McAfee: http://www.mcafee.com/stinger
- Microsoft: http://www.microsoft.com/security/scanner/en-us/default.aspx
- Sophos: http://www.sophos.com/VirusRemoval
- Trend Micro: http://www.trendmicro.com/threatdetector

[1] These programs are only examples and do not constitute an exhaustive list. The U.S. Government does not endorse or support any particular product or vendor.

The list below outlines the government organizations that you can file a complaint with if you are a victim of cybercrime.

US-CERT.gov

Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.

IC3.gov

File a complaint with the Internet Crime Compliant Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), at www.IC3.gov.

FTC.gov

If you think your computer or mobile device has been infected with malware, report it to the Federal Trade Commission at www.ftc.gov/complaint.

SSA.gov

If you believe someone is using your Social Security number, contact the Social Security Administration's (SSA) fraud hotline at 1-800-269-0271. For additional resources, visit the SSA at http://oig.ssa.gov/report-fraud-waste-or-abuse.

Stop.Think.Connect. is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™