

# A guide to the security of voice-activated smart speakers

**An ISTR Special Report**

**Analyst: Candid Wueest**

**November 2017**

Contents

Executive summary, key findings, and introduction

Voice assistants and smart speakers: What you need to know

What are the risks?

Conclusion

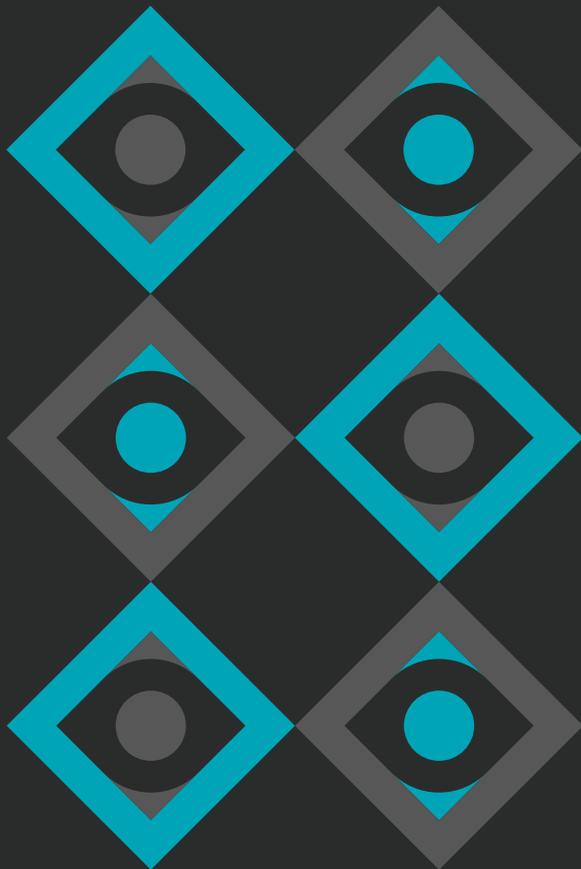
Protection



# Contents

- 3 **Executive summary, key findings, and introduction**
- 5 **Voice assistants and smart speakers: What you need to know**
- 6 [What do they do?](#)
- 6 *Other “smart” assistants*
- 7 [Actions, skills, and Easter eggs](#)
- 8 [Amazon Echo Dot](#)
- 8 *20 Alexa Easter eggs to try*
- 8 *20 Google Assistant Easter eggs to try*
- 10 [Google Home](#)
- 11 **What are the risks?**
- 12 [Security – Who can interfere with your device?](#)
- 12 *Get by with a little help from your friends (and family)*
- 12 *The curious child attack*
- 13 *The mischievous man next door attack*
- 14 *Television troubles*
- 15 *Stranger danger*
- 15 *Smart speakers could go loopy*
- 15 *Wi-Fi worries*
- 17 [Privacy](#)
- 18 *Deleting recordings*
- 19 **Conclusion**
- 21 **Protection**
- 22 *Configuration tips*
  
- 23 [About Symantec](#)
- 23 [More Information](#)

# Executive summary, key findings, and introduction



Section

00



## Executive Summary

Voice-activated smart speakers are very popular and are now integrated in many everyday objects. After smartphones, they are the next big step for voice assistants. The market is currently dominated by Amazon Alexa's Echo range, which holds 73 percent of market share, with more than 20 million devices in the U.S. alone, followed by Google Home, which holds nearly all the rest of the market.

In the course of our investigation, we found that voice-activated speakers can be triggered unintentionally through voice commands embedded in websites or TV advertisements. We also discovered that the wake-up word does not always have to be accurate to trigger the device, for example, the Google Assistant woke up for "Ok Bobo", demonstrating that unintentional triggering does happen, even during normal conversations. Fortunately, most of the commands that could be triggered inadvertently are more likely to be a nuisance than a serious security threat, and could lead to things like alarms going off during the night. The fact that smart speakers are always listening also brings up a lot of privacy concerns, however, it's important to note that the encrypted recordings are only sent to the backend once the wake-up word has been heard. So far, there is no evidence to suggest that the recordings are sold to external companies, but they are of course processed and archived by the service provider. The major providers have already started to offer free calling features, so smart speakers might soon take the place of landline phones in homes.

Also of note is that many smart speakers blindly trust the local network, meaning any compromised device in the same network could change the settings of the smart speaker or perform a factory reset without the user's agreement. Therefore, having a secure local network and a strong account password is important. A strong password is particularly important considering anyone with access to the account can listen to old recordings or change the settings of the device over the internet.

With some devices capable of conducting voice purchases, it is important to secure the settings and monitor notifications. An important security feature of smart speakers is the ability to distinguish between voices, but this is not foolproof yet.

## Key findings

- The biggest threat to the security of your voice-activated smart speaker is the other people who can access it
- It's not just other people: the TV, radio, websites, and even other smart speakers can all mess with your device—causing it to play pranks or malfunction
- Privacy concerns are still one of the biggest issues when it comes to smart speakers
- Wake-up keywords can be misheard, e.g. "Ok Bobo" triggers the Google Assistant to wake up
- Voice identification is an important feature, but current versions can still be fooled
- Attackers that gain access to the local network can change the settings of Google Home devices or perform a factory reset
- When the linked email account gets compromised, then the device could be used to spy on people
- The most likely attack vector is through vulnerabilities in streaming services, but so far we haven't seen this vector being used in the wild

## Introduction

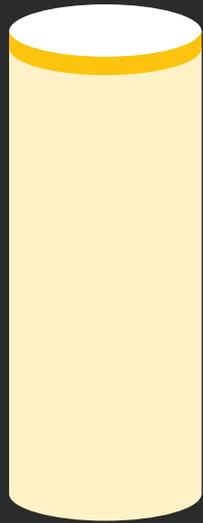
Smart speakers with built-in voice-activated assistants arrived on the scene in the last few years, with the aim of making people's lives easier, allowing us to access the perfect recipe with ease, and change our music selection without leaving our chairs.

An array of companies have announced or already sell smart speakers that integrate with Google Assistant (Google), Siri (Apple), Cortana (Microsoft), and Alexa (Amazon). Amazon Echo, Google Home, and the Apple's HomePod are probably the best known examples. But, while they make life easier in some ways, could they also be endangering people's privacy and online security?

As well as reading out recipes and playing music, some of these devices also come equipped with cameras that can be operated remotely, while others allow you to order goods online using just your voice. The range of activities that can be carried out by these speakers means that a hacker or even just a mischief-minded friend or neighbor could cause havoc if they access these devices.

