Internet Society

Top tips for Internet of Things security and privacy.

1. **Learn how to "shop smart" for connected devices.** You don't want to have to return a connected device because it is spying on you. Returning things is a pain. Learn how to "shop smart," and buy privacy respecting connected devices so you won't have to.
   - **Read the reviews.** Consumer organizations and others review connected devices and toys as part of their buying guides. Mozilla and Which? Both released buying guides for smart toys this last holiday season. See **advocacy.mozilla.org/en-US/privacynotincluded** and **www.which.co.uk/news/2017/12/connected-toys-buyers-beware-this-christmas/**
   - **Read the user agreement.** User agreements should tell you what data a smart toy collects. They also should tell you who they share that data with. Will they send your child's data to advertisers or other third parties?
   - **When buying a device, make sure it can be updated.** Another factor to consider is how long the developer will support the device with updates.
   - **Ask yourself, does this need an Internet connection or Bluetooth functionality?** If you cannot tell if a toy is safe and privacy-respecting, it may be better to buy a similar toy without the Internet or Bluetooth functionality.
2. **Update your devices and its applications.** If a device or app has an auto-update feature, turn it on! Are you really going to want to take the time to update it later? Often this is as easy as a couple of clicks. And don't forget to update the less obvious devices. Anything that's Internet connected, from your light bulbs to your thermostat, should be updated.
3. **Turn on encryption.** Some devices and services have the capability to use encryption, but don't turn encryption by default. This is like owning a safe, but leaving it unlocked. Take a few minutes to see if your devices or services are already using encryption or if you need to turn it on.
4. **Review the privacy settings on your devices and their applications.** You may be sharing a lot more than you intended through your device or its applications. Review your privacy settings to determine who can see your data on the device. Ask yourself, who do I want to see this sort of information, and who do I not want to see it. Important: when possible, avoid linking your device or its applications to social media accounts. Your social media platform does not need to know how many steps you took today, so don't tie your fitness tracker to your social media account!
5. **Stop reusing passwords.** It is tempting to reuse a password for multiple devices or services. How are you supposed to remember different passwords for everything? But, while reusing a password may be easier for you to remember, if hacked or stolen, it also makes it easier for criminals to gain access to your other devices or services. Take a few minutes to get a secure password manager and learn how to use it, or, for home devices, write down your passwords in a securely stored notebook.
6. **Use a strong password.** In addition to not reusing passwords, make sure you are using a strong password. Do not just use the default password, a simple guessable password, or a password that uses easily-accessible personal information. For those of us not willing to write down passwords or use a password manager, **this article** provides advice for creating a strong password that you can still remember.
7. **Turn off the device or disconnect it from the Internet when not in use.** To minimize the risk your device may pose to others, turn it off or disconnect it when no one is using it.
8. **Take steps to make your home network more secure.** By protecting your home network, you limit your device's exposure to online threats and help mitigate the risk devices on your network may pose to others. An easy way to make your network more secure is by using encryption, a strong password, and firewall for your home WiFi network. Firewalls are often built into routers and simply need to be turned on.

More information: internetsociety.org/getiotsmart