Internet of Things

Who?

Short Answer: Anyone

Long Answer: Anyone can use Internet of Things Devices, in fact most of the time, they are great for people who need to use assistive technology.

What?

Short Answer: Any device that can make your home or office smarter.

Long Answer: The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

According to the FBI, as more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or smartphones, IoT devices also pose security risks to consumers.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

When?

Short Answer: Anytime

Long Answer: You can buy and use Internet of Things devices at anytime, it's as simple as buying an Amazon Echo or Google Home and some Wi-Fi connected light bulbs.

Where?

Short Answer: Your house, your office, anywhere.

Long Answer: You can use Internet of Things Devices anywhere there is an internet connection.

Why?

Short Answer: IoT devices can potentially be dangerous if not secured properly, cause they are susceptible to hacking.

Long Answer: The main IoT risks include:

- An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices. The UPnP describes the process when a device remotely connects and communicates on a network automatically without authentication. UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Cyber actors can change the configuration, and run commands on the devices, potentially enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping.
- An exploitation of default passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information.
- Overloading the devices to render the device inoperable.
- Interfering with business transactions.

What an IoT Risk Might Look Like to You?

Unsecured or weakly secured devices provide opportunities for cyber criminals to intrude upon private networks and gain access to other devices and information attached to these networks. Devices with default passwords or open Wi-Fi connections are an easy target for cyber actors to exploit.

Examples of such incidents:

- Cyber criminals can take advantage of security oversights or gaps in the configuration of closed circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers. Many devices have default passwords cyber actors are aware of and others broadcast their location to the Internet. Systems not properly secured can be located and breached by actors who wish to stream live feed on the Internet for anyone to see. Any default passwords should be changed as soon as possible, and the wireless network should have a strong password and firewall.
- Criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting. The exploits allow criminals to obtain administrative privileges on the automated device. Once the criminals have obtained the owner's privileges, the criminal can access the home or business network and collect personal information or remotely monitor the owner's habits and network traffic. If the owner did not change the default password or create a strong password, a cyber criminal could easily exploit these devices to open doors, turn off security systems, record audio and video, and gain access to sensitive data.
- E-mail spam attacks are not only sent from laptops, desktop computers, or mobile devices. Criminals are also using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail. Devices affected are usually vulnerable because the factory default password is still in use or the wireless network is not secured.

How?

Short Answer: Understand how IoT devices keep up to date.

Long Answer: NCSA encourages all Internet users to follow the message of STOP. THINK. CONNECT. Make sure connected devices have security precautions, think about the consequences of the data being shared, and then connect a device to the Internet with more peace of mind. Follow these tips for a safer and more secure IoT experience:

Keep clean machines:

- Understand how to keep IoT devices up to date, including through software updates or stronger passwords.
- Keep your mobile phone and apps up to date. Many IoT devices are controlled via smartphones or tablets. Keeping your phone and associated apps up to date is an important security step.
- Pay attention the Wi-Fi router in your home – it is the main way IoT devices connect to the Internet. Use a strong password and name the device in a way that won't let people know it's your house. Keep router software up to date.
- Keep an inventory of all Internet connected devices.

Own Your Online Presence:

- Understand what's being collected: Most IoT devices collect data. Take the time to understand what information your devices are collecting and how that information is managed and used.
- Know where your data goes: Many IoT devices will send your information to be stored in the cloud. Understand where the data will reside and the security protecting your information.
- Do your research: Before adopting a new smart device, research it to make sure others have had positive experiences with the device from a security and privacy perspective.

FBI recommendations for protection include:

- Isolating IoT devices on their own protected networks.
- Disabling UPnP on routers.
- Purchasing IoT devices from manufacturers with a track record of providing secure devices.
- When available, updating IoT devices with security patches.
- Being aware of the capabilities of the devices and appliances installed in your homes and businesses.
- Using strong passwords.