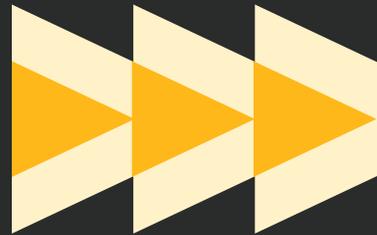
In this paper, we detail a range of issues we found with these devices, including software weaknesses, configuration issues, and badly designed processes. We will go through these issues and provide recommendations on how to connect and configure these devices as securely as possible.

# Voice assistants and smart speakers: What you need to know



Section

01



## What are voice assistants and smart speakers?

Siri, Cortana, Alexa, and Google Assistant are just some of the numerous voice assistants that exist today, with the smart speakers that have them integrated set to become a staple of modern-day living.

Smart speakers, also known as “smart home voice-activated assistants”, come in many different shapes and sizes. Put simply, they are music speakers combined with a voice recognition system that the user can interact with. Users use a wake-up word to activate the voice assistant, such as “Alexa” or “Ok Google”, and they can then interact with the smart speaker using just their voice: they can ask it questions or request that it start playing music.

There are many different types of smart speakers and voice assistants on the market at the moment [see panel], with varying levels of capabilities. Some are open for third parties to use and allow integration into cars or fridges. For example, BMW announced some of its cars would come with a built-in Alexa voice assistant in 2018, and Sonos, which manufactures speakers, has made a similar announcement. Some hotel chains have already added voice-activated smart speakers to all rooms. There are also services such as [Houndify](#) that allow users to add a voice assistant to other devices, and there is even a [Kickstarter](#) project for a flying voice assistant. As can be seen, the market for smart speakers is growing rapidly at the moment.

### Other “smart” assistants

- Apple’s HomePod, based on Siri
- Third-party speakers with integrated Cortana from Microsoft
- [MyCroft](#), an open source AI that can run on a Raspberry Pi
- Samsung [Bixby](#)
- [Djingo](#)
- [AI Buddy](#)
- [Eufy Genie](#), based on Alexa
- [Nestlé XiaoAI](#), which focuses on nutrition knowledge

According to [research by Consumer Intelligence Research Partners](#) (CIRP), the current market in the U.S. for voice-activated smart speakers is dominated by Amazon Echo (with a share of 73 percent) and Google Home (with 27 percent). There are 20 million Amazon Alexa-powered Echo units in the U.S. alone, and this is trending upwards. With these statistics in mind, for the purposes of this investigation, we focused on two of the most widely used devices:

- Amazon Echo Dot, based on Alexa
- Google Home, based on Google Assistant

## What do they do?

The main usefulness of smart speakers is that the voice-activated assistant can access all the intelligence in the backend: once activated through the keyword, it sends a recording to the backend for analysis. In the background, it makes use of speech recognition (SR) and natural language understanding (NLU) to understand the commands. The context of this is then analyzed in the cloud and a reply is sent back. The device is always listening for the trigger keyword (“Alexa” is the default in the case of the Echo Dot, and “OK Google” in the case of Google Home). The word or phrase is detected locally on the device, and only once it is matched is a recording made and sent back to the Amazon or Google servers, although a tiny fraction of sound from just before when the matched keyword is said is also sent back. The device is always listening, with no need for activation by pressing buttons or doing anything else. This reality might disconcert some people, and if it does, all the popular devices have a hardware button that allows you to mute the microphone. However, this does mean that when you want to use the voice assistant again you will have to physically unmute the device, which somewhat defeats the purpose of voice activation. [Studies](#) indicate that the voice interface could become popular among elderly people who might not want to walk to the device all the time.

The main usefulness of smart speakers is that the voice-activated assistant can access all the intelligence in the backend

Most users use these devices to switch on music, ask questions about the weather or the traffic, set alarms and reminders, or walk through a cooking recipe in hands-free mode. Smart speakers can also be used to connect to other smart home devices, allowing them to interact with the smart TV, the lights, the thermostat, or even the smart door locks. A popular option is the [If This Then That \(IFTTT\) service](#), which allows different smart systems to interact. For example, using this, a user could define that items on their reminder list are automatically synced to the To Do list on their smartphone, or that the surround system is switched on when the TV is turned on. Both Google Home and Amazon Echo smart speakers have announced that they will allow users to create “shortcuts” to condense multiple commands into a single keyword. These shortcuts are called routines and will help to automate complex processes.

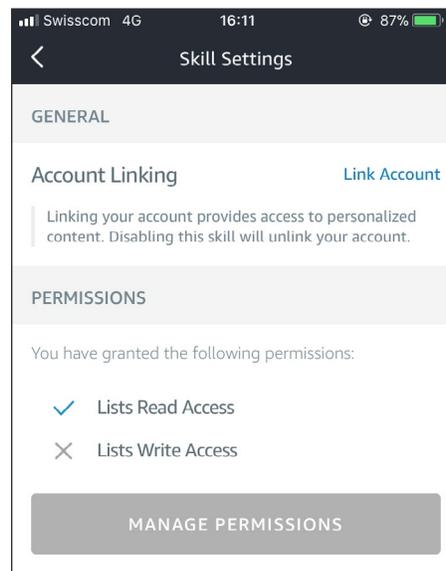
## Actions, skills, and Easter eggs

The capabilities of voice activated assistants can also be extended by additional add-on services: for Amazon Alexa they are called skills and, in October 2017, there were more than 25,000 [different](#) skills available. These skills allow the voice-activated assistant to do things like order a pizza, call a taxi, access specific news portals, or interact with other smart home devices in specific ways. With so many skills, there is already a fight for popular invocation keywords. An Alexa user can trigger a skill by saying keywords like “open”, “ask”, “launch”, “tell”, “play” or “start”, followed by the name of the app. For example, saying “Alexa, play 20 questions” will start a guessing game. This will automatically enable the skill for the given profile and list it in the smartphone app. Of course, there is the slight chance that some people may not realize they are triggering an app as the invocation word could be a common word. The Google Assistant has similar capabilities called actions, with a few hundred different ones currently available.

Anyone can create a free skill and publish it on the Amazon list. Skills are web services that will receive the transcription of the spoken command from the Amazon backend through an HTTPS request. The service then sends back the corresponding answer, which is sent to the device where it gets translated into speech. Hence, the backend service has control over what information is revealed to the app developer.

If a provider of a skill wants to access the user’s To Do or shopping list, then a special permission has to be granted in the skills section of the Alexa app on the smartphone. Once a customer grants permissions, the skill will have access to the user’s Alexa lists until permissions are explicitly revoked. At any time, the user can change the allowed access for that skill in Manage Settings on the skill’s page in the Alexa app.

The capabilities of voice activated assistants can also be extended by additional add-on services: for Amazon Alexa they are called skills and, in October 2017, there were more than 25,000 [different](#) skills available.



