Smart speakers (like the Amazon Echo shown here), appliances, and equipment connect to the Internet, allowing you to access information using voice commands, or use your mobile device or computer as a wireless controller for the smart equipment.

In this chapter, you'll learn about smart speakers and smart appliances, and discover how to overcome their potential security vulnerabilities. Topics include:

- ➔ Introduction to the Internet of Things (IoT) and smart appliances, in-home equipment, and home security tools
- ➔ Get acquainted with smart speakers and digital assistants and how to securely interact with them

BONUS

2

Work with Smart Appliances, Smart Speakers, and Home Security Tools

The Internet has become the world's largest collection of information, and it's expanding every day. In addition to computers and mobile devices being able to easily tap in to this vast and ever-evolving resource, all sorts of electronic equipment within your home can now access the Internet.

Although all this Internet-connected technology is designed to make your life easier, it's important to set up this equipment—and your home Internet service—properly to address some of the potential security vulnerabilities related to the use of these technologies.

What Is a Smart Home?

The buzzword that describes Internet-connected technologies is *Internet of Things* or IoT. What this means is that in-home appliances, security tools, and electronic devices can access the Internet to gather information and be remotely controlled or managed using a compatible computer, smartphone, smart watch, or tablet that is running a special app.

Smart speakers and digital assistants built in to mobile devices, smart watches, and computers have introduced yet another way to easily interact using voice commands.

Amazon offers its Echo line of smart speakers (www.amazon.com/echo) that includes a virtual assistant known as "Alexa." Google offers its Google Home, Google Home Max, and Google Home Mini smart speakers (https://store.google.com/us/product/google_home) that allow users to say, "Okay, Google," and follow up with a question or command. The same Google digital assistant is built in to all Android-based mobile devices.

Apple's HomePod smart speaker (www.apple.com/homepod) works with the company's Siri digital assistant, which is also built in to all Macs, iPhones, iPads, and Apple Watches. Windows 10 (or later) PCs have the Cortana digital assistant (www.microsoft.com/en-us/cortana) that responds to voice commands.

With each passing week, these digital assistants are being integrated with more types of smart equipment, allowing for this equipment to be controlled using voice commands via a computer, smart speaker, smart watch, or mobile device. Google, for example, boasts that more than 5,000 smart home devices (from more than 150 brands) can be controlled using Google Home equipment or the Google digital assistant.

With the right smart lighting system installed in your home, you could simply say, "Hey Siri, turn on the living room lights," or by installing a compatible thermostat, you could say, "OK Google, adjust the temperature to 72 degrees."

If you want to hear a specific song or listen to your favorite album using a smart speaker or mobile device, upon subscribing to a music service, such as Apple Music, Pandora, Spotify, or Amazon Prime Music, use the voice command, "Alexa, play *Sgt. Pepper's Lonely Hearts Club Band*," and the popular Beatles album will

begin playing. These music services give you on-demand access to more than 45 million songs and albums.

When you're thinking about going outside and want a weather report, simply ask the smart speaker or digital assistant for the current weather forecast, or if you're packing for a trip, ask for an extended weather forecast for the city you're traveling to. By linking your Amazon Echo smart speaker with your Amazon Prime account, for example, you can also place orders for almost anything Amazon.com sells by asking for it. For example, you could say, "Alexa, order a six-pack of Bounty paper towels."

Check for Compatibility

Amazon, Google, and Apple's smart speakers and digital assistants each work with their own collection of smart devices, appliances, music services, and online services, although there's a lot of overlap. First determine which smart speaker or digital assistant you plan to use, and then make sure you purchase smart equipment that's compatible with it.

With so many smart speaker models now available, prices have dropped dramatically, as have the prices for smart electronics and appliances. This technology can also be used to help you feel safer in your home, or protect your home while you're away.

Smart home security systems, remote video cameras, and video doorbells are readily available, easy to install, and most work with Internet-connected smartphones, tablets, computers, smart speakers, and smart watches.

There is growing concern that the smart equipment manufacturers can track what you're doing by tapping into or monitoring the communications between you and your equipment. Theoretically, these manufacturers could use (or potentially misuse) the data, or sell it to third parties.

Plus, there's always the threat of hackers being able to intercept and potentially monitor your activities as they relate to your smart equipment use. Cybercriminals could also potentially hack in to the smart equipment manufacturer's servers to steal private information about customers who use the company's smart equipment.

Taking Security Precautions When Using Smart Home Equipment

As with all Internet-related activities, in general, using these technologies is safe, secure, and practical, as long as you take the proper precautions.

These precautions include the following:

- Installing a firewall to your home Internet service. (Chapter 1)
- Using a virtual private network when connecting to the Internet using your computer, smartphone, and/or tablet. (Chapters 1, 2, and 5)
- Turning on the Wi-Fi Protected Access (WPA2) encryption protocol feature. Consult with the owner's manual for your modem or wireless router for how to turn on this feature, or call your Internet service provider. WPA2 is an industry-standard security protocol that helps smart equipment establish a secure connection with your home Internet service, in much the same way a VPN helps your computer or mobile device establish a secure connection to your Internet service.
- Creating and using strong account passwords, keeping the passwords secure, and not accidentally sharing them. Remember, a strong password should not be obvious to other people. It should contain at least six characters and incorporate upper and lowercase letters, as well as at least one number. Never use the word "password," your first/last name, your birthday, your pet's name, your spouse's name, your child's name, your anniversary date, or other obvious information. And don't use a username or password that relates to your name, address, or phone number when setting up smart equipment that'll be used within your home.
- Making sure you set up the smart equipment correctly.
- Adjusting the equipment's built-in parental controls and/or guest account controls, so you maintain full control over who can access and use the smart equipment while visiting your home, or remotely.
- Understanding what information is potentially being collected, analyzed, stored, and used by the smart equipment, smart speaker, and/or voice assistant's manufacturer, and how it's being used.

