NCJTC National Criminal Justice Training Center *of* Fox Valley Technical College

Internet of Things

The Internet of Things (IoT) includes billions of devices worldwide. Devices possess a variety of data-capture capabilities and communications features. IoT devices bring convenience, improved networking and other innumerable benefits. Some devices can increase safety and collect data to help solve crimes and identify offenders.

When wrongfully used, IoT devices can assist criminals in furthering their misdeeds. Consequently, IoT devices offer both rewards and risks. Let's examine some IoT device capabilities, their risks, and some suggestions for risk mitigation.

What are a few examples of the devices and their capabilities?

Devices

- **Home devices**: Amazon Echo, Google Home, Nest, Philips, Airfy, Eero, Skybell, Feit
- **Wearables** - Internet of Bodies (IoB): Smart watches, Rings, Implanted chips, Air Tags
- **Vehicle-mounted**: Cameras, Smart License Plates, Geo-location devices
- **Mobile Phones**: Samsung, Apple iPhone, Xiaomi, Huawei, Oppo, Vivo
- **Security Cameras**: Ring, Arlo, Logitec, Eufy, Panasonic, Nest

Device Capabilities

- Track and record movement and bodily functions of persons, property and/or vehicles
- Record audio and video of persons, places and things
- Remote operation of lights, thermostats, cameras and other electronic and body-worn devices

What are some of the risks of IoT device misuse?

- Stolen/misused data
- Identity theft, Theft of the device, Distracted driving
- Hacking & manipulation of implanted or body/worn devices
- Harassment & stalking, Surreptitious eavesdropping
- Sextortion, Financial theft
- Phishing & Spoofing for collecting user information
- Theft of propriety information, business/trade secrets

How can risks be mitigated?

- Password Hygiene
- Multi-Factor Authentication
- Network Safety - Segmentation & Segregation
- Updating and/or replacing hardware & software
- Virtual Private Network (VPN)

Resources

Dictionaries

- Dictionary of Technology Words and Phrases – Techopedia -https://www.techopedia.com/dictionary
- Dictionary of Computer Words and Phrases - Tech Terms - https://techterms.com/
- Encyclopedia of Technology - Tech Target - https://www.techtarget.com/whatis/

Passwords

- Online security and safety – USA.gov - https://www.usa.gov/online-safety
- Top 5 password hygiene tips and best practices - Tech Target
  https://www.techtarget.com/searchsecurity/tip/Top-5-password-hygiene-tips-and-best-practices

Multi-Factor Authentication

- Multi-Factor Authentication – CISA - https://www.cisa.gov/mfa
- Amazon - Alexa -
  https://amazon.com/gp/help/customer/display.html?nodeId=G3PWZPU52FKN7PW4&tag=thewire06-20&linkCode=xm2&ascsubtag=YT250097
- Apple - HomePod, Homekit - https://support.apple.com/en-us/HT204915
- Arlo - Doorbells, Security Cameras - https://kb.arlo.com/000062288/What-is-two-step-verification-and-how-do-I-set-it-up
- D-Link - MyDlink Devices - https://youtu.be/-74GNECnvnc
- Ecobee - Thermostats, Sensors, Cameras - https://support.ecobee.com/hc/en-us/articles/360040957212-Two-Factor-Authentication-2FA-
- Eufy - Devices compatible with Eufy Security App - https://support.eufylife.com/s/article/Two-Step-Verification-for-eufySecurity-App
- Google - Home, Nest - https://support.google.com/googlenest/answer/9295081?hl=en
- Microsoft - XBox - https://support.microsoft.com/en-us/account-billing/turning-two-step-verification-on-or-off-for-your-microsoft-account-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca
- Nintendo - Switch - https://en-americas-support.nintendo.com/app/answers/detail/a_id/27496/~/how-to-set-up-2-step-verification-for-a-nintendo-account
- Ring - Cameras, Lights Alarms - https://support.ring.com/hc/en-au/articles/360024511592-Two-factor-security-authentication-with-Ring-products
- Sony - Playstation - https://www.playstation.com/en-us/playstation-network/two-step-verification/
- Wyze - Cameras, Locks, Thermostats - https://support.wyze.com/hc/en-us/articles/360024402052-Two-Factor-Authentication
- Yale - Smart Locks - https://us.yalehome.com/en/yale-news/blog/latest-blog-posts/introducing-biometric-verification-for-august-and-yale-locks1/

Networking Safety

- Network Security – Checkpoint - https://www.checkpoint.com/cyber-hub/network-security/what-is-network-secur
- Network Security – vmware - https://www.vmware.com/topics/glossary/content/network-security.html
- Network Security Tutorial Video – Edureka! - https://www.youtube.com/watch?v=k-k1cflOLnQ

- Router Settings - ThioJoe -5 Router Settings You Should Change Now! https://www.youtube.com/watch?v=mJnIgjyjEtc
- Secure IoT Network Configuration - Crosstalk Solutions - https://www.youtube.com/watch?v=6EIl8QeYbZQ

Updating Hardware & Software

- How to recognize and prevent cybercrime – CISA - https://www.cisa.gov/sites/default/files/publications/Week3TipCard-%20508%20compliant_0.pdf

Virtual Private Network

- What is a VPN? - Cisco - https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Other Resources

- Public Awareness & Prevention Guides – Europol - https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides

Frequently Asked Questions

Where can I report crimes involving my IoT devices?