Alexa skills permission dialog

The purpose of this report is not to examine how useful voice assistants are, it is to determine how secure they are, but if you are interested in examining their usefulness, there have been [various tests](#) on how good and useful the answers of voice assistants really are. What can be said for sure is that all of them are improving rapidly. Voice assistants are also getting better at learning the context of a question: if you ask for a steak restaurant nearby and then ask if they are open, it will know that you mean that specific restaurant.

As well as add-ons and shortcuts, most voice assistants have so-called [Easter egg](#) phrases [see panel]. This means that if you ask them a specific question or say a specific phrase they will answer with a funny response. They have no real purpose and are just for amusement. For example, when you tell Alexa to

## 20 Alexa Easter eggs to try

- Alexa, self-destruct.
- Alexa, what is the Prime Directive?
- Alexa, use the Force.
- Alexa, open the pod bay doors.
- Alexa, what does the fox say?
- Alexa, sing “Happy Birthday.”
- Alexa, execute Order 66.
- Alexa, who shot first?
- Alexa, what is a day without sunshine?
- Alexa, what is the Third Law?
- Alexa, is Santa Claus real?
- Alexa, rap for me.
- Alexa, tell me a random fact.
- Alexa, what comes with great power?
- Alexa, it’s a trap!
- Alexa, where is Chuck Norris?
- Alexa, are you Skynet?
- Alexa, beam me up.
- Alexa, never gonna give you up.
- Alexa, when is the end of the world?

“beam me up” it will play the beam sound from Star Trek. Try out some of the examples in the box above to see what your voice assistant says back.

## Amazon Echo Dot

The Alexa voice assistant powers the Amazon Echo Dot. The Dot is part of a range of Echo speakers offered by Amazon, all of which are powered by Alexa. As well as the Dot, this range includes: Echo, Echo Tap, Echo Plus, Echo Look, Echo Show, and Echo Spot. These devices range from small ones with just a tiny speaker to larger ones with a camera and display. The newly announced Echo Plus has a new design, and comes with features such as a ZigBee hub for smart devices like lightbulbs, while the Echo Spot, which looks like a smart alarm clock, has its own display. Another new device is the Echo Buttons,

## 20 Google Assistant Easter eggs to try

- OK Google, meow like a cat.
- OK Google, clean my room.
- OK Google, tell me about Alexa.
- OK Google, what did my cat say?
- OK Google, aren’t you a little short for a Stormtrooper?
- OK Google, is the cake a lie?
- OK Google, surprise me.
- OK Google, do you speak Morse code?
- OK Google, where’s Waldo?
- OK Google, is your refrigerator running?
- OK Google, flip a coin.
- OK Google, how do you like your coffee?
- OK Google, spin the wheel.
- OK Google, what is your quest?
- OK Google, crystal ball.
- OK Google, who you gonna call?
- OK Google, show me the money.
- Ok Google, beatbox.
- OK Google, what am I thinking right now?
- OK Google, serenade me.

which allows users to interact with the Amazon Echo through Bluetooth, during trivia games, for example. The Echo range was first launched at the end of 2014, and it has seen significant growth in that time.

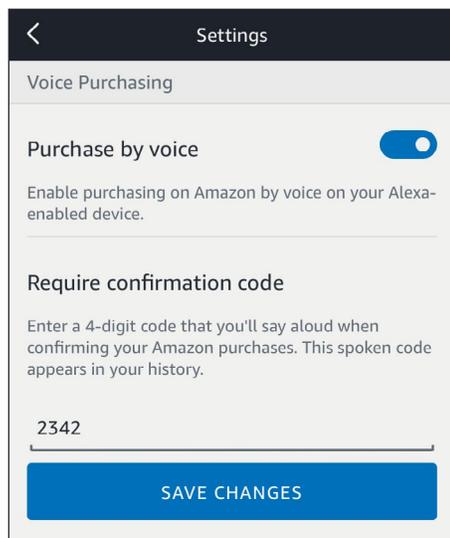
The Dot that we tested has a small built-in speaker that can be connected to a higher-end speaker through Bluetooth or with a cable, if required. The device wakes up when you say “Alexa”, although you can configure it such that the wake-up word is “Amazon”, “computer”, or “Echo” instead.

The settings for the device can be configured through a smartphone app or through the [Alexa.com website](https://alexa.com). This is also where you can listen to all previous recordings and delete them if you want. However, deleting all recordings may degrade the learning factor for your specific voice pattern and mean you

have to start again from scratch. The Dot automatically checks for updates and downloads and installs them.

There is **cooperation** between Microsoft's Cortana and Alexa, allowing each voice assistant to use the power of the other service, for example, by saying "Alexa, open Cortana", or vice versa.

The voice purchasing option is enabled on the Alexa assistant by default, which means that anyone can use the assistant to order goods if the linked account is a Prime account with one-click ordering enabled. An order can be issued by saying something like "Alexa, order batteries". Items can also be added to the shopping list for later by saying "Alexa, add paper towels to my cart". However, Alexa will describe the item and tell you the price before it is ordered. Any order has to be verbally confirmed and a notification is sent by Amazon allowing for cancellation within 30 minutes. Optionally, a four-digit PIN code can be enabled for security. This is definitely a recommended option if you want to use the purchasing feature. The Voice ID feature that should be able to distinguish between different voices was not available at the time of testing. According to the description, if Alexa recognizes your voice, it will not ask you for the purchasing PIN code anymore, if one is enabled.



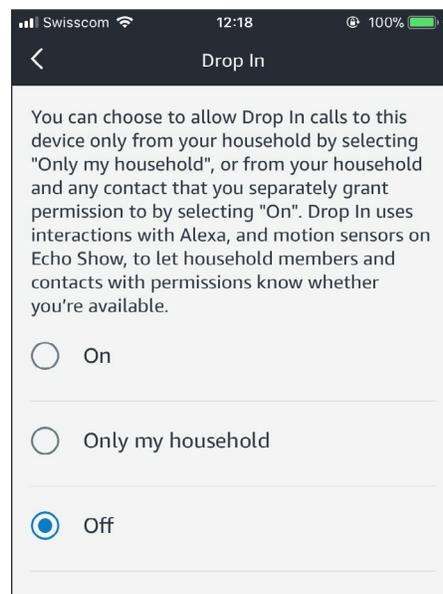
Alexa voice purchasing settings

Amazon Echo devices also offer a feature called **drop-in** and voice calls in some countries. At the time of writing, it is available in the U.S., the U.K., Germany, and Austria. This feature is not on by default; a user needs to enable Alexa Calling and Messaging first and then enable the "drop" function. The owner of a device can then authorize other people from their

address book to call in and use the device as an intercom. When a remote user drops in, the receiving user at home will hear a beep and see a green glow, but does not have to do anything to accept the drop-in call. This might sound a bit scary, especially in connection with the Echo Show device, which has an integrated camera and screen. However, a user can disable the drop-in feature in the settings or limit it to authorized contacts.

