November 2024

TechTidbit.com

brought to you by Tech Experts

Keeping Work Devices Secure: Protecting Your Business

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

It's common practice for employees to use work laptops for personal tasks. Whether it's checking email, scrolling through social media, or watching a quick video, many people mix business with personal activities on work devices. At first glance, it may seem harmless—but it could actually be a big security risk for your business.

A recent study revealed that 90% of employees use company laptops for non-work activities. This often includes high-risk actions like visiting unsecured websites, streaming questionable content, and even accessing parts of the dark web. Each of these activities can open the door to malware, phishing attacks, and other cybersecurity threats, putting sensitive company data at risk.

As remote and hybrid work arrangements become the norm, it's tougher than ever to control what happens on work devices. Employees working from home or on the go are likely connecting to public Wi-Fi networks, plugging in personal USB drives, and blurring the lines between work and personal usage. Younger employees, in particular, seem more inclined to take these digital risks. This behavior makes it easier for hackers to take advantage of weak points, which can have serious consequences for businesses.

Adding to the concern, 18% of employees don't have any cybersecurity software on their work devices, and another 7% aren't even sure if they do. Without adequate protection, a single compromised device can be all it takes to give cybercriminals a way into your business.

Privacy is another issue to consider. A third of employees admit they'd feel uneasy knowing their employer could see their personal activities on a work laptop. This discomfort is understandable, but it highlights the need for clear policies that protect both employees' privacy and your business' security.

So, how can business owners address these risks? Here are a few steps that can make a big difference:

Implement Clear Policies: Make sure employees understand what's allowed—and what isn't—when it comes to using company devices. It's important to outline specific guidelines that address acceptable use, privacy expectations, and potential consequences.

Strengthen Security Measures: Every company device should be equipped with up-to-date cybersecurity software. This is a straightforward but effective way to prevent threats from taking hold.

Use Remote Management Tools: With the right tools, your IT team (or partner) can monitor devices, manage security settings, and respond to threats in real-time, regardless of where your employees are working. These tools can also help maintain a clear boundary between work and personal usage on company devices.

Educate Your Team: Help employees understand the risks of using work devices for personal activities. A little knowledge goes a long way—when people know how their behavior impacts security, they're more likely to follow best practices.

Balancing convenience and security can be challenging. Working with an experienced IT partner like us can help you implement these measures smoothly, keeping your business secure without disrupting daily operations.

If you'd like to discuss how we can support your business in managing device security, feel free to reach out.

A recent study revealed that 90% of employees use company laptops for non-work activities. This often includes high-risk actions like visiting unsecured websites, streaming questionable content, and even accessing parts of the dark web.

Tech Experts®
Information Technology Professionals

Empowering clients to do more with technology.
We support, manage, and optimize business IT.

Need Help? Email support@MyTechExperts.com, or call (734) 240-0200

Top Technologies Transforming Customer Service

"Through AI-powered chatbots, businesses can offer instant responses to common inquiries, reducing wait times and allowing human agents to focus on more complex issues."

Customer service is the foundation of any successful business, and with each passing year, customer expectations continue to rise. Meeting these expectations requires more than just dedication; it demands the right tools and technologies. Research shows that more than half of customers now prefer self-service options to speaking with a representative, reflecting the growing desire for quick, accessible solutions.

Here's a look at some of the top technologies reshaping customer service and helping businesses stay competitive:

Artificial Intelligence (AI) and Machine Learning

AI and machine learning are revolutionizing customer service, transforming everything from customer interactions to internal operations. Through AI-powered chatbots, businesses can offer instant responses to common inquiries, reducing wait times and allowing human agents to focus on more complex issues. Additionally, machine learning algorithms can analyze past interactions to improve responses, predict needs, and personalize service, enhancing the customer experience in meaningful ways.

Omnichannel support

Today's customers use multiple channels to reach out—phone, email, chat, social media, and more—and they expect a smooth, consistent experience across each one. Omnichannel support integrates these various touchpoints, allowing customers to switch channels without repeating information. This not only improves customer satisfaction but also helps companies provide a seamless, unified service experience.

Cloud-based customer service platforms

Cloud technology has brought unprecedented flexibility and scalability to customer service. By moving customer service operations to the cloud, companies can easily scale their support capabilities up or down, ensuring they can handle peak times or unexpected surges in demand. Cloud platforms allow agents to work from anywhere, making remote and hybrid customer service teams effective and responsive.

Self-service solutions

Self-service tools like knowledge bases, FAQs, and community forums empower customers to find answers on their own. Not only does this reduce the burden on customer service teams, but it also meets the preferences of customers who prefer solving issues without direct assistance. By offering robust self-service options, companies can boost satisfaction while freeing up resources for more complex inquiries.

Data analytics and customer insights

Data analytics has become an invaluable tool for understanding customer behavior and preferences. By analyzing customer interactions and feedback, companies gain insights that can shape more personalized and proactive service. For instance, if data shows recurring issues or common questions, businesses can address these proactively through FAQs or dedicated service strategies, ultimately improving the customer experience.

Robotic process automation (RPA)

RPA uses software "robots" to perform repetitive, rule-based tasks, such as data entry, form processing, or responding to basic queries. By automating these routine tasks, RPA frees human agents to focus on complex and high-value activities. This not only improves efficiency but also allows employees to spend more time solving nuanced problems, creating a better experience for customers.

