May 2023

TechTidbit.com

brought to you by Tech Experts

A Four-Day Week Doesn't Mean Four-Day Security

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

Are you one of the many companies around the world that's looking at a four-day working week? Perhaps you've already made the leap.

Or, do you find that your team takes more time off during the summer months?

For lots of businesses, it's never going to work. But those that have tried it have generally found it to be hugely positive. It improves your employees' experience, making them more loyal, engaged, and productive.

It can help to attract and retain better talent, while improving your brand reputation. And let's not ignore the cost savings of shutting down the office for an extra day.

But it has to be done right. Forcing people to cram the same amount of work into fewer hours could be a recipe for burnout and exhaustion.

That can lead to corners being cut, which in turn could lead to a cyber security disaster. Even if processes aren't being intentionally skipped, human error due to a lapse in concentration becomes inevitable.

According to the World Economic Forum's 2022 Global Risk Report, nearly all cyber security issues can be traced back to human error.

What does that mean for your business?

If you're considering a four-day week, work closely with your people to make sure they aren't experiencing additional pressure. And never assume that fewer office hours means you can relax your cyber security.

You should reassess your measures to make sure they stand up to the change in working patterns, paying particular attention to remote access and VPN policies. Also revisit your procedures so that all routine tasks are still accounted for in the new working week.

Comprehensive security policies become even more important when you change a working routine, and you may also want to beef up your approach.

Consider introducing 'zero trust' strategies if you haven't already. These give people access to only the files, software, and systems they need to do their job – and nothing more.

Finally, refresh employees' cyber security awareness with regular training. If security practices are not followed, it's often because they are not fully understood.

There's a lot to think about, but professional advice is always on hand. If it's something you're considering, just get in touch.

If you're considering a four-day week, work closely with your people to make sure they aren't experiencing additional pressure. And never assume that fewer office hours means you can relax your cyber security.

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).

What Is App Fatigue And Why Is It A Security Issue?

"Employees overwhelmed with too many app alerts tend to ignore them. When updates come up, they may quickly click them away. They feel they can't spare the time right now and aren't sure how long it will take."

The number of apps and web tools that employees use on a regular basis continues to increase. Most departments have about 40-60 different digital tools that they use. 71% of employees feel they use so many apps that it makes work more complex.

Many of the apps that we use every day have various alerts. We get a "ping" when someone mentions our name on a Teams channel. We get a notification popup that an update is available. We get an alert of errors or security issues.

App fatigue is a very real thing and it's becoming a cybersecurity problem. The more people get overwhelmed by notifications, the more likely they are to ignore them. Just think about the various digital alerts that you get.

They come in:

- Software apps on your computer
- Web-based SaaS tools
- Websites where you've allowed alerts
- Mobile apps and tools
- Email banners
- Text messages
- Team communication tools such as Slack or Teams

Some employees are getting the same notification on two different devices. This just adds to the problem.

This leads to many issues that impact productivity and cybersecurity. Besides alert bombardment, every time the boss introduces a new app, that means a new password.

Estimates are that the average employees is already juggling about 191 passwords. They use at least 154 of them sometime during the month.

How Does App Fatigue Put Companies at Risk?

Employees Begin Ignoring Updates

When digital alerts interrupt your work, you can feel like you're always behind. This leads to ignoring small tasks seen as not time-sensitive. Tasks like clicking to install an app update.

Employees overwhelmed with too many app alerts tend to ignore them. When updates come up, they may quickly click them away. They feel they can't spare the time right now and aren't sure how long it will take.

Ignoring app updates on a device is dangerous. Many of those updates include important security patches for found vulnerabilities.

When they're not installed, the device and its network are at a higher risk. It becomes easier to suffer a successful cyberattack.

Employees Reuse Passwords (and They're Often Weak)

Another security casualty of app fatigue is password security. The more SaaS accounts someone must create, the more likely they are to reuse passwords. It's estimated that passwords are typically reused 64% of the time.

Credential breach is a key driver of cloud data breaches. Hackers can easily crack weak passwords. The same password used several times leaves many accounts at risk.

Employees May Turn Off Alerts

Some alerts are okay to turn off. For example, do you really need to know every time someone responds to a group thread?

But, turning off important security alerts is not good.

There comes a breaking point when one more push notification can push someone over the edge.

What's the Answer to App Fatigue?

It's not realistic to just go backward in time before all these apps were around.

But you can put a strategy in place that puts people in charge of their tech, and not the other way around.

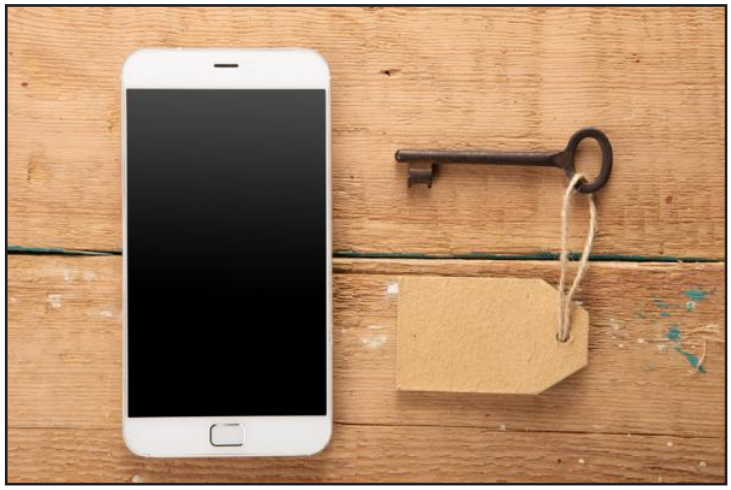
- Streamline your business applications
- Have your IT team set up notifications
- Automate application updates
- Open a two-way communication about alerts

Don't Forget Your Phone's Security Settings

It's common for people to rely on their personal phones to keep in touch at work.