The voice purchasing option is enabled on the Alexa assistant by default, which means that anyone can use the assistant to order goods if the linked account is a Prime account with one-click ordering enabled.

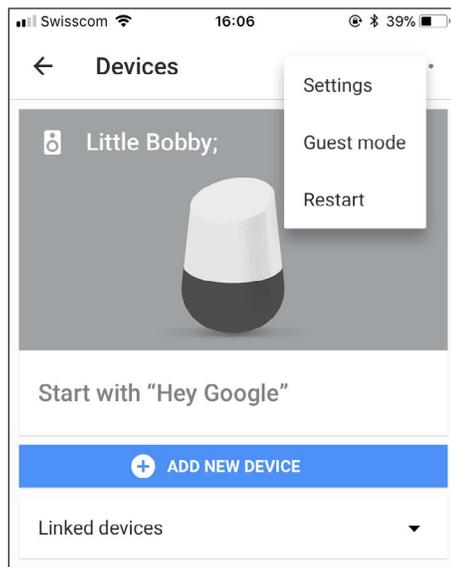
Besides the drop-in feature, Alexa is also capable of making calls, and sending voice messages or text messages to Echo devices, and to the Alexa app on smartphones. However, if you want to enjoy some quiet time, Alexa offers a Do Not Disturb mode. In order to enable it, simply say "do not disturb me". It can be disabled again by the user saying "turn off, do not disturb me". Amazon also recommends that users periodically update their contacts book so the device can better match who can be called.



Alexa drop-in settings

### Google Home

In October 2017, Google announced two new smart speaker models: the Google Home Mini and the Google Home Maxi, increasing the total number of speaker variants in its range to three. The voice assistant service used in the backend by the Google Home smart speaker is called Google Assistant. The trigger keywords used are “OK Google” and “Hey Google”. In testing we also found that it worked with slightly modified words like “Hey Bobo” or “OK Hodor”.



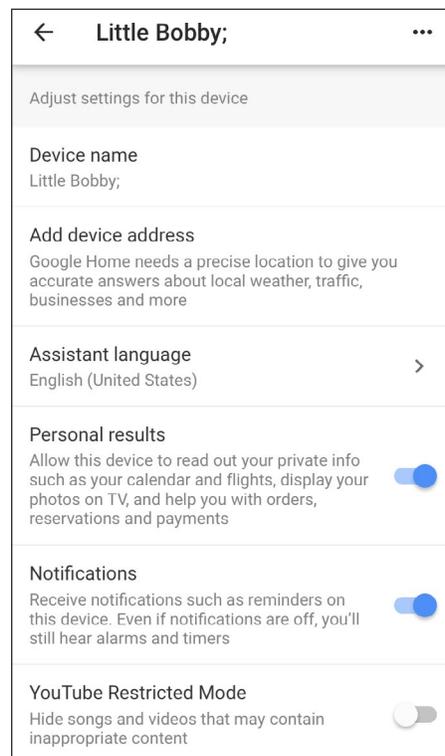
Google Home app settings

Already there have been some controversies with these new products, with a journalist who was given a Google Home Mini in advance of its general release [discovering that the device was making recordings even if he hadn't said the wake-up word or phrase](#). Google said this was a hardware problem that has to do with the activation button on the device that was registering “phantom touches” and activating. Google said it has since patched this flaw. Google Home automatically checks for updates and downloads and installs them. The updates are downloaded over cleartext HTTP but the content is cryptographically signed.

In August 2017, Google [announced](#) a partnership with Walmart for its online shopping. This could mean that in the near future the Google Assistant will be integrated closely with Google Express shopping, providing the ability to order various products by voice, similar to how Alexa is used on the Amazon products.

The Google Assistant can also help you find your phone if you've misplaced it. If you say, “OK Google, where is my phone?” it will make the phone ring on full volume.

Google also has a “voice match” feature that it claims is capable of distinguishing different voices, which can be associated with different profiles. This is one of the most important features as it can prevent other people from gaining access to your personal information. Once it is set up, access to Calendar and To Do lists is restricted to the profile that created them. However, it does not totally ignore unrecognized voices as long as they are accessing non-personal functions, although this may change in the future. Google Assistant allows up to six different profiles to be [linked](#) with their corresponding voice patterns. During setup, Google warns that the distinguishing does not work in 100 percent of cases and, indeed, a quick test showed that my brother's voice was confused as my own.



Google Home settings

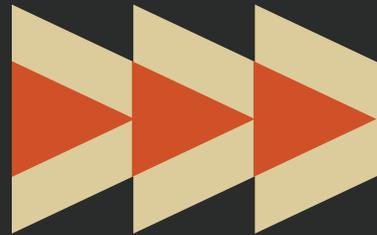
Google Home also has a broadcast feature that allows it to send messages to all connected smart speakers in the home. In addition, Google Home currently offers a calling [feature](#) in the U.S., which at the moment allows users to call any landline or mobile number in the U.S. and Canada for free. There is no setup required and you can simply say “Hey Google, call mom”, for example. Through the voice recognition it will know who speaks and will search the contact list for a matching entry. There is a big push to offer calling functionality on smart speakers and they might soon rival conventional telephones in the home.

# What are the risks?



Section

02



## What are the risks?

Now that you understand how these devices work, the real question is: What are the risks they could pose to your cyber security?

### Security – Who can interfere with your device?

#### Get by with a little help from your friends (and family)

Anyone who has access to your device could potentially interfere with it. If you have friends or family over for dinner, it is possible that they might interact with your smart speaker to play a prank on you, which would be a fairly harmless way to exploit their access. For example, they could add an early alarm for Sunday morning.

Someone with unsupervised physical access to your smart speaker could also potentially modify the device or its settings. For example, there is a [known attack](#) with older Echo devices that allows anyone to replace the firmware, add their own code to the device, and turn it into a listening device. Of course, if you're concerned your friends may carry out such a hack, you may have bigger things to worry about, but it serves as a good warning to be careful when buying second-hand IoT devices that might have been tampered with. Also, if you're a bit retro and still have a dedicated home phone answering machine, complete with a speakerphone so you can listen in real time

to who is calling, then there is the chance that someone could leave you a message that triggers your smart speaker. The same applies to people sending you messages or calendar entries that will be read out loud.

