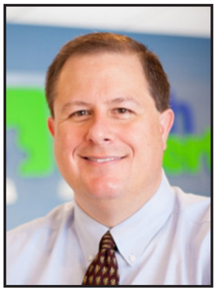
July 2022

TechTidbit.com

brought to you by Tech Experts

# Are Two Monitors Really More Productive Than One?



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

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.

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."

So, what are the advantages of adding a second 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.

> 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 $125 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.

# The Way We Use Passwords Is Finally Changing

*"Recently we've heard that tech giants Microsoft, Apple and Google have joined forces to kill off the password and introduce its replacement."*

Passwords are a problem that companies are always trying to fix, but they are still essential for accessing pretty much anything online. And even now people aren't changing them after a breach and then still use the same password to access multiple sites.

Reused passwords are a potential security problem because if a password has been compromised once, then hackers can use it to access other accounts if it's been used as the sign-in for another site.

Truth be told, passwords are annoying for most people. If you look at the best practice password advice, it's creating work for everyone:

- Generate long random character passwords rather than using everyday words that can be guessed by cyber criminals' automated software
- Use a different password for every single application
- Never write passwords down or share with a colleague

This is why we tell our clients to use a password manager. It's a safe way to generate highly secure passwords, store them, and fill in login boxes so you don't have to.

Recently we've heard that tech giants Microsoft, Apple and Google have joined forces to kill off the password and introduce its replacement.

That's called a passkey.

It's very simple. To login to something, you'll use your phone to prove it's really you.

Your computer will use Bluetooth to verify you're sat nearby. Because Bluetooth only works a short distance, this should stop many phishing scams.

Then it'll send a verification message to your phone. You'll unlock your phone in the usual way, with your face, fingerprint, or PIN.

And that's it. You're logged in.

We could see this new no-password login being introduced to some of the world's biggest websites and applications over the coming year. Exciting!

## You've Got Questions... We've Got Answers!

**I think I've clicked an unsafe link. What should I do?**
The faster you act, the less damage or data loss you'll suffer. Get in touch with your IT support partner immediately. It's always a good idea to have a response and recovery strategy in place for when this happens.

**My external drive isn't showing up when connected.**
First, make sure it's powered up! Then try it in a different USB port, and then a different device. This will let you know if it's the drive or your device that's the issue. You may need to manually enable it in Windows.

**What's the best antivirus software for my business?**
Not all antivirus software is equal, and the best solution for your business may be completely different than it would be for the company next door. It depends on your infrastructure. We'd love to help with a recommendation, so get in touch.

**How can I make my display more organised?**
Consider adding a second monitor. Not only will this allow you to better organize your apps and windows, but it will also give you more workspace.

**Can my phone be hacked?**
Yes! As well as the risk of phishing and smishing (that's phishing via text message), you also put your data at risk by connecting to public Wi-Fi. Fake apps can be an issue.

**How do I know if my Teams app is up to date?**
Just click on the three dots next to your profile picture and select 'Check for Updates' from the menu. If you're using Windows 11, you'll need to check under settings -> about Teams.

# 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.

Malware is an umbrella term that encompasses many different types of malicious code. It can include viruses, ransomware, spyware, trojans, adware, key loggers, and more.

The longer that malware sits on your system unchecked, the more damage it can do. Most forms of malware have a directive built in to spread to as many systems as possible. So, if not caught and removed right away, one computer could end up infecting 10 more on the same network in no time.

Early detection is key so you can disconnect an infected device from your network and have it properly cleaned by a professional.

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

## Strange pop-ups on your desktop

Some forms of malware can take on the disguise of being an antivirus app or warranty notice that pops up on your screen.

Hackers try to mimic things that users may have seen from a legitimate program, so they'll be more apt to click without thinking.

If you begin to see a strange "renew your antivirus" subscription alert or a warranty renewal that doesn't quite make sense, these could be signs that your PC has been infected with adware or another type of malware.

## New sluggish behavior

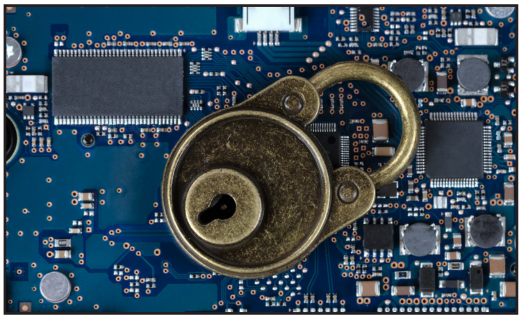
Computers can become sluggish for a number of reasons, including having too many browser tabs open at once or running a memory-intensive program. But you'll typically know your computer and the types of things that slow it down.

If you notice new sluggish behavior that is out of the ordinary, this could be an infection. One example would be if you don't have any programs open except notepad or another simple app, and yet you experience freezing.

When malware is running in the background, it can often eat up system resources and cause your system to get sluggish.

