October 2022

TechTidbit.com

brought to you by Tech Experts

Do You Know Exactly What Services Your Staff Are Signing Up For?

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

Whatever problem, need, or want you have… there's a cloud application out there that can help you.

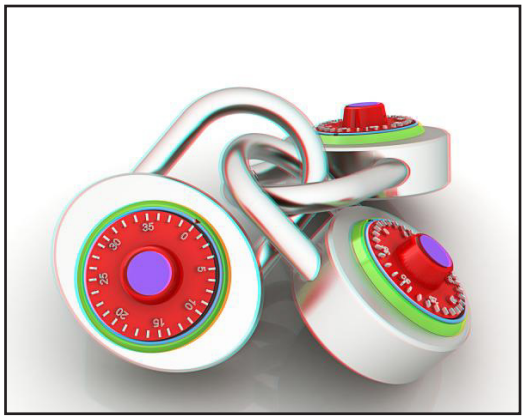
We've never lived in a such a rich time for problem solving. Every day, hundreds of new services launch to make our lives easier and help us be more productive.

These applications all live in the cloud. They're known as Software as a Service – or SaaS – because you don't load any software onto your device. You use them in your browser.

We would argue this SaaS revolution over the last 15 to 20 years has played a critical part in shaping the way we work today.

However, there's an issue. Many businesses aren't 100% aware of what new services their staff have signed up for. And this problem isn't a financial one; it's a security one.

Let's give you a scenario. Suppose a member of your team, Janice, is trying to do something creative, but just can't with her existing software. She Googles it and finds a cool application.



Janice signs up for an account, and as she's in a rush she uses the same email address and password as her Microsoft 365 account. Yes, reusing passwords is very bad practice. But this gets worse.

She uses the application for half an hour to achieve what she needs to do… and then forgets it. She's got no intention of upgrading to a premium subscription, so she abandons her account.

That's not an issue… until a few years later. Janice is still on your staff; in fact, she's been promoted to a financial position. And then that SaaS application is hacked by cyber criminals, and all its login credentials are stolen.

It's well-known that cyber criminals will try stolen details on other sites, especially big wins like Microsoft 365.

Can you see the issue here?

Janice's 365 account would be compromised, and she'd have no idea how it happened. She won't remember an app she used for half an hour years before.

But now, criminals have access to her email, which might include banking information or two-factor codes.

The answer is to have a solid policy in place about who can sign up for what kind of service. Also, ask your technology partner if they have any way to track what apps are being used across your business.

And definitely get a password manager for your staff… this will generate a new long, random password for each application, remember it, and autofill login boxes.

Password managers encourage good password practice because they make it easy.

However, there's an issue. Many businesses aren't 100% aware of what new services their staff have signed up for. And this problem isn't a financial one; it's a security one.

"It's dead, Jim..." Say Goodbye To Internet Explorer

"To ease the transition away from Internet Explorer, Microsoft added IE Mode to Edge. This mode makes it possible for organizations to still use legacy sites that may have worked best in IE."

After being the main entry to the Internet in the late 1990s and early 2000s, Internet Explorer (IE) is gone. In June, Microsoft dropped the web browser from support.

IE ushered in the age of connection to the world in 1995 and held a majority of the browser market share for many years. In 2014, Internet Explorer still held about 59% of the global market share, with Chrome at 21%. But just two years later, IE lost its top spot to Chrome and trailed behind another newcomer, Safari.

In 2015, the writing was already on the wall when Microsoft released a new browser, Edge. Edge was destined to take IE's place as the official browser installed on Windows systems.

It's inevitable, the longer technology is driving work and home life, that we're going to lose some of our favorites. Adobe Flash Player is another technology that used to be widely used and is now gone. So, now that IE has reached its end of life (EOL), what happens next?

Microsoft Will Redirect Users to IE Mode in Edge
According to Microsoft, now that IE is officially out of support, it will redirect users. A new experience is underway. Those opening this outdated browser will instead land in Microsoft Edge with IE mode.

To ease the transition away from Internet Explorer, Microsoft added IE Mode to Edge. This mode makes it possible for organizations to still use legacy sites that may have worked best in IE.

When in IE mode, you'll still see the Internet Explorer icon on your device. But if you open it, you'll actually be in Microsoft Edge

Microsoft Will Be Removing Internet Explorer Icons in the Future
Microsoft isn't yet getting rid of the IE icons that appear in places like the taskbar and Start menu on Windows. But it will in a future update. Users can expect to see those removed at some point.

