TN Department of Finance & Administration | Strategic Technology Solutions

The future of IoT devices

Predictions about the future of IoT devices

What is the Internet of Things, or IoT?

The Internet of Things — IoT, for short — is made up of devices that connect to the internet and share data with each other. IoT devices include not only computers, laptops and smartphones, but also objects that have been equipped with chips to gather and communicate data over a network – everything from a smart speaker to a thermostat.

Connected devices offer convenience, like helping you make a grocery list, or savings, like when you turn down the heat at home remotely while you're on vacation.

Here are several predictions about the future of IoT.

By 2025, it is estimated that there will be more than to 21 billion IoT devices

With more than 4.7 billion things now connected to the internet, by next year, that will have increased to nearly 11.6 billion IoT devices. That number is expected to 21 billion in 2025.

Cybercriminals will continue to use IoT devices to facilitate Distributed Denial of Service (DDoS) attacks

In 2016, the world was introduced to one of the first "Internet of Things" malware — a type of malicious software that can infect connected devices such as DVRs, security cameras, and more. The Mirai malware accessed routers and IoT devices using the default password and usernames, then turned the affected devices into a botnet to facilitate a DDoS attack to overwhelm websites with internet traffic. The attack ended up flooding multiple networks, bringing a variety of major, well-known websites and services to a halt for hours. This type of malware is called "open source," which means the code is available for anyone to modify.

Artificial intelligence will continue to become a bigger thing

Smart home hubs, thermostats, lighting systems, and even coffee makers collect data on your habits and patterns of usage. When you set up voice-controlled devices, you allow them to record what you say to them and store those recordings in the cloud. In most cases, the data is collected

to help facilitate what is called machine learning.

Machine learning is a type of artificial intelligence that helps computers “learn” without someone having to program them. The computers are programmed in a way that focuses on the data that they receive. This new data can then help the machine “learn” what your preferences are and adjust itself accordingly. For instance, when a video website suggests a movie you might like, it’s has likely learned your preferences based on your past choices.

Routers will continue to become more secure and smarter

Because most consumer IoT devices reside in the home and can’t have security software installed on them, they can be vulnerable to attacks. Why? A lot of manufacturers work to get their IoT products to market quickly, so the security may be an afterthought. This is where the home router plays a very important role. The router is essentially the entry point of the internet into your home.

While many of your IoT connected devices cannot be protected, the router can help provide some protection. A router provides security, such as password protection, firewalls (to block unwanted access), and the ability to configure it to only allow certain devices to work on your network.

Router makers will likely continue to seek new ways to boost IoT security.

IoT Device Recommendations

If you connect, you must protect: Whether it’s your computer, smartphone, gaming console, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating system. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you’re using an external hard drive, make sure that your computer’s security software scans it for viruses and malware. Finally, be sure to periodically back up any data that cannot be recreated such as photos or personal documents.

Protect your cloud credentials: IoT devices normally use your everyday cloud credentials like Facebook, Google, Instagram and others, to setup, configure and operate. Those cloud credentials are the easiest way to gain access and compromise your IoT system. You can protect your cloud credentials by changing the password frequently, and refrain from using those credentials on public Wifi and PCs.

Today’s information security is much broader than simply the states network. STS’s mission covers all aspects of the security of the state’s data and information that includes; privacy, compliance, awareness, cyber incidence response and risk management. No longer is information security simply responsible for maintaining a secure network, but it now plays a key role in risk and reputation management for the state.

Information is the life-blood of any business; it is often the most valuable of a business’ intangible assets. Your awareness of the basics of cyber security is a major part of our state’s operational resilience strategy, and that strategy requires an investment of time and money. Your investment in reading and participating in this year’s National Cyber Security Awareness Month drives the actions and activities that builds and sustains a culture of cyber security.

Thank you for your continued efforts in helping to keep the states data secure, you are our first line of defense. If you see something cyber suspicious, please contact the STS Customer Care Center at 615-741-1001.

As always, we will continue to offer cyber security bulletins on how to further protect and secure your identity, your privacy or your personal computing.

And remember, sec_rity is not complete without U!

Best regards to all,

Curtis Clan | Chief Information Security Officer