More than meets the eye: Cyber violations of privacy are more disturbing than you think

DATA PRIVACY SOLUTIONS | NOV 26, 2014

The level of sophistication of cyber hackers is often times underestimated or thought to impact “other people” or “other companies.” As a recent episode of “Modern Family” shows us, potential targets such as private webcams are a growing cause for concern. While not a “hacking” incident for the Dunphy family, it did demonstrate the potential for more “exposure” on your webcam than maybe you wanted. A recent article by Michael Cowling in The Conversation points out that there are literally millions of private webcams that are potentially subject to cyber attack, which is a recipe for embarrassment, potential criminal activity, and the unintended consequence of technologic advances.

One pressing reason for concern is that a list of thousands of webcams was publicized in September of 2014. The list, posted on a website by Russian hackers, remains in the public domain and there is reason to believe that other such lists may also exist. As Cowling notes in his article, a different website lists more than 17,000 webcams from more than 120 countries that are still set to default mode and are subject to hacking. What is more, there have been reports and even videos posted to the web via social media sites showing hackers who have accessed televisions with webcams and have violated the most basic of privacy expectations – a person's home and their personal conduct there.

How do you combat these attacks on your privacy?

First, and perhaps the easiest to do, is to change the default settings on any device. There is a reason that software companies include this option when setting up a new device and/or software platform. Hackers routinely use the standard “factory settings” that users fail to change or personalize as a means to gain access to the device.

Second, users should know what the device is capable of and limit who has access to it. Customers are often drawn to a product or service that allows them to remotely use the webcam to see into their home, workplace or other location to check on their children, pets, employees, and any number of other reasons. Because a user accesses the webcam over a local network, it creates a new entry point for a bad actor trying to gain access to the device. Whether the hacker intends to use the information or sell the access to the webcam to others, the danger is very real from a physical and cyber risk. If you can see no one is home, so can a potential intruder. The benefits of the additional security the webcam provides becomes an access point.

Finally, always be aware. What is a safe and protected system today may not be tomorrow. While often times thought to be a bother, software updates can patch holes and improve security on a device from lessons learned by another party who was successfully hacked. Saving yourself by learning from someone else’s misfortune is good practice.

The risks and rewards of deploying new and better technology do not get smaller with each new option or feature. In fact, they seem to grow exponentially. Applying basic principles of risk management dramatically reduces the likelihood of unintended access. Changing the factory default of new devices is a simple first step to making it harder to access your device. Following password protection protocols also heightens the bar over which a hacker must go to access devices or larger systems. And, keeping the bad guys out from the start is much easier and less damaging to you and your business than trying to patch the holes and repair the damage.