April 2023

TechTidbit.com

brought to you by Tech Experts

Data Backup Alone Is No Longer Enough

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

Small businesses are increasingly relying on digital data to manage their operations. From financial records to customer information, digital data is the lifeblood of small businesses in today's digital age. However, with the growing amount of data comes the need for increased data protection measures.

Backups are essential for protecting data in the event of a system failure or other unexpected event. But it's important to understand that backups alone are not enough to ensure the safety and security of your business's data. In addition to backups, businesses need to implement data protection measures to prevent data breaches, cyber attacks, and other forms of data loss.

Here are a few reasons why data protection is essential for small businesses:

Protecting sensitive data

Small businesses often collect and store sensitive data, such as customer names, addresses, social security numbers, and financial information. This information is valuable to cybercriminals, who can use it for identity theft, financial fraud, and other criminal activities. Implementing data protection measures, such as encryption and access controls, can help to prevent unauthorized access to sensitive data.

Preventing data loss

Data loss can occur for many reasons, including hardware failure, system crashes, and cyber attacks. Without proper protection in place, businesses risk losing valuable data, which can have significant financial and operational consequences. Redundant storage systems and disaster recovery planning can help to prevent data loss and ensure business continuity.

Regulatory compliance

Many small businesses are subject to regulatory requirements, such as HIPAA, PCI-DSS, and GDPR, which mandate the protection of sensitive data. Failure to comply with these regulations can result in fines, legal action, and damage to the business's reputation. Implementing more robust data protection can ensure compliance with regulations and avoid costly penalties.

Protecting intellectual property

Small businesses often create and store valuable intellectual property, such as patents, trademarks, and trade secrets. This intellectual property is vulnerable to theft and misuse, which can have significant financial and competitive consequences. Measures such as access controls and monitoring systems can help to protect intellectual property from theft and misuse.

With cyber crime at an all-time high, backups alone are not enough to ensure the safety and security of your business's data. Encryption, access controls, redundant storage systems and disaster recovery plans are essential for protecting sensitive data, preventing data loss, complying with regulations, and protecting intellectual property.

Small business owners should prioritize data protection as an essential component of their IT strategy. The potential benefits, including enhanced security, improved compliance, and reduced risk of data loss, far outweigh the costs.

If you'd like to discuss additional data protection measures for your business, give us a call. We can help you assess your risks and develop a comprehensive data protection plan that meets your business's unique needs.

Data protection is essential for small business success. That's why we offer a range of data protection solutions, including encryption, access controls, and disaster recovery planning. We're here to help you protect your business's data and ensure the long-term success of your business.

Small business owners should prioritize data protection as an essential component of their IT strategy. The potential benefits, including enhanced security, improved compliance, and reduced risk of data loss, far outweigh the costs.

Protecting Your Small Business: IT Security Tips

"Cyber insurance can help to protect your business in the event of a data breach or cyber attack. Cyber insurance policies can help to cover the costs associated with data recovery, legal fees, and other expenses related to cyber attacks. Consider consulting with an insurance professional to determine if cyber insurance is right for your business."

Small businesses are increasingly reliant on technology to manage their operations. From storing customer data to conducting financial transactions, businesses of all sizes rely on information technology (IT) to keep their operations running smoothly.

However, this reliance on technology also makes small businesses vulnerable to cyber attacks and data breaches. In this article, we'll discuss some key IT security tips that small business owners can use to protect their companies from cyber threats.

Keep software up-to-date

One of the simplest ways to improve IT security is to ensure that all software is kept up-to-date. Software updates often include security patches that address vulnerabilities and other issues that could be exploited by cybercriminals. By keeping software up-to-date, you can help to reduce the risk of cyber attacks and protect your company's data.

Use strong passwords

Passwords are the first line of defense against unauthorized access to your business's digital assets. It's important to use strong passwords that are difficult to guess or crack.

Passwords should be at least twelve to 16 characters long and include a mix of uppercase and lowercase letters, numbers, and symbols. To help remember passwords, consider using a password manager, which can generate and store strong passwords for you.

Limit access to sensitive data

Not all employees need access to all data. Limiting access to sensitive data can help to reduce the risk of data breaches.

