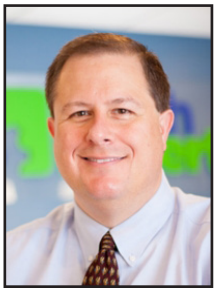
January 2016

TechTidbit.com

brought to you by Tech Experts

My Predictons For The Top Security Threats Of 2016



Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

The year 2015 certainly saw its share of unusual technological security breaches, ranging from the Ashley Madison hack to controlling Jeeps from afar.

With the ever-growing breadth of technology services and gadgets, the opportunities to exploit them grows as well.

These are my predictions for the top security threats for the coming year:

Cloud Services

While cloud services solve countless storage and file-sharing issues for businesses, they also amass huge amounts of sensitive information in a single spot. We expect to see hackers try to sneak past the security measures in place on these services to hit paydirt on business data.

Hacktivism

In this day and age, forget traditional activism. Many think that in order to really get the public's attention, you have to hit the target where it hurts – their technology.

Although this isn't a new concept, it may soon grow, thanks to exploit sites where people can download the necessary codes for hacking without any specialized knowledge.

Hardware

This type of targeting has traditionally been limited to research and academic facilities, but it may increase in scope simply due to its old-school approach.

We are so busy scouring the Internet at large for risks that it is simple to overlook attacks that take place right under our noses.

We are so busy scouring the Internet at large for risks that it is simple to overlook attacks that take place right under our noses.

Ransomware

For the average individual, ransomware perhaps poses the greatest risk because anyone who downloads the code can fall victim. Ransomware basically locks down your computer, encrypts all of its information, and then requests a fee in exchange for the digital key that unlocks everything stored on your device.

Vulnerabilities

Hackers will continue to target software as a means to amass information and gain control to private systems.

While attention to Flash and Java may cool down as they fall into disuse, there will always be new software to attack, including Microsoft's new browser, Edge.

Wearables

As people adopt wearables like fitness trackers and smartwatches into their day-to-day lifestyles, hackers are surely examining these new opportunities to exploit.

Granted, cybercriminals likely have no use for knowing how many steps you took or stairs you climbed, but wearables could easily be used as back doors to their connected mobile devices.

While you can't implement iron-clad security against would-be hackers, use common sense in your digital practices. Always run a business-class, constantly updated anti-virus and anti-malware suite!

Methods like keeping applications updated, using strong passwords, and not downloading anything you're not positive you can trust go a long way in keeping you safe from cybercriminals.

We're proud to partner
with the computer industry's
leading companies:

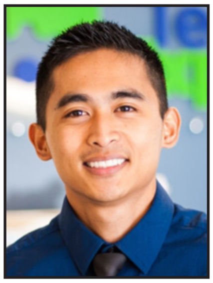
Microsoft Partner

Microsoft. Small Business Specialist

Business Partner IBM

Don’t Pay A Ransom To Get Your Data Back

> *“Before reaching for your credit card to pay a hacker’s demands… stop, take a deep breath, and think objectively about the situation.”*



Michael Menor is Vice President of Support Services for Tech Experts.

Requesting a ransom from victims is an unfortunate trend gaining momentum in the hacking world. This is typically done using ransomware (where hackers encrypt data and request money for the key) and distributed denial of service attacks (where hackers threaten to overwhelm a system with traffic, thus knocking it offline).

In both scenarios, hackers are looking for the victim to pay up…or else. Should they?

The answer should be obvious: absolutely not.

However, when a person’s valuable data becomes encrypted or they receive a legitimate threat to take down their servers, emotions often get in the way and they’ll end up “paying the piper.” Hackers know this, which is why their ransom methods employ fear tactics.