Of course, speech recognition on computers is not something new. We [demonstrated](#) 10 years ago how speech recognition on Windows Vista could be misused to unwillingly delete files. As, currently, most smart speakers do not have a screen with a browser, it is not very realistic for an attacker to simply shout, for example, "open website myBadSite.tld" with the intent to run an exploit on the site to infect the smart speaker. But newer models like the Amazon Echo Show do have a screen and a browser. Although the browser is not accessible by default, with the [help of a trick](#), the user can still open any website they want. Opening up the Privacy Policy allows you to jump to Amazon.com and from there you can move to Google.com, in the end allowing you to search for any website and open it. Hence, if a vulnerability in the mobile browser used by the smart speaker is discovered, an unattended guest could direct the browser to a malicious site and compromise the device.

#### The curious child attack

Probably one of the biggest worries of smart speaker owners is that someone could use the device to make a purchase without them realizing, and this is indeed a danger.

# The attack of the curious child

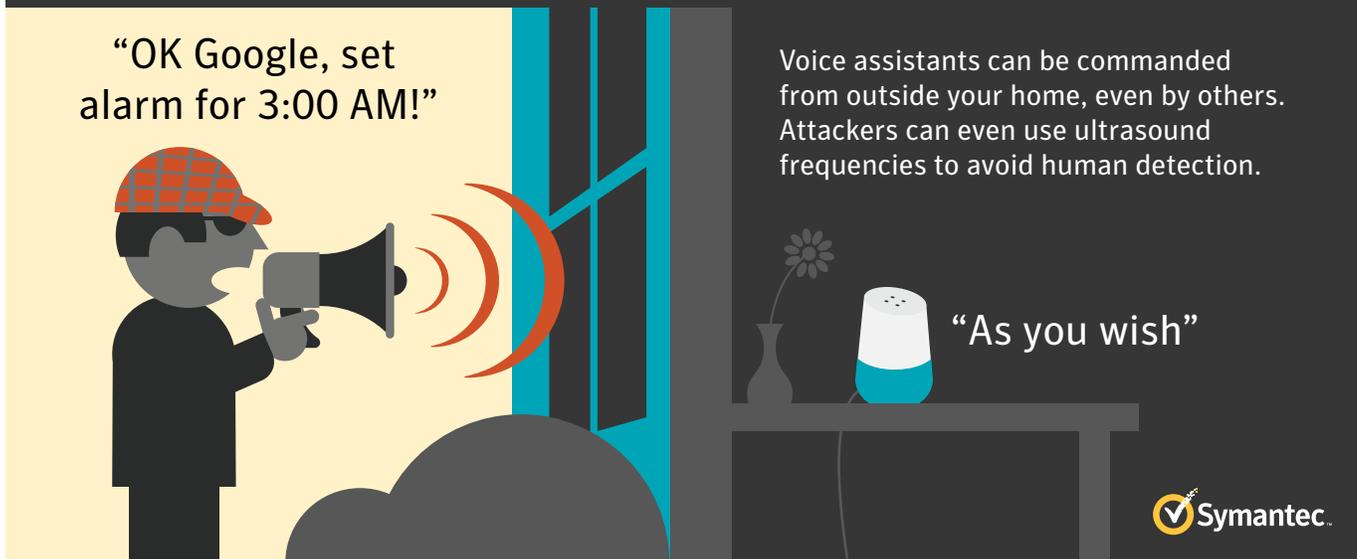
Unexpected item in the shopping cart? Take care to configure devices to avoid unwanted purchases, even from your nearest and dearest.

“Alexa, order me a Mega Bear please”

“MEGA BEAR ONLY \$290 GET YOURS NOW!”



# Tale of the mischievous neighbor



There have been various reports of children ordering [toys](#) through Alexa without the knowledge of their parents. The voice assistant will ask to confirm the purchase, to prevent accidental shopping, but if the child really wants it they might do this as well. Unfortunately, in this scenario, an extra passcode for orders doesn't help much either, as children have a good memory and learn quickly, with some children far better at operating gadgets than their parents. So when they hear you say the password even just once, they might easily use it as well. You can disable all purchase options in the account, but unfortunately this would also limit you from using the order feature. Another option, of course, is to talk to your child, explain how things work, and trust they won't exploit it, though monitoring for accidental purchase confirmation messages is probably still advisable. As mentioned above, with the newer versions of voice assistants, the device is capable of differentiating between voices, which can help prevent anyone else from ordering from your device. However, you have to enable this feature and "train" the voice assistant and, as mentioned above, it does not yet appear to be completely foolproof.

Pets, too, could cause you problems: in September 2017, a [parrot](#) in London apparently managed to order gift boxes through Alexa without its owners noticing. If the bird had ordered food for itself, I would have been really impressed, but the order was for golden gift boxes.

## The mischievous man next door attack

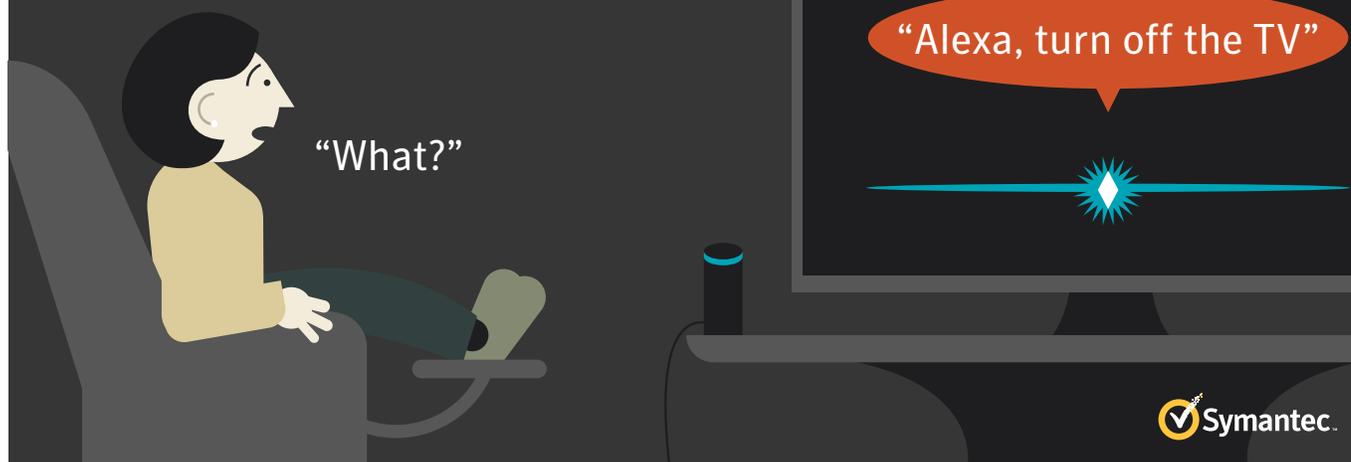
If you live in an apartment block with multiple neighbors, it is possible that some of them may know you have a smart speaker. A neighbor who wanted to cause mischief could potentially send commands to the smart speaker in ultrasonic frequencies that are too high for the human ear to hear, but which can be detected by smart speakers. In August 2017, a [researcher](#) demonstrated that it is possible to transmit voice commands that are not audible to the human ear to smart speakers. This is not surprising as, for example, the Google Home smart speaker uses ultrasonic frequencies to send the PIN code to nearby devices when guest mode is enabled. A similar attack was carried out against voice-activated assistants on smartphones in 2015, where [electromagnetic waves](#) were picked up by the cable of plugged-in earphones and triggered the commands.

