June 2024

TechTidbit.com

brought to you by Tech Experts

Work From Home Employees... Out Of Sight, Out Of Mind?

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

Having your employees work from home or their local coffee shop is the norm now. And while there are loads of benefits to this new attitude to work, it's easy to overlook a crucial aspect of keeping operations secure: The home set-ups of remote employees.

Here's the thing - neglecting remote security can lead to some serious headaches down the line. And you already have enough business headaches, right?

Imagine this: Your employee's laptop, which holds loads of sensitive company data, gets breached because their home Wi-Fi network wasn't properly secured.

Or worse, a malware infection spreads from their kid's device to their work laptop, putting your entire network at risk. That's scary.

A little vigilance and some regular checks can prevent these risks and keep your business and its data much safer.

So, let's talk about devices. Encourage your remote workers to treat their work devices like Fort Knox. That means regular updates and patches, robust protective software, and strong, unique passwords (password managers are your best friend for this).

Remind them to avoid risky behaviors like downloading software from unofficial sources or clicking on suspicious links.

Next, address home networks. A weak Wi-Fi password is asking for trouble.

Encourage your employees to set a strong password for their home network (again, a password manager can remove the hassle of this). And while they're at it, remind them to enable encryption and hide their network's SSID (Service Set Identifier) to add an extra layer of security.

And it's not just about devices and networks – physical security matters too. Use biometrics to protect logins. Remind your team to keep their work devices secure when they're not in use, whether that means locking them away in a drawer or simply keeping them out of sight from prying eyes.

And if they're working from a shared space like a coffee shop, remind them to be cautious of public Wi-Fi and to keep an eye on their belongings.

Regular checks are key to staying on top of security. Schedule routine audits of remote set-ups to ensure everything gets a thumbs up. This could include checking for software updates, reviewing network configurations, and providing refresher training on best security practices.

Want a hand with that? We can help - get in touch.

Encourage your remote workers to treat their work devices like Fort Knox. That means regular updates and patches, robust protective software, and strong, unique passwords (password managers are your best friend for this).

Don't Skip It! Why You Shouldn't Skip Regular Vulnerability Assessments For Your Company

"Some businesses may be tempted to forego vulnerability assessments. They might think it's too costly or inconvenient. Small business leaders may also feel it's just for the "big companies." But vulnerability assessments are for everyone."

Cyber threats are a perpetual reality for business owners. Hackers are constantly innovating. They devise new ways to exploit vulnerabilities in computer systems and networks.

For businesses of all sizes, a proactive approach to cybersecurity is essential. One of the most crucial elements of this approach is regular vulnerability assessments. A vulnerability assessment is a systematic process that identifies and prioritizes weaknesses in your IT infrastructure.

Some businesses may be tempted to forego vulnerability assessments. They might think it's too costly or inconvenient. Small business leaders may also feel it's just for the "big companies." But vulnerability assessments are for everyone.

Why vulnerability assessments matter

The internet has become a minefield for businesses. Cybercriminals are constantly on the lookout for vulnerabilities to exploit. Once they do, they typically aim for one or more of the following:

- Gain unauthorized access to sensitive data
- Deploy ransomware attacks
- Disrupt critical operations

Here's why vulnerability assessments are crucial in this ever-evolving threat landscape:

- **Unseen Weaknesses:** Many vulnerabilities remain hidden within complex IT environments.
- **Evolving Threats:** Experts discover new vulnerabilities all the time. Regular assessments ensure your systems are up to date.
- **Compliance Requirements:** Many industries have regulations mandating regular vulnerability assessments.
- **Proactive Approach vs. Reactive Response:** Identifying vulnerabilities proactively allows for timely remediation. This significantly reduces the risk of a costly security breach. A reactive approach is where you only address security issues after an attack.

The high cost of skipping vulnerability assessments

- **Data Breaches** - Unidentified vulnerabilities leave your systems exposed.
- **Financial Losses** - Data breaches can lead to hefty fines and legal repercussions as well as the cost of data recovery and remediation.
- **Reputational Damage** - A security breach can severely damage your company's reputation. It can erode customer trust and potentially impact future business prospects.
- **Loss of Competitive Advantage** - Cyberattacks can cripple your ability to innovate and compete effectively. This can hinder your long-term growth aspirations.

The benefits of regular assessments

- **Improved Security Posture:** Vulnerability assessments identify and address vulnerabilities.
- **Enhanced Compliance:** Regular assessments help you stay compliant with relevant industry regulations.
- **Peace of Mind:** Knowing your network is secure from vulnerabilities gives you peace of mind.
- **Reduced Risk of Costly Breaches:** Proactive vulnerability management helps prevent costly data breaches.
- **Improved Decision-Making:** Vulnerability assessments provide valuable insights into your security posture.

Vulnerability assessments are not a one-time fix. Your business should conduct them regularly to maintain a robust cybersecurity posture. By proactively identifying and addressing vulnerabilities, you can significantly reduce your risk of cyberattacks.

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).

Think About Recovery Before The Attack Strikes

Let us set the scene. It's an ordinary Wednesday. You're in the zone, minding your own business, getting things done, and making those boss decisions that keep your company running smoothly. Suddenly, without warning, BAM... you get hit with a cyber attack.

Panic mode kicks in.

But here's the thing: These attacks are far more common than you might think. And guess who the favorite targets are? Surprisingly, it's not the big multinational corporations but small and medium-sized businesses (SMBs) like yours.

The consequences of a cyber attack? We're talking about severe financial losses, significant data loss, and reputation damage that can take years to recover from. The whole nine yards.

However, it doesn't have to be that way. If you have a recovery plan in place, you can turn what could be a total nightmare into merely "an annoying inconvenience."