Planning your customer service roadmap

With so many technologies available, it can be challenging to know where to start. Each business has unique needs, and the best approach to implementing new technologies is to have a clear roadmap. Our team of IT consultants can help you evaluate your current setup, identify key areas for improvement, and design a technology roadmap that aligns with your business goals.

Six Simple Steps to Enhance Your Email Security

Email is a fundamental communication tool for businesses and individuals alike. But it's also a prime target for cybercriminals. Cyberattacks are increasing in sophistication. This means enhancing your email security has never been more critical.

By taking proactive measures, you can protect your sensitive information as well as prevent unauthorized access and maintain communication integrity. Here are six simple steps to enhance your email security.

Use strong, unique passwords

Passwords are the first line of defense for your email accounts. A weak password is like an open invitation for cybercriminals. To enhance your email security, use strong, unique passwords. Ones that are difficult to guess.

Consider using a password manager. Remembering several complex passwords can be challenging. A password manager can help you generate and store unique passwords for all accounts. With a password manager, you only need to remember one master password. This simplifies the process while enhancing security.

Enable two-factor authentication (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your email accounts. Even if someone gets hold of your password, they won't be able to access your account. They would need the second factor of authentication to do that.

Enable 2FA for all your email accounts. Most email providers offer this feature and setting it up usually takes just a few minutes. This simple step significantly improves your email security.

Be cautious with email attachments and links

Email attachments and links are common vectors for malware and phishing attacks. Clicking on a malicious link or attachment can give attackers access to your system. Exercise caution to protect your email security.

Before opening an attachment or clicking on a link, verify the sender's identity. If you receive an unexpected email from someone you know, contact them. But do it through a different channel to confirm they sent it. For emails from unknown senders, exercise extra caution.

Keep your email software updated

Software updates often include security patches that address vulnerabilities in your email client. Keep your email software updated. This ensures you have the latest protections against known threats.

Most email clients and operating systems offer automatic updates. Enable this feature. It ensures your software stays up to date without requiring manual intervention. Automatic updates reduce the risk of missing critical security patches.

Use encryption for sensitive emails

Encryption adds a layer of protection to your emails. It encodes the content, making it readable only by the intended recipient. This ensures that even intercepted email information remains secure.

If you're sending encrypted emails, make sure the recipients know how to decrypt them. Provide clear instructions about how to access the encrypted content securely.

Watch your email activity

Regularly monitoring your email activity can help you detect suspicious behavior early. By keeping an eye on your account, you can take swift action if something seems off.

Many email providers offer activity alerts. They notify you of unusual login attempts or changes to your account settings. Enable these alerts to stay informed about your account's security status.

Review your email account activity on a regular basis. This includes login history and devices connected to your account.

"Many email providers offer activity alerts. They notify you of unusual login attempts or changes to your account settings. Enable these alerts to stay informed about your account's security status."

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).

Is Your Company Data at Risk? A Guide to Data Backup and Recovery

Picture coming to work one day and discovering all your essential business files - client data, financial records, project documents - are gone. Data loss can happen for many reasons: accidental deletion, hardware failures, cyberattacks, and even natural disasters. It's not something anyone anticipates, but every business is at risk, and a solid data backup and recovery plan is crucial.

Research shows that nearly 60% of small businesses close within six months after major data loss. Backing up data means creating secure copies of your files that can be restored if something goes wrong.

Why Backups Matter

Data backups protect your business from:

- Accidents: Deleting important files by mistake.
- Hardware Failures: When devices crash, data stored only on that device is at risk.
- Cyber Threats: Ransomware and other attacks that can lock you out of your data.
- Compliance Needs: In many industries, data retention is required by law.

Steps to build your backup and recovery plan

First, identify critical data. List the essential files and databases you need to protect - think customer records, finances, and project information.

Next, select a backup method. On-site backups store data on local storage It is quick but can be vulnerable to physical risks like fires, hardware failures and environmental factors.

Cloud backups keep your data off-site, usually with a cloud provider like Amazon. This protects it from local threats and makes it accessible anywhere.

The downside to cloud-only backups is recovery. In the event of a catastrophic failure, such as a failed server, your data must be downloaded from the cloud, which can take days depending on how large your data set is.

Hybrid backups combine on-site and cloud options. It offers the best of both worlds - protecting your data from a local disaster, but also providing quick recovery in the event of data loss.

Automate backups

Automated backups save time and reduce the risk of forgetting. Humans get busy, forget, or procrastinate - automated backup software will run when it is supposed to, and alert if there's a failure.

Test your backups

Regularly check your backups to ensure you can recover data if necessary. Years ago when tape backups were in use, we were called in to help an accounting firm that suffered a server failure and wasn't able to get help from their "IT guy."

The office manager was diligent about changing their backup tapes every day, up to keeping a log and checklist next to the server.

However, the old IT company never actually checked the backups. There was an error nearly a year before that had prevented any backups running properly for 11 months.

Plan for recovery

Outline steps for restoring data, who's responsible, and the expected timeframe to minimize downtime during a crisis. It is vitally important you understand the true time to recover in the event of a disaster.

If you're ready to improve your data backup and recovery, reach out to our team for guidance. We can help create a plan that keeps your business secure and your data accessible, no matter what happens.

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

Copyright © 2024 Tech Experts® All Rights Reserved.

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.