July 2023

TechTidbit.com

brought to you by Tech Experts

Boost Your Team's Engagement With Better Tech

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

The stresses and pressures of the cost of living crisis are hitting many people hard. That makes employee engagement more of a challenge than ever.

As a business, you might be finding it hard yourself. It may not be possible to offer salary rises that keep pace with inflation.

And at the same time, you might be asking more of your people or making changes to the workplace that are hard for some to adjust to.

The last thing you want is to lose good people just when you need everyone firing on all cylinders.

That's why some of the most effective engagement strategies right now involve relieving the stress and tedium of repetitive tasks and removing workplace frustration - with the added benefit that you become more efficient in the process.

Most businesses now offer some form of remote working. But it's common for people to feel 'left out in the cold' if it's not easy for them to keep communication channels open. Making team interactions seamless can make a big difference to the happiness of your people – and even to your customers.

How do you do this? Start with better collaboration tools. They can improve project management, strengthen relationships, reduce wasted time, and even encourage better feedback.

Technology can also automate dull and repetitive tasks. No one's going to complain about that, and faster working will provide a productivity boost.

Collaboration tools can be useful for team engagement, whether your team is working in the office, working from home, or you're using a hybrid model. Applications such as Teams and Slack build a sense of community for your team.

When you respond to your people's frustrations by providing the right tools, they'll feel listened to and valued. And if they feel that they're getting things done, they'll become more engaged and more motivated.

There's an overwhelming range of tools available that often make bold claims about their ability to transform your business.

We can help to cut through the sales patter and get to the heart of what's right for you. So if you're looking at a tech solution to improve employee engagement, let's talk.

Start with better collaboration tools. They can improve project management, strengthen relationships, reduce wasted time, and even encourage better feedback.

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).

Fake Software Ads Used To Distribute Malware

"Ads first take you to a benign-looking website – which the crooks have created. This then redirects you to a malicious site that convincingly impersonates a genuine page. That's where the malware lurks waiting for a click, beyond Google's reach."

Google is most people's first port of call for help or information online – something cyber criminals are using to their advantage.

Specifically, they are targeting Google ads, impersonating campaigns for popular software such as Grammarly, Slack, Ring, and many others. This is nothing to do with those companies, but to the untrained eye they look like the real deal… which is how they're tricking people into clicking the ads.

If you're not using an ad blocker, you'll see promoted pages at the top of your Google search results. These look almost identical to the non-promoted, down page organic search results, so you or your people could easily be tempted to click.

It's a complicated scam. Criminals clone the official software websites, but instead of distributing the genuine product, when you click download they install 'trojanized' versions. That's geek speak for malware that disguises itself as real software.

Google is working to protect us by blocking campaigns it's able to identify as malicious. But criminals have tricky ways around that too.

Ads first take you to a benign-looking website – which the crooks have created. This then redirects you to a malicious site that convincingly impersonates a genuine page. That's where the malware lurks waiting for a click, beyond Google's reach.
Worse, in many cases, you'll still get the software you're trying to download, along with a hidden payload of malware. That makes it harder to tell that your device or network has been infected and may give the malware longer to do its job.

To stay protected, train your team about the dangers and make sure everyone is on the lookout for anything that doesn't seem quite right.

Encourage people to scroll down the Google results until they find the official domain of the company they're looking for, and make it a policy that people seek permission before downloading any software – no matter how innocent it may seem.

You could also consider using an ad blocker in your browser. That will filter out any promoted results from your Google search for some extra peace of mind.

For help and advice with training, software policies and network security give us a call at (734) 457-5000, or email info@mytechexperts.com.

SIX IMMEDIATE STEPS YOU SHOULD TAKE IF YOUR NETFLIX ACCOUNT IS HACKED

Netflix is one of the most popular and well-known streaming services. The platform has become an essential part of many people's daily entertainment routines. Unfortunately, like any online service, Netflix accounts can be vulnerable to hacking.

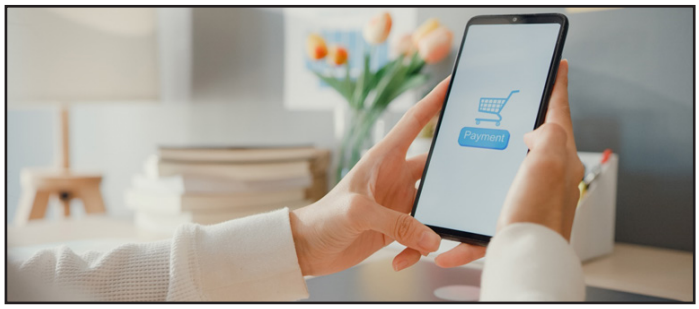
You might not think something as benign as Netflix could represent a security risk to your business. In most cases, your company laptop (as well as any devices your spouse or children might use) are connected to the same home network as your streaming services. This gives cyber-criminals an easy way to gain a foothold into your equipment.

Hackers take advantage of "phishing overload." Once they breach your account, they're usually quiet for a bit, hoping you'll mistake the Netflix suspicious login warning for a fake.

Here are some things to do right away if you fear your account is hacked:

1. Go to the Netflix site & try to log in.
2. If you can log in, change your password immediately.
3. If you can log in, remove any strange payment methods
4. Contact Netflix support and let them know that you think you've been compromised (don't skip this step).
5. Watch your bank statements.
6. Change the password for other accounts that used the same one as your Netflix account.

Is Your Online Shopping App Invading Your Privacy?



Online shopping has become a common activity for many people. It's convenient, easy, and allows us to buy items from the comfort of our homes. But with the rise of online shopping, there are concerns about privacy and security.

Not all shopping apps are created equally. Often people get excited and install an app without checking privacy practices. Apps can collect more data from your smartphone than you realize. Whether you use your phone for personal use, business use, or both, your data can be at risk. So can your privacy.