So, what should your recovery plan include? Well, let's start with prevention. Prevention is absolutely key. Investing in solid cybersecurity measures such as firewalls, antivirus software, and regular security checkups can go a long way in keeping your business safe. And don't underestimate the importance of educating your team about good cyber hygiene – this includes using strong passwords, recognizing phishing attempts, and not clicking on suspicious links.

Next, it's crucial to have a game plan for when the inevitable happens. This means having clear protocols in place for how to respond to an attack. Know who to call, what immediate steps to take to minimize the damage, and how to communicate with your stakeholders. Quick and decisive action can significantly reduce the impact of an attack.

One of the most critical components of your recovery plan is data backups. Regularly backing up your data to a secure location can be a true lifesaver in the event of an attack. This ensures that even if your systems are compromised, you still have access to your important files. Make sure your backups are done frequently and stored in a location that is not connected to your primary network.

Moreover, practice makes perfect! Regularly test your recovery plan to ensure it's effective and up to date. Conducting drills and simulations can help you identify any weaknesses in your plan and make necessary adjustments. After all, you don't want to wait until disaster strikes to discover that your plan has more holes than a block of Swiss cheese.

It's also important to consider the legal and regulatory aspects of cybersecurity. Different industries have different requirements when it comes to data protection and breach notification. Ensure that your recovery plan complies with all relevant laws and regulations. This not only helps protect your business but also builds trust with your customers and partners.

In the aftermath of an attack, communication is key. Be transparent with your customers, employees, and other stakeholders about what happened, what steps you are taking to address the situation, and how you plan to prevent future incidents. Honest and timely communication can help mitigate reputation damage and maintain trust.

Finally, consider partnering with cybersecurity experts who can provide additional support and guidance. They can help you develop a comprehensive recovery plan, conduct regular security assessments, and stay up to date with the latest threats and best practices. Cybersecurity is a complex and ever-evolving field, and having experts on your side can make a significant difference.

Cyber attacks may be scary, but with a solid recovery plan in place, you can rest easy knowing your business is armed and ready. Remember what they say: Fail to prepare, prepare to fail.

If you need assistance in creating your recovery plan, don't hesitate to get in touch. We're here to help you safeguard your business and ensure you're prepared for whatever comes your way.

"Regularly backing up your data to a secure location can be a true lifesaver in the event of an attack. This ensures that even if your systems are compromised, you still have access to your important files. Make sure your backups are done frequently and stored in a location that is not connected to your primary network."

Beware of Deepfakes! Learn How to Spot the Different Types

Have you ever seen a video of your favorite celebrity saying something outrageous? Then later, you find out it was completely fabricated? Or perhaps you've received an urgent email seemingly from your boss. But something felt off.

Welcome to the world of deepfakes. This is a rapidly evolving technology that uses artificial intelligence (AI). It does this to create synthetic media, often in the form of videos or audio recordings. They can appear real but are actually manipulated.

Deepfakes have already made it into political campaigns. In 2024, a fake robocall mimicked the voice of a candidate. Scammers wanted to fool people into believing they said something they never said.

Bad actors can use deepfakes to spread misinformation and damage reputations. They are also used in phishing attacks. Knowing how to identify different types of deepfakes is crucial in today's world.

So, what are the different types of deepfakes, and how can you spot them?

Face swapping deepfakes

This is the most common type. Here the face of one person is seamlessly superimposed onto another's body in a video. These can be quite convincing, especially with high-quality footage and sophisticated AI algorithms. Here's how to spot them:

- **Look for inconsistencies:** Pay close attention to lighting, skin tones, and facial expressions. Do they appear natural and consistent throughout the video? Look for subtle glitches such as hair not moving realistically or slight misalignments around the face and neck.
- **Check the source:** Where did you encounter the video? Was it on a reputable news site or a random social media page? Be cautious of unverified sources and unknown channels.
- **Listen closely:** Does the voice sound natural? Does it match the person's typical speech patterns? Incongruences in voice tone, pitch, or accent can be giveaways.

Deepfake audio

This type involves generating synthetic voice recordings. They mimic a specific person's speech patterns and intonations. Scammers can use these to create fake audio messages and make it seem like someone said something they didn't. Here's how to spot them:

- **Focus on the audio quality:** Deepfake audio can sound slightly robotic or unnatural. This is especially true when compared to genuine recordings of the same person. Pay attention to unusual pauses as well as inconsistent pronunciation or a strange emphasis.
- **Compare the content:** Does the content of the audio message align with what the person would say? Or within the context in which it's presented? Consider if the content seems out of character or contradicts known facts.
- **Seek verification:** Is there any independent evidence to support the claims made? If not, approach it with healthy skepticism.

Text based deepfakes

This is an emerging type of deepfake. It uses AI to generate written content like social media posts, articles, or emails. They mimic the writing style of a specific person or publication. Scammers can use these to spread misinformation or impersonate someone online. Here's how to spot them:

- **Read critically:** Pay attention to the writing style, vocabulary, and tone. Does it match the way the person or publication typically writes? Look for unusual phrasing, grammatical errors, or inconsistencies in tone.
- **Check factual accuracy:** Verify the information presented in the text against reliable sources. Don't rely solely on the content itself for confirmation.
- **Be wary of emotional triggers:** Be cautious of content that evokes strong emotions. Such as fear, anger, or outrage. Scammers may be using these to manipulate your judgment.

Staying vigilant and applying critical thinking are crucial in the age of deepfakes.

Familiarize yourself with the different types. Learn to recognize potential red flags. Verify information through reliable sources. These actions will help you become more informed and secure and protect you from these threats.

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