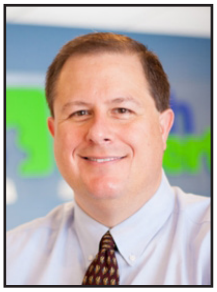
July 2024

TechTidbit.com

brought to you by Tech Experts

Wallet? Check. Planner? Check. Laptop? Uh oh... Laptop…? Laptop???



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

Summer time is travel time! Whether it's a trip across the state or across the country, everyone needs a break. But picture this: You've had a great trip up north with the family, and you're packing to head home. You're balancing your luggage, kids, shopping bags, and your laptop case. It's only when you get home that you realize, with a sinking feeling, that your laptop is nowhere to be found. Is it still at the hotel, maybe?

And then panic sets in as you remember all the sensitive data stored on that device.

This scenario is a nightmare, but it doesn't have to turn into a full-blown crisis. Having a solid plan in place can mitigate the risks associated with a lost or stolen work device.

Here's what you should do if you find yourself in this situation:

First and foremost, create an environment where employees feel comfortable reporting a lost or stolen device immediately. Your team needs to know that the sooner they inform the company, the better. Emphasize that there will be no blame or punishment – what matters most is safeguarding the data.

Ensure that all work-issued devices have remote wiping capabilities. This is your first line of defense. When a team member reports a laptop missing, your IT team should be able to remotely wipe the device, erasing all data to prevent unauthorized access.

Before a device is lost, proactive measures can make a world of difference. Make sure all company devices are encrypted. Encryption converts data into a code to prevent unauthorized access. Even if someone gets hold of a company laptop, encrypted data remains inaccessible without the proper decryption key. Most modern operating systems offer robust encryption options.

Always enforce strong password policies. All company laptops should have a complex password and, ideally, two-factor authentication (2FA). This adds an extra layer of security, making it harder for anyone to access the data if they bypass the initial password protection.

Regular training is vital. Employees should understand the importance of device security and the steps to take if a device is lost or stolen. Conduct workshops and send reminders about security protocols. The more informed everyone is, the quicker and more effectively they can respond to the loss.

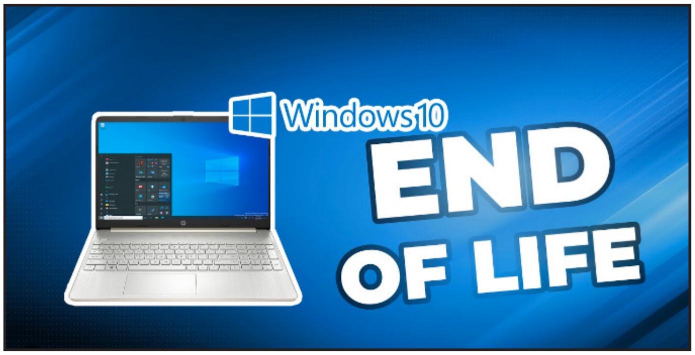
Why are these steps so crucial? If a business laptop falls into the wrong hands, the consequences can be severe. Unauthorized access to customer files can lead to identity theft and loss of client trust. Exposure of financial data could result in significant loss and legal consequences. Proprietary information could be stolen and sold. It's a nightmare.

By implementing these strategies, you can sleep easier knowing that your company's data remains secure, even if a device goes missing. It becomes a minor annoyance, not a disaster.

Ensure that all work-issued devices have remote wiping capabilities. This is your first line of defense. When a team member reports a laptop missing, your IT team should be able to remotely wipe the device, erasing all data to prevent unauthorized access.

It's Almost Time To Say Goodbye (To Windows 10)

> *"The logical next step is to upgrade to Windows 11. Before you jump in, it's crucial to check if your current hardware can support it.*
>
> *Windows 11 comes with higher system requirements, so you may need a compatibility check (there are tools available for this)."*



Microsoft announced that, come October 2025, Windows 10 will officially reach its end of life.

This means no more updates or support, which could leave your business's systems vulnerable. It's a significant shift, but you have a few options to manage the transition smoothly and make sure your operations stay secure and efficient.

