February 2024

TechTidbit.com

brought to you by Tech Experts

Unlocking The Power Of Encryption For Your Small Business: Safeguard Your Digital Assets

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

Keeping sensitive business data safe is a top priority. When you're managing a team of employees that use PCs, phones, and tablets, the importance of encryption can't be stressed enough.

Encryption is a secret code for your digital information. It scrambles your data into an unreadable format, and only someone with the right "key" can unscramble and access it. Think of it as a lock and key system for your digital assets, ensuring that even if someone gains unauthorized access to your devices or data, they can't make head nor tail of it without the key.

Your business likely stores tons of sensitive information, from financial records to customer data. Encryption ensures that even if a device is lost or stolen, your data remains safe and confidential.

And there are loads of other benefits too. Lots of industries have strict regulations regarding data security and privacy (think HIPAA). Encryption helps you stay compliant, avoiding expensive fines and legal troubles.

When clients, patients or customers know that you take their data security seriously, it builds trust. People are more likely to do business with a company that safeguards their information.

With the rise of remote work, your employees might be accessing company data from various locations. Encryption ensures that sensitive information is secure no matter where they are.

Encrypting your emails and messages keeps your communication confidential, protecting sensitive business discussions and strategies.

When you're setting up encryption for the first time you, need to think about both device encryption and data encryption.

You also need to consider encryption both while data is at rest (where it's stored) and when it's in transit (being sent from person to person). And while that may sound intimidating, you don't have to do it alone - we can help.

You may also consider training your people on encryption best practice to make sure there are no weak links in your team. After all, it only takes one false move to leave your data vulnerable. Helping everyone understand the importance of encryption and how to use it effectively is a strong protective measure.

If this is something we can help you do, we'd love to assist. Please get in touch.

With the rise of remote work, your employees might be accessing company data from various locations. Encryption ensures that sensitive information is secure no matter where they are.

Notifications: Striking A Balance At Work And Home

"But... the more tools we use, the more notifications flood our screens. During the traditional 9-5, the constant barrage of notifications can derail focus and productivity."

Notifications have become a part of our daily lives. Whether it's the ping of a new email, a message from a colleague on Teams, or a meeting reminder on your calendar, these little nudges constantly battle for our attention.

But are we reaching a tipping point with notifications?

According to recent research, the answer might be a big "YES". The study revealed that the ping, ping, ping of notifications from collaboration tools is not only a distraction at work but is also taking a toll on our precious work-life balance.

So, why are notifications becoming a nuisance, and what can we do about it?

We're living in the era of collaboration tools. From video conferencing to project management platforms, we rely on these tools to stay connected and productive.

But… the more tools we use, the more notifications flood our screens. During the traditional 9-5, the constant barrage of notifications can derail focus and productivity.

But what's annoying is when notifications creep into our downtime. One in three workers report that notifications outside of working hours have spiked over the past year.

As a society, we've created a situation where notifications disrupt our relaxation and family time.

A third of young workers aged 21-34 struggle to fully enjoy time with loved ones due to work notifications. And that may put you at risk of losing your best people.

Here's our three step take on tackling the notifications dilemma:

First, set clear boundaries. Make it understood that messages should be replied to within working hours. Practice what you preach by not sending messages outside of your own working hours (schedule-send where possible).

Second, reduce tool overload. Evaluate the collaboration tools you use. Streamline where possible.

Third, empower your employees. Teach them to use do not disturb, and how to mute non-urgent notifications.

While technology has revolutionized the way we work, it shouldn't come at the cost of our wellbeing and personal time. If we can help you and your team strike a better balance, get in touch.

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 Data Breaches Of 2023: Numbers Hit An All-time High

The battle against cyber threats is an ongoing challenge. Unfortunately, 2023 has proven to be a watershed year for data breaches. Data compromises surged to an all-time high in the U.S.

The last data breach record was set in 2021. That year, 1,862 organizations reported data compromises. Through September of 2023, that number was already over 2,100.

In Q3 of 2023, the top data breaches were:

- HCA Healthcare
- Maximus
- The Freecycle Network
- IBM Consulting
- CareSource
- Duolingo
- Tampa General Hospital
- PH Tech

Let's look at the main drivers of this increase.

The size of the surge

Data breaches in 2023 have reached unprecedented levels. The scale and frequency of these incidents emphasize the evolving sophistication of cyber threats as well as the challenges organizations face in safeguarding their digital assets.

Healthcare sector under siege

Healthcare organizations are the custodians of highly sensitive patient information. As a result, they've become prime targets for cybercriminals and hackers looking to exploit personal information.

Ransomware reigns supreme

Ransomware attacks continue to dominate the cybersecurity landscape. The sophistication of this threat has increased.

Supply chain vulnerabilities exposed

Modern business ecosystems have an interconnected nature. This has made supply chains a focal point for cyberattacks. The compromise of a single entity within the supply chain can have cascading effects.

