



Your TV Might Be Spying On You

Kiplinger's interviewed Jeremiah Grossman, chief of security strategy for cybersecurity firm SentinelOne. Read excerpts from our interview below.

From TVs to thermostats to light bulbs, more and more devices have Wi-Fi capability. Are they vulnerable to hacking? A "smart" device is a tiny, internet-connected computer with a narrower purpose than a laptop or PC. An iPhone, for example, is not a phone--it's a computer that happens to have a phone app on it. Anything connected to the internet is at risk of being hacked. As these devices become widespread, they create more points of entry for bad guys. If crooks hack your smart TV, they may or may not be able to monitor your activity through it--but they could potentially use it as a stepping-stone to attack or surveil other devices on the same network.

Do these gadgets come with security protections? Many manufacturers have an incentive to create the cheapest products they can, so they sacrifice security. And when consumers buy, say, a baby monitor, they're not necessarily looking for security. They want the right features at the lowest price.

Has there been a major attack? Through malware discovered last summer, hackers commandeered internet-connected video recording gadgets, such as baby monitors and home security cameras, to send a

massive amount of traffic to popular websites, causing outages. The perpetrators weren't particularly interested in the devices themselves, but that's not to say they couldn't have monitored them or stolen video files. There haven't been many other compromises of home devices yet, but it's going to become a bigger problem.

What information are smart devices legally collecting? Amazon Echo and Google Home are voice activated. They capture and record conversations within listening range of the microphone and send that data to the cloud for storage and analysis. Health-and fitness-related devices, such as the Apple Watch and FitBit, gather and store information about our biorhythms.

How can we guard our security and privacy? Change the default passwords that come with your devices, and keep them up to date with the latest software patches. Configure settings to the most secure and privacy-protecting options available, and disable features you don't need. Most home routers allow you to set up two distinct networks--so put your smart devices on separate networks from your PCs or laptops.