11 ways to keep IoT devices safe

Hackers are increasingly targeting IoT devices to steal data, install malware, or use them in botnets. So, following IoT device security best practices has become more important than ever.

Internet of Things (IoT) devices have grown dramatically in popularity in recent years. But this exponential growth of smart home devices has multiplied IoT security threats. Hackers are increasingly targeting IoT devices to steal data, install malware, or use them in botnets. So, following IoT device security best practices has become more important than ever.

Here are ways to help you secure IoT devices in your company and home.

1. Choose a security-focused provider

When buying IoT devices for your company or home, you should choose a provider that focuses on cybersecurity.

If a business doesn't prioritize security, chances are the devices it supplies will have security flaws that can't be patched in updates. This can leave devices and users vulnerable to attacks.

2. Apply Zero Trust security model

In the traditional security model, the device and the user only have to authenticate once when the device tries to connect to the network for the first time.

But in the Zero Trust security model, each IoT device and user will be verified whenever they try to connect to the IoT network. That way, you can make sure every user and every device is authentic.

3. Perform network segmentation

When applying network segmentation, you divide your network into smaller segments. And these shards act as independent networks.

Therefore, implementing network segmentation for connected IoT devices will reduce the attack surface and reduce security issues. This is because network segmentation makes it difficult for threat actors to traverse the network and cause severe damage.

4. Keep your device up to date

Unpatched vulnerabilities can be an entry point for hackers to gain access to IoT devices. So install all firmware updates as soon as they are available and make sure you are downloading those from the device manufacturer's website.

Take advantage of automatic updates on your IoT devices. If your device doesn't support automatic updates, schedule them to be checked manually every week.

Timely updating of IoT devices will help prevent hackers from exploiting known vulnerabilities in IoT devices.

5. Change device default password

If you do not change the default password of IoT devices, the connected devices will be vulnerable to various IoT attacks. Hackers can easily guess the usernames and passwords of vulnerable devices. And once threat actors take control of your devices, they can add them to the IoT botnet.

That is why it is important that you immediately change the default password and create an unbreakable password that you can remember.

You can also start using a password manager or generator to generate and manage passwords for multiple IoT devices.

6. Enhance device settings

Your IoT devices may come with default privacy and security settings. These settings often benefit the device manufacturer more than you, especially when it comes to privacy.

Therefore, you should closely examine the security and privacy settings of your IoT device. If you see options to enhance privacy and security, turn them on.

7. Disable unused features

Turning off unused features on IoT devices is another way to protect your connected devices from hackers. IoT devices come with many features, and you may not be able to use all of them. For example, some devices may have a web browser that is not needed in your use case.

If you enable all the features and services available on the device, the attack surface expands; Threat actors will have more opportunities to exploit vulnerabilities in IoT devices.

Get in the habit of periodically reviewing live features and services. If you see anything unnecessary for your particular use case, disable it to reduce the risk.

8. Enable MFA whenever possible

Multi-factor authentication (MFA) is an authentication method that requires a user to provide two or more factors to gain access to a device. For example, instead of just asking for a username and password, the authentication server might require an additional factor such as an OTP to grant access to the device.

If your IoT device supports MFA, you must implement it. Doing so adds an extra layer of security. But be wary of MFA fatigue attacks, which, if successful, can help hackers bypass authentication.

9. Invest in security solutions

IoT systems are constantly in the sights of hackers; Deploying a robust IoT security solution is a must to protect your IoT ecosystem.

With a quality IoT security solution, you can:

1. View all IoT devices in your network and understand the security risks involved.
2. Implement a Zero-trust policy to prevent unauthorized access.
3. Monitor for threats and vulnerabilities.
4. Prevent known and zero-day attacks with virtual patching and real-time IoT threat intelligence.
5. Evaluate devices with weak credentials.

Examples of good IoT security solutions include Microsoft Defender for IoT, Quantum IoT, and Forestcout IoT security.

10. Improved physical security

Hackers find ways to gain access to IoT devices, including breaking into your home or office. When securing your IoT devices, you should also consider the physical security of those devices.

Keeping sensitive IoT devices in safe places, adding functionality to disable connected devices when someone takes control of them, and only allowing authenticated access to sensitive devices are some of the ways. to enhance the physical security of your IoT devices.

11. Router Security

A WiFi router is a gateway between your IoT devices and the Internet. Hackers gaining access to your router and WiFi can jeopardize the security of connected devices and the entire network.

So, in addition to securing IoT devices, you should also secure your router and WiFi network. Here are some quick tips to get you started:

1. Change the default router credentials.
2. Change the default SSID to prevent hackers from guessing your router manufacturer.
3. Use WPA2 or .
4. .

In addition, you should also update the router's firmware.

Unsecured devices connected to the network pose many security risks. With IoT devices connecting online, hackers can exploit vulnerabilities to perform various malicious activities and even take advantage of broader access to the network. Take appropriate measures to increase the security of your IoT devices.