NATIONAL CYBERSECURITY ALLIANCE

IoT AT HOME: CYBERSECURE YOUR SMART HOME

Internet-connected devices are helping homeowners increase efficiency, reduce costs, conserve energy and a whole host of other benefits. However, with all of these benefits come risks to privacy and security. NCSA recommends consumers connect with caution, and take steps to secure these devices.

IOT SECURITY TIPS

DO YOUR HOMEWORK

Before purchasing a new smart device, do your research. Check out user reviews on the product, look it up to see if there have been any security/privacy concerns, and understand what security features the device has, or doesn't have.

CHANGE DEFAULT USERNAMES AND PASSWORDS

Many IoT devices come with default passwords. Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

PUT YOUR IOT DEVICES ON A GUEST NETWORK

Why? Because if a smart device's security is compromised, it won't grant an attacker access to your primary devices, such as laptops.

IoT stands for Internet of Things. **Consumer IoT** refers to the billions of personal devices, such as home appliances, smartphones, wearable technologies, toys, etc. that are connected to the internet, collecting and sharing data.

NATIONAL CYBERSECURITY ALLIANCE

IoT AT HOME: CYBERSECURE YOUR SMART HOME

IOT SECURITY TIPS

CONFIGURE YOUR PRIVACY AND SECURITY SETTINGS
The moment you turn on a new “smart” device, configure its privacy and security settings. Most devices default to the least secure settings--so take a moment to configure those settings to your comfort level.

DISABLE FEATURES YOU MAY NOT NEED
IoT devices often come with features you will never need or use. If you can, disable those features to protect your security and privacy.

KEEP SOFTWARE UP TO DATE
When the manufacturer issues a software update, patch it immediately. Updates include important changes that improve the performance and security of your devices.

THINK OF WHERE YOU PUT THEM
Particularly for listening devices or ones with cameras, think strategically about where you place them in your home. Do you want them in a child’s room or where you have sensitive work or family discussions? Designation some of the areas of your home as “safe” rooms from IoT devices.

ADDITIONAL RESOURCES

- **FTC**: Buying or selling a “smart” home? Read this: https://www.consumer.ftc.gov/blog/2018/01/buying-or-selling-smart-home-read
- **NIST**: What is the Internet of Things (IoT) and How Can We Secure It? https://www.nist.gov/topics/internet-things-iot
- **CISA**: Securing the Internet of Things https://www.us-cert.gov/ncas/tips/ST17-001