June 2023

TechTidbit.com

brought to you by Tech Experts

Thinking Of Moving Offices Or Going 100% Remote?

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

Has hybrid and remote working left you and your team rattling around an office that's too big?

If you're now in the position of overspending on rent, utilities and cleaning, you might be thinking about downsizing to another location – or even abandoning the office completely.

That's something that will take some planning if you want a smooth transition with minimal, expensive downtime.

Moves are always stressful, and relocating your IT systems takes a bit more thought than manhandling a desk up the stairs.

So here are our top three suggestions to make it easier to shift your IT setup to a new location.

Use a checklist

Treat this like any other project. Use a to-do list where you check off each step so that nothing's forgotten. Allocate every task on the list to specific people, so everyone knows who's responsible for what.

Refer to your checklist regularly with progress reviews a month before, a week before, a day before, and on the day of the move. Have another list for unpacking at the other end.

Give your internet provider notice

We rely on internet connections for most of what we do, but it's common to allow too little time for this to be set up. It can take six weeks to arrange, install and test the connection so it's ready for the day you move in. Allow plenty of notice to avoid unwanted stress on the day of the move.

If it's a new building or a refit, specify all the outlets and connections you want – don't leave it to the builder to assume as it will cost more to make changes later.

Use a professional

If it's just a couple of machines it could be a DIY job. But for most moves, it's more involved than just disconnecting a few cables and reconnecting them. It's too easy for everything to become confusing and overcomplicated.

A good IT professional will have this process down to a fine art and will disconnect and reconnect your whole network efficiently and with minimal downtime.

If you're thinking about a move to new premises and need help planning for it, we can help… get in touch.

If it's just a couple of machines it could be a DIY job. But for most moves, it's more involved than just disconnecting a few cables and reconnecting them.

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 It Time To Ditch The Passwords For More Secure Passkeys?

"Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in."

Passwords are the most used method of authentication, but they are also one of the weakest.

Passwords are often easy to guess or steal. Also, many people use the same password across several accounts. This makes them vulnerable to cyber-attacks.

The sheer volume of passwords that people need to remember is large. This leads to habits that make it easier for criminals to breach passwords. Such as creating weak passwords and storing passwords in a non-secure way.

61% of all data breaches involve stolen or hacked login credentials.

In recent years a better solution has emerged – passkeys. Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. There is no need to enter a username and password.

This authentication technology leverages Web Authentication (WebAuthn). This is a core component of FIDO2, an authentication protocol. Instead of using a unique password, it uses public-key cryptography for user verification.

The user's device stores the authentication key. This can be a computer, mobile device, or security key device. It is then used by sites that have passkeys enabled to log the user in.

More secure

One advantage of passkeys is that they are more secure than passwords.

Passkeys are more difficult to hack. This is true especially if the key generates from a combination of biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans. Device information can include things like the device's MAC address or location.

This makes it much harder for hackers to gain access to your accounts.

More convenient

Another advantage of passkeys over passwords is that they are more convenient. With password authentication, users often must remember many complex passwords. This can be difficult and time-consuming.

Forgetting passwords is common and doing a reset can slow an employee down. Each time a person has to reset their password, it takes an average of three minutes and 46 seconds.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. This makes it much easier to log in to your accounts. It also reduces the likelihood of forgetting or misplacing your password, or worse, writing it down.

Phishing resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account.

They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. Even if a hacker had a user's password, it wouldn't matter. They would need the device passkey authentication to breach the account.

What Is Push Bombing And How Can You Prevent It?

In the fast-paced digital landscape, businesses both big and small face a multitude of challenges. One such emerging threat that has garnered significant attention is "push bombing."

This practice involves bombarding a company's push notification system with fraudulent or malicious requests, causing disruptions, overwhelming server capacities, and undermining user experiences.

Small companies, in particular, are vulnerable to the detrimental effects of push bombing as they often lack the resources and expertise to swiftly counteract such attacks.

Understanding push bombing

Push bombing refers to the deliberate act of flooding a company's push notification system with an excessive number of requests, typically generated by automated scripts or bots.

These requests are intended to exhaust server resources, disrupt normal operations, and degrade the performance of legitimate notifications.

Push bombing can lead to a series of detrimental consequences for targeted businesses, including increased server costs, diminished user experience, loss of customer trust, and even reputational damage.

Small companies often face a unique set of challenges when dealing with push bombing attacks.

Limited budgets, scarce technological resources, and a lack of dedicated security personnel make it difficult for these businesses to respond effectively. Unlike larger enterprises, small companies may not have the financial means to invest in robust security systems or hire specialized personnel to address such threats.

Consequently, they become attractive targets for push bombing perpetrators seeking vulnerabilities to exploit.