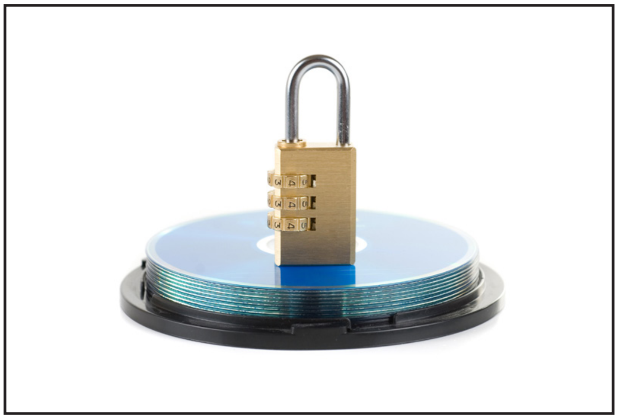
For example, ransomware like CryptoLocker will lock the user out of their computer while the screen displays a countdown to when their data will be deleted.

With DDoS attacks, a hacker may contact the victim mid-attack and promise to cease the attack for a fee. Both of these situations play straight into a person’s irrational fear, causing them to cough up cash.

Before reaching for your credit card to pay a hacker’s demands… stop, take a deep breath, and think objectively about the situation.

What guarantee do you have that these hackers will actually make good on their promise to turn over your data or cease the attack?

This guarantee is only as good as a hacker’s word, which is pretty worthless seeing as they’re, you know, criminals. Therefore, whatever you do, DON’T GIVE MONEY TO A HACKER!



By paying hackers money, you’ll only add fuel to the fire and help fund the spread of their devious acts.

Plus, there are several reported cases where a victim pays the ransom, only to still have their data deleted or the attacks on their site continue.

What’s it to them if they go ahead and follow through with the attack? They have your money, so who cares? It’s a classic case of adding insult to injury.

Need proof? There’s a recent example of this happening to ProtonMail, a Switzerland-based email encryption service.

On November 3rd, ProtonMail was threatened with a DDoS attack by the hacking group Armada Collective.

Like many companies would do, they ignored the threat, deeming it to not be credible. Soon afterward, their servers became overloaded to the point where they had to cease operations. After paying the ransom, the hackers continued the attack.

Now, consider your own situation. How much would it cost your company if you lost revenue for a full day of work, and you still had to make payroll?

For a medium-to-large sized company, losing a full day’s work would likely come to much more than a few thousand dollars. In fact, hackers understand how downtime can be so costly, which is why they feel justified asking for such an exorbitant fee.

What are you supposed to do if you were asked to pay a ransom by a hacker? The first thing you’ll want to do is contact the IT professionals at Tech Experts. We’re able to take an assessment of the attack to determine how bad it is and restore your data to a backed up version that’s not infected with malware.

When facing a hack attack, we can present you with all the options you can take – none of which will include paying a hacker money.

Yes, You Can Still Get Infected - Even With Anti-Virus

Scott Blake is a Senior Network Engineer with Tech Experts.

With the sudden release of a new variants of malware and ransomware such as CryptoWall, users are wondering why their anti-virus programs are not blocking the ransomware infection from infecting their computer.

As with many other forms of malware, the infection needs to exist before a cure or way to detect the threat can be created. This takes time and during this period of R&D, the malware spreads like wildfire.

While there are several forms and classifications of infections, there are basically only two different methods in which infections are released into your system: User Initiated and Self Extraction.

User Initiated infections are caused by a user clicking on a link within a webpage or email or by opening infected email attachment. Once opened, the malware is released and quickly spreads throughout your system.

Because the user manually clicked on or opened the link/document, most anti-virus programs receive this as an authorized override by the user and either internally whitelists the link/document or skips the scan.

CryptoWall is spread through this method, usually contained within an infected Word, Excel or PDF document. The creators of these programs take advantage of the programming of the document to hide the infection.

With the world becoming a paperless society, we are becoming more and more accepting of receiving and opening attachments sent to us through email. It has practically become second nature to just click and open anything we receive, regardless of any warning.

Self-Extracting infections are exactly what they're named. These infections require no outside assistances to worm their way through your system, infecting as they go.

The number one method creators of this form use to place their software on your system is through "piggy back" downloads.

Piggy back downloads occur when you authorize the download and install of one program and other programs (related or unrelated to the original program) are automatically downloaded and installed with it. The most common way is by downloading programs promising to speed up your computer.