Consider implementing a least privilege access model, where employees only have access to the data they need to perform their jobs. Additionally, consider implementing two-factor authentication, which requires a second form of identification beyond a password to access sensitive data.

Train employees on IT security best practices

Human error is a leading cause of cyber attacks and data breaches. Employees who are unaware of IT security best practices can inadvertently put your business at risk.

It's important to train employees on IT security best practices, such as how to identify phishing scams, how to create strong passwords, and how to safely use company devices.

Implement a firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic. Firewalls can help to prevent unauthorized access to your company's network and data. Consider implementing a firewall to help protect your business from cyber threats.

Back up data regularly

Data backups are essential for protecting your business's data in the event of a cyber attack or hardware failure.

Backups should be performed regularly and stored securely, preferably off-site or in the cloud. This can help to ensure that your business can quickly recover from a cyber attack or other data loss event.

Consider cyber insurance

Cyber insurance can help to protect your business in the event of a data breach or cyber attack. Cyber insurance policies can help to cover the costs associated with data recovery, legal fees, and other expenses related to cyber attacks. Consider consulting with an insurance professional to determine if cyber insurance is right for your business.

IT security is a critical component of small business operations. By implementing these IT security tips, you can help to protect your business from cyber threats and data breaches.

Protecting your business's data is an ongoing process that requires vigilance and attention to detail. By staying up-to-date on IT security best practices and implementing robust security measures, you can help to ensure the long-term success of your small business.

If you have any questions about IT security or would like to discuss your business's IT security needs, please don't hesitate to contact us.

Office 365: Protect Your Business From Data Loss And Cyber Attacks With These Backup Solutions

As more businesses shift to cloud-based productivity tools like Office 365, the need to backup these accounts becomes increasingly important. While many businesses assume that cloud providers automatically backup data stored in their accounts, this is not always the case.

In fact, Microsoft Office 365 recommends that businesses regularly backup their data to ensure that it is protected and easily recoverable in the event of a data loss.

Here are a few reasons why backing up Office 365 accounts is essential for businesses:

Protection against user error

Human error is one of the leading causes of data loss. Whether it's accidentally deleting a file or overwriting an important document, mistakes can happen.

By regularly backing up Office 365 accounts, businesses can quickly recover lost or deleted data, minimizing the impact of user error on their operations.

Protection against cyber attacks

Cyber attacks are a growing threat to businesses of all sizes. Ransomware, phishing, and other cyber attacks can cause significant damage to businesses, including data loss, financial damage, and reputational harm. By regularly backing up Office 365 accounts, businesses can quickly recover from a cyber attack and reduce the risk of data loss.

Compliance with regulatory requirements

Many industries and jurisdictions have specific data retention requirements that businesses must adhere to. Failure to comply with these requirements can result in fines, legal action, and damage to the business's reputation.

By regularly backing up Office 365 accounts, businesses can ensure compliance with regulatory requirements and avoid costly penalties.

Simplify migration

Backing up Office 365 accounts can also simplify the process of migrating to a new cloud provider or on-premise solution. With a backup of their data, businesses can quickly and easily move their data to a new platform without worrying about data loss or compatibility issues.

So, what are the options for backing up Office 365 accounts? Here are a few:

Native Office 365 backup tools

Microsoft provides a set of basic backup tools within Office 365. These tools can be used to backup emails, contacts, calendars, and other data within Office 365 accounts.

However, these tools have limitations, including limited retention periods and the inability to backup some types of data, such as SharePoint sites.

Third-party backup solutions

There are a variety of third-party backup solutions available that can backup Office 365 accounts. These solutions provide more advanced features than the native Office 365 backup tools, including longer retention periods, the ability to backup SharePoint sites, and more granular backup and restore options.

Hybrid backup solutions

Hybrid backup solutions combine the benefits of both on-premise and cloud backup solutions. With a hybrid backup solution, businesses can backup Office 365 accounts to both an on-premise location and the cloud, providing an extra layer of protection against data loss.

In conclusion, backing up Office 365 accounts is essential for businesses of all sizes. By doing so, businesses can protect against user error, cyber attacks, comply with regulatory requirements, and simplify migration.