Recently, security experts found a popular shopping app spying on users' copy-and-paste activity. This app was tracking users' keystrokes, screenshots, and even their GPS location. This raises the question: Is your online shopping app invading your privacy?

SHEIN is the app in question, and it's a popular shopping app with millions of users. According to reports, researchers found the app collecting data from users' clipboards. This included any text that users copied and pasted. This means that if the user copied and pasted sensitive information, the app would have access to it.

Including things like passwords or credit card numbers.

Not only that but the app was also found to be tracking users' GPS location. SHEIN was also collecting data from device sensors, including the accelerometer and gyroscope. This means that the app was able to track users' movements. As well as collecting information about how they were using their device.

The app's developers claimed that the data collection was for "optimizing user experience." A very vague explanation that's used by other app developers as well.

The developers stated that the collected data was only used for internal purposes. But this explanation wasn't enough to please privacy experts. Those experts raised concerns about the app's data collection practices.

This isn't the first time people caught an app grabbing data without users' knowledge. Many popular apps collect data from their users, often for targeted advertising purposes.

The popularity of the shopping app Temu has been exploding recently. Since the app appeared in a Superbowl Ad in 2023, people have been flocking to it.

But Temu is another shopping app with questionable data collection practices. Some of the data that Temu collects includes:

- Your name, address, phone number
- Details you enter, like birthday, photo, and social profiles
- Your phone's operating system and version
- Your IPS address and GPS location (if enabled)
- Your browsing data

Here are some tips to protect your privacy when using shopping apps.

Know what you're getting into (read the privacy policy)

Yes, it's hard to stop and read a long privacy policy. But, if you don't, you could end up sharing a lot more than you realize.

Turn off sharing features

Turn off any data-sharing features you don't need in your phone's settings, such as location services. Most smartphones allow you to choose which apps you want to use it with.

Remove apps you don't use

If you're not using the app regularly, remove it from your phone. Having unused apps on your phone is a big risk.

Research apps before you download

It's easy to get caught up in a fad. You hear your friend talk about an app, and you want to check it out. But it pays to research before you download.

Shop on a website instead

You can limit the dangerous data collection of shopping apps by using a website instead. Most legitimate companies have an official website.

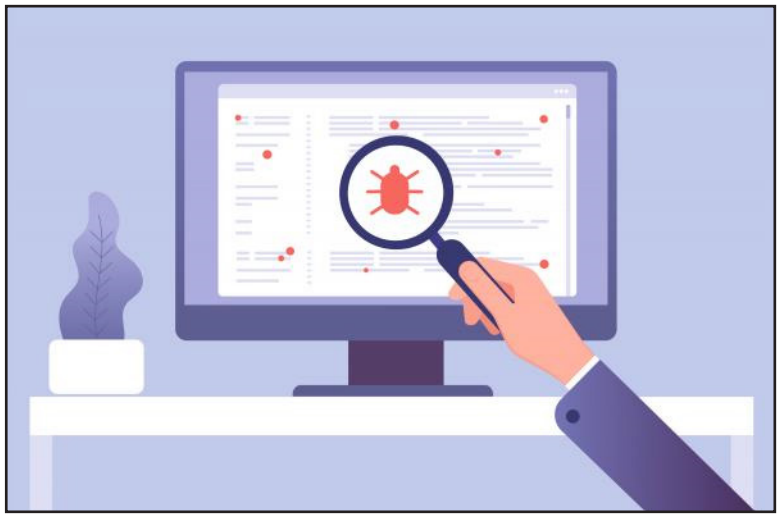
Recently, security experts found a popular shopping app spying on users' copy-and-paste activity. This app was tracking users' keystrokes, screenshots, and even their GPS location. This raises the question: Is your online shopping app invading your privacy?"

Learn How To Fight Business Email Compromise

A significant cyber threat facing businesses today is Business Email Compromise (BEC). BEC attacks jumped 81% in 2022, and as many as 98% of employees fail to report the threat.

What is business email compromise (BEC)?

BEC is a type of scam in which criminals use email fraud to target victims. These victims include both businesses and individuals. They especially target those who perform wire transfer payments.



BEC attacks are usually well-crafted and sophisticated, making it difficult to identify them. The attacker first researches the target organization and its employees online. They gain knowledge about the company's operations, suppliers, customers, and business partners.

The scammer pretends to be a high-level executive or business partner. Scammers send emails to employees, customers, or vendors.

These emails request them to make payments or transfer funds in some form.

The email will often contain a sense of urgency, compelling the recipient to act quickly. The attacker may also use social engineering tactics. Such as posing as a trusted contact or creating a fake website that mimics the company's site. These tactics make the email seem more legitimate.

According to the FBI, BEC scams cost businesses about $2.4 billion in 2021.

These scams can cause severe financial damage to businesses and individuals. They can also harm their reputations.

How to fight business email compromise

BEC scams can be challenging to prevent. But there are measures businesses and individuals can take to cut the risk of falling victim to them.

- Educate employees
- Enable email authentication
- Deploy a payment verification processes
- Check financial transactions
- Establish a response plan
- Use anti-phishing software

Get ready for the unexpected

If your business sufferes an email compromise or a ransomware attack tomorrow, do you have a contingency plan in case of any disasters? The unexpected can happen anytime, and small businesses can get hit particularly hard.

Here are ten helpful tips to get ready for anything:

1. Create a contingency plan
2. Maintain adequate insurance coverage
3. Diversify your revenue streams
4. Build strong relationships with suppliers
5. Keep cash reserves
6. Build strong outsourcing relationships
7. Check your financials regularly
8. Invest in technology
9. Train employees for emergencies
10. Stay up to date on regulatory requirements

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