Cultural Daily

Independent Voices, New Perspectives

How To Keep Your Home IoT Network Secure

Our Friends · Monday, March 16th, 2020

Security is a major concern for households and businesses that are considering the plunge into an IoT network. IoT (Internet of Things) relies on the interconnectivity of devices to allow operator access to all devices from a single platform. While convenient, this also happens to be its weakness. In 2019, security specialists revealed that 2 billion records were exposed in a mass hack. The type of information that can be exposed to hackers during such a breach includes email addresses and passwords, credit card details, full names, and social security numbers. Knowing which devices can cause issues on a home network is a good place to start.

The Kitchen Of The Future

If you've been dazzled by manufacturers to purchase a fridge that connects to the internet or a washer and dryer that can be started by an app on your phone, it's also likely that you've linked the devices on the cloud through an app. If these devices have not been secured individually and you're relying on the factory-set passwords, you're placing your entire IoT network at risk. If your fridge can access anything on any other device on the network – such as your phone and laptop – a hacker who can get past the fridge's security standards will too. It's important to change the password for each device to restrict the access to your home network.

Security Hacks vs Security Hacks

Your security camera might seem like a great way to keep an eye on things at home while you're on vacation or at work, but the very thing that needs to provide you with those added layers of security can be the weak link in your network. Security experts recommend that households invest in products from well-known and trusted manufacturers, go through the effort to change the factory-set password, and upgrade the security to a cloud-based platform that has multiple layers of security. According to DSC, video surveillance is one of the key deterrents for criminal behavior, which is why they're a preferred addition to home security.

Simple Everyday Devices

While it seems like a good idea to add every new gadget to the home network, office printers and pool pumps are notorious for providing a backdoor for hackers. In 2018, fans of PewDiePie hacked over 50,000 printers in an effort to boost the channel's subscribers. While this is obviously a case where fans were a little too enthusiastic, it leaves many households cold at the thought of how easily their networks were compromised. While the standard password-change advice still stands,

it’s also important for office and home users to be aware of their open network port on their printer. This allows hackers to gain easy access to the network.

While it’s convenient to have all devices connected for easier access, it can also pose a security risk. Check each device, change those passwords, and enlist the help of a professional to see if there are any weaknesses in the network.

Photo:  **BENCE BOROS**

This entry was posted on Monday, March 16th, 2020 at 4:59 pm and is filed under Lifestyle, Technology, Sponsored
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.