August 2019

TechTidbit.com

brought to you by Tech Experts

Top Concern For Small Businesses? Cybersecurity

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

While some might assume that fear of an economic recession would be at the top of the list of key issues small business owners concern themselves with, a recent survey found that another issue is of much greater concern: Cybersecurity.

This is no surprise.

For the past several years, cybercrimes and data breaches among companies large and small, governments, and even individual citizens have risen drastically.

While it's true that many business owners still assume a data breach at their own company is highly unlikely, with the ultimate price tag of such attacks ramping up to the millions of dollars (and recovery being hardly successful), it makes sense that companies are taking notice.

What Does a More Concentrated Focus on Cybersecurity Mean for Companies?

Company owners who are most concerned with cybersecurity are naturally becoming more involved in their companies' defense strategies. After all, a breach of data isn't just about the loss of money.

It can also mean the loss of customers (or the entire business) and a permanent label as someone who can't secure their company.

Furthermore, even if a breach doesn't close down the company, customers, clients, and investors are sure to drop their interest in a company that's lost data, money, and trustworthiness after a cyberattack. Large companies like Yahoo, Target, Equifax, and others have all felt the blow of such fallout.

How Do Most Cyber Attacks Originate?

When most people think of a cyberattack, images of an ultra-sophisticated Russian hacker sitting in a darkened basement with glowing green and blue lights comes to mind.

However, cyberattacks can come from anywhere and from anyone. They may be performed on public computers, from office buildings, at public Wi-Fi cafes, from residential homes, or even in airports.

Your own cyber attacker could be coming from across the world... or down the street. Once you find out that your company's data's been compromised... it may not really matter anyway.

Because of their cloak and dagger way of operating, cyber attackers and criminals are rarely located and seldom caught or prosecuted. Part of being a cybercriminal, after all, means knowing how to confuse and reroute IP addresses through a multitude of countries. This makes retracing the invader's steps a serious challenge — even for the most advanced IT specialists.

Therefore, the key to avoiding such attacks is, of course, to prevent them in the first place. This is the goal of an increasing number of savvy business owners.

It means putting cybersecurity first and foremost on their priority list and recruiting the help of highly-educated and trained information technology specialists.

How Can You Prevent Cyberattacks in Your Company?

The key to preventing cyberattacks is knowing how they start in the first place — and remember, it's not where most people would think.

Again, many people assume that cybercriminals work by being absolutely amazing at breaking into super-advanced and complicated security systems. But nearly all mid- and large-sized companies have advanced security systems, and they still get hacked.

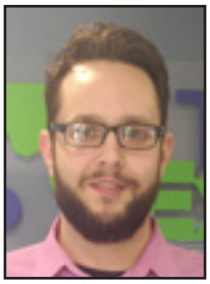
Assuming that cybercriminals can simply break into these systems is giving them too much credit.

Continued on page 3

The key to preventing cyberattacks is knowing how they start in the first place — and remember, it's not where most people would think. Again, many people assume that cybercriminals work by being absolutely amazing at breaking into super-advanced and complicated security systems. But nearly all mid- and large-sized companies have advanced security systems, and they still get hacked.

Zoom Zero-Day Bug: Webcam Hijacking And Other Intrusive Exploits

"These vulnerabilities are discovered in normal software and have been found in Windows' core system more times than you probably realize. Microsoft is typically quick to roll out updates when they have the power to fix the flaw, even if it isn't their software. This illustrates the great importance of keeping Windows up to date."



Jason Cooley is Support Services Manager at Tech Experts.

Internet safety is always a concern and there are a large number of tools available to assist with that. Depending on how much security you need, you may need to run multiple pieces of software. Antivirus, antimalware, firewalls, and even 2-factor authentication are security measures all doing different things.

Even with all of these types of security layers in place, there is no such thing as guaranteed safety. You can be as careful as possible and avoid anything seemingly questionable, but one thing you can't avoid are security exploits.

An exploit could be used to track a user's history, and possibly even every keystroke. This could potentially send passwords for anything you enter on the computer.

Recently, Zoom, a video conferencing application, was discovered to have a severe vulnerability on the Mac platform. This exploit was a very simple one: a person attempting to access your webcam could send a legitimate Zoom meeting invite, but set with certain settings on a certain server.

When the link is clicked, even without accepting the invite, the client is silently launched, turning on the end user's webcam. Even if the Mac user had uninstalled Zoom, the client would silently reinstall and launch.

Back in 2017, a much larger user base was at severe risk of an exploit that would allow hackers to silently install malware to take remote control of the user's computer. The CVE-2017-11882 exploit was a flaw in Microsoft Office software.

If Office was installed, a Visa paylink email was sent, and when the user opened the word document attached, it launched a PowerShell command installing Cobalt Strike, granting remote control to whoever deployed it.

It was not long before Microsoft had a security fix rolled out, but if the software was installed prior to installing the security update, the remote control software would persist and have free reign on not only one computer, but also be able to travel through the network.

These vulnerabilities are discovered in normal software and have been found in Windows' core system more times than you probably realize. Microsoft is typically quick to roll out updates when they have the power to fix the flaw, even if it isn't their software. This illustrates the great importance of keeping Windows up to date.

Sure, if you are at work and have an IT team like the staff at Tech Experts, your updates are managed and prioritized. While some updates are optional or just good for a more user-friendly experience, important security updates should always be installed as soon as possible. As Windows 7 updates come to an end this year, any of these types of exploits will remain unfixed. Switching to Windows 10 or replacing your computer is the only way to keep getting the latest patches for these intrusive exploits.

If you are already on Windows 10, make sure you have antivirus installed. As always, check your system regularly for updates and get help if you need it – your safety depends on it.

