December 2024

TechTidbit.com

brought to you by Tech Experts

The Number One Threat To Your Business? Ransomware

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

Imagine this: You're starting a normal day, coffee in hand, ready to tackle your to-do list. Suddenly, a red screen flashes on your computer, and a message pops up: "Your files have been encrypted. Pay up to get them back."

That's ransomware, a cyber attack that's fast becoming the number one threat to businesses worldwide. It's become a top choice for cyber criminals because it's profitable, easy to deploy, and very effective.

Cyber criminals get their ransomware software onto a computer, often from something as simple as a link in a phishing email (that's an email pretending to be from a trusted source). When clicked, it installs software that gives them access to your system, files and even backup locations.

They lock your files, making them unreadable. The cyber criminals demand payment, usually in cryptocurrency, and promise to return access once they're paid. Some even threaten to leak sensitive info if you don't comply.

It's scary and the consequences for any business are huge. It's not just the loss of data. It's expensive, time-consuming, and could break the trust you enjoy with your customers and suppliers.

So, how do you keep your business safe?

The good news is that basic security practices can go a long way. Start by training your team not to click on suspicious links or open unexpected attachments. Regularly updating applications and security software is also crucial as it closes security gaps cyber criminals might try to exploit.

Most importantly, create a reliable backup system. Set up isolated, "cold" backups that are disconnected from your main system. So, if an attack hits, your data remains untouched.

Regularly test these backups to make sure they work when you need them. In a ransomware attack, being able to restore your data from a safe backup can save your business from costly downtime or ransom demands.

Ransomware is serious, but a proactive approach can make all the difference. With the right prep, you can keep your business running smoothly. If you'd like help with that, get in touch. Call us at (734) 457-5000 or email info@mytechexperts.com.

Cyber criminals get their ransomware software onto a computer, often from something as simple as a link in a phishing email (that's an email pretending to be from a trusted source). When clicked, it installs software that gives them access to your system, files and even backup locations.

Need New Hardware? Here's Where To Start

"Beyond performance issues, consider whether your current hardware aligns with your business needs. For example, if your team is transitioning to hybrid or remote work, laptops with better portability and extended battery life may be necessary."

When your team's computers or internet start lagging, it's often a sign your hardware needs an upgrade. But with so many tech options, you may want some help knowing where to start. Upgrading hardware can feel like a daunting task, but with a bit of guidance, small businesses can make informed choices that improve efficiency, security, and productivity.

Understanding the signs you need an upgrade

Computers and other tech devices aren't meant to last forever. If your employees frequently complain about slow load times, crashing applications, or connectivity issues, it's a clear indication that your hardware might not be keeping up. Older equipment may also struggle to support the latest software updates, leaving your business vulnerable to cyber threats or inefficiencies.

Beyond performance issues, consider whether your current hardware aligns with your business needs. For example, if your team is transitioning to hybrid or remote work, laptops with better portability and extended battery life may be necessary.

Similarly, businesses managing large files or using graphics-intensive software should invest in systems with robust processing power and high-resolution displays.

Choosing the right equipment

When selecting new hardware, focus on what makes sense for your business operations. For many small businesses, reliability and scalability are the top priorities. Here are a few key items to consider:

Desktops and Laptops: Decide whether you need desktops for stationary workstations or laptops for mobility. For general office tasks, mid-range models with solid-state drives (SSDs), at least 8GB of RAM, and Intel Core i5 or AMD Ryzen 5 processors are often sufficient.

Networking Equipment: Outdated routers and switches can bottleneck your internet speeds, no matter how fast your ISP claims to be. Upgrading to Wi-Fi 6 routers or mesh networking systems can significantly improve connectivity and range, especially in larger offices.

Monitors and Accessories: Dual monitors are increasingly standard for maximizing productivity. Additionally, ergonomic keyboards, mice, and adjustable monitor stands can reduce strain and improve comfort for your team, especially for staff who work at a computer all day.

Servers and Storage: If your business handles sensitive data or large volumes of information, upgrading to a dedicated server or Network Attached Storage (NAS) device can provide better security and accessibility.

Printers and Scanners: While many offices are moving toward paperless workflows, reliable printers and scanners are still essential for certain industries. Look for multifunction devices with wireless connectivity for added convenience.

Balancing budget and long-term value

Hardware upgrades are an investment, so it's important to strike a balance between cost and value. Cutting corners to save a few dollars upfront can lead to higher expenses in the long run if equipment fails prematurely or doesn't meet your needs.

Consider working with a Managed Service Provider (MSP) to identify cost-effective options tailored to your business. MSPs often have access to bulk purchasing discounts and can recommend hardware that integrates seamlessly with your existing systems. They can also assist with setup, ensuring minimal disruption to your workflow.

The environmental impact

Finally, don't overlook the opportunity to dispose of old equipment responsibly. Many manufacturers and local organizations offer recycling programs that ensure outdated hardware is disposed of in an environmentally friendly manner. Some programs even offer trade-in credits to help offset the cost of new purchases.

Upgrading your computer hardware doesn't have to be overwhelming. By identifying your team's needs, prioritizing reliable and scalable options, and partnering with experts when needed, you can ensure your business stays competitive and efficient. Investing in the right tools today can save you time, money, and headaches down the road—and your team will thank you for it.

Watch Out! "Malvertising" Is On The Rise!

There are many types of malware. One of the most common is called "malvertising." It crops up everywhere. You can also see these malicious ads on Google searches.

Two things are making malvertising even more dangerous. One is that hackers use AI to make it very believable. The other is that it's on the rise, according to Malwarebytes. In the fall of 2023, malvertising increased by 42% month over month.

Below, we'll help you understand malvertising and give you tips on identifying and avoiding it.