- US DOJ: Crime should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement. https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime

How can I use my IoT devices to assist law enforcement?

- Some jurisdictions have "Community Camera Registration Programs". Home and business owners can register their cameras with local law enforcement for the purpose of permitting authorities to access video and/or audio pursuant to criminal investigations. Check with your local law enforcement agency to see if they have a program.

What can I do to protect my IoT devices?

- Travis Goodreau, IEEE Security: https://www.computer.org/publications/tech-news/trends/7-actionable-tips-to-secure-your-smart-home-and-iot-devices
  - Set up Your Router Correctly
  - Change the Router’s Default Name
  - Use the Highest Level of Encryption
  - Use Strong Passwords
  - Create a Separate Wi-Fi Network for IoT Devices
  - Disable Features You Don’t Use
  - Keep Your Devices Up-To-Date
  - Enable Multi-Factor Authentication
  - Employ a Next-Generation Firewall (NGFW)

What are some IoT device security tips?

- Purchase up to date IoT devices. Older devices may lack security features
- Do not buy used or refurbished IoT devices because they may contain modified hardware and/or software that makes them vulnerable to malware
- Change IoT device default usernames and passwords.

- Review device security settings and data retention terms of service
- Turn off indoor security cameras when not needed
- Disable voice purchasing on voice-active devices (Amazon Echo/Google Home)
- Educate yourself about the features, strengths, and weaknesses of your devices

What advice can I give to adults and seniors about avoiding becoming victims?

- NCOA: https://www.ncoa.org/article/protection-from-senior-scams
    - Don't act quickly based upon a falsely created sense of urgency; consult a trusted friend
    - Avoid odd payment types including gift cards and cryptocurrency
    - Be suspicious of fake caller ID's
    - Do not reveal personal information
    - Notify and seek advice from law enforcement

How can I use IoT devices to improve home security?

- Smartlocks for doors, Burglar alarm control units with door and window sensors
- Motion detectors, Cameras
- Time based or motion activated lights

What features do IoT devices have that can help solve crimes?

- Doorbell cameras and other indoor/outdoor cameras may retain audio and video that can be used to assist investigators towards solving crimes
- Smartwatch and/or fitness tracking devices and services may hold useful information
- Home assistant services may retain useful data about events and occurrences in a home
- Vehicles and associated services may have cameras, location data and other useful information

What can I do to disable the microphone on a "Smart" TV?

- Disclaimer Note: These actions may permanently disable the microphone. From Smarthomes - https://smartphonesoutions.eu/security/locate-and-disable-mic-on-smart-tv/
    - The microphone is most often placed in the TV casing facing the viewer. Look for a small hole the size of a pinhead, similar to the one found in a cell phone near the mouth area. Also note that there may be more than one microphone on the TV case.
    - An invasive and likely destructive method of blocking a microphone is to put plasticine or silicone in the hole.
    - A less invasive method is to use adhesive tape however this will only muffle the sound and not stop it.

What are the best methods for disposing of a device?

- Australian Cyber Security Center - https://www.cyber.gov.au/acsc/organisations-and-critical-infrastructure
    - Erase all data and personal information. Erasing your personal information ensures that no-one gains access to it after you have disposed of the device. Delete your online account if it is no longer needed without the IoT device.
    - Perform a factory reset of the device. A factory reset is designed to erase data kept in local storage and reset usernames, passwords and settings back to default. Check the device’s user manual or the manufacturer’s website for information on how to perform a factory reset.
    - Disassociate the device from mobile phones and other devices. Disposing of a device that still has access to your other devices, network or online accounts has the potential for others to gain access. Make sure you check your other devices and remove any pairing with the device you are disposing of. Remove any permissions granted to the mobile application that are no longer needed.

- Remove any removable media (e.g. USB flash drives, memory cards etc.) attached to the device. Removable media may contain personal data that is not deleted in a factory reset and should be physically removed, physically destroyed and disposed of separately from the device.

What technology is involved with IoT?

Sensors, micro controllers, companion circuit boards, relays, servo motors, Bluetooth networking, Zigbee networking, WiFi, Ethernet networking, LCD displays, touch screens, speakers, RFID tags, home based web servers, home network hubs, Low Powered Wide Area Networks, cellular networks, Internet broadband, cloud computing and others.

How is IoT useful in manufacturing?

IoT is used in manufacturing to improved product quality and improve plant availability. Sensors can measure tolerances of products in manufacture and alert operators if measured values drift beyond specifications. Sensors can monitor machinery for preventative maintenance. Bearing vibration can be detected early for scheduled maintenance instead of emergency maintenance. Motor use can be tracked to predict failure in advance. IoT devices save money, reduces downtime and create high quality products that have fewer returns.

How is IoT used for smart cities?

IoT can be used to monitor power, water, vehicular and pedestrian movement, climate and building energy management.

Disclaimer

This project was supported by Grant No. 5PBJA-21-GK-03995-INTE awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Version Date: September 2022