February 2025

TechTidbit.com

brought to you by Tech Experts

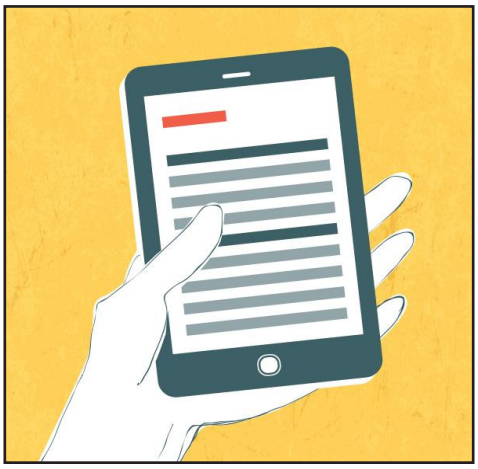
Here's Why You Should Stick To Work-Specific Tools

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

When it comes to communicating with your team, it can be tempting to stick with what's familiar. Apps like WhatsApp or Facebook Messenger are quick and easy to use. And everyone already has them on their phones, right?

But while these tools are great for sharing vacation photos or planning a get-together, they're not the best choice for work-related conversations. In fact, they could cause serious problems for your business.

You and your team often share information that's sensitive – customer details, employee records, or even financial data. Sharing this kind of information over apps that aren't designed for business use can be risky. Many of these apps don't have the advanced security measures needed to protect your business from threats like cyber criminals or malware (malicious software designed to steal or damage your data).



If this happens on a personal app which doesn't have the right security in place, your business could end up facing serious consequences. Losing access to important accounts or having private data leaked, for example.

Using business-specific communication tools, like Microsoft Teams, isn't just about security, it's also about keeping things organized. It lets you set up separate channels for different projects, share files securely, and even integrates with other apps you might be using. That means your team spends less time scrolling through endless chat threads and more time getting things done.

Personal apps can quickly get messy. Important messages get buried under GIFs and memes, and it becomes all too easy to accidentally share the wrong file - or worse, send something confidential to someone outside the company.

Switching to a proper business communication tool isn't difficult, and it's one of the best ways to protect your company's information while keeping your team running smoothly.

Need help getting started with the right tools for your business? Get in touch.

If this happens on a personal app which doesn't have the right security in place, your business could end up facing serious consequences. Losing access to important accounts or having private data leaked, for example.

The Ultimate Guide To Encryption Methods

"Encryption is like a secret language. It converts regular text into unreadable text. This unreadable text is called ciphertext. Only people who have the right key will be able to convert it into normal text, called plaintext."

Encryption is a method of securing information. It converts readable data into secret code. Only the right key can decode it. This guide will help you understand different encryption methods.

What is encryption?

Encryption is like a secret language. It converts regular text into unreadable text. This unreadable text is called ciphertext. Only people who have the right key will be able to convert it into normal text, called plaintext.

Why do we use encryption?

We use encryption to keep our information safe. It makes our data safe from hackers. This is very important for privacy and security.

How does encryption work?

Encryption uses algorithms and keys. An algorithm is a set of rules for solving problems. A key is somewhat like a password that unlocks the secret message.

There are two types of encryption: Symmetric encryption and asymmetric encryption. Symmetric encryption uses the same key for encryption and decryption. The same key is shared between the sender and receiver. It's fast but less secure when the key is shared.

Asymmetric encryption uses two keys: a public key and a private key. A public key can encrypt a message, while a private key can decrypt it. It's more secure since only the private key unlocks the message.

What are some common encryption methods?

- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- DES (Data Encryption Standard)

- ECC (Elliptic Curve Cryptography)

How do we use encryption in everyday life?

Online Shopping. When you purchase online, your payment information is encrypted. This protects your credit card information against hackers.

Messaging Apps. Apps like WhatsApp use encryption to keep your messages private. Only you and the person you are chatting with can read them.

Email Security. Many email services use encryption to protect your emails from being read by others.

What are the challenges of encryption?

Key Management. If some person loses their key, they probably will lose their data.

Performance Issues. Encryption could slow down the systems since it needs processing power for encryption and decryption.

How can you stay safe with encryption?

Use Strong Passwords. Always use strong passwords for accounts and devices. That will make hacking difficult as it will take time to access.

Keep Software Up-to-Date. Regularly update your software to protect against security vulnerabilities in software.

Use Caution with Public Wi-Fi. If you need to use public Wi-Fi, avoid sensitive transactions unless you can encrypt your internet connection using a VPN.

Ready to secure your data?

Encryption helps protect your personal information from threats. Understanding different methods can help you choose the right one for your needs. If you need help securing your data, contact us today - 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).

Top Cybersecurity Threats Small Businesses Face in 2025

Cybersecurity is no longer a problem exclusive to large enterprises. Small and mid-sized businesses (SMBs) are increasingly targeted by cybercriminals because they often have fewer resources to defend against sophisticated attacks. Being proactive about cybersecurity can mean the difference between thriving and struggling to recover from a serious breach. Here are the top ten cybersecurity threats your business faces in 2025 and tips to protect yourself.

Ransomware attacks

Ransomware remains one of the most damaging threats. Cybercriminals encrypt your business data and demand a ransom for its release. SMBs are targeted because they may lack robust backup and recovery systems. Preventative measures like regular data backups and strong endpoint security are critical.

Phishing emails

Phishing attacks trick employees into providing sensitive information, such as login credentials. These attacks have evolved to include highly personalized emails that are harder to recognize as scams. Employee training and email filtering tools can reduce the likelihood of a successful phishing attack.

