April 2024

TechTidbit.com

brought to you by Tech Experts

It's Time To Fix Your Risky Password Habits

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

We all know how important it is to keep our data safe, but sometimes our best intentions fall short. And when you have employees, you're at an increased risk of security threats and bad habits creeping in.

Here's the deal: Even if you invest in cyber security training, changing long held password habits can be a tough nut to crack. People love convenience, and remembering a ton of complex passwords just isn't their idea of a good time.

Your employees are juggling dozens of passwords for work and personal use. It's a lot to handle, and sometimes they slip up and reuse passwords across different accounts. It's a familiar story, right? And it's where the trouble starts.

When passwords are reused, it's like leaving the front door wide open for cyber criminals. If the password is breached on one site, they will try it to access other sites.

Here's how you can make sure your team stays on top of their password game.

Password audit: Ask your IT partner to do an audit of passwords and look for weak ones that should be changed.

Block weak passwords: Ask your IT partner to implement a password policy that stops common passwords from being used.

Scan for compromised passwords: Even strong passwords can be compromised. Stay one step ahead by scanning for breached passwords and prompting employees to change them.

Use password managers: Password managers securely generate then store a unique password for every different account… and fill them into the login box so your team doesn't have to.

Multi-Factor Authentication (MFA): Add an extra layer of security with MFA, where you get a code on a separate device. It's like putting a deadbolt on your front door – double the protection, double the peace of mind.

With the right tools and guidance, password security doesn't have to be hard work. If we can help you with that, get in touch - (734) 457-5000.

Scan for compromised passwords: Even strong passwords can be compromised. Stay one step ahead by scanning for breached passwords and prompting employees to change them.

Tech Experts®
Information Technology Professionals

Empowering clients to do more with technology.
We support, manage, and optimize business IT.

Need Help? Email support@MyTechExperts.com, or call (734) 240-0200

What Is Microsoft's New Security Copilot?

"A big benefit is that it integrates with natural language. This means you can ask questions plainly to generate tailored guidance and insights."

It can be challenging to keep up with the ever-evolving cyber threat landscape. Companies need to process large amounts of data as well as respond to incidents quickly and effectively. Managing an organization's security posture is complex.

That's where Microsoft Security Copilot comes in. Microsoft Security Copilot is a generative AI-powered security solution. It provides tailored insights that empower your team to defend your network. It also works with other Microsoft security products.

Microsoft Security Copilot helps security teams:

- Respond to cyber threats
- Process signals
- Assess risk exposure at machine speed

A big benefit is that it integrates with natural language. This means you can ask questions plainly to generate tailored guidance and insights. For example, you can ask:

- What are the best practices for securing Azure workloads?
- What is the impact of CVE-2024-23905 on my organization?
- Generate a report on the latest attack campaign.
- How do I remediate an incident involving TrickBot malware?

Security Copilot can help with end-to-end scenarios such as:

- Incident response
- Threat hunting
- Intelligence gathering
- Posture management
- Executive summaries on security investigations

How does Microsoft Security Copilot work?

You can access Microsoft Security Copilot capabilities through a standalone experience as well as embedded experiences available in other Microsoft security products.

Copilot integrates with several tools, including:

- Microsoft Sentinel
- Microsoft Defender XDR
- Microsoft Intune
- Microsoft Defender Threat Intelligence
- Microsoft Entra
- Microsoft Purview
- Microsoft Defender External Attack Surface Management
- Microsoft Defender for Cloud

You can also use natural language prompts with Security Copilot.

Should you use Microsoft Security Copilot?

The pros:

- Advanced threat detection
- Operational efficiency
- Integration with Microsoft products
- Continuous learning
- Reduced false positives

The considerations:

- Integration challenges
- Resource requirements
- Training and familiarization

The Bottom Line

Microsoft Security Copilot marks a significant advancement in the world of AI-driven cybersecurity solutions. This cutting-edge system boasts an enhanced ability to detect threats in real-time, greatly improving operational efficiency. Additionally, its wide-ranging integration capabilities make it an extremely versatile tool in the cybersecurity arsenal.

These features render Microsoft Security Copilot an especially attractive option for businesses that are intent on strengthening their digital defense mechanisms.

The decision to implement Copilot in your organization should be tailored to your specific business requirements. It's important to weigh factors such as your current cybersecurity infrastructure, the resources at your disposal, and the level of commitment your organization is willing to make towards ongoing training and adaptation of this sophisticated AI tool.

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).

Be Careful When Scanning QR Codes

QR codes are everywhere these days. You can find them on restaurant menus, flyers, and posters. They're used both offline and online. QR codes are convenient and easy to use. You just scan them with your smartphone camera. You're then directed to a link, a coupon, a video, or some other online content.

With the rise in popularity of QR codes comes an unfortunate dark side. Cybercriminals are exploiting this technology for nefarious purposes. Scammers create fake QR codes. They can steal your personal information. They can also infect your device with malware or trick you into paying money.

It's crucial to exercise caution when scanning QR codes. This emerging scam highlights the potential dangers lurking behind those seemingly innocent squares.

The QR code resurgence

QR codes were originally designed for tracking parts in the automotive industry. They have experienced a renaissance in recent years as a result, and they're used as a form of marketing today.

They offer the convenience of instant access to information. You simply scan a code. Unfortunately, cybercriminals are quick to adapt. A new phishing scam has emerged, exploiting the trust we place in QR codes.