## Applications start crashing

Applications should not just crash out of the blue. There is always a reason. Either the software is faulty, there's been an issue with an update, or something else may be messing with that application's files.



If you suddenly experience apps crashing, requiring you to restart the app or reboot your system, this is another telltale sign that a virus, trojan, or other malicious code has been introduced.

## Your browser home page changes

If you open your browser and land on a homepage that is not the one you normally see, have your PC scanned for malware right away. Redirecting a home page is a common ploy of certain types of malware.

The malware will infect your system and change the system setting for your default browser home page. This may lead you to a site filled with popup ads or to another type of phishing site.

Just trying to change your homepage back in your settings won't fix the situation. It's important to have the malware removed as soon as you suspect something is wrong..

## Sudden reboots

Another annoying trait of certain types of malicious code is to make your system reboot without warning.

This can cause you to lose the work you've just done and can make it difficult to get anything done. This may happen when malware is changing core system files behind the scenes.

With files corrupted, your system becomes unstable and can often reboot unexpectedly.

## Missing hard drive space

If you find that a good deal of your hard drive space that used to be open is now gone, it could be a malware infection taking up your space. Some types of malware may make copies of files or introduce new files into your system.

They will cleverly hide, so don't expect to see the word "malware" on a file search. Instead, the dangerous activities will usually be masked by a generic-sounding name that you mistake for a normal system file.

## You run across corrupted files

If you open a file and find it corrupted, this could be a red flag that ransomware or another form of malware has infected your system.

While files can occasionally become corrupt for other reasons, this is a serious issue that deserves a thorough malware scan if you see it.

## Get expert malware scanning and removal

Free online malware and virus scans aren't very reliable. Instead, come to a professional like Tech Experts that can ensure your entire system is cleaned properly.

> *"If you begin to see a strange 're-new your antivirus' subscription alert or a warranty renewal that doesn't quite make sense, these could be signs that your PC has been infected with adware or another type of malware."*

## 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**

# How To Protect Your Online Accounts From Being Breached

Stolen login credentials are a hot commodity on the Dark Web. There's a price for every type of account from online banking to social media. For example, hacked social media accounts will go for between $30 to $80 each.

The rise in reliance on cloud services has caused a big increase in breached cloud accounts. Compromised login credentials are now the #1 cause of data breaches globally, according to IBM Security's latest Cost of a Data Breach Report.

Having either a personal or business cloud account compromised can be very costly. It can lead to a ransomware infection, compliance breach, identity theft, and more.

To make matters more challenging, users are still adopting bad password habits that make it all too easy for criminals. For example:

- 34% of people admit to sharing passwords with colleagues
- 44% of people reuse passwords across work and personal accounts
- 49% of people store passwords in unprotected plain text documents

Cloud accounts are more at risk of a breach than ever, but there are several things you can do to reduce the chance of having your online accounts compromised.

## Use multi-factor authentication (MFA)

Multi-factor authentication (MFA) is the best method there is to protect cloud accounts. While not a failsafe, it is proven to prevent approximately 99.9% of fraudulent sign-in attempts, according to a study cited by Microsoft.

When you add the second requirement to a login, which is generally to input a code that is sent to your phone, you significantly increase account security. In most cases, a hacker is not going to have access to your phone or another device that receives the MFA code, thus they won't be able to get past this step.

The brief inconvenience of using that additional step when you log into your accounts is more than worth it for the bump in security.

## Use a password manager for secure storage

One way that criminals get their hands on user passwords easily is when users store them in unsecured ways, such as in an unprotected Word or Excel document or the contact application on their PC or phone.

Using a password manager provides you with a convenient place to store all your passwords that is also encrypted and secured. Plus, you only need to remember one strong master password to access all the others.

Password managers can also autofill all your passwords in many different types of browsers, making it a convenient way to access your passwords securely across devices.

## Review your privacy settings

Have you taken time to look at the security settings in your cloud tools? One of the common causes of cloud account breaches is misconfiguration. This is when security settings are not properly set to protect an account.

You don't want to just leave SaaS security settings at defaults, as these may not be protective enough. Review and adjust cloud application security settings to ensure your account is properly safeguarded.

## Don't enter passwords when on public wi-fi

Whenever you're on public Wi-Fi, you should assume that your traffic is being monitored. Hackers like to hang out on public hot spots in airports, restaurants, coffee shops, and other places so they can gather sensitive data, such as login passwords.

You should never enter a password, credit card number, or other sensitive information when you are connected to public Wi-Fi. You should either switch off Wi-Fi and use your phone's wireless carrier connection or use a virtual private network (VPN) app, which encrypts the connection.

## Use good device security

If an attacker manages to breach your device using malware, they can often breach your accounts without a password needed. Just think about how many apps on your devices you can open and already be logged in to.

To prevent an online account breach that happens through one of your devices, make sure you have strong device security. Best practices include:

- Antivirus/anti-malware
- Up-to-date software and OS
- Phishing protection (like email filtering and DNS filtering)