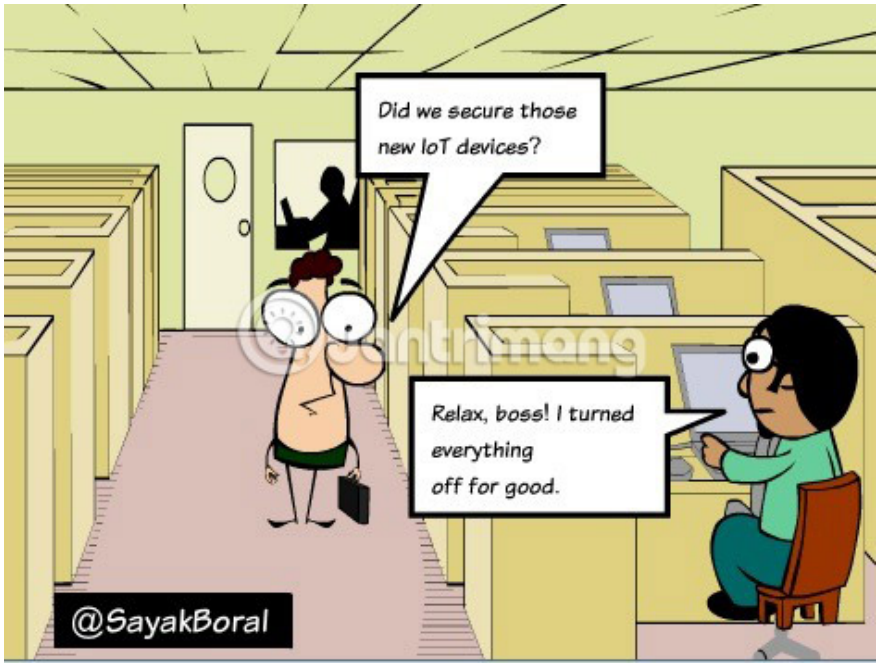
How to secure IoT device properly

Many of us do not care much about IoT device security. The biggest IoT-related security issue so far - the Dyn botnet attack - has 'knocked out' all sites including Twitter, Amazon and Spotify.

Many of us do not care much about IoT device security. The biggest IoT-related security issue so far - the Dyn botnet attack - has "knocked out" all sites including Twitter, Amazon and Spotify.

However, it hardly received much attention because the news channels that day were busy with the 2016 US presidential election. Instead of worrying about serious impacts on a large scale. Thus, the typical reaction is' Twitter collapsed? OK, I will stop using it. '

Such attitudes towards IoT security are still very popular. The most obvious solution to overcome any IoT vulnerabilities is to shut down problematic devices. However, such an indifferent approach will not last forever. It's important to be proactive and follow the tips below to be absolutely sure your IoT device is safe.



How to secure IoT devices?

1. 1. Know the vulnerability on the device
2. 2. Safe configuration
3. 3. 'Sealing' the router or Internet ports

4. 4. Ensure the Hardware Secure Module (HSM) in the device

1. Know the vulnerability on the device

The device may have weak entry points and intruders will use these weaknesses to have network access. Obviously, appreciating the threat can help users prevent defenses in their network. For example, if you have a smart door lock using WiFi, tech-savvy thieves can track when you get home. Smart speakers often record private conversations in the background.

Moreover, consumer devices such as refrigerators and TVs often operate from applications that cannot resist attacks aimed at a vulnerability on the system. Smart cars also have systems to store information about brakes, tire pressure and fuel level.

After knowing exactly where the intruder is capable of attacking, just follow the next steps below to remove those threats.

2. Safe configuration

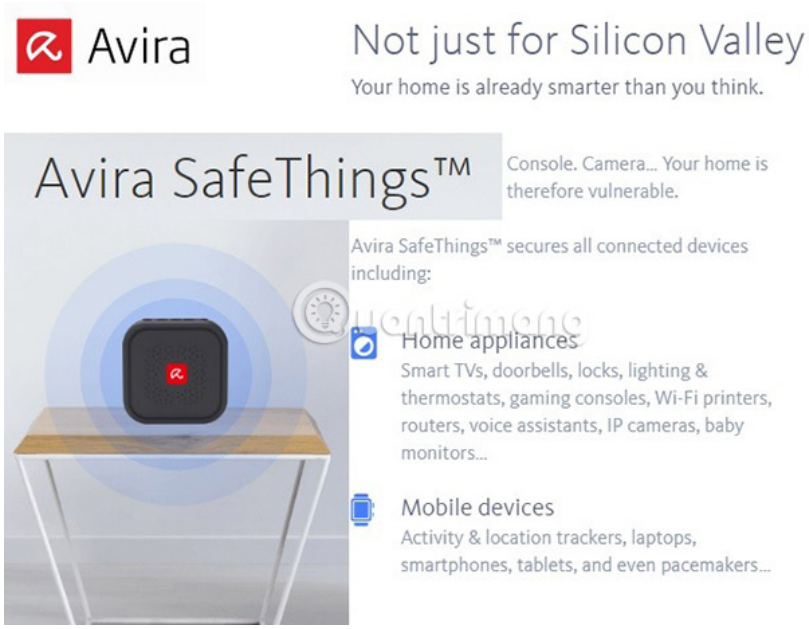
We are all excited and excited to start using a device right after opening the package. Please take 5 minutes to ensure a suitable configuration and a lot of trouble will then be removed. Many devices come with default passwords, such as 1234 or 0000, or even without a password. Changing the default password with numbers and special characters is always a habit recommended by security experts.

Many consumer IoT devices face another vulnerability: The password sent from the device to the cloud is not encrypted. If a router is compromised, this can make those devices vulnerable to tampering, hijacking DNS and brute force attacks. Therefore, the next step plays a very important role to solve these problems.

3. 'Sealing' the router or Internet ports

The weakest point of an IoT network is a router or Internet gateway, which facilitates 'communication' between devices. Readers can check online at F-Secure page to see if their router has any problems in the future. All routers require firmware updates. So if you own an old router, work with the ISP to get a new one right away. Then, do the following:

1. Update MAC addresses: Currently, all routers 'communicate' with other Internet devices through MAC addresses (random numbers such as **34: 45: 12: 22: 18).** As the number of in-house IoT devices increases, users will want to change them into a memorable name, such as 'Fridge', 'TV1', 'Doorlock' and 'Doorbell'.
2. Invest in smart home network security system: Users will be able to monitor all network-enabled devices in the home network. Solutions like Avira Safethings allow users to monitor all their connected devices from a control panel. Nest Secure and Wink Lookout from Google are some other alternatives.



4. Ensure the Hardware Secure Module (HSM) in the device

Obviously, to ensure security, people must deploy the best hardware for the network. Hardware Security Modules (HSM) are the latest technology used by IoT device manufacturers to add an additional layer of security. It is done using a method called **'Key Injections',** in which each silicon chip is provided with a unique identifier. This will protect the device from duplication, tampering and other hardware attacks. Google provides HSM services on its cloud network.

Many people are complacent that their network can resist any penetration. They are not very interested in the security of IoT devices. If you also think your smart devices are not easily attacked by hackers, think again. Whether you like it or not, smart devices still exist and will be everywhere. The attack of IoT devices will only be a problem sooner or later. Importantly, everyone needs to really care about the security of IoT devices.

What is your approach to IoT security? Leave comments in the comment section below!

See more:

1. 6 things to know about IoT security
2. 5 good habits help improve online security
3. How to use Tor browser safely

You finished reading the article "**How to secure IoT device properly**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com