Option 1: Ignoring the inevitable

You could choose to do nothing and keep using Windows 10. However, this "ostrich" approach could expose your business to serious risks.

Without updates, your systems become perfect targets for cyber attacks. The data you handle daily – customer details, financial information, and more – could be at risk. Not the best idea, right?

Option 2: Upgrade to Windows 11

The logical next step is to upgrade to Windows 11. Before you jump in, it's crucial to check if your current hardware can support it.

Windows 11 comes with higher system requirements, so you may need a compatibility check (there are tools available for this). The benefits of upgrading are plenty - enhanced security, a more intuitive interface, and new features designed to boost productivity. Windows 11 is a great way to enhance how you work.

Option 3: New hardware

If your current devices don't meet the requirements for Windows 11, it might be time for an upgrade. Don't look at investing in new hardware as a cost; it's an investment in your business's future.

New devices are faster, more efficient, and come with better security features right out of the box. It's an opportunity to streamline operations and maybe even reduce your long-term costs.

Option 4: Pay for Extended Security Updates

If upgrading isn't an option right now, Microsoft offers Extended Security Updates (ESUs) for Windows 10. This means you can still receive critical security updates, but at a cost.

For the first year, the price is manageable, but it doubles each year after that. While this can keep your systems secure a little longer, it's a temporary solution with escalating costs.

While fall 2025 might seem far away, starting your transition plan now is wise. Deciding whether to upgrade, update, or overhaul your systems takes time. Early planning helps minimize disruption and spreads out the costs associated with transitions.

If you're feeling overwhelmed by the choices or just need some expert advice tailored to your business needs, we can help – get in touch at (734) 457-5000 or info@mytechexperts.com.

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).

9 Easy Steps To Building A Culture Of Cyber Awareness

Cyberattacks are a constant threat in today's digital world. Phishing emails, malware downloads, and data breaches. They can cripple businesses and devastate personal lives.

Employee error is the reason many threats get introduced to a business network. A lack of cybersecurity awareness is generally the culprit. People don't know any better, so they accidentally click a phishing link. They also create weak passwords, easy for hackers to breach.

It's estimated that 95% of data breaches are due to human error.

But here's the good news, these mistakes are preventable. Building a strong culture of cyber awareness can significantly reduce your risks.

Why Culture Matters

Think of your organization's cybersecurity as a chain. Strong links make it unbreakable, while weak links make it vulnerable. Employees are the links in this chain. By fostering a culture of cyber awareness, you turn each employee into a strong link. This makes your entire organization more secure.

Easy Steps, Big Impact

Building a cyber awareness culture doesn't require complex strategies or expensive training programs. Here are some simple steps you can take to make a big difference.

1. Start with Leadership Buy-in

Security shouldn't be an IT department issue alone. Get leadership involved! When executives champion cyber awareness, it sends a powerful message to the organization. Leadership can show their commitment by:

- Participating in training sessions
- Speaking at security awareness events
- Allocating resources for ongoing initiatives

2. Make Security Awareness Fun, Not Fearful

Cybersecurity training doesn't have to be dry and boring. Use engaging videos, gamified quizzes, and real-life scenarios. These keep employees interested and learning.

Think of interactive modules. Ones where employees choose their path through a simulated phishing attack. Or short, animated videos. Videos that explain complex security concepts in a clear and relatable way.

3. Speak Their Language

Cybersecurity terms can be confusing. Communicate in plain language, avoiding technical jargon. Focus on practical advice employees can use in their everyday work.

Don't say, "implement multi-factor authentication." Instead, explain that it adds an extra layer of security when logging in. Like needing a code from your phone on top of your password.

4. Keep it Short and Sweet

Don't overwhelm people with lengthy training sessions. Opt for bite-sized training modules that are easy to digest and remember. Use microlearning approaches delivered in short bursts throughout the workday. These are a great way to keep employees engaged and reinforce key security concepts.

