The Internet of Things Takes Cyber Security to a Whole New Level

Posted on Oct 16, Posted by Ira Greene Category Technology

With the Internet of Things continuing to gain popularity, we're seeing more devices that connect to the Internet than ever before. However, what the users of these devices might be failing to take into consideration is the fact that the Internet is a dangerous place full of threats and other miscreants. What happens if these criminals decide to attack any of your connected devices? This is a relevant question to ask since October is Cyber Security Month, and The Internet of Things represents the next frontier of cyberspace.

The Internet of Things can increase efficiency, but at what cost? The Internet of Things isn't a phenomenon that's exclusive to the business sector; rather, all users will probably take advantage of at least one Internet of Things device at some point or another. Considering the fact that Internet-connected cars, houses, thermostats, smart watches, fitness trackers, baby monitors, and other appliances are increasing in popularity, it's not beyond the realm of possibility that hackers can take advantage of these devices in order to mess with the lives of innocent people.

The Internet Crime Complaint Center (IC3), defines Internet of Things devices as the following:

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

Thus, the need for caution cannot be emphasized enough, but whose responsibility is it to maintain the security of Internet of Things systems? **Is it the manufacturer's responsibility to build security into the device, or the user's responsibility to ensure that proper precautions are taken?** A recent statement from the IC3 suggests that it's primarily the user's responsibility to ensure that they aren't putting themselves at risk, but how accurate is this statement? ZDNet argues that it's pretty much impossible to convince everyone of cybersecurity's importance, primarily because some people just don't care enough to do something about it until it's far too late.

What's strangely absent from the IC3's statement is the lack of vendor responsibility. Shouldn't security be a primary goal for manufacturers that are producing Internet of Things devices? Considering how the vast majority of users taking advantage of Internet of Things devices can't be considered security professionals, it's silly to think that they will understand the risks associated with using these devices unless they're explicitly warned. Thus, managed service providers like Lighthouse Technology Solutions have taken on this responsibility ourselves by spreading security best practices to the Washington DC community.

In the meantime, you should take every possible action to ensure that your own Internet of Things devices aren't putting you, your family, and your business, at unnecessary risk. Here are some suggestions:

- Only purchase Internet of Things devices from manufacturers who are known to produce security-minded products.
- Keep your Internet of Things devices up-to-date with the latest security patches and updates.
- Educate yourself on how Internet of Things devices communicate with each other.
- Change all default passwords to strong passwords that use multiple letters, numbers, and symbols, and change these passwords frequently.

As a potential Internet of Things user yourself, it's important that you understand the risks versus rewards of using these devices. Lighthouse Technology Solutions wants to help you and your employees understand how Internet of Things devices work, and how you need to protect yourself from the risks. Give us a call at 703-533-LTSI (5874) and ask us a few questions about how we can improve your network security from the Internet of Things.

Tags: Tagged in: Internet Security The Internet of Things