January 2019

TechTidbit.com

brought to you by Tech Experts

Top 5 Cybersecurity Predictions For 2019

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

Cyber threats are a genuine danger for businesses, no matter their size or industry. Companies that face data breaches are likely to fail within months after the attack, according to the National Cyber Security Alliance. Security issues can ruin your reputation and cause expensive damage to your company.

In 2019, we are already predicting increased cyber crimes to steal more data and resources. The FBI reported that over $1.4 billion in losses were experienced by companies and individuals in 2017.

These expenses come from increasing security, losing information, losing physical resources, ransomware payouts, scams and more. The most significant sources of cybercrime included:

- Email compromise
- Confidence fraud
- Non-payment or delivery scams
- Corporate data breach
- Investment scams
- Identity theft
- Personal data breach
- Real estate/rental fraud
- Credit card fraud

Looking forward into 2019, we are preparing to face some of the biggest and hardest attacks yet. Hackers are working to build faster and smarter tools that get around the security systems and regulations that organizations and companies have in place.

Companies have to be prepared for cybercrimes that could wreak havoc on their customers or business. Most industries have strict compliance and regulations to keep data safe and can face fines or even jail time if they are not diligent in their cybersecurity efforts. Here are the five major cybersecurity trends we expect to see in 2019:

Multi-Factor Passwords

The password alone is becoming increasingly easy for hacker entry. Fingerprints, ear scans and even social security numbers are all increased measures of security to help battle cybercrime.

Using multi-factor passwords is going to be a crucial part of security for 2019 for both personal data and organizational strategies. A large amount of data breach occurs due to human error or negligence so multi-factor passwords can help decrease some of those occurrences.

Data Privacy and GDPR

The EU pushed businesses everywhere when they required the adaptation of the General Data Protection Regulation (GDPR). Many companies and organizations that didn't have dealings in the EU started making changes to prepare for the level of modifications expected so they wouldn't be scrambling to catch up later. The regulations that went into effect this past May are still going to have a significant impact on 2019.

Rise of Cryptojacking

Last year, ransomware cost over $1 billion in damages, but we see a shift towards cryptojacking as the more popular attack. Ransomware takes a lot of research, social engineering and development. In many cases, the payments have gotten smaller because companies, educational institutions and organizations are refusing to pay the ransom at all.

Cryptojacking is stealing cryptocurrencies by leveraging the computers of an unsuspected user without their knowledge or permission.

When a cyber criminal puts the crypto mining program into effect (often in a JavaScript), the system will slow its processing power as it also operates the mining efforts. This can cause whole systems to falter, leading to sluggishness or downtime for businesses.

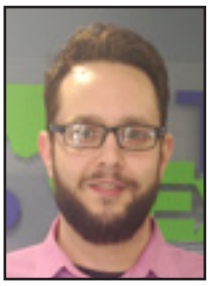
Best case means lost productivity, but a worst case might mean blackouts if the attack occurs on electrical utility computers or cause huge issues for patients if the attack is happening to a hospital. This method

Continued on page 4

Looking forward into 2019, we are preparing to face some of the biggest and hardest attacks yet. Hackers are working to build faster and smarter tools that get around the security systems and regulations that organizations and companies have in place.

Challenges Of Staffing In An Increasingly Tech World

"For every industry, modernization is becoming a matter of 'when' rather than 'if.'"



Jason Cooley is Support Services Manager at Tech Experts.

"Good help is hard to find." It's something you have probably heard before. It has been said for generations.

Hiring fresh graduates is always tough as they are unproven and likely accepting their first jobs in their field. Hiring experienced workers costs more money and they most likely need better incentives to switch jobs.

However, fresh graduates may have more experience with recent industrial developments – and experienced workers may not feel the need to adapt to new innovations until it's absolutely necessary.

So what happens when all paths forward intersect? Where experienced workers are becoming underqualified as the requirements of their jobs change? Where younger people want more than they are worth because they have general technical skills to go along with their chosen path?

This affects the workforce as a whole, not only IT. Much like any other field, we have our own challenges with staffing as time moves forward. Careers in IT obviously have a broad range of computer skills as a requirement, but there are industries where using a computer wasn't always needed.