5. Conduct Phishing Drills

Regular phishing drills test employee awareness and preparedness. Send simulated phishing emails and track who clicks. Use the results to educate employees on red flags and reporting suspicious messages.

But don't stop there! After a phishing drill, take the opportunity to dissect the email with employees. Highlight the telltale signs that helped identify it as a fake.

6. Make Reporting Easy and Encouraged

Employees need to feel comfortable reporting suspicious activity without fear of blame. Create a safe reporting system and acknowledge reports promptly. You can do this through:

- A dedicated email address
- An anonymous reporting hotline
- A designated security champion employees can approach directly

7. Security Champions: Empower Your Team

Identify enthusiastic employees who can become "security champions." These champions can answer questions from peers as well as promote best practices through internal communication channels. This keeps security awareness top of mind.

Security champions can be a valuable resource for their colleagues. They foster a sense of shared responsibility for cybersecurity within the organization.

8. Beyond Work: Security Spills Over

Cybersecurity isn't just a work thing. Educate employees on how to protect themselves at home too. Share tips on strong passwords, secure Wi-Fi connections, and avoiding public hotspots. Employees who practice good security habits at home are more likely to do so in the workplace.

9. Celebrate Success

Recognize and celebrate employee achievements in cyber awareness. Did someone report a suspicious email? Did a team achieve a low click-through rate on a phishing drill? Publicly acknowledge their contributions to keep motivation high. Recognition can be a powerful tool. It helps reinforce positive behavior and encourages continued vigilance.

The Bottom Line: Everyone Plays a Role

Building a culture of cyber awareness is an ongoing process. Repetition is key! Regularly revisit these steps. Keep the conversation going. Make security awareness a natural part of your organization's DNA.

Cybersecurity is a shared responsibility. By fostering a culture of cyber awareness your business benefits.

> *"Regular phishing drills test employee awareness and preparedness. Send simulated phishing emails and track who clicks. Use the results to educate employees on red flags and reporting suspicious messages."*

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

Protect Your Business From A Data Leak With The Microsoft Edge Browser

Microsoft Edge for Business has just rolled out new data leak control capabilities. And that could be a good thing for keeping your sensitive info safe.

What are data leak control capabilities?

In plain English, they help prevent your sensitive information from getting out to the wrong people. Think of it as having an extra lock on your digital doors, making sure only the right people can access your important data.

Every business handles sensitive information, whether it's financial records, client details, or proprietary data. If this information leaks, it could mean big trouble: Financial loss, legal headaches, and a hit to your reputation.

This new feature in Microsoft Edge helps keep your data secure by making sure only authorized people can access it. It also stops accidental sharing.

Depending on your industry, you may have strict rules about data protection. These new controls can help you stay on the right side of regulations.

And let's not forget your customers. They're more aware than ever about data privacy. Using a browser with strong data leak controls shows you're serious about protecting their information, which can boost their trust in your business.

Microsoft Edge for Business has added this new feature into an easy-to-use package. You can set policies on how data can be shared – like stopping certain types of data from being copied or emailed to unauthorized recipients. This way, you're less likely to have accidental leaks.

It uses artificial intelligence to spot potential threats and unusual data movements. Edge can alert you to a potential leak before it happens, giving you a chance to act proactively.

If you're already using other Microsoft products like 365 or Microsoft Teams, good news: Edge for Business integrates smoothly with them, letting you apply consistent data protection across all your tools.

Ready to give it a spin? Here's what to do:

1. Update your browser: Make sure all your business's devices are using the latest version of Microsoft Edge for Business. This makes sure you have all the newest features and security updates.

2. Set your policies: Work with your IT support partner to set up data sharing policies that make sense for your business. Microsoft provides guidelines and templates to help you get started.

3. Train your team: Make sure your employees know about the importance of data security and how to use the new features. A quick training session can do the trick.

4. Monitor and adjust: Keep an eye on how things are working and tweak your policies as needed. You want to find a balance that keeps your data secure without disrupting your workflow.

Better still, why not get our team to just do this for you? Give us a call at (734) 457-5000.