THE SMART HOME CYBER HYGIENE CHECKLIST

Our homes are becoming smarter and, as cool as that is, what's even cooler are people who are as smart as their smart homes.

The last thing we want is a cyber criminal being able to unlock our smart locks or take a peak through our smart cameras.

With that said, here is a Smart Home Cyber Hygiene checklist.

BEFORE YOU DO ANYTHING

Be sure you actually need to connect.
The best and easiest way to protect yourself from the dangers brought on by the digitally-connected age is to not connect if you don't need to. Does your refrigerator really need to be able to send you text messages? Does your toaster need to be able to take a selfie?

Research before you buy.
Keeping your smart home secure starts with what you buy. It's a good idea to stick to well-known, established brands with a strong track record in hardware, as much as possible. Look for devices that make it easy to update software, change default passwords or disable unnecessary features.

Consider professional installation.
If things seems too complicated, get some help and let the pros make sure your smart devices are installed with security in mind.

DURING THE SET UP

Register with the manufacturer.
This will allow you to get all the new software updates. Also, make sure to check what permissions have been granted during the set up - don't allow access to anything that isn't necessary.

Set up a guest network.

Make sure to give the guests in your home the ability to log onto a separate network that doesn't tie into your IoT devices.

Safeguard your devices.

Make sure you change your default username and password (This is good advice for anything). Also, turn off other manufacturer settings that don't benefit you, like remote access, which could be used by cybercriminals to access your system.

Two-Factor Authentication.

If your smart-device apps offer two-factor authentication, make sure to take advantage of it. This gives you an added layer of authentication on top of your password, like a code sent to your phone. Two-factor authentication makes things harder on the criminal.

ONGOING THINGS TO CONSIDER

Update!

Good advice for any technology is to make sure that your device software is always up to date.

Know What You Have Connected.
The best way to have a secure mindset with smart devices is to know what devices you have actually connected to your home network. If you don't know, simply turn off your Wi-Fi and see what stops working.

Consider an upgrade.

Is it time to upgrade anything you already have for a more secure device?

Watch out for outages.

A hardware outage may result in an unsecured state for your device. Make sure you check on them after you notice an outage.

Avoid public Wi-Fi networks.

Public Wi-Fi is super vulnerable to attacks. Never manage your smart devices from a public Wi-Fi connection. Use your data, a secure VPN or wait until you come home.

WHEN MOVING ON

Factory reset devices before getting rid of them.
When you decide to throw away, sell or give away your smart device, make sure you take the necessary precautions to remove all your data. Don't let the next person get their hands on it or give them the ability to communicate with other devices on your network.

By Danny Pehar