In the ultrasonic attack scenario, the attacker needs an extra speaker and amplifier and needs to be close to the device. However, an attacker could also simply shout commands through a closed door when you are not at home to trigger the speaker, therefore, it is very important that any automated purchase options are switched off or secured.

Unfortunately, there is currently no easy way to prevent anyone from, for example, setting an alarm on the smart speaker for 2:00 in the morning once they are in range of audibility. It goes without saying that it is not a smart idea to link your smart door lock to your voice-activated assistant, as this could allow someone to let themselves into your house by simply shouting loudly at your smart speaker.

# A case of talking televisions

Did you know your voice assistant can take commands from other devices such as the TV or radio?



## Television troubles

Simply watching television or listening to the radio can also trigger interaction with smart speakers. This has been noticed by various marketing people too, and they have attempted to use it to their advantage. For example, in April 2017, Burger King launched a TV advertisement that would trigger any nearby Google home devices by mentioning in a calm voice, "OK Google, what is the Whopper burger?" This triggered the smart speaker to read out the Wikipedia page about the Whopper burger. However, the aforesaid page was then edited multiple times by different parties, leading to mixed results for the advertising company. Three hours after the ad first aired, Google changed the processing on the backend system, so that the ad would no longer trigger a response from the smart speaker. It looks like the specific sound clip has been blacklisted inside Google's voice recognition system and therefore no longer triggers any response.

This highlights the power that the provider of the backend system has. If there was some self-replicating malware spreading from one smart speaker to another over voice, then it would be quickly stopped at the central backend system. Burger King got around the filter fix by slightly modifying the ad and replacing the original voice with a [different person's](#), to get the same effect. The modified ad was also quickly blacklisted by Google and no longer works. Many people were unhappy with this invasion on their smart home device, but it doesn't constitute hacking—it is just using the features provided on the device. At least the ad didn't say, "OK Google, turn off the

TV". Google's own [Super Bowl ad](#) in February triggered the devices in people's homes as well, although without a proper command request, nothing happened.

There have also been [instances](#) where Google added a promo snippet suggestion of an upcoming movie that sounded like an advertisement into its device's summary-of-the-day report. After multiple users complained about the sneaked-in message, the promo was removed from the daily summary.

Another example of external influences interfering with smart speakers was seen in September 2017, when a [South Park episode](#) triggered the Google Home, Alexa, and Siri devices of the audience. In the TV series, Cartman tries to get smart speakers to say juvenile phrases such as "big hairy balls", which worked in the TV show, but also triggered devices at home.

A malicious attacker could also attempt to hijack the TV signal to stream their own content. For example, researchers have found an [exploit for DVB](#) in the past that could change the TV broadcast. The same applies to sound-streaming services. Last year, multiple Spotify users [reported](#) that their account was hijacked and started playing strange unknown music. Although none of these cases were used to trigger smart speakers, but instead to generate revenue for certain songs, they could have been used for other shenanigans as well. Not to mention that if you still listen to analog radio, there are many devices out there that allow people to broadcast their own content on any of the popular frequencies.

**Stranger danger**

Similarly, strangers could annoy you by embedding sound clips on websites, similar to the advertisements. If the speakers on your computer or smartphone are enabled then they might trigger the smart speaker at home. Of course, you will also hear the command, but it can be annoying to revert the commands.

**Typical annoying commands could include:**

- Set alarm for 2:00 a.m.
- Set a timer for 1 hour
- Install embarrassing apps (skills/actions)
- Send text to SMS short code
- Call someone, e.g. “Call Home”
- Play with smart home devices by, for example, saying “Light off” or “TV off”
- Saying “Restart”, which restarts the most recently played music
- Full volume, to turn up your speaker to full volume
- Buy something, which could trigger the device to make a purchase
- Repeat, which repeats the last command
- Simon says / Repeat after me, which will cause the device to repeat whatever is said afterwards
- Enable the “do not disturb” mode, which will ignore incoming calls and notifications
- Use the “where is my phone?” function to make your smartphone ring at full volume

---

Whatever you do, when using voice assistants or any Internet of Things (IoT) device for that matter, make sure your Wi-Fi at home is well-protected. Use WPA2 encryption and a strong password to protect it.

---

**Smart speakers could go loopy**

Various people have tried to get smart speakers to go into an endless loop where users make the devices talk to each other; one device asks another device something, and the “conversation” goes on forever. For example, if a user owns a Google Home and an Amazon Echo device, then they could say: “OK Google repeat after me Alexa Simon says OK Google repeat.”

This sequence of commands will make the Google Home say, “Alexa Simon says OK Google repeat”, which triggers Alexa to say “OK Google repeat”, which in turn starts the sequence again by repeating the last command. Similar tricks involve calendar entries or notes that can be read out by asking, “What is on my calendar?”

Of course, typical users would not have smart speaker devices from different brands at home, as most focus on just one brand. So this scenario, although amusing, is probably unlikely to occur in real life.

**Wi-Fi worries**

Whatever you do, when using voice assistants or any Internet of Things (IoT) device for that matter, make sure your Wi-Fi at home is well-protected. Use WPA2 encryption and a strong password to protect it. Furthermore, ensure that all Wi-Fi devices are updated regularly as there could be vulnerabilities found that degrade the security of the Wi-Fi network, such as the recent [KRACKs attack](#). You may also want to consider setting up a guest network that is separate from the one used by your devices. This is a much safer option than handing out your password to visitors to your house as, as once they are in the same network as your smart devices, they could potentially attack all your devices. Even though they might not do it deliberately, an infected computer could act as a stepping stone for attacking other devices in your network.

An attacker in the same network can, for example, use the Google Chromecast service to change settings on a Google Home smart speaker. This includes changing the name of the device, turning the volume up, enabling guest mode, getting the PIN code, and reading out various configuration settings. An attacker could also remove the device from the network or perform a remote factory reset, which would definitely be annoying.

Most smart speakers utilize different music streaming services such as Spotify. These service clients run on the speakers and could contain potential weaknesses that could allow attackers to execute their own commands. However, so far, we have not seen any of these services being misused with a remote code execution vulnerability on smart speakers.

