• By Murray Slovick

A TECH TO WATCH

Protecting Against Cyberattack

How can you reduce your chances of being a cyber victim?

Insecure devices can compromise your privacy.

Electronic home products — such as smart thermostats, home surveillance cameras, smart refrigerators and lights — offer convenience enabled by internet connectivity. But like phones, tablets and laptops, these connected consumer technology products must be secured against cyberattack.

Insecure devices can compromise your privacy, allow sensitive data to fall into the hands of bad actors or be hijacked and disrupt your use of the internet. In addition, without having the ability to determine which vulnerabilities affect products, device manufacturers can't create a "patch" and update their products to fix these vulnerabilities.

Common Cyberattacks

Malware is a term that describes malicious software, including ransomware and viruses. Malware breaches a network when a user clicks a dangerous link or email attachment that installs risky software. Once inside the system, malware can disrupt components and render the system inoperable or install software to steal the victim's information.

Phishing is the practice of sending fraudulent communications that appear to come from a trusted source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.

Spoofing is when an attacker impersonates an authorized device or user to steal data, spread malware or bypass access control systems.

Eavesdropping occurs when a hacker intercepts, deletes or modifies data transmitted between two devices. A type of man-in-the-middle (MitM) attack, eavesdropping occurs when hackers insert themselves into a two-party transaction, interrupt the traffic and then steal the data.

Comprehensive Security

This should cover the device, apps and the cloud. Weaknesses associated with the app, and particularly the cloud, is far more damaging. Rather than hacking a specific user's product, manipulating the cloud can simultaneously hack many products of the same type.

Protecting the whole network rather than individual devices is what products like Bitdefender Box, F-Secure Sense, Firewalla and Trend Micro Home Network Security do. Once activated, these protection systems scan all traffic passing in and out of your home network, preventing intrusions, and blocking hacking attempts and web threats.

Some of these solutions simply join the network and do its security work without taking on the tasks of a router. Others can also function as a router. Either way the end result provides insight into what's on your network, along with what your computers and mobile devices are doing, such as:

- Detecting new devices connecting to your network and disabling them if needed.
- Detecting if apps are performing malicious activities in the background.
- Scanning your network to discover open ports on devices.

Additional steps to protect against cyberattack without the assistance of protective software include:

- Use a strong password that makes it harder for cyber criminals to compromise your household devices. Passwords should be at least eight characters long combining upper- and lower-case letters, numbers and symbols.
- Make sure your device automatically locks after a brief period of inactivity. This way, if you misplace your device, you reduce the opportunity for someone to access your personal information.
- Turn off capabilities such as Bluetooth, network connections, mobile wallets and near field communications when they are not needed. These features can provide easy access for a nearby, unauthorized user to retrieve your data.
- Make sure you trust the app provider and download from the Google Play Store, Apple's App Store, or other trusted sources as they proactively remove known malicious apps to protect users.

Firms routinely release security updates for devices such as laptops and smartphones to address software vulnerabilities. The same could be done for consumer technology devices. Some of these updates are automatic, but others require users to install them — worth the effort to avoid being a victim. ■

vs148/Shutterstock