TN Department of Finance & Administration

Strategic Technology Solutions

# 2021 NCSAM National Cybersecurity Awareness Month

## Week 4
## Cybersecurity First
## #BeCyberSmart

---

**CYBERSECURITY STARTS WITH YOU**

Every time you use the Internet, you face **choices** related to your security. Friends can be selected, links clicked, websites accessed, and wireless networks can be joined. Your security and the security of the nation depends on making **secure online decisions**. Making the Internet more safe and secure requires all of us to take responsibility for our own cybersecurity posture.

**CYBERSECURITY: WHAT IS IT?**

Cybersecurity is the art and science of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Cybersecurity is making sure that your online presence, your smart devices, your information in cyber space stays safe and out of the hands of the wrong people.

**POOR CYBERSECURITY?**

As with most things, being online has inherent risks. Some are more severe than others. But poor cybersecurity can make you, and often those you connect with, more **vulnerable** to those risks. Your computer can be vulnerable in many ways. A malicious attacker can hack into your system and change your files, or you can be attacked by malware. Even if you take the best precautions, you can't always prevent these things, such as:

- Exposure of customer data and the associated costs
- The costs of litigation
- Ransomware incidents -- if paid, ransomware can cost tens of thousands of dollars

**POTENTIAL THREATS**

- **Phishing**. Phishing attacks use emails and malicious websites that appear to be trusted organizations, such as charity organizations or online stores, to obtain user personal information.

- **Malware**. A computer can be damaged or the information it contains harmed by malicious code (also known as malware). A malicious program can be a virus, a worm, or a Trojan horse. Hackers, intruders, and attackers, all of whom are in it to make money off these software flaws. Despite their benign intentions and curiosity, their actions are usually contrary to the intended uses of the systems they exploit.

- **Identity Theft and Scams**. Identity theft and scams are crimes of opportunity, and even those who never use computers can be victims. There are several ways criminals can access your information, including stealing your wallet, overhearing your phone call, dumpster diving (looking in your trash) or picking up a receipt that contains your account number. While you cannot guarantee that you will not be a victim of identity theft, you can lower your risk by doing the following:

**SIMPLE TIPS**

Use and maintain **anti-virus software** and a **firewall**. Use an antivirus program and a firewall to protect your computer from viruses and Trojan horses that could steal or modify your data. When software notifies you of an update, called a **patch**, be sure to update as soon as possible to prevent hackers from exploiting known issues or vulnerabilities. Also, set-up an automatic, regular spyware scanning routine to catch vulnerabilities.

Establish computer usage **guidelines**. Help children understand how to use the computer, other connected devices, and the internet safely. Have candid, age-appropriate conversations with younger users to help them understand the do’s and don’ts of cybersecurity. These conversations can protect your data by setting clear boundaries and guidelines.

Double check email **attachments**. An email that looks as if it came from someone you know doesn't necessarily mean it did. It is possible for viruses to alter the return address so that it looks like the message came from someone other than the sender. Before opening any attachments, verify that the message is legitimate by contacting the person who sent it. Use caution even from people you know, be wary of unsolicited attachments.

Trust your instincts. As the old saying goes, “if it is too good to be true, it probably is.” Some antivirus software might not have the latest virus protections because attackers are constantly releasing new viruses. However, always be sure to scan documents and attachments with antivirus software before opening them. Do not open suspicious emails or attachments and turn off automatically downloading attachments. But always remember technology can only help so much, so trust your instincts!

For more information visit https://cybersafetn.gov

Best regards to all,

Curtis


**Curtis Clan** | Chief Information Security Officer, CISSP