



TECH TALK

“Insider Tips to Make Your Business Run
Faster, Easier and More Profitable”

INSIDE THIS ISSUE:

Which Form of MFA Is the Most Secure?	Page 1	Top 6 Mobile Device Attacks	Page 2
Gadget of The Month	Page 1	Tech Tip of The Month	Page 2
Are Two Monitors Better than One?	Page 2	Should I Switch to Microsoft's Edge Browser?	Page 2
Using Windows 365 Cloud PC	Page 2	Technology Trivia	Page 2



We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing Technology!

– Carl Hamilton
Founder CEO

WHICH FORM OF MFA IS THE MOST SECURE? WHICH IS THE MOST CONVENIENT?

Credential theft is now at an all-time high and is responsible for more data breaches than any other type of attack.

With data and business processes now largely cloud-based, a user's password is the quickest and easiest way to conduct many different types of dangerous activities.

One of the best ways to protect your online accounts, data, and business operations is with multi-factor authentication (MFA).

It provides a significant barrier to cybercriminals even if they have a legitimate user credential to log in.

This is because they most likely will not have access to the device that receives the MFA code required to complete the authentication process.

What Are the Three Main Methods of MFA?

When you implement multi-factor authentication at your business, it's important to compare the three main methods of MFA and not just assume all methods are the same.

There are key differences that make some more secure than others and some more convenient.

Let's take a look at what these three methods are:

SMS-based

The form of MFA that people are most familiar with is SMS-based.

This one uses text messaging to authenticate the user.

The user will typically enter their mobile number when setting up MFA. Then, whenever they log into their account, they will receive a text message with a time-sensitive code that must be entered.

On-device Prompt in an App

Another type of multi-factor authentication will use a special app to push through the code. The user still generates the MFA code at log in, but rather than receiving the code via SMS, it's received through the app.

This is usually done via a push notification, and it can be used with a mobile app or desktop app in many cases.

Security Key

The third key method of MFA involves using a separate security key that you can insert into a PC or mobile device to authenticate the login.

The key itself is purchased at the time the MFA solution is set up and will be the thing that receives the authentication code and implements it automatically.

The MFA security key is typically smaller than a traditional thumb drive and must be carried by the user to authenticate when they log into a system.

Now, let's look at the differences between these three methods.

Most Convenient Form of MFA?

The most convenient form of MFA, it would be the **SMS-based MFA**.

Most people are already used to getting text messages on their phones so there is no new interface to learn and no app to install.

The SMS-based is actually the least secure because there is

malware out there now that can clone a SIM card, which would allow a hacker to get those MFA text messages.

Most Secure Form of MFA?

If your company handles sensitive data in a cloud platform then it may be in your best interest to go for better security.

The most secure form of MFA is the **security key**.

The security key, being a separate device altogether, won't leave your accounts unprotected in the event of a mobile phone being lost or stolen. Both the SMS-based and app-based versions would leave your accounts at risk in this scenario.



The Sony WH-1000XM5 wireless headphones are the the next generation to the ever popular WH-1000XM4 headphones, which have consistently been listed among the most popular and well-regarded wireless headsets in the market.

The XM5 boast an updated design and improved sound quality.

Featuring one of the best in class active noise cancelling in their class the XM5 are pricey, but worth every penny.

ARE TWO MONITORS REALLY MORE PRODUCTIVE THAN ONE?

When you see those people with two monitors, you may assume they do some specialized work that requires all that screen space, or they just really like technology.

But having the additional display real estate that a second screen provides can benefit anyone, even if you're doing accounting or document work all day.

According to a study by software developer Mavenlink, 73% of surveyed businesses say they spend over an hour per day on average just switching between different apps.

Productivity Research on Dual-Screens

Jon Peddie Research looked at the benefit of using two screens over several years. It found that overall, employees in all types of jobs **can improve productivity by an average of 42%.**

The company's namesake put it simply by saying, *"The more you can see, the more you can do."*

What Are the Advantages of Adding a 2nd Screen?

Do More in Less time

The biggest advantage to using a second monitor is that you can do more in less time because you're not struggling to get to the windows you need when you need them.

Expands Screen Space for Laptops

Connecting your laptop to a monitor can significantly improve the experience and make it like working on a normal desktop PC. You can either choose to mirror your entire screen or still make use of the laptop screen for some activities while using the larger screen for others.

