July 2018

TechTidbit.com

brought to you by Tech Experts

The Ransomware Threat Is Growing- Here's Why

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

One of the biggest problems facing businesses today is ransomware. In 2017, a ransomware attack was launched every 40 seconds and that number has grown exponentially in 2018. What are the main reasons for this type of escalation and why can't law enforcement or IT experts stop the growing number of cyber-attacks?

Ransomware Trends

One of the reasons involves the latest trends. The art of ransomware is evolving. Hackers are finding new ways to initiate and pull off the cyber-attack successfully.

Hackers rarely get caught. So, you have a crime that pays off financially and no punishment for the crime. The methods of attack expand almost daily. Attack vectors increase with each new breach. If cyber thieves can get just one employee to click on a malicious link, they can take over and control all the data for an entire company.

If you go to work in the morning and find that hackers have locked up all your data and are demanding a $2,000 payment in bitcoin, do you pay it or not? Most business owners pay the ransom. It's easier and cheaper and it gets everyone back to work much faster.

One of the major keys to this cyber-attacks success is the fact that criminals keep the ransom amounts fairly low. If you can simply pay $2,000, get all your files back and move on, then why not do so?

Contributing Factors

One of the most crucial contributing factors to this crime is the cryptocurrency revolution. If criminals had to rely on bank accounts and credit cards for payment, their crimes would soon be solved and they would be caught and placed in jail.

But cryptocurrency is perfect for Internet-based crimes. It's untraceable and that makes ransomware a practically unsolvable crime.

The only safe way to pay for illegal materials is to use a completely untraceable form of payment. The answer is cryptocurrency.

But there are other contributing factors as well: social engineering, known and unknown software vulnerabilities, and poorly configured servers and workstations.

Most of these vulnerabilities do have a workable solution. It's just a matter of finding out where you are most at risk and taking steps to close up those weaknesses. A good IT managed services company can assess your current IT infrastructure and make recommendations for improving it. Consider it an investment in your company's future.

What Can You Do As a Business Owner?

Knowing that all these things are true and things are not going to just suddenly get better, you have to ask yourself how you can protect your company from cyber thieves. The number one way that all security experts agree on is better employee training. Thieves most often trick an employee into clicking on a bad link. The human factor is the weakest link in the cyber-security chain.

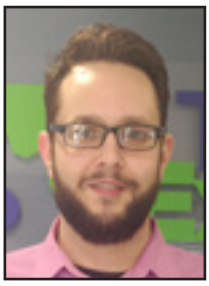
But the good news is that training your employees doesn't have to be expensive or time consuming. Ask a local security expert to come out once a month and address all your employees.

The experts can educate everyone about the latest cyber threats. They can share helpful information about what phishing scams are and how to spot a suspicious email. If you don't have the budget for it, you could even ask the security expert to do his talks on YouTube and then send links to everyone in your organization. Make watching these security briefs mandatory for all employees.

If you go to work in the morning and find that hackers have locked up all your data and are demanding a $2,000 payment in bitcoin, do you pay it or not? Most business owners pay the ransom.

Work From Anywhere: How A VPN Can Help You

"The concept of a VPN and how it works is fairly straightforward. You may be asking yourself how safe it is. A VPN is typically viewed as one of the best layers of protection, not just for connecting to a network offsite, but for also hiding the data transmitted while doing so."



Jason Cooley is Support Services Manager at Tech Experts.

Work. Most of us have to do it and, typically, we spend around a third of our lives doing it. While you are already dedicating a third of your life to your job, sometimes there is a need to get more work done.

The old statement that "there aren't enough hours in the day" really applies to a lot of hardworking people who go above and beyond the expected contribution.

The dependency on technology is constantly increasing and, because of this, many of us have jobs that depend on computers.

Often, these jobs require us to be at work in our office, whether it be to run applications hosted on the work server or to access documents.

So, say you have a few extra hours of work to do. You need to use a program at your office or maybe just some stored documents. Now, you have to go in to the office on a day off… unless you have a VPN setup.

What is a VPN?