Preventive measures for small businesses

While it may be challenging for small companies to completely eradicate the risk of push bombing, there are several key, low-cost preventive measures they can take to minimize the impact of such attacks:

Implement rate limiting: By setting thresholds for the number of push notifications allowed per second, small companies can regulate the flow of requests and prevent overwhelming their systems.

Rate limiting helps distinguish legitimate user requests from automated ones and ensures a more balanced distribution of server resources.

CAPTCHA implementation: Employing CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) in push notification sign-up forms can effectively deter automated bots from inundating the system with fake requests.

CAPTCHAs require users to complete a challenge, thus confirming their human presence and preventing malicious activities.

Monitor traffic patterns: Vigilant monitoring of network traffic can help small companies identify abnormal patterns indicative of a push bombing attack.

Employing security tools that provide real-time alerts and anomaly detection capabilities can enable proactive response and mitigation.

Two-factor authentication (2FA): Implementing 2FA for push notification subscriptions can add an extra layer of security. By requiring users to verify their identities through a secondary authentication method, such as SMS codes or email confirmations, small companies can significantly reduce the risk of unauthorized subscriptions by bots.

Collaborate with security experts: Small companies can benefit from partnering with reputable cybersecurity firms or consultants.

These experts can assist in conducting security assessments, implementing protective measures, and providing guidance on responding to push bombing attacks, thus augmenting the company's overall security posture.

As digital threats continue to evolve, it is crucial for small companies to remain proactive in safeguarding their push notification systems against push bombing attacks.

By implementing preventative measures such as rate limiting, CAPTCHAs, traffic monitoring, 2FA, and seeking professional guidance, small businesses can fortify their defenses and mitigate the risks associated with push bombing.

As technology advances, it is essential for companies of all sizes to prioritize cybersecurity to maintain the trust and confidence of their customers, ensuring smooth operations and sustained growth in an increasingly digital world.

"Push bombing can lead to a series of detrimental consequences for targeted businesses, including increased server costs, diminished user experience, loss of customer trust, and even reputational damage."

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

The Transformative Power Of Cloud Computing For Small Businesses

Small companies face numerous challenges, including limited resources, budget constraints, and the need to stay technologically relevant. Thankfully, advancements in technology have leveled the playing field, empowering small businesses with tools and solutions that were once only accessible to larger enterprises.

One such technology that has revolutionized the way businesses operate is cloud computing.

Cost savings

Traditional on-premises IT infrastructure can be expensive for small businesses, requiring significant upfront investments in hardware, software licenses, and maintenance.

Cloud computing offers a more cost-effective alternative. With cloud services, small businesses can leverage scalable resources and pay only for what they use, eliminating the need for infrastructure investments.

Collaboration and remote work

The ability to collaborate effectively is essential for small businesses to thrive.

Cloud computing facilitates seamless collaboration by providing a centralized platform accessible to employees from anywhere with an internet connection.

Cloud-based tools such as project management systems, document sharing platforms, and real-time communication apps enable teams to work together efficiently, regardless of their physical location.

This capability is especially valuable for small businesses with remote workers or distributed teams, fostering productivity and efficiency.

Data security

Protecting sensitive business data is a critical priority. Cloud computing offers robust security measures, including data encryption, regular backups, and advanced authentication protocols.

Storing data in the cloud reduces the risk of data loss due to hardware failures, theft, or natural disasters.

Cloud service providers typically have dedicated security teams and advanced threat detection systems, ensuring a higher level of data security than many small businesses can achieve on their own.

Flexibility and accessibility

Cloud computing provides small businesses with unparalleled flexibility and accessibility. Employees can access critical business applications and data from any device with an internet connection, enabling remote work and enhancing productivity. This flexibility also extends to the ability to quickly scale resources up or down based on business needs.

Cloud-based services also ensure that software and applications are regularly updated, eliminating the burden of manual updates and ensuring access to the latest features and security enhancements.

Competitive advantage

Adopting cloud technology can provide small businesses with a significant competitive advantage.

It allows smaller companies to access enterprise-level tools, applications, and infrastructure that were once exclusive to larger organizations.

This leveling of the playing field enables small businesses to innovate, streamline operations, and deliver enhanced customer experiences.

Cloud computing has emerged as a transformative technology for small businesses, offering a wide array of benefits, including scalability, cost efficiency, enhanced collaboration, data security, and improved flexibility.

By embracing cloud services, small businesses can leverage the power of advanced IT infrastructure without the burdensome costs and complexities associated with traditional on-premises solutions.

The cloud empowers small businesses to compete effectively, drive innovation, and achieve growth in an increasingly digital and interconnected world.