November 2020

TechTidbit.com

brought to you by Tech Experts

Is There A Hidden Intruder Lurking In Your Business?

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

If you're like us, you believe you have the best, most trustworthy people working for you.

But have you ever considered the possibility you may have someone unknown hidden within your business, trying to cause a lot of damage and make a lot of money at the same time?

This might sound a little far-fetched. Perhaps something that's more likely to happen in a film than in your business.

But actually, you'd be surprised. Cyber criminals are targeting businesses exactly like yours all the time.

Because often, small and medium sized businesses don't spend big bucks on their cyber security. Hackers know this. And will put a lot of effort in to try to exploit that.

We're seeing a rise in ransomware attacks. This is the computer attack where a hacker locks you out of your systems and data. And you must pay a ransom, typically in Bitcoin, to get access again.

While it's not a new crime, it's one of the fastest growing crimes online.

Ransomware attacks are often successful because the hackers have managed to access a network, then sit quietly within it for weeks or even months without being detected.

This gives them plenty of time to secretly prepare their attack. And make it virtually impossible for even the best IT security experts to undo their damage once an attack has been launched.

Thanks to the surge in home working this year and an increase in remote network access, many businesses are making it just too easy for hackers.

They bide their time, investigate your business and set up everything in their favor… just waiting for the right time to launch their attack.

Reality check: This kind of attack can cripple your business.

Hackers will encrypt or delete all your data, leaving you to:

• Explain the breach to your clients
• Try to restore what you've lost (that's if you have a working backup saved off-site that hasn't been affected) and clean up your network
• Or just pay the large ransom to undo the damage

It can cost thousands. And accounts for a scary number of businesses going under. The biggest news-making ransomware event in was the Baltimore City government.

The city's computer system was hit with a ransomware infection in May 2019 that kept the city's government crippled for over a month.

Estimates put the cost to recover at over $18 million dollars, although the cybercriminal behind the malware only demanded $76,000 worth of Bitcoin. The attack reportedly impacted vaccine production, ATMs, airports, and hospitals and took months to recover.

But if you know the warning signs to look out for, you can dramatically reduce your risk of falling victim to a hidden hacker, already in your system.

Our data security experts have helped to foil this type of attack. And we'd like to help you.

Can we offer your business a breach detection review? During the review, our specialists can carry out a detailed network check to detect if there has been any unauthorized activity.

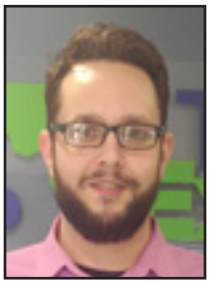
They can look for the warning signs of a breach, and give you some advice for preventing this kind of attack in the future.

Before we carry out the review, we'll need to have a quick video call (no more than 15 minutes) to discuss your current security, your business, and to answer any questions you may have. Give us a call at (734) 457-5000.

Thanks to the surge in home working this year and an increase in remote network access, many businesses are making it just too easy for hackers.

Say Goodbye To Owning Microsoft Office

"While the announcement came originally involving Exchange server, the end result is the same: Microsoft will make you switch, and it won't be a choice anymore."



Jason Cooley is Support Services Manager at Tech Experts.

In the workplace, some would say there is nothing as important as ensuring your productivity. Working with computers is likely a part of your job to some degree. If you are working in an office setting, you likely spend a large amount of time on computers.

There is no doubt a difference in daily tasks between different fields, but there are also many similarities. No matter your industry, you are likely familiar with Microsoft Office programs. Excel, Word, and Outlook are the most commonly used software from the Microsoft Office suite.

Microsoft Office is not cheap. Many businesses will use their current version until it is no longer supported. If 30 users need a new version of Office or a subscription, it has been more cost effective in the past to purchase a copy of the program to use for years until the software becomes unsupported.

This is all going to change. Recently, Microsoft made the announcement regarding the newest version of Exchange Server, their mail server platform. "This is going to be a version of Exchange that will only be available with the purchase of a subscription," said Greg Taylor, director of product marketing for Exchange.

This applies to Exchange server, but also applies to Office as they try to move to a month-to-month, pay-as-you-go service. Email hosting and all of your apps are now something you can't own.

This can result in one of two things, depending on your business. It could be the perfect time to start moving your employees over to the month-to-month model if they aren't already subscribed.

Alternatively, it can be a burden on someone who will need to switch many users to the pay-by-month model. Microsoft wants the recurring revenue generated in a subscription service, and they don't mind forcing you into it.

While the announcement came originally involving Exchange server, the end result is the same: Microsoft will make you switch, and it won't be a choice anymore. For Exchange, 2019 Exchange server will be the last in the line that you can purchase and own.

Once that is out of the support window, you would need to move your licensing to the new subscription model.

As this applies to Office as well, many people may worry about when the changes will need to occur. The changes will not need to be made any time soon if you just purchased, say, Office 2019. You will have a few more years (likely three to four, based on past end of support dates) before you have to pull the trigger.

However, users holding out with Office 2013 will have to make a decision a lot sooner as the security updates end.

The switch to a subscription model is for Microsoft's benefit. Assuming you used your Office software for five years, you will end up paying more for the new subscription service over those five years.

On the other side of things, you will always have the newest version of Office available to you as every major update and every new version is included.

While it is not an immediate concern, you should start to consider what your Office needs are as time moves forward. Like the rest of the world, Microsoft is always changing.

Targeted Attacks On Small Businesses Are On The Rise

Mark Funchion is a network technician at Tech Experts.

Many of us have heard of ransomware. This is an attack where someone gains access to a system and encrypts all of the data until a ransom is paid. Once they get their money, they either unencrypt the data… or not. There is no guarantee that paying the ransom will actually work.

Most attacks in the past, both viruses and ransomware, were the "spray and pray" variety. Basically, the attackers would send out thousands (or hundreds of thousands) of emails and hope that a small percentage of them were successful. This procedure worked, but the success rate was low and the attackers had to have a large volume to make it successful.

The more profitable attacks that are on the rise are targeted attacks. These attacks rely on quality rather than quantity. Research goes into the attacks that then target a single or very few companies. These attackers will even go as far to check a company or institution's financial information to see how much of a ransom they can expect to get.

In addition to demanding a ransom for the data to be decrypted, there is often a threat that the data will be released if the ransom is not paid. The threat of data being released can lead to the ransom being paid even if the target has a way to recover from the attack.

While many home users would hate to have their data released, it would not be completely devastating in most cases. If you are a financial, medical, or education institution, it could end your business or severely harm it. These institutions all contain sensitive information of their employees and clients.

For this reason, a recent spike has been seen in the UK involving their schools. Attackers are seeing schools as an easier target in today's environment with the increase in remote learning. Banks and hospitals have been targeted numerous times before, and their main goal is to be as secure as possible, spending large amounts of money on it.

Schools and universities, on the other hand, are concerned with security, but they're in a position today with COVID where they need to have fairly open access.

As colleges are pivoting to a distance learning model on a scale never envisioned, they have to allow more and more access in. This means more and more devices the schools have no direct control over, creating potential entry points into the network.

Although most of you reading this are not educational institutions, there is no industry or business (regardless of size) that is safe from a potential attack. Having a good network security system in place with effective backups is critical.

Don't rely only on a day or a few days' worth of backups either; some attacks will infect a system, then remain dormant for a while, hoping to outlive the backups you have available.

Having a technology partner who understands the dangers and how to recover is essential. You cannot just plug in a firewall and use an antivirus software and consider yourself protected.

Your business should have an incident response plan that includes backups and restore procedures, as well as testing. You also need to make sure you have a procedure to keep all of your systems up-to-date with the most current patches. Making sure any remote sessions are secure and using 2FA whenever possible is another area often overlooked too.

The list of vulnerabilities is endless, but we are here to assist. Let us provide you the security and comfort that your business is protecting not only your data, but your users from a potential breach.

"In addition to demanding a ransom for the data to be decrypted, there is often a threat that the data will be released if the ransom is not paid. The threat of data being released can lead to the ransom being paid even if the target has a way to recover from the attack."

What Exactly Is "The Cloud?"

You may have come across people talking about 'cloud' storage and software that runs in 'the cloud.'

But what exactly is 'the cloud,' and why should you care about it?

A place for networking

The cloud is a bunch of servers that are connected to each other over the internet.

Tech firms like Google, Microsoft, Apple, Facebook, and Amazon run huge networks of servers that let their customers (us) log in using different devices.

Can you imagine a situation where all your photos from the last 10 years were only held on your phone and not stored safely elsewhere? How many memories would you lose if your phone went missing?

The high freedom, convenience, and security offered by the cloud has seen a huge shift to cloud computing over the last few years.

It's powerful stuff

Cloud infrastructure allows you to run apps and access data across multiple devices without needing to have everything installed on your devices.

This opens opportunities for businesses to offload computing and storage resources to cloud service providers, gaining the flexibility to easily boost or reduce resources as their needs change.

A real perk of running software in the cloud is that it means highly sophisticated applications can run from your computer or phone, with the cloud doing all the heavy lifting.

This can significantly reduce the amount you need to spend on your devices and how often they need to be replaced.

The cloud is also a collaborative place to be. Tools like Microsoft 365 and Google Workspace make it super easy to share documents and work as a team. You can even work together in real-time and give each other instant feedback as you go.

Ignore its fluffy reputation: The cloud's a tough cookie

When set up and managed correctly, the cloud is the safest place to keep your data.

Let's be honest, which is more likely: Colin leaving his laptop in a bar again? Or the might of an Amazon or a Google getting hacked?

If Colin loses that laptop, he'll get a slap on the wrist. If Google get hacked, it would cost them millions and millions of dollars and cause irreparable damage to their reputation.

Different types of cloud

There are three main types of cloud.

Private cloud
The private cloud is a network of servers that are dedicated to supporting a single business.

The hardware is solely dedicated to this business, and they allow organizations like the CIA and banks to have full control over every aspect of their cloud environment.

Public cloud
The public cloud refers to networks of servers that are wholly controlled by cloud service providers. Clients share resources with other people.

The public cloud costs less than setting up a private cloud, and there is far less maintenance and an extremely high level of reliability.

Hybrid cloud
Some firms like to mix and match private and public clouds for different needs. Hybrid cloud setups let businesses quickly move between the two as their needs change.

We'll help you to make sense of it all.

When embracing the cloud, it's best to have an experienced hand guide you to the right solutions.

Working with the right IT support partner early will help make sure that you head in the right direction. And make the most of the opportunities that cloud computing offers. Give us a call at (734) 457-5000 if you'd like more information.

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