That's not always the best idea, and there are lots of good reasons to provide company phones to your team (would you want to own the number and block access to sensitive data if somebody left?)

But whoever owns the device, you need to make security your top priority. Cyber criminals know how much valuable information lives on our mobiles, and they're making phones a target.



If you don't already have a mobile security and management strategy in place, it's time you did. Here are our top 5 ways to keep phones secure:

Set minimum upgrade requirements

Cyber crooks and device manufacturers both work in three-year cycles. That means that, as threats evolve, so do the protections that address them. Upgrade devices to follow this cycle, and even if you're using BYOD (bring your own device), enforce this rule if employees want to use their personal phone for work.

Implement mobile device management

MDM allows you to track the location of devices, lock/wipe their data remotely, and can help you access remote support for any issues. That means your data stays safe, even in cases of a lost or stolen phone. You can also create a list of apps that are to be blocked for security reasons.

Set up MFA (Multi-Factor Authentication)

Make sure all devices have biometric locks requiring facial or fingerprint ID to open them, and that all apps require MFA to log in. Only allow employees access to the software and files they need for their job.

Always update everything

Like all your devices, phones need to have the latest updates installed as soon as they become available. If you have MDM in place, it's possible to schedule updates across the entire team at the same time – ask us for more info.

Regular awareness training

You should hold regular cyber security training for your team that includes mobile devices. Your people are your weakest link when it comes to security. Keeping them up to speed on security risks can improve compliance.

It's easy to overlook mobile devices when it comes to keeping your data secure, but it's a vital step in protecting yourself against cyber attacks.

"Cyber crooks and device manufacturers both work in three-year cycles. That means that, as threats evolve, so do the protections that address them. Upgrade devices to follow this cycle, and even if you're using BYOD (bring your own device), enforce this rule if employees want to use their personal phone for work."

TECHNOLOGIES TO GIVE YOU AN ADVANTAGE

Customers look for convenience. In today's world that means technology that makes their life easier.

From webforms to POS systems, you need to keep the customer experience in mind in all you do.

When people aren't happy with their experience interacting with a company, they leave.

And their experience might not have anything to do with your products or services. Maybe they found it hard to navigate your website.

Technology is key to converting website visitors into clients. These techonologies can give you that edge:

- Cloud Forms
- Digital Signatures
- Smart Chatbot
- SMS Notifications
- Business Mobile App
- FAQ Kiosk
- VoIP Phone System

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

These Everyday Objects Can Lead To Identity Theft

You wouldn't think a child's toy could lead to a breach of your personal data. But this happens all the time.

What about your trash can sitting outside? Is it a treasure trove for an identity thief?

Many everyday objects can lead to identity theft.

Old smart phones

Our smartphones and tablets have become extensions of ourselves, storing a vast amount of personal information. If lost, stolen, or compromised, these devices can provide unauthorized access to sensitive data, including emails, contacts, financial apps, and social media accounts.

Make sure you clean any old phones by erasing all data or destroying the device.

Wireless printers

Protect wireless printers by ensuring you keep their firmware updated. You should also turn it off when you don't need it.

Trash can

Identity theft criminals aren't only online. They can also be trolling the neighborhood on trash day. Discarded items in your trash can reveal personal information that identity thieves can exploit. Dumpster diving is a common tactic used to extract valuable data, such as bank statements, credit card receipts, or pre-approved credit offers.

Always shred or destroy any documents before disposing of them, even those that may not seem sensitive at first glance.

It's also wise to invest in a cross-cut shredder, which provides better protection compared to strip-cut shredders.

USB sticks

You should never plug a USB device of unknown origin into your computer. This is an old trick in the hacker's book. They plant malware on these sticks and then leave them around as bait.

Old hard drives

When you are disposing of an old computer or old removable drive, make sure it's clean. Just deleting your files isn't enough. It's best to get help from an IT professional to properly destroy your old computer hard drive.

We have a special drive crushing tool at Tech Experts - just let us know if you need some drives recycled.

Physical documents

Physical documents, such as bank statements, bills, medical records, and tax documents, contain a wealth of personal information. Disposing of them carelessly or leaving them unattended can be an open invitation to identity thieves.

Always shred sensitive documents before discarding them, especially those containing financial or personally identifiable information. Furthermore, consider digitizing important documents and securely storing them on encrypted devices or cloud platforms with strong authentication measures.

Children's IoT devices

You should be wary of any new internet-connected kids' devices you bring into your home. Install all firmware updates and do your homework.

ATMs

This is called skimming. Malicious actors can use hidden devices on ATMs or card readers to steal your card information during transactions.

Identity theft can have devastating consequences, impacting both your personal and financial well-being.

Safeguarding physical documents, securing mail, keeping wallets and purses safe, protecting mobile devices, and properly disposing of personal trash are essential steps in minimizing the risk of identity theft. Remember, vigilance and informed decision-making are key.