Edge Will Import Browser Data from IE
What about your favorites, saved passwords, and other settings that you have in IE? Microsoft Edge will import these from Internet Explorer for you, so they're not lost.

This will include things like your browsing history and other data stored in the browser. You'll then be able to access these in the Microsoft Edge's settings area.

With IE Retired, What Do You Need to Do Now?
Uninstall Internet Explorer. It's risky to keep older technology that is no longer supported on your system.

Cybercriminals love to exploit older tools that are not receiving any security updates. This leaves an open invitation to breach your network and steal your confidential data.

The Biggest Vulnerabilities Hackers Are Currently Exploiting

Software vulnerabilities are an unfortunate part of working with technology. A developer puts out a software release with millions of lines of code. Then, hackers look for loopholes that allow them to breach a system through that code.

The developer issues a patch to fix the vulnerability. But it's not long before a new feature update causes more.

It's like a game of "whack-a-mole" to keep your systems secure.

Without ongoing patch and update management, company networks are vulnerable. And these attacks are completely avoidable.

82% of U.S. cyberattacks in Q1 of 2022 were due to exploiting patchable vulnerabilities.

What new vulnerabilities are lurking in products from Microsoft, Google, Adobe, and others? We'll go through several. These were recently noted in a warning by the Cybersecurity and Infrastructure Security Agency (CISA). Make sure to patch any of these vulnerabilities in your systems.

Microsoft Vulnerabilities
• CVE-2012-4969: An Internet Explorer vulnerability that allows the remote execution of code.
• CVE-2013-1331: This Microsoft Office flaw enables hackers to launch remote attacks.
• CVE-2012-0151: This Windows vulnerability allows user-assisted attackers to execute remote code.

Google Vulnerabilities
• CVE-2016-1646 & CVE-2016-518: These Chrome & Chromium engine vulnerabilities both allow attackers to conduct denial of service attacks.

Adobe Vulnerabilities
• CVE-2009-4324: This is a flaw in Acrobat that allows hackers to execute remote code via a PDF file.
• CVE-2010-1297: A Flash Player vulnerability that allows remote execution and denial of service attacks. (Flash Player is no longer supported, so you should remove it).

Netgear Vulnerability
• CVE-2017-6862: This router flaw allows a hacker to execute code remotely.

Patch & Update Regularly!
These are a few of the security vulnerabilities listed on the CISA list. You can see all 36 that were added at https://www.cisa.gov

How do you keep your network safe from these and other vulnerabilities? You should patch and update regularly. Work with a trusted IT professional (like us) to manage your device and software updates. This ensures you don't have a breach waiting to happen lurking in your network.

Small Businesses Are Attacked By Hackers Three Times More Often Than Larger Ones

Have you felt more secure from cyberattacks because you have a smaller business? Maybe you thought that you couldn't possibly have anything that a hacker could want?

Didn't think they even knew about your small business?

Well, a new report out by cybersecurity firm Barracuda Networks debunks this myth. Their report analyzed millions of emails across thousands of organizations. It found that small companies have a lot to worry about when it comes to their IT security.

Barracuda Networks found something alarming. Employees at small companies saw 350% more social engineering attacks than those at larger ones. It defines a small company as one with less than 100 employees. This puts small businesses at a higher risk of falling victim to a cyberattack. We'll explore why below.

Why Are Smaller Companies Targeted More?

There are many reasons why hackers see small businesses as low-hanging fruit and why they are becoming larger targets of hackers out to score a quick illicit buck.

Small Companies Tend to Spend Less on Cybersecurity

When you're running a small business, it's often a juggling act of where to prioritize your cash. You may know cybersecurity is important, but it may not be at the top of your list. So, at the end of the month, cash runs out, and it's moved to the "next month" wish list of expenditures.

Small business leaders often don't spend as much as they should on their IT security. They may buy an antivirus program and think that's enough to cover them.

But with the expansion of technology to the cloud, that's just one small layer. You need several more for adequate security.

Hackers know all this and see small businesses as an easier target. They can do much less work to get a payout than they would trying to hack into an enterprise corporation.

Every Business Has "Hack-Worthy" Resources

Every business, even a 1-person shop, has data that's worth scoring for a hacker. Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable. Cybercriminals can sell these on the Dark Web. From there, other criminals use them for identity theft.

