Smart Appliances Serving as Gateways for Ransomware

April 11, 2017 - A new report from the National Cyber Security Centre in England should have people thinking twice before they connect their new refrigerator or thermostat to their home network. The report deals with the issue of lacking cyber security in many connected devices that consumers are now adding to their homes at a rapid pace. These devices can serve as gateways, making entire networks vulnerable to hacking and ransomware.

The issue with connected devices isn't the devices themselves. It's the way that consumers install them. Since most of us are lazy, when we bring a new device home, most of us read the "rapid setup" instructions. We want to see the device working as quickly as possible and then we tend to think that we don't need to do anything else.

Unfortunately, all smart devices come from the factory with a universal password that can be used to access them. At the very least, those passwords need to be changed because factory set passwords are readily available via the internet. Anyone can look them up.

Once a hacker gains access to your smart device, that device can be held hostage, and potentially rendered useless, for ransom. Even worse, your entire network and every other device on it is now vulnerable. Overall, a very expensive lesson to learn.

There are things that we can all do to protect ourselves. First, if you own a smart deviceâ€¦ including a smart phoneâ€¦ that connects to your home network, give it a new password.

If you are having a new smart device professionally installed, ask the installer to show you how to reset the passwordâ€¦ don't ask the installer to do this for youâ€¦ and reset it as soon as he leaves.

You may also want to consider partitioning your home network so that all of your smart devices are separate from your computers. You'll probably need to hire someone to do this, but it can save you a lot of headaches in the long run.

While the vast majority of people being hit with ransomware demands are infecting their systems by clicking on bad links or opening corrupted files, there is a growing trade in ransomware that enters networks through smart devices. This is a

trend that is only going to grow. It is up to consumers to protect themselves. Having your refrigerator connected to the internet may be a nice convenience when you make an unplanned visit to the store. But it will become a big aggravation as soon as it is rendered useless your entire home network is corrupted until a ransom is paid.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS