Munich RE

Simple Defenses: Preventing a Home Data Breach

Risk Solutions

Hartford Steam Boiler
One State Street
P.O. Box 5024
Hartford, CT 06102-5024
Tel: (800) 472-1866
www.munichre.com/hsb

The proliferation of personal smart phones and in-home connected technologies, Bluetooth systems, high-speed Internet and Wi-Fi networks, has created easy entry points for hackers.

Anyone with an Internet connection is exposed. In fact, in the past 12 months, more than one-third of US consumers experienced a computer virus, hacking incident or other cyber-attack, and 18 percent experienced online fraud leading to theft of money or property.*

As hackers evolve, they keep finding security flaws in the newest "smart" Internet of Things (IoT) devices. If an attacker can use a weakness in an IoT device to access a person's home network, computer or mobile device, they may be in danger of having their identity stolen. This can result in outstanding bench warrants, damaged credit scores, and tax/health insurance related issues.

It's important for consumers (homeowners or renters) to take steps to prevent such activity. Here's how:

1. Secure your smartphone. It seems obvious to set up strong passwords (long/complex), but many people still do not use passcodes to lock their smartphones. Almost all IoT devices are controlled by a smartphone app, so phones have become key entry points to homes. In the case of smart locks, phones are actually the keys to physical homes. Be cautious of this fact as hackers are on the hunt.

2. Think before purchasing or installing apps on smartphones or tablets. Before purchasing products or installing apps – even those to control a connected home – read the Privacy Policy. This Policy outlines the type of data the app will access from each device, what data it will collect, and what will be done with that data.

   Do not download any apps that prompt you to quickly download, as they may contain malicious code and security flaws designed by hackers. Once an infected app is downloaded, hackers can see personal emails, passwords, contacts, security network information, and much more.

3. Know the device. IoT devices are designed to be fast, convenient and easy to get up-and-running, so they often do not include adequate security protections to ward off the bad guys.

1866
Hartford Steam Boiler

It's important to create a device inventory, learn the features they have and disable the ones that seem unsafe. For example, some smart TVs are able to listen to conversations. It's often best to disable these features, held within the Settings menu. Also be sure to modify the privacy and security settings according to projected usage and be sure to install updates when prompted to do so.

4. When not using Bluetooth, turn off the feature. Many new items in the home are wired with Bluetooth functionality – think: smart toothbrushes, toy dolls, sound systems, etc. While they make for easy connectivity, such devices have recently been hacked into because their owners left on the Bluetooth option.

5. Purchase only new devices in unopened packaging from reputable retailers. As with any new expensive device, there is a black market for counterfeits that have limited security protections. Do not be tempted to buy devices from anyone else other than a reputable retailer, as it may be a scam.

6. Wipe/reset to factory defaults. When replacing connected devices or selling a home, devices should be restored to factory default settings. This will ensure that any personal information contained on the devices has been removed.

7. Secure the network to which the devices connect. Don't broadcast a wireless network name, or Service Set Identifier (commonly referred to as an SSID). Change default usernames and passwords (make them complex – nothing that can be easily guessed, such as children's names, birthplace, etc.) on home routers and smart devices. Make sure smart devices are not connected directly to the Internet, but rather through a firewall.

8. Set up two-factor authentication for all online accounts. Typical password protection relies on verifying an individual's identity by asking him/her about something only he/she should know (the password). However, once someone else knows that password, he/she can convincingly pass as the actual account owner.

   Two-factor authentication relies on something only the account owner should know (the password) and authenticates something only he/she should have (typically a phone). This makes it much more difficult for a hacker to masquerade as the account owner.

   For additional security tips, Stopthinkconnect.org is a great resource.

9. Check insurance policies closely. While a typical Homeowners Policy may cover the costs of the resulting damage (think: theft, spoilage, etc.), they generally do not respond to costs associated with restoring the systems that have been compromised in the attack. An insurance agent can help clarify what is/is not covered in a Homeowners Policy.

* Data from Zogby Analytics and HSB Group.

© 2016 The Hartford Steam Boiler Inspection and Insurance Company. All rights reserved.