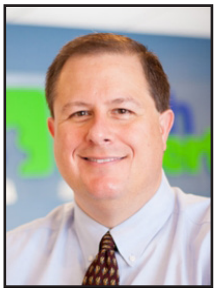
March 2021

TechTidbit.com

brought to you by Tech Experts

Microsoft 365 Is The Best Thing For Staff Productivity



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

Pandemic + Work From Home = relying on technology more than ever before.

The tools available in Microsoft 365 have developed to help us stay productive wherever we're working.

If you've been using Microsoft's software for years, now's a good time to discover new features.

If you haven't started exploring yet, you're missing out on loads of ways to boost productivity and make your life easier. Here are some of the main things to explore.

Microsoft Teams

Teams has made communication and collaboration even more effective than traditional ways of working face-to-face.

Long gone are the days when different versions of the same documents were flying around on email. Set up Teams correctly and your colleagues can work together in real-time - with only one master copy of a document that's shared and discussed.

You can even turn the clock back to previous versions if somebody makes an error or heads in the wrong direction.

Setting up dedicated channels within Teams lets defined groups of people focus on specific projects and topics. This makes sure people only get notified about the work they're involved in. Which keeps Teams from being overwhelming or confusing.

It's a space to help your team work with a focused level of productivity.

Don't know how to do something?

Try the search box at the top of Microsoft's apps

The search box is very smart, and can often be the quickest way to do what you need to do. Instead of Googling your question, this handy box will often take you straight to the button you need to press.

This can help save you a lot of time as it avoids the need to research online. It'll also make sure you get an answer specific to your version of Word, Excel, or whichever Microsoft 365 app you're using.

MyAnalytics

MyAnalytics is a productivity insights tool to help your people work smarter. By offering specific data on how you work, MyAnalytics is designed to help you improve how you spend your time and effort.

Along with lots of other tailored advice, it includes data on how much uninterrupted time you have – you know, time each day when you can focus on your actual work.

Now that so many of us are balancing home life and work life in the same location, this data can really help to plan and structure your work.

As well as providing you with data, MyAnalytics also offers suggestions for specific things you can try to improve the way you work.

For example, it can automatically add a couple of hours of dedicated focus time to your calendar each day to block anybody else from stealing the time you need to get things done.

For example, it can automatically add a couple of hours of dedicated focus time to your calendar each day to block anybody else from stealing the time you need to get things done.

It also helps to link together the various apps you use by offering suggestions based on your activity.

One example of this is how MyAnalytics in Outlook can give you a notification to highlight any outstanding tasks you've set up related to the person you're speaking with.

Handle Your Email With Care (Even With A SPAM Filter)

"Links are easy to manipulate; they can be made to look legitimate, but they'll actually take you to a different site or start downloading a program or virus."

Mark Funchion is a network technician at Tech Experts.

A lot of the communication we do today is by email. Naturally, that makes it a favorite avenue for malicious individuals to attack your system. A SPAM filter can help considerably, however nothing is 100% effective – and there is a fine line between "too aggressive" and "not aggressive enough."

Turning up the aggressiveness of the filter may stop the bad mail while at the same time improperly labeling legitimate messages as SPAM. Even with a SPAM filter, you should handle your email with care.

Here are a few tips to potentially save you from opening a message or attachment that is nefarious in nature.

The first rule is "just don't do it." It is tempting to just click that link or open that attachment.

You may even do it without a second thought. Scam emails can be very sophisticated, and they will often look like they are real.

Before you do anything, take a moment and consider a few things. If you are sent an attachment from someone you don't know, never open it. If the fishy attachment or email is from someone you do know but it was not expected, reach out the sender to make sure they actually sent it.

Next, don't jump the gun on clicking links that are sent to you. Links are easy to manipulate; they can be made to look legitimate, but they'll actually take you to a different site or start downloading a program or virus.

With links, there are two things you can do.

First, you can open a browser and go directly to the site to bypass all links. This is the safest option, especially when you get an "urgent alert" about your account that "requires immediate action."

If you can't go to the page directly through the website, you can hover your cursor over the link. A box will pop up previewing the destination you're actually being sent to.

If a link looks strange and doesn't match the company website, don't click on it. Also, look closely at the link as it may look just like a real one at first glance. Unless you are 100% sure the link is legitimate, do not click on it.

Another giveaway is that the message is poorly written with a lot of grammatical errors. If the message sounds like whoever wrote it doesn't use English as their first language (and it is not from a foreign company you do business with), delete the message. Do not open or click on anything in the message.

The last point is that it's usually not a good idea to unsubscribe from scam emails.

This may seem counterintuitive, but when you unsubscribe, you usually put your email address in to confirm you no longer want these messages.

Unfortunately, that lets the scammer know your email address is active. They will continue to send emails to this account or may sell it off as an active email.

Rather than unsubscribe from the email, block the sender. They will not know your email is active, and if they do send another message to you, it will not be received.