Working retail in today's world will no doubt require use of a computer for most employees from time to time. Selling insurance? Most, if not all, processing is done on a computer. A loan department at a bank is going to use a computer and so are the tellers. Gas station? Fast food? All are places you will typically see computers and other technology in use.

It can be intimidating when industries like construction move away from pen and paper. Your accountant uses computers, and now you probably will too. Major trucking companies may leave the paper logbooks behind in lieu of digital recordkeeping.

So what happens to the employee at the construction company who has been there for 20 years with no computer skills? He is a foreman and all reporting is now done on a tablet then uploaded over a VPN to the main office every day. It's a complex new skill to learn, especially when put against those who can operate tech with no effort… and who are asking for the same (or lower) salary.

For some people, they may feel like they have to learn a whole new career just to keep up with their own. As challenging as it is for the veteran employee, the same challenge can be had for a new hire. You face the challenge of not only the day-to-day job duties, but also with learning how to use five new pieces of software.

The challenge for employers is probably the most difficult. Keeping your old employees may be just as hard as finding new ones.

As new systems are implemented, experts of antiquated processes become dispensable if they can't become acclimated. Hiring a recent graduate gives you an employee who knows those new systems, but they may be too "green" and make mistakes experienced workers already learned, adding stress to the environment.

Depending on the size of the company and the industry, there will always be unique staffing challenges. Not everyone will be forced to use a computer or a tablet for work, or you may not be able to employ someone who isn't proficient with one. As tough as the market is for job seekers, I'd argue it's a lot tougher on those tasked with hiring the next class of experts.

One thing that's clear is that we aren't going to back-track on technology due to the benefits. For every industry, modernization is becoming a matter of "when" rather than "if." Employees and employers alike will have to keep up.

HTTPS And Why The Internet Still Isn't Secure

Frank Deluca is a field service technician at Tech Experts.

HTTPS stands for "Hyper Text Transfer Protocol Secure" and it is the secure version of HTTP, the protocol over which data is sent between your browser and the website you're connected to.

Most web traffic online is now sent over an HTTPS connection, making it "secure." In fact, Google now warns that unencrypted HTTP sites are "Not Secure."

So why is there still so much malware, phishing, and other dangerous activity online?

"Secure" Sites Have a Secure Connection

In previous iterations of Chrome, it used to display the word "Secure" along with a green padlock in the address bar when you were visiting a website using HTTPS. Modern versions of Chrome simply have a little gray padlock icon next to the navigation bar, without the word "Secure."

That's partly because HTTPS is now considered the new baseline standard. Everything should be secure by default, so Chrome only warns you that a connection is "Not Secure" when you're accessing a site over an HTTP connection. The reason for the removal from displaying the word "Secure" is that it may have been a little misleading. It may have easily been misconstrued to appear like Chrome was vouching for the contents of the site as if everything on the page is "secure." But that's not true at all. A "secure" HTTPS site could be filled with malware or phishing attempts.

HTTPS Does Not Mean A Site is "Secure"

HTTPS is a solid protocol and all websites should use it. However, all it means is the website operator has purchased a certificate and set up encryption to secure the connection.

For example, a dangerous website full of malicious downloads might be delivered via HTTPS. The website and the files you download are sent over a secure connection, but they might not be secure themselves.

Similarly, a criminal could buy a domain like "www.bankofamerica.com," get an SSL encryption certificate for it, and imitate Bank of America's real website. This would be a phishing site with the "secure" padlock, but again, it only refers to the connection itself.

HTTPS Stops Snooping and Tampering

Despite that, HTTPS is great. This encryption prevents people from snooping on your data in transit, and it stops man-in-the-middle attacks that can modify the website as it's sent to you. For example, no one can snoop on payment details you send to the website.

In short, HTTPS ensures the connection between you and that particular website is secure. No one can eavesdrop or tamper with the data in-between.

HTTPS Is An Improvement

Websites switching to HTTPS helps solve some problems, but it doesn't end the scourge of malware, phishing, spam, attacks on vulnerable sites, or various other scams online.