VPN stands for Virtual Private Network. The internal network at your office would be considered a private network.

The IP addresses are not broadcasted for everyone to see and there is almost certainly some sort of security device keeping unwanted traffic out.

With a VPN, it creates a tunnel from your computer to your office, creating the illusion that you are actually inside that private network.

The VPN program will put your computer on the network virtually, hence the name Virtual Private Network.

The concept of a VPN and how it works is fairly straightforward. You may be asking yourself how safe it is. A VPN is typically viewed as one of the best layers of protection, not just for connecting to a network offsite, but for also hiding the data transmitted while doing so.

In theory, data transmitted over a VPN cannot be accessed or intercepted. This is why a VPN is viewed as a simple and safe way to access your private network, as well as to browse the Internet privately (private does not mean anonymous).

What are all the things a VPN can do for you?

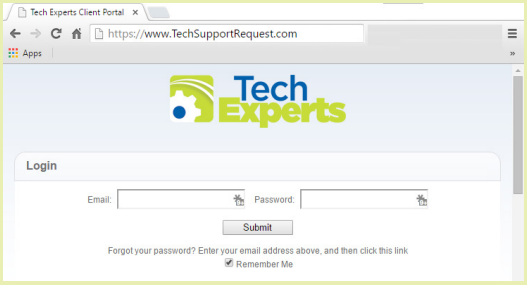
A correctly configured VPN can put you on a network from anywhere where you have an Internet connection.

With a VPN setup, you can now work on those documents. You can use your software that is only available in the office where the database is hosted. You can even send print jobs over the VPN to a printer in your office. A fellow staff member needs a document printed and you are at home? No problem, you can send the request just like you were at your desk.

Who needs a VPN?

While a VPN doesn't benefit everyone, it sure can make your life a little easier if you're a road warrior, and maybe even score you some more time at home.

The cost and setup of a VPN is not at all daunting, making it a viable option for anyone with a need to access files and programs they normally couldn't without being in their office.



Create new service requests, check ticket status, and review invoices in our client portal:
http://TechSupportRequest.com

Attackers Embed Malware In Microsoft Office Documents To Bypass Browser Security

Chris Myers is a field service technician at Tech Experts.

Cyber attacks continue to increase at a rapid rate. In 2016, there were 6,447 software security vulnerabilities found or reported to authorities. In 2017, that number rose to 14,714, more than double the previous year. Halfway through 2018, we are at 8,177 with no signs of slowing.

One of the biggest avenues of attacks is Adobe Flash Player, which has been a leading source of vulnerabilities for over 20 years.

Modern browsers have been phasing out Adobe Flash over the past 5 years. In December 2016, Google Chrome completely disabled Flash Player by default.

Mozilla Firefox started to block the most vulnerable parts of Flash Player by default in 2016 and 2017.

The latest Flash Player vulnerability, designated CVE-2018-5002 by Adobe, aims to circumvent those browser changes by hiding the attack in a Microsoft Excel file, which is then distributed by targeted emails disguised as legitimate bulletins from hiring websites.

To hide this from anti-virus software, the hackers went another step further by not including the malicious code directly in the Excel file. Instead, they just embed a small snippet that tells the file to load a Flash module from somewhere else on the Internet. Due to this, the file appears to be a normal Excel document with Flash controls to anti-virus applications.

CVE-2018-5002 is what's known as a Zero Day vulnerability, which means it was used by attackers before it was discovered and patched.

This particular vulnerability appears to have been used in the Middle East already.

In one instance, businesses in Qatar received an email that mimicked "bayt.com," a Middle Eastern job search website. The attackers sent the email from "dohabayt.com."

With Doha being the capitol of Qatar, it was easy to assume that dohabayt was simply an extension of the main website.

However, a true branch of bayt.com, known as a subdomain, would be separated by a period like so: doha.bayt.com. Once the target was tricked into opening the email, they were directed to download and open the attached Microsoft Excel file named "Salaries."

This was a normal-looking table of average Middle Eastern job salaries, but in the background, the attack was already going to work.