Credential theft

Cybercriminals are constantly searching for login credentials to access business systems. They often steal these through phishing, malware, or by exploiting weak passwords. Implementing multi-factor authentication (MFA) can significantly improve your security posture by requiring additional verification beyond a password.

Insider threats

Insider threats—whether malicious or accidental—pose a serious challenge for small businesses. Employees, contractors, or even former staff may misuse access to your systems. Limiting access to sensitive data and monitoring user activity can reduce the chances of insider incidents or account compromises.

IoT device exploits

As more businesses adopt Internet of Things (IoT) devices like smart cameras, thermostats, and inventory trackers, these devices have become a growing attack surface. Many IoT devices have weak security protocols, making them vulnerable. Ensure that all devices are updated regularly and segregated from critical business networks.

Supply chain attacks

Cybercriminals are increasingly targeting SMBs by compromising third-party vendors or software suppliers. This can result in malware infections and data breaches without any direct attack on your business. Vetting vendors, limiting their access to your systems, and monitoring for suspicious activity can help defend against supply chain attacks.

Zero-day vulnerabilities

Zero-day vulnerabilities are newly discovered flaws in software that hackers can exploit before developers issue a fix. These vulnerabilities are difficult to prevent entirely but can be mitigated by keeping your software up to date and using security tools that detect abnormal behavior.

Distributed Denial-of-Service (DDoS) attacks

DDoS attacks flood a business's network or website with traffic, causing service disruptions. While these attacks are often used to target large companies, SMBs can also be affected. Implementing DDoS protection services can prevent attacks from overwhelming your network and keeping you from doing business.

Social engineering scams

Social engineering involves manipulating people into revealing confidential information or performing harmful actions. Attackers may impersonate trusted contacts or authority figures to gain access to your systems. Training employees to recognize these tactics and verifying unusual requests can reduce risk.

How to protect your business

Understanding these threats is only the first step. Here are some actionable strategies to help secure your business:

Invest in Employee Training: Regularly educate employees on cybersecurity best practices and how to recognize threats.

Use Multi-Factor Authentication (MFA): Adding an extra layer of security to logins helps prevent unauthorized access.

Regular Backups: Ensure you have automated backups of critical data and test your recovery procedures.

Implement Network Monitoring: Continuous monitoring of your network can detect suspicious activity early, allowing you to respond quickly to potential threats.

Partner with a Managed Service Provider (MSP): A trusted MSP can monitor your systems, provide threat intelligence, and ensure security updates are applied consistently.

Cybersecurity doesn't have to be overwhelming. By addressing these top threats and taking a proactive approach, your business can stay one step ahead of cybercriminals and safeguard your operations in 2025.

"Cybercriminals are increasingly targeting SMBs by compromising third-party vendors or software suppliers. This can result in malware infections and data breaches without any direct attack on your business."

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

Business Premium Is Your Next Smart Move

Running a business comes with challenges you might not expect, like phishing emails, stolen devices, or ex-employees still accessing your systems.

While Microsoft 365 Business Standard is a great package for getting work done, it doesn't offer the advanced security and management tools needed to handle these risks.

That's where Microsoft 365 Business Premium comes in.

Business Premium gives you everything you love about Business Standard – apps like Word and Excel, email hosting, Microsoft Teams, and OneDrive for cloud storage. And it adds powerful features to keep your business secure and efficient.

Take cyber threats, for example. Phishing emails, designed to trick you into clicking dangerous links, can install malware (malicious software) that locks your files or steals sensitive data. With Business Premium, Microsoft Defender for Business scans for these threats and stops them in their tracks. It's like having a 24/7 security guard for your data.

Device management is another big advantage. If an employee loses their laptop, Business Premium's Microsoft Intune lets you remotely erase company data, protecting your sensitive information. You can also set policies to ensure every device connected to your business is secure.

And then there's protecting your confidential information. Business Premium uses Purview Information Protection to label sensitive files and control who can access them. Even if an email gets forwarded outside your company, the protections stay in place, safeguarding your data wherever it goes.

These tools aren't just nice to have, they're essential for modern businesses facing growing cyber security threats. The added cost is a small investment for the confidence that your team, data, and reputation are protected.

Upgrading to Business Premium can help prepare your business for the future. If you're ready to take that step, it's worth every penny. We can help you get started – get in touch.

Should You Use A Password Manager?

Password managers keep our online accounts safe. They store all our passwords in one place. But are they hackable?

What are password managers?

Password managers are like digital vaults: they save all your passwords inside themselves. You need only remember one master password to then gain access to all of your other passwords. This makes keeping a lot of accounts much easier to handle.

Dedicated password managers are difficult to hack if configured properly. While hackers are always hunting for ways to steal your information, a properly configured password manager has a complex password and two-factor authentication. This makes it very difficult to crack.

You can protect your password manager by using a strong master password. The master password is the "key" that unlocks all of your other passwords. Use a mix of letters, numbers, and symbols, or better yet, a secure passphrase that is easy to remember, but hard to guess.

Be sure to enable two-factor authentication. 2FA adds an important layer of security.

What happens if a password manager gets hacked?

If you've set up your password manager properly, the chance of it being hacked is extremely low. However, if your password manager is compromised, you should:

- Change your master password immediately.
- Determine which accounts could be affected and change their passwords as well.
- Consider shifting to another password manager.
- Keep up to date with any security news about your manager.

The benefits of using a password manager usually outweigh the risks. They help you create strong, unique passwords for each account.

Choosing a reputable password manager with good reviews and security features is key. Do some research before deciding which one to use.

Using a password manager will go a long way in enhancing your online security. If you need help in selecting which one, give us a call at (734) 240-0200.