What is "malvertising?"

Malvertising is the use of online ads for malicious activities. One example is when the PlayStation 5 was first released. It was very hard to get, which created the perfect environment for hackers. Several malicious ads cropped up on Google searches. The ads made it look like someone was going to an official site. Instead, they went to copycat sites. Criminals design these sites to steal user credentials and credit card details.

Google attempts to police its ads, but hackers can have their ads running for hours or days before they're caught. These ads appear just as any other sponsored search ad. They can also appear on well-known sites that have been hacked or on social media feeds.

Tips for protecting yourself from malicious online ads

Review URLs carefully
You might see a slight misspelling in an online ad's URL. Just like phishing, malvertising often relies on copycat websites. Carefully review any links in the ads.

Visit websites directly
A foolproof way to protect yourself is not to click any ads.

Instead, go to the brand's website directly. If they truly are having a "big sale," you should see it there. Just don't click those links and go to the source directly.

This image was generated by an AI engine.

Use a DNS filter
A DNS filter protects you from mistaken clicks. It will redirect your browser to a warning page if it detects danger. DNS filters look for warning signs. This can keep you safe even if you accidentally click a malvertising link. Often, you'll see a block page.

Do not log in after clicking an ad
Malvertising will often land you on a copycat site. The login page may look identical to the real thing. One of the things phishers are trying to steal is login credentials.

If you click an ad, do not input your login credentials on the site, even if the site looks legitimate. Go to the brand's site in a different browser tab.

Don't call suspicious ad phone numbers
Phishing can also happen offline. Some malicious ads include phone numbers to call. Unsuspecting victims may not realize fake representatives are part of these scams. Seniors are often targeted; they call and reveal personal information to the person on the other end of the line.

Stay away from these ads. If you find yourself on a call, do not reveal any personal data.

Don't download directly from ads
"Get a free copy of MS Word" or "Get a Free PC Cleaner." These are common malvertising scams. They try to entice you into clicking a download link. It's often for a popular program or freebie. The link actually injects your system with malware to do further damage.

A direct download link is likely a scam. Only download from websites you trust.

Warn others when you see malvertising
If you see a suspicious ad, warn others. This helps keep your colleagues, friends, and family more secure. If unsure, do a Google search. You'll often run across scam alerts confirming your suspicion.

Foster a culture of cyber awareness

It's important to arm yourself and others with this kind of knowledge. Foster a culture of cyber-awareness to ensure safety and better online security.

"Google attempts to police its ads, but hackers can have their ads running for hours or days before they're caught. These ads appear just as any other sponsored search ad. They can also appear on well-known sites that have been hacked or on social media feeds."

Contact Information

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

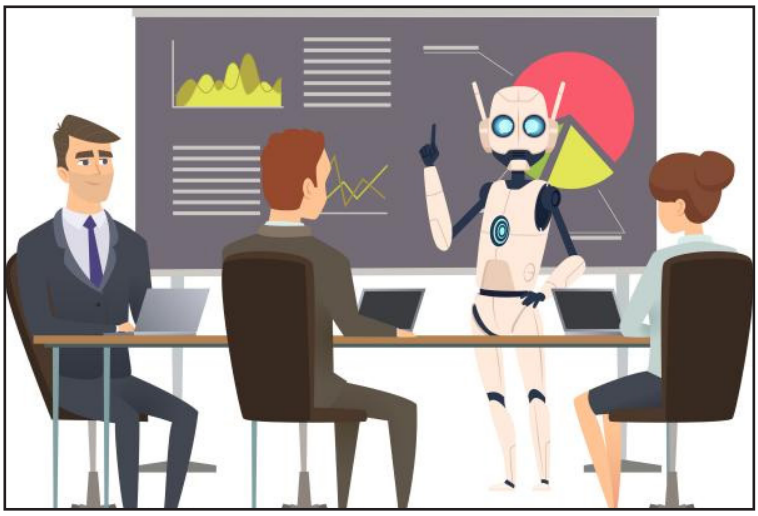
Main Office
(734) 457-5000
info@MyTechExperts.com

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

Why Small Businesses Need Cybersecurity Training for Employees



Your team is the first line of defense against cyber threats, but without proper training, they may also be your biggest vulnerability. From spotting phishing emails to practicing safe browsing habits, employee cybersecurity training is essential for protecting your business.

Cybercriminals target small businesses because they often lack robust defenses, relying instead on trust and good intentions. Unfortunately, these qualities make employees prime targets for attacks like phishing or social engineering. A single click on a malicious link can open the door to data breaches, ransomware, or other costly disruptions.

Training your team doesn't have to be a major production. Simple, practical lessons can make a big difference. Start with the basics: teaching employees to recognize the red flags of phishing emails. Suspicious links, poor grammar, or an urgent tone asking for personal information are all common giveaways. Encourage them to verify requests before acting, especially when handling sensitive data.

Password security is another critical area to address. Employees should use unique, complex passwords for different accounts and avoid writing them down. Better yet, implement a password manager to simplify the process. Two-factor authentication adds an extra layer of protection, making it harder for hackers to gain access.

Safe browsing habits should also be part of your training. Remind your team to avoid clicking on ads, downloading attachments from unknown sources, or visiting suspicious websites. Tools like DNS filters can provide an additional safeguard against accidental clicks.

Finally, regular practice is key. Consider running simulated phishing campaigns to test your team's ability to spot threats. Review the results and provide constructive feedback to improve their skills over time. A well-trained employee is far less likely to fall for scams, keeping your business safer.

Investing in cybersecurity training isn't just about preventing threats.

It builds a culture of awareness and responsibility, ensuring everyone plays a role in safeguarding your company's data. In the long run, this proactive approach can save you significant time, money, and headaches.

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).