How To Avoid Being Infected

The fake email scenario described above is known as phishing. Phishing is the attempt to disguise something as legitimate to gain sensitive information or compromise their computer.

The word phishing is a homophone of fishing, coined for the similarity of using bait in an attempt to catch a victim.

The attack described above was a type of phishing known as spear phishing, where the attacker tailored their methods specifically to the intended victim.

They disguised the email as a local site used for job or employee hiring, and the file as a desirable database of salary information.

Phishing emails are most easily identified by checking the sender's email address. Look at the unbroken text just before the ".com".

If this is not a website known to you or if it contains gibberish such as a random string of numbers and letters, then the email is almost always fake.

While the attack above was sophisticated, most phishing emails simply try to trick the user by saying things like "Your emails have been blocked, click here to unblock them" or "Click here to view your recent order" when you did not actually order anything.

Always be vigilant. When in doubt, forward the email to your IT department or provider for them to check the email for viruses or other threats.

"The latest Flash Player vulnerability, designated CVE-2018-5002 by Adobe, aims to circumvent those browser changes by hiding the attack in a Microsoft Excel file, which is then distributed by targeted emails disguised as legitimate bulletins from hiring websites."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

How Can You Improve Your Online Privacy?

Frank Deluca is a field service technician at Tech Experts.

You have probably heard about the myriad of security blunders that have plagued the business and IT worlds. We've seen considerable security and privacy miscues from some of the world's biggest businesses, organizations, and government agencies.

This includes data breaches, attacks from hackers, privacy concerns, and theft where massive amounts of private user data were lost and/or misplaced. If major institutions can fall victim to these privacy and security lapses, then so can individuals and society at large.

The Internet can certainly be a scary, confusing place, especially for the uninitiated, but there are many ways in which you can protect yourself, mitigate risk, and increase your privacy while having an online presence.

Use Strong Passwords For Your Sensitive Accounts

Using strong, unique passwords (symbols, long phrases, capitalization, punctuation) can help you avoid that gut-wrenching feeling that you get when you realize that someone has hacked your account and has access to your personal information. Not knowing what's going to happen to your work or your memories is something no one wants to experience.

Creating strong and unique passwords for each of your online accounts is a smart practice. The reason is quite simple: if one of your online accounts is hacked, then the others will soon follow. Consider a password manager like LastPass or Keeper to create, store, and manage your passwords.

Don't Allow Or Accept Cookies From Third Parties

The purpose of the computer cookie is to help websites keep track of your visits and activity for convenience. Under normal circumstances, cookies cannot transfer viruses or malware to your computer.

However, some viruses and malware may try to disguise themselves as cookies, replicating after deletion or making it easier for parties you can't identify to watch where you are going and what you are doing online.

Because cookies are stored in your web browser, the first step is to open your browser. Each browser manages cookies in a different location. For example, in Internet Explorer, you can find them by clicking "Tools" and then "Internet Options." From there, select "General" and "Browsing history" and "Settings."

In Chrome, choose "Preferences" from the Chrome menu in the navigation bar, which will display your settings. Then expand the "Advanced" option to display "Privacy and security." From there, open "Content settings" and "Cookies."

Use A VPN Or VPN Provider

A virtual private network, or VPN, can help you secure your web traffic and protect your anonymity online from snoops, spies, and anyone else who wants to steal or monetize your data.

A VPN creates a virtual encrypted tunnel between you and a remote server operated by a VPN service. All external Internet traffic is routed through this tunnel, so your data is secure from prying eyes. Best of all, your computer appears to have the IP address of the VPN server, masking your identity.

To understand the value of a VPN, it helps to think of some specific scenarios in which a VPN might be used. Consider the public Wi-Fi network, perhaps at a coffee shop or airport.

Normally, you might connect without a second thought. But do you know who might be watching the traffic on that network? If you connect to that same public Wi-Fi network using a VPN, you can rest assured that no one on that network will be able to intercept your data.

Additional tips: keep your Windows operating system and your applications such as Microsoft Office up to date at all times, don't post private information on your social media accounts, and use browser ad/tracking blockers.