Why VoIP Is Taking Businesses By Storm

Alexander Stahl is a help desk intern at Tech Experts.

Communication is key in business, and with the rise of Voice over Internet Protocol (VoIP), communication has improved drastically. When phone calls can be made over the Internet, doors open for businesses.

First, VoIP offers businesses a consistent and full-time presence. Whether an employee is at their desk or out of the office, VoIP allows for incoming and outgoing calls to multiple devices using the same phone number.

For example, your employee may start their day in the office answering calls with their desk phone. After lunch, when they are scheduled for field work, they can take those same calls using VoIP software from their MSP. This makes for easy accessibility to clients, and it allows for your employees to be easily contacted by clients.

VoIP software is also very user friendly. It allows for easy call transferring and parking through the use of your desktop, and it provides seamless navigation of call queues and phone availability.

VoIP services also typically allow for users to easily see which of their coworkers are available, away, or busy at the moment.

This makes for efficient communication within a business.

Another integral part of business communications is the security behind the phone calls you are making. Home phones are different as it doesn't matter too much if you and your uncle's conversation is leaked, but in the business world, phone calls house sensitive information and a breach in phone system security could be detrimental to any business.

Although VoIP breaches can be accomplished, they are much harder to achieve than tapping a traditional phone system, leaving your business safer and far more secure.

When it comes to running a business, one of the main focuses must be reliability. Luckily enough, on top of all the other benefits of using a VoIP system, the reliability of the system is just the same as that of a traditional phone system. It could eventually become a more reliable system for making calls though.

Due to advancements in the field, more emphasis is put on Internet connectivity in businesses, so better software and systems will be put in place to upgrade your VoIP experience. In addition, many businesses have backup Internet connections, making a VoIP system far more reliable than a phone system in this instance.

One of the great parts about VoIP is the quality of your calls. Rather than hearing static, spotty audio, or having calls drop, VoIP call quality is fantastic. Calls are clear, understandable, and only have about a 20 millisecond delay for audio.

If your bandwidth can already handle all that your business needs on a day-to-day basis, there will be no problem with the quality of your VoIP calls.

VoIP is the future of business communications. With all of VoIP's features, reliability, quality, and easy accessibility in mind, it's no wonder that businesses across the globe are dialing into VoIP systems. Even as VoIP systems dominate, they continue to grow every day with new features to propel the ease of accessibility of the product. Is VoIP right for your business? Call us today at (734) 457-5000 and we can give you direction on upgrading your phone system.

"When it comes to running a business, one of the main focuses must be reliability. Luckily enough, on top of all the other benefits of using a VoIP system, the reliability of the system is just the same as that of a traditional phone system."

Top Concern For Small Businesses, Continued From Page 1

Instead, most cybercriminals gain access much in the way vampires are said to gain access to their victims:

Essentially, by being invited.

While lore claims that vampires must be invited into a home before they can step foot inside, cybercriminals also work their magic by essentially being given access to sensitive data by unknowing company employees — or even CEOs and other upper management members themselves.

It's called phishing, and it's the number one way cyber attackers gain security access to companies', organizations', governments', and individuals' data.

If you are a business owner who's concerned about the cybersecurity of your company in 2019, you're on the right track. While the growth of your business and the frightening possibility of a recession are surely important to you as well, everything can be lost in an instant if your company is attacked by a cybercriminal.

Taking steps now to better train your employees and enlist the right cybersecurity professionals to protect your business is wise and responsible.

Five Social Media Mistakes Businesses Must Avoid

Social media is an incredible chance for your brand to interact directly with your audience and grow it even further. If you're not able to manage your social media marketing properly however, you'll simply waste time and resources, or worse, actually harm your brand's reputation.

Here are five key social media marketing mistakes that your business must avoid at all costs:

Discussing Hot-Button Topics

Some topics, especially political and religious ones, are simply not worth bringing up. This is especially true in today's divisive political environment.

You'll end up dividing your audience and perhaps even bringing negative attention onto your brand. It's better to avoid these issues altogether and playing it a bit safer with your choice of topics.

Winging It

Social media marketing is the same as any other digital marketing strategy. You need to know what you want to get from it. If you don't have specific goals for your social media strategies, you'll never know exactly what to do or when they're successful.

Take the time to think about what you really want from each social media platform, and brainstorm about what you must do to get there.

Posting For the Sake of It

Research has found that the number of social media posts you need to be making on a daily and weekly basis is quite frequent in order to truly engage with and grow your audience.

On Twitter, for example, you may need to Tweet up to 15 times per day. However, you cannot forego quality for the sake of quantity.

Treating All Platforms the Same

It's likely that you have a presence on a wide variety of social media platforms. At the very least, Facebook and Twitter, and then probably a couple out of Snapchat, Instagram, YouTube, Pinterest, etc. The problem is when you treat all social media platforms the same. The average audience on Facebook and Twitter are much different. People use Instagram differently than they use Pinterest. If you want to truly thrive on social media, you need to understand each platform and what your audience is looking for on it.

Ignoring Negative Activity

It's critical that you don't get defensive on social media, but you cannot simply let negative feedback go unanswered. Not only does it further harm the relationship between you and the individual complaining, but it also adds some legitimacy to the complaint for everybody else to see.

After all, if you had a reasonable response to the complaint, why wouldn't your company voice it? Make sure that you have dedicated customer service resources handling your social media comments in a professional, expedient manner.

By avoiding the key social media marketing mistakes listed above, your business will be in a great position to not only survive on social media platforms, but thrive on them. Your audience will be engaged and energized, and you'll reach more people than you ever thought possible!

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