June 2018

TechTidbit.com

brought to you by Tech Experts

Time-Saving Tricks for Microsoft Outlook 2016

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

Microsoft Office 365 offers a number of useful tools for today's busy professionals including some new shortcuts for Outlook 2016. With so many companies now using Outlook as their major email program, Microsoft works to improve its operation with each annual update.

A number of the great features in this program are also found in other MS Office programs. For instance, if you're familiar with Word, then learning how to use Outlook will be much simpler.

New Changes for Outlook 2016

Using Outlook 2016, you can do a lot more than send and receive emails. You can also manage your calendar, set appointments, schedule meetings, and create/ manage groups.

In addition to being able to set up various types of groups, you can set up groups in Yammer. Yammer has become a central place where teams can exchange files, get updates and have conversations with others.

In Outlook 2016, distribution lists are now known as contact groups. Though the instructions for setting up each type of group vary a bit, they're very similar.

Users can find the instructions for setting up each type of group online or by using the F1 key in Outlook. The new Outlook has many helpful features like this to make your workday go smoother and help you improve efficiency. Below are some tips and tricks for getting the most out of Outlook.

Turn Off Notifications

There are several ways to turn off notifications in Outlook. This is an easy way to stop all those interruptions that prevent you from getting your work done each day.

Go to the taskbar and click on the triangle. The programs that are already available will show up. Right-click the Outlook icon and you will get a list of things you can do. One of them is turn off notifications. Uncheck the box that says "Show New Mail Desktop Alert."

If you have Outlook open, you can also go to File>Options>Mail. Here, there are many options. Click on, "Turn off notifications". You can also personalize your mail client here.

Setting Up Meetings Automatically

One of the favorite shortcuts in Outlook 2016 is the one for setting up a meeting. There are actually several good ways to do this. Drag an email from your Inbox to the Calendar icon at the bottom of Outlook. This will automatically set up a meeting.

You can turn any email into a meeting by doing this. Another effective method, with your email open, click on "Reply with meeting". This is found on the ribbon in the "Respond" group. Clicking on "Reply with meeting" will send out an invitation to everyone who was addressed in the email.

Instant Messaging a Group

This is a good way to get a fast answer from team members who may be involved in an important project with a fast-arriving due date. Open your last email about this topic or from one of the members of the email. Next, click on IM>Reply All.

Continued on page 4

Using Outlook 2016, you can do a lot more than send and receive emails. You can also manage your calendar, set appointments, schedule meetings, and create/ manage groups.

Network Security: What Does Your Firewall Do For You?

"Using the Internet to pay bills, access banking information, or even applying for loans is commonplace. We must be prepared to protect our identity and personal information. Now, whether you are talking about your home or your business, network security starts with a firewall."

Jason Cooley is Support Services Manager at Tech Experts.

"Security." It's a word that we are all familiar with, but it can have many different meanings depending on context. Security to people nearing retirement age may mean financial security for their future.

At a large event like a concert, it could mean both security guards and the overall security of the event.

However, as time goes by, the word security has become increasingly related to the digital world.

Using the Internet to pay bills, access banking information, or even applying for loans is commonplace. We must be prepared to protect our identity and personal information.

Now, whether you are talking about your home or your business, network security starts with a firewall.

So what is a firewall?

A firewall, in terms of network security, can be a physical device that your incoming and outgoing data is routed through. It could also be a program on your device that can strengthen and supplement your devices' security.

Both of these have different capabilities and purposes and can be used individually or together.

While there are different types, their essential function is the same. A firewall is put in place to allow or deny traffic, based on a set of security rules.

In a business setting where many staff members use a computer daily, a firewall can be put in place to block unwanted traffic.

A simple security rule to check for secure certificates can stop unwanted traffic easily.

Websites have security certificates, so when you access a page, your firewall can check the certificate. If the certificate is digitally signed and known as trusted, the firewall will allow traffic to proceed.

Search results can often display links of potentially harmful websites.

A firewall adds a layer of security making sure your employees don't accidently find themselves on a website that could compromise your network.

