August 2023

TechTidbit.com

brought to you by Tech Experts

Is Your Team Suffering From Cyber Security Fatigue?

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

Recently, we've seen a concerning trend among businesses: cyber security fatigue.

It's a phenomenon that occurs when people become overwhelmed and desensitized to the constant barrage of cyber threats and security alerts they face on a daily basis.

You may be thinking, "My business is too small to be a target for cyber criminals."

Unfortunately, that couldn't be further from the truth. In fact, small businesses are often targeted precisely because they are seen as easier targets.

Cyber criminals know that small businesses don't have the same resources as larger corporations, making them more vulnerable to attacks.

So, how can you tell if your business is suffering from cyber security fatigue? Here are a few signs to look out for:

- Your employees are ignoring security alerts or taking shortcuts to get around them
- You've had a data breach or cyber attack in the past, but didn't take significant steps to prevent it from happening again
- You're relying solely on antivirus software to protect your business
- You haven't updated your security protocols in a while

If any of these sound familiar, it's time to take action. Here are a few ideas to help you combat cyber security fatigue and keep your business secure:

Invest in employee training

Your employees are your first line of defense against cyber threats. Make sure they understand the risks and are trained in proper security protocols.

Use multi-factor authentication

This adds an extra layer of security by requiring users to provide additional verification before accessing sensitive information.

Keep your software up to date

Many cyber attacks happen because of outdated software that contains vulnerabilities. Make sure all software is regularly updated to the latest version.

Partner with a trusted IT support provider

We can provide ongoing support and monitoring of your systems, ensuring that your business stays secure and up to date.

Don't let cyber security fatigue put your business at risk. By taking proactive steps to improve your security, you can protect your business and enjoy peace of mind. Remember, the best defense is a good offense! If we can help, get in touch.

Cyber criminals know that small businesses don't have the same resources as larger corporations, making them more vulnerable to attacks.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Meetings Are Making Your People Less Productive

"For projects that have a visual element, digital whiteboards are your new best friend. These handy tools allow for collaboration wherever, whenever, and replicate the feeling of being in an actual conference room."

Are you one of the many businesses that still offers your people the flexibility of remote or hybrid working?

If so, you're probably relying on video meetings a lot more than you usually would. And that makes sense, because it feels like the easiest way to get people together at the same time.

But meetings can be a real drag for everyone at some stage. Whether you're dealing with introverted employees who are hesitant to speak up, scheduling conflicts that make it tough to get everyone in the same virtual room, or colleagues who try to take all the credit for your brilliant ideas (the worst!), meetings can actually slow down your productivity.

So what are some simple solutions to help?

For projects that have a visual element, digital whiteboards are your new best friend. These handy tools allow for collaboration wherever, whenever, and replicate the feeling of being in an actual conference room. Plus, they don't put anyone on the spot, so introverted employees can contribute without feeling self-conscious.

And for projects that don't require visuals? Maybe collaborative docs could be a good alternative for you. These documents are easily shared and distributed, making it easy for team members to work together in real-time or asynchronously.

Let your team know that they don't need to respond immediately to every notification or email. And if you really want to free up some time for deep-focus work, consider implementing a "no meetings" policy like Shopify has done.

This empowers your team to work when they're most effective, regardless of their time zone.

When it comes to productivity, transparency is key! So have you considered prioritizing public channels over direct messages? It can be a game-changer for your team as it helps everyone understand how different individuals and teams work, and increases workers' faith in their managers.

In fact, research shows that employees who trust their leadership are 50% more engaged at work! And when it comes to clarifying priorities, the responsibility falls on leadership. Make sure you're coaching your direct reports and giving regular feedback. Consider consolidating work in one platform to make things simpler.

By choosing the right tools and minimizing time spent in meetings, you can increase your productivity and get more done in less time. So why wait? If we can help you get started, get in touch.

- The first domain name ever registered was symbolics.com on March 15, 1985. At the time, there were only six other domain names in existence, making symbolics.com one of the earliest websites to exist on the internet
- About 51% of internet traffic is not human. More than 30% is made up of hacking programs, spammers, and phishing scams
- According to Nordpass, the most commonly used password is "password" which, despite being easily hackable, is still used by 5 million people worldwide. Crazy!

Zero-Click Malware Is The Latest Cyber Threat

In today's digital landscape, cybersecurity threats continue to evolve. They pose significant risks to individuals and organizations alike.

One such threat gaining prominence is zero-click malware. This insidious form of malware requires no user interaction. It can silently compromise devices and networks.

One example of this type of attack happened due to a missed call. That's right, the victim didn't even have to answer. This infamous WhatsApp breach occurred in 2019, and a zero-day exploit enabled it. The missed call triggered a spyware injection into a resource in the device's software.

A more recent threat is a new zero-click hack targeting iOS users. This attack initiates when the user receives a message via iMessage. They don't even need to interact with the message of the malicious code to execute. That code allows a total device takeover.