While Microsoft provides some basic backup tools within Office 365, third-party backup solutions offer more advanced features and greater flexibility.

If you're unsure about the best backup solution for your business, consider consulting with a trusted IT advisor or cloud backup specialist. We can help you assess your risks and develop a comprehensive backup plan that meets your business's unique needs.

At Tech Experts, we offer a range of backup solutions for Office 365 accounts, including native Office 365 backup tools, third-party backup solutions, and hybrid backup solutions. We understand the importance of protecting your business's data and are here to help you develop a backup plan that meets your unique needs. Don't leave your business's data to chance – backup your Office 365 accounts today.

"Microsoft provides a set of basic backup tools within Office 365. These tools can be used to backup emails, contacts, calendars, and other data within Office 365 accounts.

However, these tools have limitations, including limited retention periods and the inability to backup some types of data, such as SharePoint sites."

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

Smartphones Are Now The Preferred Device For Mobile Work

Smartphones have taken over from laptops as most people's preferred portable work tool.

They enjoy the flexibility and, perhaps obviously, they're easier to carry around than a laptop or a tablet.

It means that mobile connectivity and reliable broadband have become two of the largest IT considerations. In turn, that creates a different set of security risks.

If a number of your people need a phone to do their job, here's a big thought: Would they be better off using a work-issued phone instead? If an employee has contact with customers, would you want to own their phone number in case they left?

And there are security considerations that might be best handled on company-issued phones. That includes rolling out security updates, managing secure mobile gateways, and administering passwords.

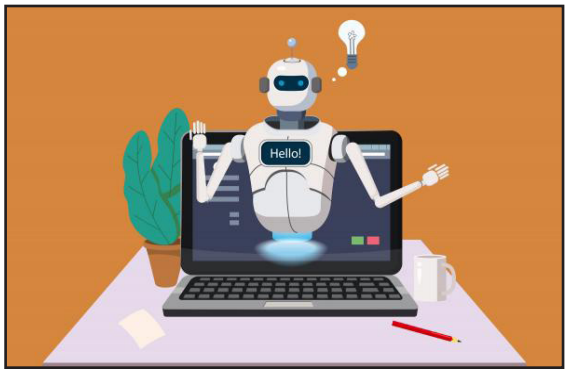
You should make sure data on the device is encrypted, not only to protect data from cyber criminals, but to make sure your information is safe should the phone be lost or stolen. Can the phone be remotely wiped?

The software installed on the phone should be policed too. You may need a policy that limits or blocks the use of third-party software. This can also help establish a boundary between work and personal tasks.

As with most tech, this isn't a case of set it and forget it. You need to make sure updates are run on time, and remotely audit company-issued devices to ensure they're secure, protected and don't contain any malicious applications.

Is this something we can help with? Your technology headaches are exciting for us! Get in touch, we'd be glad to help out.

What's All The Fuss About AI And ChatGPT?



ChatGPT is a chatbot that uses artificial intelligence, allowing you to talk to it in a very human way. It's been making the news around the world for some of the remarkable possibilities it seems to be creating. But what exactly is it, and why is it making such waves?

ChatGPT is trained on real human language. It can answer questions, and even compose documents, like emails, essays and computer code. The exciting thing is the way it allows you to have a natural-feeling conversation with it to generate different responses – perhaps adding more detail, or asking it to use less technical language.

It was created by research company OpenAI, which is funded and managed by some of the most influential names in tech. And while it's still in its research and feedback-collection phase, it's currently free to use (with limitations).

It's different to a search engine because it's designed with conversation in mind. While it can answer questions, it doesn't search the internet for information. Everything is learned from training data (it has no knowledge past 2021). So, while many people have started using ChatGPT to write essays and articles, the facts may not be accurate. In fact, tech media website CNET recently had to issue multiple major corrections after it created 78 articles using the chatbot.

Because it's trained on huge amounts of text published online by humans, it's had trouble telling fact from fiction, and has also been found to reproduce some unwanted biases – for instance against women and people of color.

It's not changing the world just yet. But it's already clear that there is huge potential for both individuals and businesses alike.

Have you tried ChatGPT yet? What are your feelings about using AI in your business? We'd love to hear your thoughts. (P.S. A human wrote this article!)