Cyber security essential for smart homes

By Chelsea-Lynn Brotzki

While smart home technology brings many conveniences, it also can attract cyber attacks.

Corporations are no longer the only ones looking at cyber security. Increasingly, homeowners whose networks can make them vulnerable to cyber extortion, cyberattack and online fraud are seeing cyber security as a necessity.

Smart home technology – once out of reach to all but the most affluent homeowners – is becoming more affordable and prevalent. Now just a click of a button or swipe of a finger on a phone can allow most anyone to view home security camera images, monitor front-door access and control home heating and cooling systems. The networks that keep homeowners connected to their homes also make them potential targets of cyberattack.

THE RISKS

It doesn't take much to imagine:

- door locks not responding to passcodes
- thermostats being set at 100 degrees
- a stranger watching children through a video baby monitor
- an inability to control lights and home theater equipment

Cyber extortion, one of the most common cyberattacks, can occur when personal information or a network is locked and held for ransom. Extortionists often demand payment in bitcoin or other digital currency. Theoretically, after the payment is made, the extortionist will supply a code or cipher to unlock personal data or a network. However, many times the extortionists take the currency and do not unlock the data.

Cyber extortion could include holding the smart home system ransom, not just the homeowner's personal data on a server. After the home is hijacked, the consequences could be endless, including physical damage to the home. For example, while a family is away in the winter, a northern climate home could have the heat turned off, resulting in a large water claim from frozen pipes. The consequences can be substantial for a single action taken by a criminal, let alone when these individuals attack multiple aspects of the smart home system.

CYBER SPYING

Sometimes criminals hack into a system with the goal of spying on the home to identify opportune moments to commit burglaries or other crimes. Criminals may not reveal themselves immediately, and their presence within the network may not be detected without firewalls or network security devices. Even with security in place, networks can be attacked, but the devices may mitigate the severity. To be as effective as possible , all network security should be updated as suggested by the manufacturer and must be kept up-to-date with the technology available.

INSURANCE COVERAGES

Insurance companies are responding to cyber threats by adding coverages for these new risks. Not only do these coverages provide assistance at the time of the attack, but many include access to specialized resources to help mitigate the risk or prevent these crimes from occurring.

For your protection:

- Consult a professional information technology or information security specialist as you plan your smart home network
- Seek advice about which network software and hardware safeguards to implement and maintain
- Ask your local, independent insurance agent about the personal cyber security coverages that are available as well as specialty services offered through third-party vendors.

MORE INFORMATION

Blog post: Protect your privacy on the ‘internet of things’

Blog post: Is a DIY security system right for you?

This loss control information is advisory only. The author assumes no responsibility for management or control of loss control activities. Not all exposures are identified in this article. Contact your local, independent insurance agent for coverage advice and policy service.