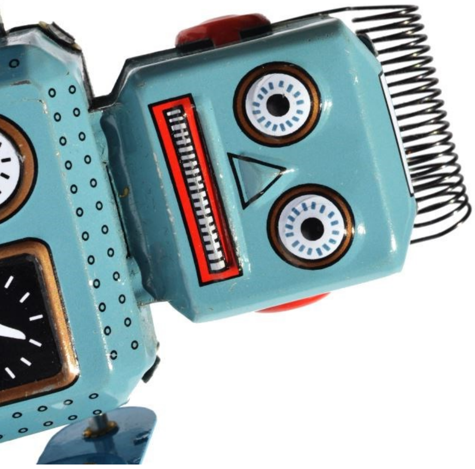
# 10 Smart Tips to Keep Hackers out of your Home

Did you know your smart TV, baby monitor, fridge and thermostat are a way for cyber criminals to break into your personal network?



Just as you'd protect your work networks with software and passwords, you need to transfer those same online practices to your home to protect your devices from being hacked.

To keep devices quick and easy to use, they're often launched with default codes, passwords and user names that aren't changed, exposing your IP addresses to the internet where hackers can find them. These security flaws can be used to breach home devices, exposing personal and financial information, computer files, webcams, thermostats and smart TVs. This could be theft, ransom, hijacking. With 80% of consumers using home networks, the risk of a cyber attack is high.

It's possible that a personal device could be commandeered by a hacker and you wouldn't realize it. Unlike a computer, where you would notice that it was running slower or access to your email might be locked, it's more difficult to tell if someone is nosing around your smart refrigerator or accessing the baby monitor.

You might notice the light on your camera is on when you're not broadcasting, or the connected thermostat starts heating when you haven't turned the heat on, or the refrigerator starts to thaw out. Smart televisions also have very real vulnerabilities and allow hackers and others access into a home without anyone being aware that they are being watched…

**How do hackers find your network?** Generally hackers are opportunists, looking for sheer volume for DNS attacks. Some devices such as smart TVs provide an opportunity for ambient listening so a hacker could hear what's going on in your house. It's possible to turn off this option, which frequently operates when the TV is turned on. Since the camera on the TV could be activated, this also becomes an invasion of privacy issue.

**1. Don't forget those updates**
It's important to make sure that appliances, phones and other electronics have the latest updates and security patches, since they frequently fix vulnerabilities that have been discovered since the device was issued.

**2. Keep social media and financial activity separate**
Clicking on the wrong link can allow a Trojan or other virus to enter your computer. Consider using one computer just for financial transactions like online banking and another for social media, email and other online activities. Secure your routers and other devices added to a home network to prevent unauthorised intrusions.

**3. Yes, security matters**

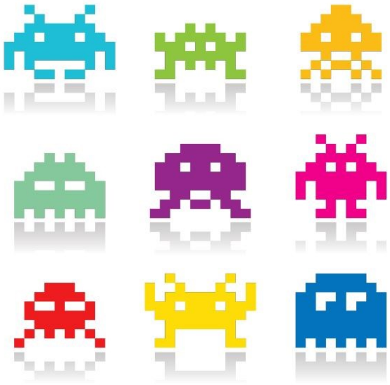
Just like you would protect your network at work, the same basic computer hygiene also applies to your home. If you're using WiFi, don't broadcast the network name. Make sure to change any default settings, names or passwords when installing new smart devices. Install new devices behind a firewall rather than linking them through a home computer. The risks have also changed with technology. Instead of hackers taking over and encrypting your computer, they can take over your thermostat and turn it down in the dead of winter and hold it for ransom until you pay the ransom.

**4. Set up authentication**

Many online accounts from your email to financial organizations offer two-factor authentication - a password and a code sent to a mobile device or email to verify who is accessing the account. Setting up dual authentication provides an added layer of protection for your accounts. Make sure that passwords are complex (not birthdays or children's names), difficult for someone to guess and include a combination of letters, numbers and symbols.

**5. Secure your smartphone**

We do everything on our smartphones from online banking and shopping to buying movie tickets and more. If you have not password-protected your phone, set it up immediately. Many phones also offer a fingerprint access option as well. Why is this important? Most smart devices have some sort of smartphone app that allows you to access it from your phone, making it a critical entry point to your house for anyone who commandeers your phone.



**6. Make smart app purchases**

Only purchase apps from recognised app stores such as Google, because those purchased from third parties may not have the same level of testing for flaws. Also make sure to read the privacy policies so you know who has access to your information, what information is being accessed and who it will be shared with. Beware of downloading any apps that prompt you to do a quick download, because these versions may include malicious code or security flaws that would allow hackers access to your device.

**7. Turn off the Bluetooth option**

When you're not using the Bluetooth feature on a device, turn it off to prevent any ambient listening or access by unauthorized persons. Most mobile phones, tablets and other items offer this type of functionality. Devices such as baby monitors and smart speakers can then be hacked through the Bluetooth function.

### 8. Purchase new devices

When buying IoT devices, purchase those that are unopened and unreturned from retailers. Some people will buy devices, infect them with a security flaw or malicious code and then return them to the retailer. Look at how the device is made, designed and how it is used, and change the passwords when you connect them.

### 9. Wipe your information

If you're purchasing a new device and disposing of an old one, wipe any data and reset it back to the factory default settings to make sure any personal information is removed and inaccessible to someone who might gain access to the device.

### 10. Check your insurance policies

In the event of a breach, check your homeowners' or identity theft insurance policies since the policies may help provide access to forensic and other experts who can help with the aftermath. In addition, some level of indemnification coverage may be available for identity theft or other effects from the breach.

Once a hacker accesses a home network, they may be able to control a full range of devices that manage the home's environment.

### What to do after the cyber attack

If one or more of your devices are hacked, disconnect it immediately without altering any settings or running any scans. Find a professional forensics firm who can help identify how far the attack went and what was impacted. Contain and remediate the situation without destroying the ability for a specialist to follow what happened.

Where to report the breach depends on the type of incident involved. In the case of identity theft, it may be necessary to file a police report and notify all financial institutions such as banks and credit card companies.

The bottom line is to be aware of what you're doing. Understand the risks associated with deploying this technology and treat these devices as you would your computer.

If you're concerned about your risks in this area, talk to La Playa about how insurance can help.

**Credit:** PropertyCasualty360 Patricia L. Harman, October 31, 2016