NATIONAL CYBERSECURITY ALLIANCE

IoT AT WORK: CYBER SECURE YOUR SMART BUSINESS

Internet-connected devices are helping businesses 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. Remember that every new internet-connected device you use is another entry point for a cyber criminal. NCSA recommends businesses connect with caution, and take steps to secure these devices.

TAKE-ACTION 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"

IoT refers to the billions of personal devices, such as personal assistants, smartphones, wearable technologies, security systems, etc. that are connected to the internet, collecting and sharing data.

staysafeonline STAYSAFEONLINE.ORG staysafeonline

NATIONAL CYBERSECURITY ALLIANCE

IoT AT WORK: CYBER SECURE YOUR SMART BUSINESS

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 any features you don’t need.

UPDATE SOFTWARE

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

THINK ABOUT WHERE YOU PUT THEM

Particularly for listening devices or ones with cameras, think strategically about where you place them in your office. Do you really want an IoT device with listening or camera capabilities in the same room you have sensitive/confidential conversations with colleagues? Designate some of the areas of your office as “safe” rooms from IoT devices.

CREATE A PROCESS

Don’t allow devices to be purchased or connected to your corporate network without first having been vetted by your trusted security professional.

ADDITIONAL RESOURCES

☑ **Cybersecurity and Infrastructure Security Agency:** Securing the Internet of Things
https://www.us-cert.gov/ncas/tips/ST17-001

☑ **National Institute of Standards and Technology:** What is the Internet of Things and How Can We Secure It?
https://www.nist.gov/topics/internet-things-iot

☑ **Trend Micro**: First Steps in Effective IoT Device Security:
https://www.trendmicro.com/vinfo/hk-en/security/news/internet-of-things/the-first-steps-in-effective-iot-device-security