TN Department of Finance & Administration | Strategic Technology Solutions

Cybersecurity and Privacy Bulletin

Top Cyber Threats

The Center for Internet Security (CIS) polled respondents and found that the Internet of Things (IoT) was the biggest cyber threat in 2017. This shouldn't be a surprise given some of the prominent cyberattacks of 2016 were bolstered by compromised IoT devices. Here are some quick primers on why these are threats to everyday users, and how you can work to protect yourself.

- Internet of Things (IoT): The top identified threat, the Internet of Things, is comprised of everyday objects and household items that are connected to the Internet; i.e., smart TVs, routers, smart thermostats and smart home devices. Although convenient, these devices often have very few security features, little to no security support and often remain in use with default passwords. These easily compromised devices can be used to attack others, slowing your Internet access and possibly preventing access to popular sites like Twitter, Amazon and Spotify. When purchasing and using IoT or connected home devices, be sure to:
    - Change the default passwords that come preloaded on the device to strong and unique passwords. . Use at least 8 characters including uppercase and lowercase letters, numbers and symbols
    - Keep up-to-date on patches and updates as they become available.

- Don’t Reuse Passwords: Unfortunately, many people tend to re-use the same login credentials between many of their accounts due to the difficulty of remembering multiple passwords. This can allow cyber criminals to take the stolen credentials and attempt to use them to access the compromised victims’ other online banking, shopping and other accounts.

- Don’t be quick to click on links or attachments.

    - APT: Advanced Persistent Threat (APT) refers to cyber threat actors operating for or on behalf of nation-state governments. They look to compromise, steal, change or destroy information for the purposes of espionage, disruption or destruction. State and local governments, critical infrastructure, universities and the employees of all of these entities are targeted by this threat. Users can reduce the risk from this type of threat by thinking twice before opening suspicious emails/attachments or clicking links.

    - Ransomware is a form of malware that aims to block a user from having access to their own systems by maliciously encrypting the infected computer’s files. Once access is blocked, the ransomware then requests money (a ransom) in order to restore access. Cyber criminals are commonly spreading this particular malware through malicious email attachments. Keep your systems and antivirus software patched and up to date with the most recent versions. Additionally, be extremely wary of suspicious emails, and do not open attachments or click on the links from untrusted sources.

- Cyber safety tips for home: Be suspicious of unsolicited emails, text messages and phone callers. Use discretion when providing information to unsolicited phone callers, and never provide sensitive personal information via email. If you want to verify a suspicious email, contact the organization directly with a known phone number. Do not call the number provided in the email. Ask the company send you something through the US mail (scammers won’t do this).Only open an email attachment if you are expecting it and know what it contains. Be cautious about container files, such as .zip files, as malicious content could be packed inside. Do not follow links embedded in an unsolicited email but visit websites by typing the address into the address bar. Keep your antivirus software up-to-date to detect and disable malicious programs such as spyware or malicious programs that can enable a remote attacker to have access to or send commands to a compromised computer.