This same principle works for home networks and can allow you to set some security rules. These rules can be put in place to help keep Internet usage safe, especially with children around the house. A firewall can also block certain content.

In an office setting, you could turn off access to social media to stop staff from accessing sites that aren't needed to complete work.

It can block certain search engines and even limit the use of unsecure versions of websites.

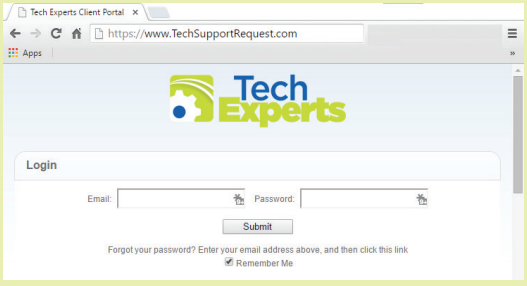
At home, you can block content from websites you don't want your family to have access to.

There is also the option of having active network times. You can have your Wi-Fi network only active during business hours, keep your kids off their devices at bedtime, or limit access to certain days.

There are many other things that your firewall can do to help keep your network safe.

Keeping your network secure has the potential to save you thousands of dollars, depending on the number of devices and your dependency on those devices.

Safety and security always has a high value to you. It can also help you rest easier knowing that either your business, or your family, is a little bit safer.



Create new service requests, check ticket status, and review invoices in our client portal:
http://TechSupportRequest.com

53% Of Businesses Have Publicly Exposed Cloud Services

Chris Myers is a field service technician at Tech Experts.

Malware comes in many different forms and is used by hackers in a number of different ways. It can be used to steal information, locate vulnerabilities in your IT systems for a secondary attack, or simply to cause damage.

There are countless hackers out there just waiting for your business to leave your data vulnerable. With the introduction of the cloud, you felt a bit more secure and slept slightly better at night – but now, it seems that was precisely what hackers wanted us to do.

A recent Cloud Security Trends study found that 53% of businesses using cloud storage accidentally expose their data to the public. This is like securing your whole house, locking all doors and windows, and then going to sleep with the garage wide open.

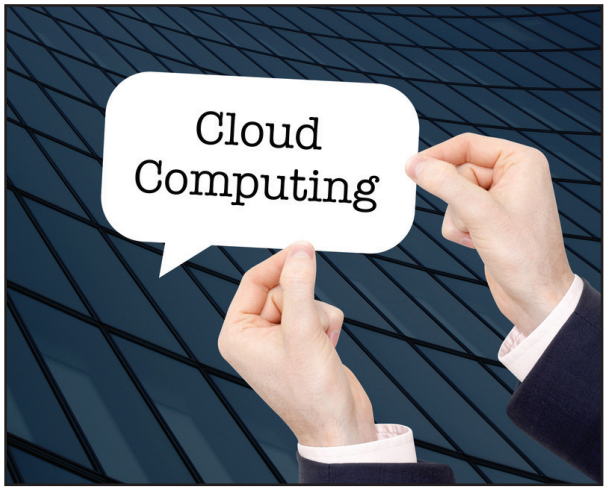
This doesn't just point the finger at small businesses either. The study showed that even big-name companies such as Amazon Simple Storage Service (Amazon S3) had inadvertently exposed one or more of these services to the public.

The scary thing is that the previous survey showed this was occurring only 40% of the time. Now, this number has grown to 53%.

This study was conducted in 2017 between the months of June to September. Within those two months, they found that businesses are not only exposing their own data but they are also neglecting vulnerabilities in their cloud. When you ignore these things, you put not only your customers at risk but also the livelihood of your company as well.

What Are You Exposing?

The report shows that businesses weren't solely leaking data such as customer information, but incredibly dangerous information such as access keys and other private data as well.



These cyber-attacks commonly expose data such as personal health information, financial information, passwords and usernames, trade secrets, and intellectual property. With two million new malware attacks launching every day, it's more important than ever to stay in a constant state of vigilance.

Ignoring Vulnerabilities

A common misconception is that it's the service provider's responsibility to keep cloud data safe – this is not true. Most of the damage caused by ignoring vulnerabilities can be prevented by training.