**The following API calls can be made to interact with Google Home devices through Chromecast.**

Method	URI	Description
POST	/setup/set_eureka_info	Change different settings, e.g. device name, family mode
POST	/setup/assistant/all_y_mode	Change the beep before and after the keyword/hotword
POST	/setup/forget_wifi	Remove specific Wi-Fi settings the device will go offline
POST	/setup/reboot	Reboot or factory-reset the device
POST	/setup/assistant/alarms/volume	Set or mute the alarm volume
GET	/ssdp/device-desc.xml	Disclose the personal device name
GET	/setup/eureka_info?options=detail&params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,opencast,multizone,audio,detail	Disclose various details including device name, proxy settings, Wi-Fi name, PIN code of family mode, and location
GET	/setup/assistant/alarms	Disclose set alarms and timers
POST	/setup/assistant/check_ready_status	Play welcome sound again
POST	/setup/assistant/notifications	Enable the Do Not Disturb mode
POST	/setup/assistant/set_night_mode_params	Change the night mode setting for LED and volume
POST	/setup/bluetooth/discovery	Enable Bluetooth discovery
GET	/setup/bluetooth/get_bonded	
GET	/setup/configured_networks	Disclose any saved Wi-Fi network name
POST	/setup/scan_wifi	Disclose nearby Wi-Fi network names
GET	/setup/scan_results	

**The following simple request reveals the name of all configured Wi-Fi networks from a Google Home device.**

Request: `http://192.168.0.XX:8008/setup/configured_networks`

Response: `[{"ssid":"NotYourWIFI","wpa_auth":1,"wpa_cipher":1,"wpa_id":0},{"ssid":"MyWifi","wpa_auth":7,"wpa_cipher":4,"wpa_id":1}]`

**Meanwhile, the following command line will reboot the device:**

```
curl -H 'Origin:https://www.google.com' -H 'User-Agent:com.google.android.apps.chromecast.app/1.24.37.7 (Linux; U; Android 6.0.1; SM-J510FN Build/MMB29M)' -H 'Content-Type:application/json' -H 'Content-Length:16' -H 'Host:192.168.0.XX:8008' -H 'Connection:Keep-Alive' -H 'Accept-Encoding:gzip' -X POST 'http://192.168.0.XX:8008/setup/reboot' --data-binary '{"params":"now"}
```

The devices may have other vulnerabilities too, for example it has been [demonstrated with the Bluetooth issues collectively known as BlueBorne](#) that it's possible for an attacker to take over a smart speaker if they are in range. Fortunately, the BlueBorne vulnerabilities have since been patched by Google and Amazon.

## Privacy

One of the main concerns for many people when it comes to voice-activated speakers is privacy. This is understandable, as these smart speaker devices are in your home and always on, with the capability to be always listening to what you are saying and doing. There have been incidents in the past of smart TVs and smart toys sending back recordings to their servers when users were unaware they were recording, which is another reason why smart speaker vendors try to make the process as transparent as possible.

However, voice-activated assistants are meant to work in such a way that the smart speaker is permanently listening for the keyword to be said, with the processing done on the device offline. Once the wake-up word like "OK Google" is detected, the device will start recording and only then send the captured, encrypted audio back to the cloud service of the vendor for processing. A LED light comes on on the device to indicate that it is recording. The data is stored on the backend server and associated with your account. This data is also used to "train" the voice assistant to understand your pronunciation better in the future.

One has to hope that none of these data centers suffers a breach in the future. Having said that, all modern smartphones have the same recording capabilities and risks, and for them we actually already have seen malware on smartphones in the wild, but people still use voice assistants on smartphones without giving it a second thought.

Of course, incidents like the one mentioned earlier in this whitepaper—[where a flaw meant the new Google Home Mini was literally always listening to its owner](#)—can occur, and are likely to only increase people's anxiety when it comes to concerns around smart speakers and privacy. The bug has been fixed in October through a software update, but it shows that the devices could technically be used to always listen in and record everything.

For many areas, the user can decide for themselves if they want to grant the smart speaker access to their private calendar or emails. For some, it might even be an option to create a new, unrelated account just for the smart speaker, if they are not using any of the personalized features.

All the major device manufacturers do provide the required privacy policies that explain what is recorded and how it is processed:

### Google's privacy policy:

*"Google Home listens in short (a few seconds) snippets for the hotword. Those snippets are deleted if the hotword is not detected, and none of that information leaves your device until the hotword is heard. When Google Home detects that you've said 'OK Google,' the LEDs on top of the device light up to tell you that recording is happening, Google Home records what you say, and sends that recording (including the few-second hotword recording) to Google in order to fulfill your request. You can delete those recordings through My Activity anytime."*

### Amazon Alexa's privacy policy:

*"You control Alexa with your voice. Alexa streams audio to the cloud when you interact with Alexa. Alexa processes and retains your Alexa Interactions, such as your voice inputs, music playlists, and your Alexa to-do and shopping lists, in the cloud to provide and improve our services."*

During a murder [investigation](#) in Bentonville in November 2016, the police confiscated an Amazon Echo from the suspect's house and requested the voice recordings from Amazon. The police did not specify what data they expected to find in the recordings—given that only recordings made after the keyword is said are saved, it is unlikely that much relevant information would be present. To our knowledge, Amazon did not release any of the recordings in this case. But the case does serve to highlight the privacy issues around voice-activated assistants.

Formal complaints have already been [filed](#) with the authorities to investigate how far always-on listening devices are allowed to go in regards to privacy. With all the different laws and various countries, it is unclear at the moment if, for example, you have to inform your visiting friends that you have a smart speaker at home that might record them. Furthermore, many liability questions regarding processing errors are still open. For example, who pays if your voice assistant thinks it heard "heating on" and your electricity bill goes through the roof?

There is also the issue of storing recordings of minors. According to the Children's Online Privacy Protection Act (COPPA) in the U.S., service providers must have the verifiable consent of the parents when collecting data from children under 13 years old. There has been an ongoing [debate](#) as to whether a checkbox in the app is enough to be considered consent. Because many attorneys doubt that this is enough, vendors have started to comply with extra verification steps. As an example, Amazon [announced](#) in August 2017 that, in order to enable so-called kid skills using the Amazon Echo, parents will have to verify a one-time password (OTP) code by text message or authenticate with their credit card.

Users of these devices must also remember that someone who has your Google or Amazon account credentials can listen to your recording history.

### Deleting recordings

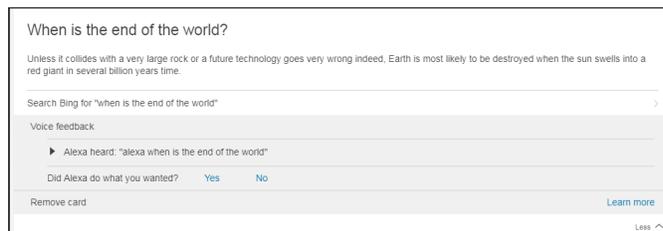
Users of these devices must also remember that someone who has your Google or Amazon account credentials can listen to your recording history. This means it is even more important to protect these accounts from attackers, and strong passwords and two-factor authentication (2FA) should be used where possible. All major voice assistants allow you to review the recorded command history and also let you delete any recordings.