Emergence of insider threats

The rise of insider threats is adding a layer of complexity to cybersecurity. Organizations must distinguish between legitimate user activities and potential insider threats.

IoT devices as entry points

The proliferation of Internet of Things (IoT) devices has expanded the attack surface. There's been an uptick in data breaches originating from compromised IoT devices.

Critical infrastructure in the crosshairs

Critical infrastructure has emerged as a prime target for malicious actors seeking to wreak havoc and sow chaos. From power grids and transportation systems to financial institutions and healthcare facilities, the vital systems that underpin modern society have found themselves squarely in the crosshairs of cyber attackers.

The role of nation-state actors

Nation-state actors are entities sponsored or supported by governments to engage in cyber activities, including espionage, sabotage, and other malicious actions, often for political, economic, or strategic purposes.

These actors operate with the resources, capabilities, and backing of a nation-state, allowing them to conduct highly sophisticated and coordinated cyber campaigns.

Nation-state actors are increasingly playing a role in sophisticated cyber campaigns. They use advanced techniques to compromise sensitive data and disrupt operations.

The need for a paradigm shift in cybersecurity

The surge in data breaches underscores the need to rethink cybersecurity strategies.

Collaboration and information sharing

Collaboration among organizations and information sharing within the cybersecurity community are critical. Threat intelligence sharing enables a collective defense against common adversaries.

"Modern business ecosystems have an interconnected nature. This has made supply chains a focal point for cyberattacks. The compromise of a single entity within the supply chain can have cascading effects."

Cybersecurity Tips For Everyday Life

When it comes to cybersecurity, we often rely on our IT experts and installed software to protect our systems from digital threats.

From tech support to firewalls, a lot of tools and people contribute to our online safety!

In the midst of all of this, we can sometimes forget that we, too, play a critical role in guarding our systems and networks. At home or in the office, we each have a responsibility to protect the private data in our care.

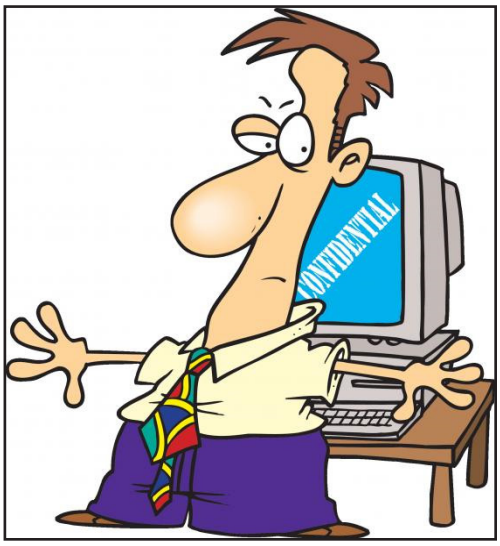
Human error

Human error is actually responsible for 95% of cyberattacks. YOU are the number one threat to your own private data! You can also be its greatest defense.

How might you put yourself at risk? It can be as simple as clicking on malicious links, opening attachments from unknown senders, or sharing sensitive data by mistake. One wrong click, if your devices and systems aren't properly equipped to defend themselves, can be disastrous.

Social engineering

Then there are social engineering attacks, which use human psychology to trick people into revealing sensitive information or taking actions that compromise security. Because they rely on you acting emotionally against your better instincts, even people who are aware of the risks can easily fall victim to social engineering attacks. It only takes one moment of weakness!



We also play a part in protecting private data whenever we brush up on our Security Awareness Training. That knowledge helps us to identify and track potential threats, which help prevent them from happening in the first place! We are also responsible for reporting suspicious activity to the appropriate teams, which can help identify and respond to attacks early on, before they cause significant damage.

They say "it takes a village," and that rings just as true in the digital landscape of cyberspace! Together we can make the Internet a safer place to spend our time.

Always back up your data

Data loss can happen to anyone, at any time. It can be caused by a hardware failure, software corruption, malware attack, fire, theft, or simply human error. Backing up your data is crucial to protect yourself from these events. It will also save you the time, money, and stress of losing your data.

When you're wondering what to back up on your system, the answer is simple: Save everything that you don't want to lose. That includes personal documents, like photos, music, videos, emails, financial documents, and other memories and files that you don't want to lose. You might also want to do this for application data, which includes settings and save files for those programs that you use frequently.

System files are essentially the applications and processes which your computer (or whatever device you're considering) need to run. Backing up system files helps make system recovery seamless if anything happens. If a crucial file is corrupted or destroyed, it could crash your whole system irrecoverably.

Then, at least once per month, you should back up your storage files to another, separate location so you have two versions saved in case one file gets corrupted. Some cybercriminals go straight after your saved storage, hoping to excavate a large amount of data at once.

Automatic backups ensure your continued protection whether you forget or are otherwise prevented from doing it on time.

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