DATA PRIVACY MONTH: JANUARY 28 - FEBRUARY 28

At work, please forward all suspicious messages to abuse@ucdavis.edu.

Only seek IT technical support from 1-916-734-HELP.

Learn more: https://health.ucdavis.edu/itsecurity/

Security and Privacy in the Connected Home

Stay cyber-safe with your Internet of Things devices!

Did you ever wonder what it would be like to have smart home? You could remotely change the temperature in your house, you could tell your lights to come on, or ask your refrigerator if you need to get milk at the grocery store, all from your smart home device or smartphone. You could play video games and access all your streaming services from one device, or know who is at your door from your connected doorbell.

The Internet of Things (IoT) is introducing these features into our homes by rapidly applying connectivity to everyday appliances and home features. As IoT devices become a part of our daily lives, we need to address the added security risks and privacy concerns that are reintroduced by smart technology.

Read on for more information on how to enjoy a connected home while keeping your data private and secure.
Internet of what? Internet of Things! What’s that?

The Internet of things (IoT) is the network of devices that contain electronics, software, actuators, and connectivity that allows them to connect, interact, and exchange data. IoT extends Internet connectivity to devices and everyday objects, embedding them with technology so that they can communicate and interact over the Internet and be remotely monitored and controlled.

Be Cyber-Smart with IoT Devices

- If you don’t need to connect a device to the Internet, don’t. If a device isn’t connected, it isn’t as big of a cybersecurity risk.
- Isolate IoT devices from other devices on your network by creating a separate Wi-Fi network just for them. This protects your other devices if your connected IoT devices are compromised.
- Research the privacy, security, and accessibility options that are available to customize your device. You may find some options that provide greater security and privacy if you opt in. Take advantage of the extra security when a device offers multi-factor authentication (MFA). MFA allows you to use your password and username with an added step of receiving a verification code or providing a fingerprint through a scanner. If MFA is available, it’s worth using.
- Always update your devices and apply patches when available. When selecting which IoT devices to purchase, make sure they offer patching and updates from the manufacturer to keep them up-to-date. Enable auto-updates on any IoT devices that support them.
- Setup a separate unique, strong password for every device. Don’t share credentials across devices.
- Replace devices when they are no longer supported by the vendor, as security flaws will remain unpatched.
- Turn off Universal Plug and Play if it is available on the device. You don’t want the device having this ease of connectivity with so little control.
- When requested to provide information to use a device, do not provide personally identifiable information (PII) like Social Security Numbers and dates of birth. If you must share PII to use the device, you may want to consider a different make or model or keeping it off your home network.