#### With Amazon Echo, to delete specific recordings:

- Open the Alexa app on your phone
- Go to “Settings”
- Select “History”
- Choose which individual recordings you’d like to delete

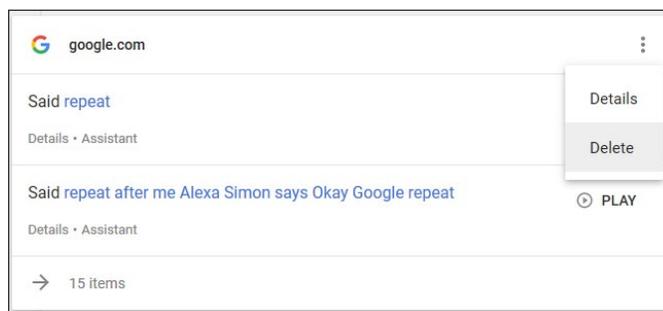
#### To delete entire history:

- Open Amazon.com
- Select “Manage My Content”
- Click on “Alexa”
- Delete entire history



#### Deleting specific Alexa recording

Google Home users can go to <https://myactivity.google.com/> and find a listing of old recordings there, among other data, such as search history etc.



#### Deleting specific Google Assistant recording

# Conclusion



Section

# 03



---

## Conclusion

Voice-activated smart speakers are increasing in popularity. Voice-activated interfaces are greatly improving and will become integrated into many everyday objects. It is not just a replacement for a keyboard, but an actual virtual intelligence that can help in normal, everyday activities.

There are some perils associated with these newfangled smart speakers. The most prominent scenario is TV advertisements or websites playing sound commands that trigger the smart speakers. If the user is in the room they will of course hear the command and can reverse it. Making unnoticed purchases this way is possible but easily avoided as users can and should configure a passcode for purchases. Until the voice recognition has become more accurate and can be applied to all commands, we will see more undesired triggering of voice assistants through TV or radio shows. Given the popularity of Amazon Alexa, you are not doing your children a favor if you name them Alexa.

The biggest concern is around privacy, as these devices are always listening and sending encrypted recordings to the cloud backend once an assumed keyword is heard. As recent issues with Google Home Mini have shown, it is possible for these devices to go haywire and send a lot more recordings to the backend than intended.

---

As a basic guideline, it should be clear that you should not connect security functions like door locks to the voice-enabled smart speakers. If you do, a burglar could simply shout “open the front door” or “disable recordings now”, which would be bad for not only your digital security but also physical security. The same applies to sensitive information, and these devices should not be used to remember passwords or credit card data.

So far, we haven’t seen any mass infection of smart speakers with malware and it is unlikely to happen anytime soon as these devices are not directly reachable from the internet, and are usually protected against Cross-Site Request Forgery (CSRF) attacks. Nearly all possible attacks rely on the misuse of official commands and not on modifying the actual code running on the devices. Since all command interpretation will go through the backend server, the provider has the capability to filter out any malicious trigger sequence, as has been demonstrated by Google after the Burger King advertisement. As always with software, there is a risk that some of the services, such as commonly used music streaming services, may have a vulnerability and that the device could be compromised through it. The devices may have other vulnerabilities too, for example it has been demonstrated with the [Bluetooth issues collectively known as BlueBorne](#) that it’s possible for an attacker to take over a smart speaker if they are within range. Fortunately, the BlueBorne vulnerabilities have since been patched by Google and Amazon. Therefore, all devices should use the auto-update function to stay up to date.

Most of the bigger issues can be avoided by proper configuration and deciding how much information should be linked to the device, but preventing a mischief-maker from setting an alarm for 2 a.m. on the smart speaker can prove very difficult.

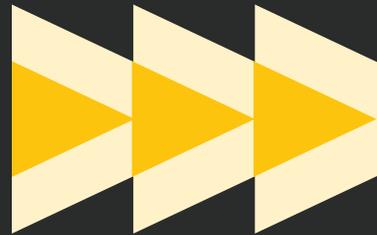
A guide to the security of voice-activated smart speakers

# Protection



Section

04



---

## Protection

After setting up a smart speaker device at home, it is important to configure it securely. Below you can find a few tips that help you focus on the security and privacy settings. The configuration is done through the mobile app or the website. If you are worried about the security of your smart devices at home, then you might consider the [Norton Core](#) secure router, which can help secure your home network, and all the devices on it, from attacks.

---

## Configuration tips

- Be selective in what accounts you connect to your voice assistant. Maybe even create a new account if you do not need to use the calendar or address book.
- For Google Home you can disable “personal results” from showing up.
- Erase sensitive recordings from time to time, although this may degrade the quality of the service (as regards the device “learning” how you speak, etc.).
- If you are not using the voice assistant, mute it. Unfortunately, this can be inconvenient as most likely it will be switched off when you actually need it.
- Turn off purchasing if not needed or set a purchase password.
- Protect the service account linked to the device with a strong password and 2FA where possible.
- Use a WPA2 encrypted Wi-Fi network and not an open hotspot at home.
- Create a guest Wi-Fi network for guests and unsecure IoT devices.
- Lock the voice assistant down to your personal voice pattern, when available.
- Don't use the voice assistant to remember private information such as passwords or credit card numbers.
- Pay attention to notification emails, especially ones about new orders for goods or services.
- Consider enabling a beep sound at the beginning and end of command recognition.
- Disable unused services, such as music streaming services.
- Do not turn off automatic update functions on the device.

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

Symantec Worldwide: <http://www.symantec.com>

ISTR and Symantec Intelligence Resources: <https://www.symantec.com/security-center/threat-report>

Symantec Security Center: <https://www.symantec.com/security-center>

Norton Security Center: <https://us.norton.com/security-center>





**Symantec Corporation**  
**World Headquarters**  
350 Ellis Street  
Mountain View, CA 94043  
United States of America

+1 650 527-8000  
+1 800 721-3934

[Symantec.com](http://Symantec.com)

Copyright © 2017  
Symantec Corporation.

All rights reserved.  
Symantec, the Symantec  
Logo, and the Checkmark  
Logo are trademarks or  
registered trademarks of  
Symantec Corporation or  
its affiliates in the U.S. and  
other countries. Other names  
may be trademarks of their  
respective owners.

For specific country offices  
and contact numbers, please  
visit our website. For product  
information in the U.S., call  
toll-free 1 (800) 745 6054.

**11/17**