SPAM filters are great and they are essential. Still, remember that they are not 100% effective. Even with protection in place, it is wise to proceed with caution.

Take a moment to look for signs that the message is not from who it seems. These few seconds can save you a lot of time and money by avoiding disaster.

Using Teams while working from home? Sick of the constant notifications when you're trying to get your head down? Just mute the conversation for a while. Select the conversation, click 'More options,' then 'Turn off notifications.' You can do the same to turn the back on when you're ready to jump back into the chat.

Make Remembering Passwords A Thing Of The Past

Using weak passwords is risky. So is using the same password across different services.

If you do this, it means that once somebody has your email address and password, they'll find it incredibly easy to access your other accounts.

This can wreak havoc on your digital life and within your business. And the damage can spill over into serious real-world inconvenience too.

This is especially true if identity theft is involved, or if they've managed to break into your social media or bank accounts.

Data breaches happen every day. And once your passwords and email addresses are out there, you never know whose hands they'll end up in (many get sold on something called the Dark Web, a kind of hidden internet for criminals).

```
-left: 10px;
-right: 10px;
g-left: 10px;
g-right: 10px;
weight: bold;
low: auto;

login" id="login_form" >
t color='red'><b>Authentication Failed
"dError1" class="dError1">Please contact the

<saml-auth-status>-1</saml-auth-status>

"window.top.location='/php/login.php'
```

But what can you do to keep your passwords safe and your digital accounts secure?

Use a password manager

Instead of scratching your head to come up with a new password for each account, use a password manager to automatically generate long, random, strong passwords.

It'll also remember them for you. You only need to remember one password… the master password to access the password manager.

The best password managers let you customize how long your passwords are, and what kind of characters they should include. And will keep them 100% safe while still giving you easy access across all your devices.

We can set you up with an Enterprise Password Manager (the one we use) and train you and your team on how to best use it - simply get in touch!

Turn on multi-factor authentication (MFA)

As well as setting up a password manager, turn on multi factor authentication (MFA) wherever possible. When you log in to your accounts, you'll need to enter an additional security code as second means of keeping your account secure.

These codes can be sent to you by text message or email. Better still, you can set up an authentication app on your phone that refreshes with unique codes every few seconds. Some applications also support a hardware security key that you plug into your computer or that displays security codes that rotate every 60 seconds.

Multi factor authentication is available on most software and is considered a highly effective tool against hackers.

Even if they've got your login details they can't get in without your phone.

We recommend you implement this for all apps your staff use.

After an initial bit of discomfort, they'll soon get used to it. We can guide you and your team through the whole process - just give us a call!

> *"The best password managers let you customize how long your passwords are, and what kind of characters they should include. And will keep them 100% safe while still giving you easy access across all your devices."*

Would You Know If You Were Being Smished?

Ooof… you'd hope so, right? Sounds uncomfortable.

But push away whatever image that word has put in your head, and turn your attention to your mobile phone.

Smishing is the text message version of phishing.

What's phishing again? It's where criminals send you an email, pretending to be someone else (like your bank), to try to get sensitive information from you.

Yes, these cyber criminals really are resourceful. And the more ways there are to try and infiltrate your data, the more they'll use different platforms.

Just like with phishing, smishing attempts are not always as easy to spot as you might think.

Most of them pretend to be sent from a recognised business - like your network provider, for example - rather than just a random number. Some look like they've come from someone you know personally.

They'll ask you to click a link to take an action like checking your monthly bill, updating your account information, or maybe to pay a bill. It's usually the kind of message you would expect to see from that business.

But if you click that link… you've potentially given them access to your device. And that means they may have access to your data, passwords, and any other information stored on your phone.

Terrifying.

Protecting yourself is really similar to the way you'd deal with a phishing attempt on your email:

- Never click on any links unless you're certain the sender is who they say they are
- If you're unsure, contact the company (or person) on their usual number to check
- And if an offer seems too good to be true, it usually is (sorry, you didn't really win that competition you never even entered)

Consider this our number one most important golden rule: Never click a link if you're not expecting it. Wait to verify it with the sender first.

Is Your Business Data Encrypted?

Encryption can be a confusing subject for most people.

Is it a good thing or a bad thing?

We understand the confusion. Thanks to the surge in ransomware, you could be forgiven for thinking that encrypting data is definitely a bad thing. After all, if it's encrypted, how on earth will it be usable?

However, when you encrypt your own data, you're adding a level of protection to it. It means that should it be stolen; it'll be unusable to anyone else.

But less than 50% of companies have standardized end-to-end encryption set up. While they have some level of encryption, they don't have a documented standard that covers every area of their business.

And it's not only hackers and other cyber criminals that could benefit from a business' lack of data encryption. Lost or stolen devices put that data at risk too.

When you consider that a laptop is stolen every 53 seconds, it's leaving businesses more vulnerable than they should be.

Microsoft 365 automatically encrypts business data by default. But if you have no other encryption set up across your applications and files, it's time to speak to your IT support partner.

If we can help you, please don't hesitate to get in touch.

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

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