TechXplore

Considering buying a smart device? To protect your security, ask yourself these five questions

February 22 2022, by Iain Nash

Credit: Unsplash/CC0 Public Domain

Houses are getting smarter: smart thermostats manage our heating, while smart fridges can monitor our food consumption and help us order groceries. Some houses even have smart doorbells that tell us who is on our doorstep. And of course, smart TVs allow us to stream the content we want to watch, when we want to watch it.

If that all sounds very futuristic, a recent survey tells us that 23% of people in western Europe and 42% of people in the U.S. use smart devices at home.

While these smart devices are certainly convenient, they can also present security risks. Any device with an internet connection can be compromised and taken over by attackers.

If a compromised smart device has a camera or microphone, an attacker may access these and any data on the device can be read, viewed, copied, edited or erased. The compromised smart device may start to look at your network traffic, trying to find your usernames, passwords and financial data. It may look to take over other smart devices that you own.

For example, an attacker could adjust the temperature on a smart thermostat, making the house too warm, and demand a ransom be paid to let you take back control of your central heating. Alternatively, a smart CCTV system can be taken over and the data watched by an attacker or deleted after a burglary.

Smart devices can also be made to attack other systems. Your smart device can become part of a "botnet" (a network of compromised smart devices under the control of a single person). Once compromised, it will search for other smart devices to infect and recruit into the botnet.

The most common form of botnet attack is called a distributed denial of service attack (DDoS). This is where the botnet sends hundreds of thousands of requests per second to a target website, which prevents legitimate users from accessing it. In 2016 a botnet called Mirai temporarily blocked internet access for much of North America and parts of Europe.

In addition to DDoS attacks, your smart devices can be used to spread ransomware—software that encrypts a computer so it can only be used after a ransom has been paid. They can also be engaged in cryptomining (the "mining" of digital currencies which earns the attacker money) and financial crime.

There are two main ways for a smart device to be compromised. The first is via simple default credentials, which is where a smart device has a very basic username and password pre-installed, such as "admin" and "password," and the user hasn't changed these.

The second is by mistakes in the code of the smart device, which an attacker can use to get access to the device. These mistakes (called vulnerabilities) can only be fixed by a security update released by the maker of the device and known as a "patch."

How to be smart AND safe

If you're thinking about buying a new smart device, here are five questions to keep in mind which can help increase the security of your new device and your home. These questions can also help you ensure that the smart devices that you already own are secure.

1. Do I really need a smart device?

While internet connectivity can be a convenience, is it actually a requirement for you? Devices which don't have a remote connection are not a security risk, so you shouldn't buy a smart device unless you actually need your device to be smart.

2. Does the device have simple default credentials?

If so, this is a serious risk until you change the credentials. If you buy this device and the default username and password are easy to guess, you will need to change them to something that only you will know. Otherwise the device is very vulnerable to being taken over by an attacker.

3. Can the device be updated?

If the device can't be updated, and a vulnerability is discovered, neither you nor the manufacturer will be able to prevent an attacker from taking it over. So always check with the seller that the device's software can be updated. If you have a choice, you should choose a device with automatic updates, rather than one where you have to install updates manually.

If you already own devices which can't be updated, consider either removing their internet access (by disconnecting them from your wifi) or buying new ones.

4. How long has the manufacturer committed to supporting the device?

If the manufacturer stops releasing security updates your device will be open to compromise if a vulnerability is subsequently found. You should confirm with the seller that the device will be supported for at least as long as you expect to use it.

5. Does the manufacturer run a 'bug bounty' program?

These are schemes where a company will pay a reward to anybody who identifies vulnerabilities in their code base. Not every company runs them, but they suggest that the manufacturer takes the security of their products seriously. Details will be on the manufacturer's website.

It's not easy to tell if your smart device has been hacked. But as long as your smart devices are supported by their manufacturers, update themselves when they need to and come with strong credentials, it won't be easy for an attacker to gain access.

If you are worried that your device has been hacked, perform a factory reset, change the username and password to something new and unique, and apply any available updates.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Considering buying a smart device? To protect your security, ask yourself these five questions (2022, February 22) retrieved 18 April 2024 from https://techxplore.com/news/2022-02-smart-device.html