VA
U.S. Department of Veterans Affairs
Office of Information and Technology

Protecting Data When Using Internet of Things Devices

The Internet of Things (IoT) is the universe of internet-connected items. This includes your laptop, smartphone, wearables like smartwatches and virtual reality devices, as well as appliances, vehicles, cameras, gaming consoles, or anything else that you own that connects to the web. IoT devices are equipped with sensors, processing ability, and software that connect and exchange data with systems over the Internet.

Due to the vast array of IoT devices used at home and at work, hackers are constantly attempting to find unprotected or forgotten machines to gain entry to the network and extract sensitive data, especially on government networks. It is vital that all devices on a network be monitored and controlled to mitigate security vulnerabilities.

Securing Your Internet of Things

While this kind of connectivity provides great benefits, it also presents new privacy and cybersecurity challenges. Fortunately, with some precautions you can keep your IoT secure:

Do Your Homework: The security of IoT devices can range wildly. Before purchasing a new smart device, spend a few minutes researching it. Look up user reviews and see if there have been any security or privacy concerns. Find out what sort of security features the product has and understand its vulnerabilities.

Set Privacy Settings to Your Comfort Level: The moment you turn on a new smart device, immediately open its privacy and security settings. Configure them to your comfort level. Remember, many devices default to the least secure settings, and you shouldn’t assume those default settings are set to what you would like. Your device might default to sharing your behavior and location data with the manufacturer, for example. Think about what sort of data you’re comfortable with your devices collecting and sharing.

Enable Multi-Factor Authentication (MFA): Secure every device with multi-factor authentication if possible because this adds another level of security that cannot be breached even if a cybercriminal obtains your password. Common examples of MFA are authenticator apps or a code sent via text message.

Don’t Use a Feature? Disable It!: Just like how you set your privacy settings to your comfort level, think about what features of a device you use. IoT devices often come with features you will never need or use. See if you can disable those features to protect your security and privacy.

Change the Default Passwords: One of the most important steps you can take to improve a new device's security is to immediately change its default passwords. Default passwords are typically extremely easy to crack, but many people never take the simple step of changing them. Always create a password unique to that device that is at least 12 characters long and utilizes letters, numbers, and symbols.

Stay on Top of Updates: Beyond changing the default passwords, the next most important habit to keeping your Internet of Things secure is by keeping all your devices updated. When the manufacturer issues a software update, patch it immediately. Updates include important changes that improve the performance and security of your devices. Often, you can turn on automatic updates. This means that as soon as an update is available, your device will automatically download and install it, although you might have to restart the device for installation to complete.

Be Mindful of Where You Place Devices: Many smart devices feature microphones and cameras, and these can sometimes be activated without your permission. Sometimes this is caused by hackers, but sometimes the devices are designed this way to collect data. Either way, you should think about where you put smart devices in your home.

Remember, when you use smart devices, you need smart security!

For More Information Contact VA Privacy Service
Privacy Hotline: 202-273-5070 | Email VA Privacy Service