How the scam works

The scammer prints out a fake QR code. They place it over a legitimate one. For example, they might stick it on a poster that advertises a product discount or a movie. You come along and scan the fake QR code, thinking it's legitimate. The fake code may direct you to a phishing website. These sites may ask you to enter sensitive data such as your credit card details, login credentials, or other personal information.

Or scanning the QR code may prompt you to download a malicious app. One that contains malware that can do one or more of the following:

- Spy on your activity
- Access your copy/paste history
- Access your contacts
- Lock your device until you pay a ransom

The code could also direct you to a payment page. A page that charges you a fee for something supposedly free.

Tactics to watch out for

Malicious codes concealed: Cybercriminals tamper with legitimate QR codes. They often add a fake QR code sticker over a real one. They embed malicious content or redirect users to fraudulent websites.

Fake promotions and contests: Scammers often use QR codes to lure users into fake promotions or contests. When users scan the code, it may direct them to a counterfeit website.

Malware distribution: Some malicious QR codes start downloads of malware onto the user's device.

Tips for safe QR code scanning

Verify the source: Verify the legitimacy of the code and its source.

Use a QR code scanner app: Use a dedicated QR code scanner app rather than the default camera app on your device.

Inspect the URL before clicking: Before visiting a website prompted by a QR code, review the URL.

Avoid scanning suspicious codes: Trust your instincts. If a QR code looks suspicious, refrain from scanning it.

Update your device and apps: Keep your device's operating system and QR code scanning apps up to date.

Be wary of websites accessed via QR code

Don't enter any personal information on a website that you accessed through a QR code. This includes things like your address, credit card details, login information, etc. Don't pay any money or make any donations through a QR code.

"You come along and scan the fake QR code, thinking it's legitimate. The fake code may direct you to a phishing website. These sites may ask you to enter sensitive data such as your credit card details, login credentials, or other personal information."

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

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.

Insights from the 2023 Annual Cybersecurity Attitudes and Behaviors Report

We are living in an era dominated by digital connectivity. As technology advances, so do the threats that lurk in the online world.

Often, it's our own actions that leave us most at risk of a cyberattack or online scam. Risky behaviors include weak passwords and lax security policies, as well as thinking "This won't happen to me." This is why human error is the cause of approximately 88% of data breaches.

The National Cybersecurity Alliance and CybSafe publish a report on cybersecurity attitudes and behaviors. The goal is to educate both people and businesses on how to better secure their digital landscapes.

This year's study surveyed over 6,000 people across the U.S., Canada, the U.K., Germany, France, and New Zealand. The survey asked about several things including knowledge of cybersecurity risks, security best practices, and challenges faced.

The report reveals some eye-opening insights, including how people perceive and respond to cyber threats as well as what they can do to improve their cybersecurity posture.

We are online... a lot

It's no surprise that 93% of the study participants are online daily. The logins we create continue to expand, as well as those considered "sensitive." Sensitive accounts hold personal information that could be harmful if stolen.

Nearly half (47%) of the study's respondents have ten or more sensitive online accounts. This amplifies risk, especially if people are using the same password for two or more of those accounts.

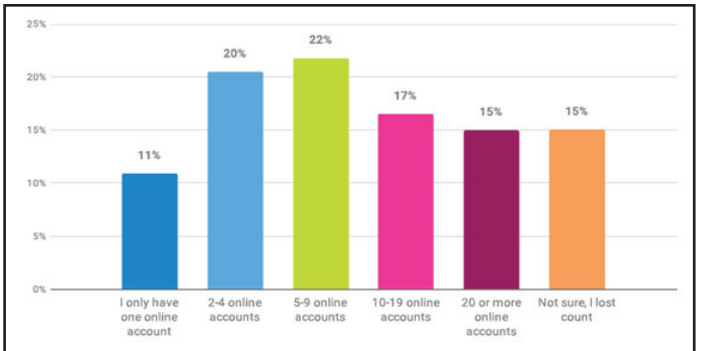

Figure 1. ***"Overall, how many sensitive online accounts that hold personal information do you have?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Online security makes people frustrated

Most people (84%) feel that online security is a priority. But as many as 39% feel frustrated, and nearly the same amount intimidated. It can seem that you just can't get ahead of the hackers. Just over half of people thought digital security was under their control. That leaves a whole lot that don't think so.

But that is no reason to let down your defenses and become an easy target. There are best practices you can put in place to safeguard your online accounts that work, including:

- Enabling multi-factor authentication on your accounts
- Using an email spam filter to catch phishing emails
- Adding a DNS filter to block malicious websites
- Using strong password best practices

People need more access to cybersecurity training

One way to reduce human errors associated with cybersecurity is to train people. The survey found that just 26% of respondents had access to cybersecurity training.

It also broke this down by employment status. We see that those not actively employed are most lacking. Even those employed can use more training access and encouragement. Just 53% report having access to cybersecurity awareness training and using it.

Employers can significantly reduce their risk of falling victim to a data breach by improving their security awareness training.

Cybercrime reporting is increasing

Over a quarter (27%) of survey participants said they had been a victim of cybercrime. The types of cybercrimes reported include:

- Phishing (47%)
- Online dating scams (27%)
- Identity theft (26%)

Millennials reported the most cybercrime incidents. Baby Boomers and the Silent Generation reported the fewest.

No matter where you fall in the generations, it's important to adopt security best practices and be vigilant about your online security.