Side-by-Side Comparisons Are Easier

There are a lot of tasks that require looking at data in two windows.

With two monitors, you have the screen real estate you need to fully open both windows and have them right next to each other so you can easily do your work.

More Freedom During Video Calls

With dual screens, you can choose which screen you want to share during meetings, and still have apps open on the other screen that no one can see.

Fairly Inexpensive Productivity Booster

Purchasing another display is a fairly low investment when looking at technology.

A monitor can be purchased for anywhere between £100 to £250 on average.

And with a 42% average productivity boost, it can have a pretty sweet ROI.

Need Help Improving Productivity?

There are several productivity boosts that you can get using the right technology tools, and they don't have to cost a fortune.



PROS & CONS OF USING THE WINDOWS 365 CLOUD PC

While many companies have moved most of their workflows to the cloud, there is still a key component of office operations that is location-based.

Most companies still rely on desktops and laptops to allow employees to access critical software and as their main workstation.

This can become inconvenient if you're doing work from one location. For example, if you work both at the office and home, in one of those places, you'll be without your "main computer." This can be a real problem when it comes to needing to access certain files or possibly working from a slower device than you're used to.

What is Windows 365?

Windows 365 is a cloud-based PC. Your entire operating system and everything that sits on it (settings, files, software, etc.) is loaded on a cloud server instead of your device. You can then access this through an online portal on your device (desktop, laptop, tablet, etc.).

Windows 365 can be accessed through any type of device, from anywhere, just like other cloud services. You can install applications, personalize your desktop, and do all the things you normally do on a computer. The main difference is that the computer operating system is now in the cloud.

Windows 365 Pros

- Access Your Computer Anywhere
- Perfect for the Hybrid Work World
- Better Access to Device Security & Administration

Windows 365 Cons

- You Can Only Use It Online
- A Slow Connection Ruins the Experience
- There is a Danger of Service Outage

Is a Cloud PC Right for Your Business?

There are several instances when Windows 365 offers big benefits to a company.

TOP 6 MOBILE DEVICE ATTACKS YOU NEED TO WATCH OUT FOR

Smartphones and tablets are often the preferred device for communications, web searching, and accessing many types of apps. They're more portable and can be used from anywhere.

You need to be on the lookout for the most prevalent mobile device threats that allow your data to be leaked or breached. Here's a roundup of what those are.

- Mobile Malware Hidden in Apps
- Unprotected Communications
- Public Wi-Fi & Man-in-the-Middle Attacks
- Juice Jacking on Public USB Charging Stations
- Non-Updated Devices
- Text-based phishing (smishing)

SIGNS THAT YOUR COMPUTER MAY BE INFECTED WITH MALWARE

Approximately 34% of businesses take a week or longer to regain access to their data and systems once hit with a malware attack.

Keep an eye out for these key warning signs of malware infection so you can jump into action and reduce your risk.

- Strange Popups on Your Desktop
- New Sluggish Behavior
- Applications Start Crashing
- Your Browser Home Page is Redirected
- Sudden Reboots
- You're Missing Hard Drive Space
- You Run Across Corrupted Files
- PC "Processing Sounds" When There Shouldn't Be

SHOULD I CONSIDER SWITCHING TO MICROSOFT'S EDGE BROWSER?

Microsoft Edge recently surpassed Firefox in worldwide desktop browser market share and is now the #3 Desktop browser in the world behind Chrome and Safari.

Why has Edge become so popular? One reason is that it adopted the Chromium framework in 2020, the same one that Chrome uses.

Edge is the replacement for Internet Explorer, but it's taken a while for it to become mainstream. It seems that now is its time.

Should you switch to Edge? Here are a few features to help you decide.

- Make saved websites easier to find using Collections
- Coupons are served up for you as you shop online
- Get instant price comparisons
- See pricing history for best-price trends
- Great security features, like Defender SmartScreen
- Grab quick screenshots with Web Capture

TECHNOLOGY TRIVIA

Each month you have a chance to win a £25 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

The question this month is:

Who was the tech CEO that in 1999 said, "You have zero privacy anyway..."?

The first person to email me at hello@hamiltonsystems.co.uk with the correct answer gets a £25 Amazon Gift Card!

