12/8/16

By Adam Levin, co-founder of Credit.com and IDT911

In October 2016, there was a distributed denial of service (DDoS) attack that caused serious traffic issues at major internet destinations like Amazon, PayPal and a host of other heavily trafficked sites. You may be giving a gift this holiday season that could make a similar attack possible.

Spot check: Does the gift you plan to give connect to the internet? If you answered “Yes,” keep reading.

A DDoS attack makes an online site or service unavailable by swamping it with enough fake requests to crash the targeted system. The DDoS attacks that happened in October were made possible by devices (largely webcams) that are equipped to connect to the internet — and the available fix is a lot simpler than the looming problem. If you read “webcams,” and decided to stop reading, I encourage you to read a bit further.

‘Tis the Season for the Internet of Things

Any device that connects to the internet poses certain risks to your household and potentially (via DDoS attacks) to the rest of the world, because there are vulnerabilities that allow hackers to use that connectivity to stage attacks such as the above DDoS events. While the October attacks were largely carried out by hijacking webcams, other devices, such as a Smart TV or appliance, could be targeted in the future, and what too many of these items have in common is default user names and passwords. Users don’t change them because they don’t see the threats. Meanwhile, they are easy to look up. More than 60 default user name and password combinations were identified (and published) following the October attacks.

Think of an IoT device as something like all those gifts that require batteries. But if you’re giving a smart device to a friend or family member this holiday season, you might want to consider providing the recipient with a prompt to change the user name and password to something unique as well as long and strong.

Unlike the batteries-not-included gift, an IoT device will still work with the default settings in place, but for the purposes of your security and that of the recipient of your gift, act like it won’t and advise them to always change their user name and password before use.

An Old Threat That Has Come of Age

If the past few years have taught us anything, it’s that identity thieves , fraudsters and scammers are on the prowl, going after any information they can use to make a buck. The other big lesson is that they think way outside the box. That’s their job: to case a target and figure out how to nail it. When an architect builds a bank, he or she thinks about structural integrity, function, aesthetic considerations, and security. It’s all tied together. When a thief looks at the same structure, he or she looks for vulnerabilities. The thief has the easier job. A wrecking ball doesn’t need good ideas.

When it comes to IoT, the bad guys are looking at a bank that is still under construction. The walls are incomplete; we may not even agree yet on where the walls are supposed to be. But the money’s already in there.

If you need more reason to change your default passwords — or to encourage your loved ones to do the same — over the holidays, consider that long before the most recent DDoS attack more than 73,000 unsecured webcams and surveillance cameras were made available on Russian websites to voyeurs from around the globe, effectively turning their owners into the unwitting stars of their own reality shows. The site listed the cameras by country. The spreadsheet was impressive. The United States was well represented. In every case, victims ignored safety protocols and installed the cameras with their default login and password — admin/admin or another easy-to-guess combination findable on any number of public-facing websites.

What to Do

In a perfect world, IoT would be … well, perfect. In the real world, IoT is still in the early years of its evolution, with all the lawlessness and chaos that implies. Indeed, smaller companies are rushing IoT products to market in a mad dash to beat bigger brands that have more at stake when it comes to security. As a result, you can’t always be so sure that your data is going to be safe .

Over the past few years, we’ve learned the hard way that there is no such thing as too safe or secure when it comes to cybercrime, and there is a whole host of organizations out there — both big and small — that are doing a miserable job of protecting you. And even if they do everything right, as things stand now in the world of information security, you may still be vulnerable.

Define Vulnerable

The added convenience provided by the IoT is obvious, but the security issues may not be. Are your fitness records hackable by a third party? Are they linked to social media ? How much information is required to access them? A login? A password? And what’s to stop a hacker from locking or unlocking your front door, disabling your alarm system, or turning off your heat during a blizzard or your lights during a home invasion — all with an app? The answer is, not very much.

Other common devices that are password protected should immediately come to mind here. Whether it is your household printer, your wireless router or your DVR, there are folks out there who are very curious about you, not because they value you as a human being, but because they can create value from any plugged-in human — whether by fraud or extortion or (in a more old-fashioned mode) getting the information they need to rob you blind when you’re not home. And even if they don’t want to know about you, they may want to enlist your devices in a spam-distribution effort or a DDoS attack.

The number of people who don’t change default passwords is staggering, as evidenced by the 73,000 wide-open webcams on that Russian website. There’s a major disconnect here, and it’s specific to the IoT. On the internet proper, it seems the message has finally sunk in and people are beginning to make themselves harder targets — making sure their privacy settings are tight and their passwords are both strong and changed frequently. But when it comes to the IoT, there is still more learning to be done — hopefully not the hard way .