MONTHLY
Cyber Security
Newsletter

Security Tips

Mississippi Department of
Information Technology Services

Security Services Division

May 2020

Six Steps to Securing IoT Devices and Taking Back Your Privacy

From the desk of Thomas F. Duffy, MS-ISAC Chair

In today's world we are more connected than ever — not only to each other but to our devices. For example, people now have the ability to open and close their garage doors and even start their cars directly from their phones. But what information do we put at risk when we do all of these amazing things?

Securing Internet of Things (IoT) devices and keeping personally identifiable information (PII) safe and secure these days is of the utmost importance.

IoT Information Collection

When you buy the latest IoT device, you need to be aware of two things: First, IoT devices collect your information, and second, that information is always accessible.

So, what exactly is information collection? Think of a common streaming service, like Netflix. Once you sign up, you'll start receiving emails from Netflix letting you know they've added a new TV show that you might enjoy. And the thing is, they're usually right! That's because your viewing history and ratings have been transmitted through an algorithm to determine what else you'd be willing to watch, and thus, continue your subscription. Now imagine every device you have on your home network collecting this type of information. It's a scary thought!

Keeping Your Information Secure on IoT Devices

While technology enables you to control your life from your fingertips, your information is at everyone else's fingertips as well. Security isn't fun or flashy, and because of this, some companies do not give it the consideration it deserves before they bring their products to market.

Very often when you buy an IoT device or utilize a company's service you have unknowingly allowed them to collect information about you. That agreement you have to sign before you can use any of their items is written by their lawyers, and unfortunately, without

Quick Guide:

6 Steps to Protect Yourself and Your Devices

1. Change Default Passwords
2. Automate Patches and Updates
3. Set-up Multi-factor Authentication (MFA)
4. Utilize a Password Manager
5. Update Default Settings
6. Avoid Public Wi-Fi

saying yes you can't use that fancy new gadget. All of these companies know it, which is why hundreds of pages sit between you and your new purchase.

6 Steps to Protect Yourself and Your Devices

1. **Change Default Passwords**: On devices that are connected to your network you should always make sure you change the default password. It doesn't matter if it's a new security camera or a new fridge. Creating new credentials is the very first step in securing your IoT devices and protecting your privacy. Research has shown that a "passphrase" is safer than a password. What does this mean? It means 1qaz!QAZ is less secure than Mydogsliketochasethechickensaroundtheyard! which is also much easier to remember.
2. **Automatic Patches and Updates**: In today's "set it and forget it" society, many electronic devices can take care of themselves. Quite often technology has a setting that allow for automatic updates. This is an important setting to turn on when securing IoT devices.
3. **Set-up Multi-factor Authentication (MFA)**: MFA security settings are growing in popularity. This is as simple as receiving a text or code that you need to type in while signing on to a system. Often times within the account preferences of your device, you can set up an Authentication Application. If you can't find this option call customer service, chances are it exists somewhere.
4. **Utilize a Password Manager**: Keep usernames and passwords unique. Most password manager applications can generate a random password for you, and will allow you to store them safely.
5. **Update Default Settings**: Check to see which settings are turned on by default, especially if you don't know what they mean. If you are unfamiliar with FTP or UPnP, chances are you are not going to use them or even notice that they are off.
6. **Avoid Public Wi-Fi**: It may be convenient to connect to a public Wi-Fi, but think again! If the Wi-Fi network does not require a password, then anyone can listen in on your computer's information. Some public Wi-Fi networks are deliberately set up in the hopes that people will use it so they can steal information or credentials.

   Remember that just like you lock your front door to protect the valuables inside, these days you also need to lock your IoT devices to protect your information and your privacy.

Provided By
MS-ISAC
Multi-State Information

STOP | THINK
CONNECT™