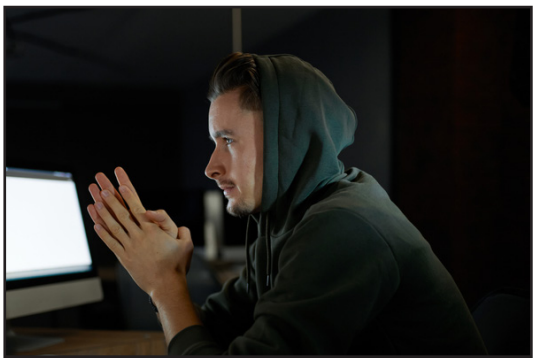
Understanding zero-click malware

Zero-click malware refers to malicious software that can do a specific thing. It can exploit vulnerabilities in an app or system with no interaction from the user. It is unlike traditional malware that requires users to click on a link or download a file.

The dangers of zero-click malware

Zero-click malware presents a significant threat. This is due to its stealthy nature and ability to bypass security measures. Once it infects a device, it can execute a range of malicious activities including:

- Data theft
- Remote control
- Cryptocurrency mining
- Spyware
- Ransomware
- Turning devices into botnets for launching attacks



This type of malware can affect individuals, businesses, and even critical infrastructure. Attacks can lead to financial losses, data breaches, and reputational damage.

Fighting zero-click malware

To protect against zero-click malware, it is crucial to adopt two things. A proactive and multilayered approach to cybersecurity. Here are some essential strategies to consider:

Keep software up to date
Regularly update software, including operating systems, applications, and security patches. This is vital in preventing zero-click malware attacks. Software updates often contain bug fixes and security enhancements.

Put in place robust endpoint protection
Deploying comprehensive endpoint protection solutions can help detect and block zero-click malware. Use advanced antivirus software, firewalls, and intrusion detection systems.

Use network segmentation
Segment networks into distinct zones. Base these on user roles, device types, or sensitivity levels. This adds an extra layer of protection against zero-click malware.

Educate users
Human error remains a significant factor in successful malware attacks. Educate users about the risks of zero-click malware and promote good cybersecurity practices. This is crucial.

Encourage strong password management. As well as caution when opening email attachments or clicking on unfamiliar links.

Use behavioral analytics and AI
Leverage advanced technologies like behavioral analytics and artificial intelligence. These can help identify anomalous activities that may indicate zero-click malware.

Conduct regular vulnerability assessments
Perform routine vulnerability assessments and penetration testing. This can help identify weaknesses in systems and applications.

Uninstall unneeded applications
The more applications on a device, the more vulnerabilities it has. Many users download apps then rarely use them. Yet they remain on their device, vulnerable to an attack.

Only download apps from official app stores
Be careful where you download apps. You should only download from official app stores. And always keep your apps updated using your device's app store application.

"One example of this type of attack happened due to a missed call. That's right, the victim didn't even have to answer. This infamous WhatsApp breach occurred in 2019, and a zero-day exploit enabled it. The missed call triggered a spyware injection into a resource in the device's software."

Contact Information

Tech Experts Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

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

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Do You Still Believe In These Common Tech Myths?

Is it okay to leave your smartphone charging overnight? Do Macs get viruses? And what about those 5G towers? What's going on with those?

Common tech myths can often lead to misunderstandings. They can even hinder your ability to fully use various tools and devices.

Let's debunk some of the most common tech myths that continue to circulate and explore the truth behind them.

Myth 1: Leaving your device plugged in overnight damages the battery

First is one of the most persistent tech myths. Leaving your device plugged in overnight will harm the battery life. But this myth is largely outdated.

Modern smartphones, laptops, and other devices have advanced battery management systems.

These systems prevent overcharging. Once your device reaches its maximum charge capacity, it automatically stops charging. So, feel free to charge your gadgets overnight without worrying about battery damage.

Myth 2: Incognito mode ensures complete anonymity

While incognito mode does provide some privacy benefits, they're limited.

For example, it mainly prevents your device from saving the following items:

- Browsing history
- Cookies
- Temporary files

However, it does not hide your activities from your internet service provider (ISP). Nor from the websites you visit.

Myth 3: Macs are immune to viruses

Another prevalent myth is that Mac computers are impervious to viruses and malware. It is true that Macs have historically been less prone to such threats compared to Windows PCs. This does not make them immune.

It's true that in 2022, 54% of all malware infections happened in Windows systems and just 6.2% happened in macOS.

But as of January 2023, Windows had about 74% of the desktop OS share to Mac's 15%. So, it turns out the systems aren't that different when it comes to virus and malware risk.

The data shows the infection rate per user on Macs is 0.075. This is slightly higher than Windows, at 0.074. So, both systems have a pretty even risk of infection.

Myth 4: More megapixels mean better image quality

When it comes to smartphone cameras, savvy marketing sometimes leads to myths. Many people believe that more megapixels equal better image quality. This is a common misconception.

Other factors, in addition to megapixels, play a significant role, such as:

- The size of individual pixels
- Lens quality
- Image processing algorithms
- Low-light performance

A camera with a higher megapixel count may produce larger images. But it does not guarantee superior clarity, color accuracy, or dynamic range. When choosing a smartphone or any camera, consider the complete camera system.