Here are some of the data that hackers will go after:

- Customer records
- Employee records
- Bank account information
- Emails and passwords
- Payment card details

Small Businesses Can Provide Entry Into Larger Ones

If a hacker can breach the network of a small business, they can often make a larger score. Many smaller companies provide services to larger companies, including digital marketing, website management, accounting, and more.

Vendors are often digitally connected to their client's systems.

This type of relationship can enable a multi-company breach. While hackers don't need that connection to hack you, it is a nice bonus.

Small Business Owners Are Often Unprepared for Ransomware

Ransomware has been one of the fastest-growing cyberattacks of the last decade. So far in 2022, over 71% of surveyed organizations experienced ransomware attacks.

The percentage of victims that pay the ransom to attackers has also been increasing. Now, an average of 63% of companies pay the attacker money in hopes of getting a key to decrypt the ransomware.

"Every business, even a 1-person shop, has data that's worth scoring for a hacker. Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable. Cybercriminals can sell these on the Dark Web. From there, other criminals use them for identity theft."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Nine Tips To Keep Mobile Devices Safe

The reality is, mobile devices are less safe than desktop computers. Boosting security on such devices is essential if you use them in business.

Information on your team members' mobile devices is no longer limited to just phone numbers and contacts. They now contain much more significant data, such as emails, passwords, and other account details.

That's why keeping those mobile devices secure is key to shielding your reputation and minimising the risk of losing money.

Fortunately, you can implement robust safety measures to protect your smartphones and tablets. This article will cover the nine best practices in improving cybersecurity on mobile devices.

Establish a sound security policy

Before issuing tablets or smartphones to your teams, create an effective usage policy. Define rules about acceptable use and determine the penalties for violating them.

Your employees must be aware of the security risks and measures that can help them reduce the risks. They should know that they are the first line of defense against cybercrime.

Ensure the operating system is up to date

Updating Android and iOS operating systems improve overall user experience, but their most significant role is in addressing security vulnerabilities. Therefore, install updates as soon as the developer rolls them out to reduce exposure to cybersecurity threats.

Enable password protection

A complex password or PIN can help prevent cybercriminals from accessing mobile devices. Besides using alphanumeric combinations, you can also use facial or fingerprint recognition, depending on what suits your employees.

If you opt for digits and letters, don't share the combination with people outside your company. On top of that, be sure that your staff doesn't store them on their phones. Unmarked folders and physical wallets are a much safer option.

Only install business apps

Lenient download policies can allow your team members to install non-business apps. Downloading such apps might seem harmless, but they are also infamous for their harmful advertising codes and many other threats.

To mitigate this risk, tell your employees they can only download and use apps necessary for their roles.

Avoid public Wi-Fi

Your team may need to use public Wi-Fi networks in emergencies to send crucial emails or schedule a meeting. However, connecting to such networks can expose confidential company information to cybercriminals using the same network.

The easiest way to minimise this risk is to provide a high-quality Internet plan that features roaming services for your remote workers.

Leverage phone tracking

Losing company-issued mobile devices is unfortunate, but it's not the end of the world.

Enabling Android Phone Tracker, Find My Phone on iOS, or other device-tracking software can help locate your lost smartphones. Some programs also enable you to remove data on your stolen devices remotely.

Installing these apps takes a couple of minutes and gives you much-needed peace of mind. With it, even if your staff loses their mobile device, cybercriminals are less likely to get their hands on the content.

Use mobile device management (MDM)

For even more security, you may want to integrate with a reliable MDM. It's an excellent way to separate personal and business information while allowing your team members to set up robust security measures on their devices.

In most cases, cloud-based software is the most affordable, flexible, and manageable type of MDM. Many platforms let you check out device information, update and manage apps, configure your devices, create restrictions, and remove content remotely.

Screen messages

Cybercriminals frequently employ SMS phishing to trick your team into clicking dangerous links. They pose as someone credible, asking your staff to share confidential information.

If your employees encounter such messages, they should delete them or alert the IT department. Another great idea is to avoid opening the SMS and block the sender.

Practice blocking and whitelisting

Many threats can compromise your company due to employee errors. For example, a team member may not realize they're downloading a malicious app that allows thieves to steal data from their mobile devices. Blocking and whitelisting can enable you to protect your employees from these risks by determining which sites and apps are safe.