Safe Home

SAFE CIRCLE

Many homes today contain Smart Home products. Have you ever wondered are your devices protected? Can someone hack me using my smart items? Understand the risks and take advantage of available security features. Whether you have a full smart home network or just a simple voice assistant, there are steps you can take to ensure no one hacks your home.

What is IoT?

Internet of Things (IoT) are everyday objects that connect to the internet. These connected devices can be activated using voice commands or controlled by downloading and using an app or via a Bluetooth or Wi-Fi connection. They are otherwise known as smart objects; i.e. smart tvs, thermostats, etc.

Know the Risks

This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed. The scale of interconnectedness created by the Internet of Things increases the consequences of known risks and creates new ones. Attackers take advantage of this scale to infect large segments of devices at a time, allowing them access to the data on those devices or to, as part of a botnet, attack other computers or devices for malicious intent.

Secure your home network and your router

- Change the default username and password
- Change the default SSID
- Log out of the management website for your router
- Configure Wi-Fi Protected Access 2 (WPA2)
- Disable Wi-Fi Protected Setup (WPS)
- Turn the network off when not in use
- Disable Universal Plug and Play (UPnP) when not needed
- Upgrade firmware regularly
- Disable remote management
- Monitor for unknown device connections using your router's management website

Home Networking Tip

Consider creating a separate network and password for guests.

Having a separate guest network and a unique guest password allows you to control network traffic and helps protect the password for your personal home network. Remember to use strong passwords for both the guest network and your personal network.

Deloitte.

For questions and additional resources, please contact safecircle@deloitte.com.

Safe Home

What is a voice assistant? A voice assistant is a digital assistant that uses voice recognition and voice synthesis to listen to specific voice commands and return relevant information or perform specific functions requested by the user.

Learn how to secure your voice assistant.

Alexa, Google Assistant, Siri, Cortana, or others — can do cool things like tell you the weather, order your favorite pizza, or turn your lights off before bed. And, depending on which permissions you give, voice assistants may also do things like read your emails and access your calendar and contacts. They can listen all the time, ready to be activated by a "wake word" (like "Alexa" or "OK, Google"). But they might even turn on and start listening when you least expect it. Here are some privacy questions to consider, along with some different ways to secure your voice assistant:

Know when it's listening

Each time you interact with it, your voice assistant records what you say. It might also do that when it thinks it's heard the wake word. If you want to be sure, that sensitive information isn't picked up by your smart speaker, look for settings to mute your device so it's no longer listening. Check your settings or the manufacturer's website to find out how to do that.

Check the privacy policy

Some voice assistant manufacturers have had employees listen to audio recordings say, to make their products work better. Check the privacy policy for your voice assistant to understand how your audio recordings are handled and who can listen to them.

Check your settings

Periodically, look at your history and delete old recordings. You can do this by going to the voice assistant app or account on the manufacturer's website. You also may be able to set it to auto-delete recordings.

Lock down your login

Create a strong password for your voice assistant. Avoid common words, phrases, or information in your passwords. Don't reuse existing passwords from other accounts. If another account gets hacked, a hacker could try that password to get into your voice assistant. For more tips, check out this Password Checklist.

Know what's connected to your voice assistant

It might be convenient to enable shopping, or to link your email account so your voice assistant can read your emails out loud. But do you want everyone who uses your voice assistant to be able to shop, or get your emails? If not:

- Add a PIN to control whether others can use voice commands to buy things
- Check to see if you can add a passcode for access to your email
- Check your settings to find out how to make these changes

Source: How To Secure Your Voice Assistant and Protect Your Privacy | Consumer Advice (ftc.gov)

Deloitte.

For questions and additional resources, please contact safecircle@deloitte.com.

Deloitte.

For questions and additional resources, please contact safecircle@deloitte.com.