- Purchasing only smart equipment from well-known and reputable manufacturers instead of less expensive, generic brands that you've never heard of that may not adhere to the latest industry guidelines or standards pertaining to security or privacy.
- Changing the factory default settings for each piece of smart equipment for your home, whether it's a smart light system, thermostat, remote door lock, or a major appliance, to use a unique username and password, as well as how it's identified on your network (when applicable).
- Not connecting your smart equipment to a public Wi-Fi Internet connection. Connecting to a public or your neighbor's Wi-Fi in the immediate geographic area can create a security vulnerability that hackers can exploit.
- Installing the most current software updates to the equipment, and use it with the most recent version of the equipment's proprietary mobile app on your mobile device. Using the most up-to-date version of your computer or mobile device's operating system and web browser is also important.

Using Smart Security Cameras for Remote Viewing

Low-cost remote video cameras, video doorbells, remote door locks, and home security systems offer peace of mind when you're at home or away because they can help protect against unwanted intruders.

If you'll be using this type of smart equipment, make sure you set up a secure password for accessing the equipment remotely.

Some people grant access to this type of smart equipment to caregivers or relatives that live elsewhere as a way to check on them remotely. If you choose to allow others to remotely access the live video feeds (and audio) from your home video cameras, make sure you know what areas are covered, and that the equipment is positioned to offer security as well as ample privacy.

Be sure to revoke access to people who no longer need it. For example, if you no longer employ a housekeeper or caregiver, change the passwords to your smart equipment immediately.

Also, instead of sharing the master account password for certain types of smart equipment (such as remote door locks), when possible, set up guest accounts. These offer limited functionality that you can also monitor and easily deactivate at any time.

Being Aware of Security Precautions When Using a Smart Speaker

A smart speaker is designed to be connected to your home Internet service and have continuous Internet access. The speaker continuously monitors its surroundings, listening for the command designed to activate it, such as "Alexa," "Hey, Siri," "Hey, Cortana," or "Okay, Google."

The speaker analyzes your spoken question or command and accesses the Internet or remotely controlled smart devices in your home to comply with your request. Smart speakers have been around since 2014, and they've become extremely popular. They are very affordable, and what they are capable of continues to expand.

What's important to understand is that your smart speaker itself is not too intelligent. To use its "intelligence," it must digitally record what you say and send the recording to a remote server, where a state-of-the-art artificial intelligence program analyzes the recording (within a few seconds), and instructs the speaker what needs to happen next.

When a smart speaker transmits information that it collects from your home via the Internet, there is potential security vulnerability, especially if your home Internet connection is not secure.

When setting up a smart speaker, have it learn your voice, and be sure to set the parental controls so your kids or grandchildren can't start issuing commands to make online purchases or control equipment in your home.

Learn to Speak to Your Smart Speaker

After you set up and install a smart speaker (or use the digital assistant that's built in to your computer, smartphone, smart watch, or tablet), take the time to learn what it's capable of, and learn how to speak with it to achieve the desired results.

Because the capabilities of this technology are continuously evolving, periodically do an Internet search for a complete directory of commands your smart speaker or digital assistant will understand. For example, if you own a Google Home smart speaker, type the search phrase, "Google Home commands" into a search engine's Search field.

It's Not All Good

Smart Devices Are Often Listening

The purpose of a smart speaker or digital assistant is to constantly listen for the command "Hey, Siri," "Okay, Google," or "Alexa," to wake up and process your command, question, or request. By default, however, some equipment—such as a smart TV or cable TV/DVR (digital video recorder) boxes—is listening to conversations and gathering information about your viewing habits to anticipate what you'll request next.

The TV manufacturers or cable TV companies can use this information to learn about your habits and personalize advertising to you. If you have smart equipment that can monitor conversations in your home, such as a TV, you can turn off the feature via the device's Settings menu. You may have to search for the proper Settings command by accessing multiple submenus to find it, but if you're not comfortable with your smart equipment listening in your home, turn off the feature.

After a software update is installed, menu options are sometimes reset to their default settings, so you may need to again turn off the feature that allows the equipment to "listen" to your conversations.

Some smart video cameras automatically record and store security video footage on a remote server (via the Internet). Decide whether you're comfortable having this footage stored remotely, potentially giving third parties access to it.

As you're shopping for smart equipment, do some Internet research on the security of that product. For example, if you're about to purchase a smart lighting system, in a search engine's Search field, type, "*[Insert Smart Lighting Make and Model]* Security Issues," and read articles about product security vulnerabilities or customer complaints.

When you set up your smart equipment, pay careful attention to the wording of the privacy policy from the equipment's manufacturer and agree to the terms only if you're

comfortable with them. Make sure you understand how and what information will be collected, monitored, shared, and potentially sold by the manufacturer.

Keep in mind that the privacy laws in most states (and at a federal level) are several years behind the technology. The laws don't adequately protect consumers who use smart equipment.

Tapping in to the Potential of Smart Home Technology

Whether you want to make equipment in your home remotely controllable, or you want the added security of having a caretaker or relative be able to remotely check in on you, smart home technology offers tremendous potential.

Many consumer electronics stores and hardware stores (such as Best Buy and Home Depot) have entire departments dedicated to smart home technology where you can see demonstrations of the latest equipment and learn what's possible. After the equipment is set up and installed correctly, as long as you maintain a secure Internet connection in your home, most smart home equipment is easy to use and offers minimal privacy and security risks.