Resolve to be Ready!

Cyber Threats to Prepare for in 2018

BY BRUCE MENZIES

I don't know who said it first but: "Innovation will always outpace regulation." What does that mean? Wherever and whenever there are rules, regulations, obstacles, hindrances, impediments, barriers—wherever and whenever these are present—someone, somewhere will find a way around them. (In other words: "Where there's a will, there's a way).

Computer hackers are constantly finding new targets and refining their tools they use to break through cyber defenses. Here's a couple significant threats to look out for and prepare for this year.

More Huge Data Breaches

We thought it was a really big deal when Home Depot data was compromised back in 2014. Reports indicated hackers stole information on 56 million customers. Were you one of them? Essentially it was the credit card information and Email address that were stolen.

In recent years other companies like Anthem, Sony, US Office of Personnel Management, JP Morgan Chase, Uber, Target Stores, Ebay, and Yahoo's three billion users were all hacked. And lest we forget, last year a cyberattack on Equifax credit reporting agency led to the theft of Social Security numbers, birth dates, and other data on almost half the U.S. population! It was a blunt reminder that hackers are thinking big when it comes to targets. Other companies that hold lots of sensitive information will be in their sights in 2018.

Has your name and information been collected and stored in a data farm? Well, do you have a credit card? Ever had a mortgage? Car loan? Do you receive Social Security or Disability benefits? Then your personal information, Social Security numbers, birth date, family names and address are probably sitting in a data farm being stored, collected, traded, marketed, vended, tweeted, but above all monetized.

So how can you prepare to minimize damage from a data breach?

- When not paying with cash or check pay with a credit card whenever you have the option. Data security expert Adam Levin says, "With a credit card, it's their money. With a debit card, it's your money. With a credit card, in the event it becomes compromised, you make one phone call, they change the number," Levin said.
- Get into the habit of reviewing all your bank and credit card statements often to catch irregularities right away. "It just a few minutes," said Levin.
- Levin says a third important step is to sign up for something known as transactional monitoring. "Transactional monitoring will notify you every time any activity occurs in your account."
- A fourth important step applies to everyone who has their online financial accounts or apps set up to remember their password and user ID. Levin says that may be convenient but it's also a big open door for fraud when cyber thieve manage to steal online account information. Levin adds that too many smart phone owners are setting themselves up for fraud and I-D theft by not keeping their phone password protected.

Adam Levin is the founder of IDentity Theft 911.

Ransomware in the Cloud

The past year has seen a plague of ransomware attacks, with targets including big companies such as FedEx. Ransomware is a relatively simple form of *malware* (computer virus) that cracks defenses and locks down computer files using strong encryption. Hackers then demand ransom in exchange for digital keys to unlock the data.

Ransomware can prevent you from accessing your documents, photos, and other important files plus employ pesky social engineering tactics to pressure you to pay the ransom. Some ransomware, for instance, display a countdown showing the time you have left to pay the ransom. Some ransomware even play an audio file, informing you about the infection and what to do to get access to files

How does your computer become infected with ransomware?

A typical ransomware infection can begin with the computer operator innocently opening an Email message that carry *trojans* (remember the Trojan horse story?), which installs the ransomware and holds the computer hostage.

A big target in 2018 will be Cloud computing businesses, which store mountains of data on the Internet for companies. But smaller entities, such as individuals, can be vulnerable, and even a modest hack could lead to a payday for the hackers involved.

So how can you minimize the risk of ransomware infecting your computer?

As with all threats, prevention is key. This is especially true for threats as damaging as ransomware.

Experts say you should:

- Back up your important files regularly. Consider using the 3-2-1 rule: Make three backup copies, store in at least two locations, with at least one offline copy. Use a Cloud storage service, like OneDrive, which is fully integrated into Windows 10, to store an archive of your files. You can try to restore your files from backup in the event of a ransomware infection.
- Install and use an up-to-date antivirus solution. In Windows 10, Windows Defender Antivirus is built-in and need only to be enabled. Learn how.
- You've heard this before but don't click links or open attachments on Emails from people you don't know or companies you don't do business with.
- Make sure your software and virus detection software is up-to-date to avoid exploits.

Hey, in 2018 let's be smart and safe and *resolve to be ready!* ■