However, the shift toward HTTPS is still great for the Internet. According to Google's statistics, 80% of web pages loaded in Chrome on Windows are loaded over HTTPS. Plus, Chrome users on Windows spend 88% of their browsing time on HTTPS sites.

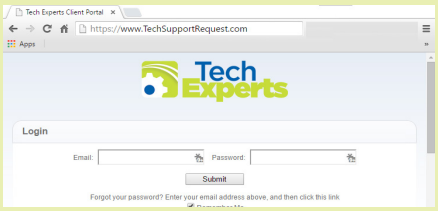
This transition does make it harder for criminals to eavesdrop on personal data, especially on public Wi-Fi or other public networks. It also greatly minimizes the odds that you'll encounter a man-in-the-middle attack on public Wi-Fi or another network.

It's still no silver bullet. You still need to use basic online safety practices to protect yourself from malware, spot phishing sites, and avoid other online problems.

"HTTPS is a solid protocol and all websites should use it. However, all it means is the website operator has purchased a certificate and set up encryption to secure the connection."

Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com



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

Wannacry Ransomware Continues To Be A Problem For Some

It's been almost two years since the outbreak of the Wannacry ransomware epidemic. Unfortunately, all this time later, some companies are still dealing with the fallout. According to the latest research, Wannacry is still infecting hundreds of thousands of computers around the globe.

WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.

A number of factors made the initial spread of WannaCry particularly noteworthy: it struck a number of important and high-profile systems, including many in Britain's National Health Service; it exploited a Windows vulnerability that was suspected to have been first discovered by the United States National Security Agency; and it was linked by Symantec and other security researchers to the Lazarus Group, a cybercrime organization connected to the North Korean government.

As grim as that sounds, it's not all bad news. After all, the malware has been rendered harmless by the now famous "kill switch" discovered by Kryptos Logic security researcher Marcus Hutchins, who found a glaring flaw in the design of the software. The flaw allowed him to register a domain and encode it with instructions that would keep the ransomware component of Wannacry from activating and actually encrypting files.

That, however, did nothing to get rid of the malicious code infecting legions of PCs around the world. Sadly, much of the code remains in place on infected machines, silently lurking in the background. Kryptos Logic is uniquely positioned to know, since they control the kill switch domain and have continued to monitor traffic to it since building the kill switch on it. To this day, their site continues to be pinged by new IP addresses as the now toothless infection continues to spread.

It's not hard to see why the removal of a piece of malware that has been rendered suddenly toothless takes a lower priority for busy and often harried IT security professionals. Leaving the code in place on infected machines is not without risk, however.

It is possible, however unlikely, that the hackers who built the program to begin with could find a way to get around the kill switch. If that should happen, then we'll be facing the full fury of the epidemic all over again, something no one in the field of digital security wants to contemplate.

The bottom line is simply this: If you were impacted by Wannacry when the outbreak initially occurred, it's worth double checking to make sure that all traces of the malicious code are gone from your network.

Top 5 Cybersecurity Predictions For 2019, continued

of cybercrime is less time consuming to set up, more accessible for the hacker to implement, provides a higher payout and often is harder to track.

AI Attacks

We are seeing a heightened increase in artificial intelligence (AI) and machine learning (ML) that cybercriminals are using to focus their attacks.

Hackers are using these systems to train and fine-tune their own programs with malicious intent while maintaining a strategic distance.

IoT Regulation

The Internet of Things (IoT) is a grouping of intelligently connected systems that might include vehicles, devices, appliances, electronics, software, connectivity and actuators. These primarily are unregulated and we expect 2019 to be the year when the security issues here may finally be addressed.

This may require certifications or a governmental agency to step in and formulate laws. With increased connectivity, the threat of IoT security breaches are genuine public safety concerns and shouldn't be taken so lightly. Companies that produce these connective devices and software should already be carefully considering these concerns and how to best keep the users protected.

We know tech threats are a genuine issue for your business. Outsourcing tech support or tech help is one way to ensure you have all of your bases covered.

If you need help implementing security, contact us today. We offer the strategies, technology and expertise to keep you protected!