Securing smart speakers and digital assistants

Smart speakers and digital assistants like Amazon Echo, Google Nest, Apple HomePod, and Sonos Era are integral to many modern households.

These devices offer convenience and efficiency, from controlling smart appliances with your voice to playing music to providing quick answers to questions like, what's the temperature outdoors? However, security risks come with this convenience. By following some simple steps, you can enjoy your devices and protect your data.

1. Understand the risks

Like any device or gadget that connects to the internet, digital assistants are vulnerable to cyber threats. Hackers can exploit these devices to gain unauthorized access to personal information and device data, which could include eavesdropping on conversations. Cybercriminals might also use them as entry points to your home network and other devices, like your laptop. Being aware of these risks is the first step toward staying safe online.

2. Do your homework

Research security features and privacy policies beyond comparing prices and features when shopping for smart speakers. Check out user reviews, media critiques, and, especially, any reports of security issues related to a smart speaker brand. Choose reputable brands with a history of providing regular security updates and support.

3. Change the default password right away

With any internet-connected device like a smart speaker, your first action should be changing the default password. Not only are default passwords usually short and easy to guess, but some device manufacturers publish them online. While the process of changing the default passwords is different for different devices, here is generally what to do:

1. **Access device settings:** Open the app associated with your smart speaker.
2. **Find security settings:** Navigate to the security or account settings section.
3. **Change password:** Create a strong password unique to the account, at least 16 characters long, and a random mix of letters, numbers, and symbols.

Use a password manager to generate and store strong passwords!

4. Turn on multi-factor authentication (MFA)

Multi-factor authentication (MFA) adds an extra layer of security to an account or device by requiring additional verification beyond your password. You can typically enable MFA through the app settings associated with your smart speaker.

5. Configure privacy settings to your comfort

When you set up a new smart speaker, it's crucial to configure its privacy settings to match your comfort level. Be aware of what data, including audio recordings, the speaker collects and how that data is stored. Using the privacy settings in the device's app, decide what data you're comfortable sharing and turn off unnecessary data collection. Pay special attention to how your voice recordings are handled—you can delete them regularly.

6. Turn on automatic updates

Manufacturers regularly release software and firmware updates that are vital for maintaining the security of your smart speakers. These updates often include patches for security vulnerabilities, for example. Install updates as soon as they are available for your device. We recommend turning on automatic updates so your device always has the latest security enhancements.

7. Use a guest wi-fi network for smart devices

To keep your computers, smartphones, and everything else connected to your home wi-fi network, you should set up a guest network for your Internet of Things devices, like your digital assistant. Since all connected devices are a point of access to your router, using a guest network for your smart speakers enhances security by isolating them from your main network. While the process might be different for your router, to set up a guest network, you should:

1. **Access router settings:** Log in to your router's admin interface, which might be an app on your phone.
2. **Create a guest network:** Set up a separate guest network for your smart devices. The password should still be unique, long, and complex!
3. **Connect devices**: Connect your smart speakers and other IoT devices to this guest network. Also, when company comes over, have them connect to the guest network instead of your main network.

8. Disable unnecessary features

Smart speakers often come with numerous features, and you might not use all of them. Disabling these reduces the risk of their exploitation by cybercriminals. Some features you might have turned on but never use might include:

- Remote access features.
- Integration with social media.
- Unused third-party skills or apps.

By disabling unnecessary features, you reduce the "attack surface" of your digital assistant.

9. Think about where you place your speaker

Smart speakers are equipped with microphones and, sometimes, cameras. Because of this, they should be placed strategically around your home.

- **Avoid sensitive areas:** Don't place devices where you have sensitive conversations or want privacy, such as bedrooms or home offices.
- **Designate safe zones:** To ensure privacy, keep certain rooms free from digital assistants.

Mindful placement ensures unauthorized surveillance can't happen where you value privacy the most. Although rare, smart speakers could possibly be used to listen in to your household, although they're more likely to be used for "botnets." Additionally, well-established brands are much more secure than cheap ones.

10. Monitor device activity

Keeping an eye on device activity logs will help you spot suspicious behavior. Open the app associated with your smart speaker and navigate to the activity log. This feature might also be called the security log. Check your smart speaker

regularly, like every few weeks, if it “lives” in one location. If you notice anything suspicious, act immediately. This probably includes changing the device’s password. You should also contact customer support for more assistance.

Smart speaker security is important!

Securing your smart speakers and digital assistants is crucial to protecting your privacy and data. By adopting a few behaviors, you significantly bolster the security of your smart home. Stay aware and proactive to ensure your digital assistants serve you safely and securely.