Infections can also exist on your system and lay dormant for long periods of time, waiting for the computer to reach a certain calendar day or time. These infections are called "time bomb" infections. Just like piggy back infections, they require no outside assistance to infect your system.

They are mostly found buried in the registry of the system or deep within the system folders. Because they are not active on the time of placement, most anti-virus programs will not detect them.

Active reporting through toolbars is another means of becoming infected over time.

When a user downloads and installs a toolbar for their browser, they authorize at the time of install that it is okay to install and all of its actions are safe.

However, most toolbars are actively scanning, recording, and reporting back to the creator. They also act have conduits for installations of other unwanted programs behind the scene.

If left unchecked, those additional programs can become gateways for hackers to gain access to your system and spread even more infections.

To help stop the spread of malware/ ransomware such as CryptoWall and its variants, we need to become more vigilant in our actions when either surfing the Internet or opening email and attachments.

The best rule of thumb to follow for email is: if you don't know the sender, or you didn't ask for the attachment, delete it. As for websites, read carefully before you download anything and avoid adding toolbars.

> *"Infections can also exist on your system and lay dormant for long periods of time, waiting for the computer to reach a certain calendar day or time."*

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

How to Up Your PowerPoint Game

Back when PowerPoint first came out, it didn't take a lot of finesse to create something visually appealing and exciting. Now, however, PowerPoint and its similar counterparts like Keynote and Prezi, are old hats. It is no longer sufficient to add some generic photos and bullet points that outline your speech to grab your viewers' attention.

In fact, such uninspiring presentations have led to the coinage of the phrase "death by PowerPoint" to describe PowerPoint strategies that fall flat and leave those forced to watch them on the verge of sleep.

Here are a few things to keep in mind when crafting your next presentation:

• Avoid the following kiss-of-death PowerPoint photo types. Some images have been overused to the point of having little to no meaning. This, consequently, leaves viewers bored because the photos add nothing to the material covered in the presentations. Archery targets, cogs, business people preparing to race or grouped around a monitor, jigsaw pieces, hand gestures, and globes are among these types of images.

• Instead, think outside the box when choosing photos for your PowerPoint presentations. For example, pass over an image of a handshake to represent a partnership and choose something more untraditional like cheese and crackers or a needle and thread.

• Don't hesitate to use some of Microsoft's newly released tools to showcase your images. For example, you can create animations using Morph or try things like frames or transparencies. However, when using such tools and enhancements, make sure they fit the overall theme and feel of your presentation.

As such, your extras will be a seamless part of your PowerPoint and not stick out like a sore thumb.

• Most importantly, focus on the content of your PowerPoint presentation. That is, after all, the purpose – to inform and effectively convey ideas. Your photos are meant to complement your content, not overshadow it.

How to Cut Down Your Mobile Data Usage

With unlimited mobile data plans being few and far between, it is imperative to monitor and manage your data usage to prevent outrageously high cellular bills. Even if you have an unlimited plan grandfathered into your service, there are other benefits to cutting down your mobile data usage, including increased battery life on your device and faster service in general. Try these tips to keep your data usage at a minimum:

• Track your usage. It's impossible to set a usage goal or identify problems without knowing how much data you use and how you use it. Within the settings of your smartphone, you can easily find how much data you've used in a billing period and even set warnings for when you approach your data limits.

• Identify what applications use the most data. This can also be done within your smartphone's settings where you can see app usage at a glance and can also set warnings or cut-off limits at this level. After assessing how much data each application uses, you may even want to delete the most data-hungry ones.

• Take advantage of free WiFi. A wide array of businesses offer free wireless Internet service as a perk to customers, so don't pass up the opportunity to get your high-usage needs met at no expense to you. You can even configure your settings where applications only update when WiFi is available.

• Put the stymie on streaming music and video. While you may like to show your friends the latest footage off of YouTube or listen to your playlists while on a run, these activities come with a high data usage price tag. Try waiting to view videos until WiFi is available and make your playlists available offline to listen to them at will without any costly data usage.

Just by implementing these simply usage-reducing and awareness strategies, you can greatly decrease your cellular data bill and the workload on your smartphone device. This is a win-win no matter how you look at it.