If your staff is trained to recognize weaknesses, then they can be more proactive in fighting against them. More than 80% of businesses are not managing host vulnerabilities in the cloud. Vulnerabilities include insufficient or suspicious credentials, application weaknesses, and inadequate employee security training.

Complex Attacks

Not all the attacks and vulnerabilities are the fault of the business. Some of these attacks are far more complex than most businesses are prepared for, including big-name companies. These sophisticated attacks not only know and bypass the company's vulnerabilities but also various application weaknesses.

What Can You Do About It?

The first action you can take against attacks is recognizing suspicious IP addresses. Have a policy in place for identifying, flagging, and isolating suspicious IP addresses. Spending a few extra minutes of your time could save months of recovery and downtime.

It's important to pay attention to mistakes that others have made so you don't suffer the same consequences. Be sure to train and certify the IT staff you already have. Cyberattacks are guaranteed, but what isn't guaranteed is how prepared your business is to thwart off those attacks.

"There are countless hackers out there just waiting for your business to leave your data vulnerable. With the introduction of the cloud, you felt a bit more secure and slept slightly better at night – but now, it seems that was precisely what hackers wanted us to do."

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

Google Study Reveals Phishing Attacks Are The Biggest Threat To Web Security

A recent study by Google and UC Berkeley suggests that cyber thieves are successfully stealing 250,000 valid usernames and passwords every week.

The study, which was based on 12 months of login and account data that was found on criminal websites and forums, aimed to ascertain how the data had been hacked and the actions that can be employed to avoid criminal activity in the future.

Google claims the research is vital for developing an understanding of how people fall victim to scammers and hackers and will help to secure online accounts.

The research found that, over a 12-month period, keyloggers (programs that monitor every keystroke that someone make on a computer) stole 788,000 account credentials, 12 million were harvested via phishing (emails or phone calls that con people into handing over confidential data), and an incredible 1.9 billion were from breaches of company data. The study found the most productive attacks for cyber-thieves came from phishing and keylogging. In fact, in 12%-15% of cases, the fraudsters even obtained users' passwords.

Malicious hackers had the most success with phishing and were able to pick up about 234,000 valid usernames and passwords every week, followed by keyloggers who managed to steal 15,000 valid account details per week.

Hackers will also look to gather additional data that could be useful in breaching security measures, such as the user's Internet address (IP), the device being used (Android versus Apple) and the physical location. Gathering this data, however, proved far harder for those with malign intent.

Of the people whose credentials were secured, only 3.8% also had their IP address identified, and less than 0.001% had their detailed device information compromised.

Google said in a follow-up blog post that the research would be used to improve the way it detects and blocks attempts to misappropriate accounts.

Historical data of the physical location where users logged on and the devices they used will increasingly be used as part of a range of resources that users can use to secure their accounts.

The research, however, did acknowledge that the account hacking problem was 'multi-pronged' and would require countermeasures across a number of areas including corporate networks.

Education of users is set to become a 'major initiative' as the research also revealed that only 3.1% of people whose account had been hijacked subsequently started using enhanced security measures such as two-step authentication (Google authenticator or a similar service) after control of a stolen account was regained.

Time-Saving Tricks for Outlook 2016, From Page 1

This will send out a response as an instant message. Team members who are online will get notified immediately via instant message.

Quick Access Toolbar

Customize this toolbar located at the very top left portion of Outlook. You can add the commands that you most often use so that they're handy. This can be done in any Microsoft Office program.

Go up to the very top left portion of the screen where you'll find the quick access icons. Click on the triangle at the end. This opens a drop-down list. One of the options is "more commands."

Getting Help

These are just a few of the many ways that Microsoft Outlook 2016 will help you get all your work done without too much extra labor and stress.

Learning these shortcuts, tips, and tricks can help you modify Outlook so that it's customized just for you.

If you take a little extra time each day to learn one Time Saving Tip, you'll get the most out of the program. In addition to the articles and tutorials found at Microsoft, you can also find hundreds of YouTube videos that will show you exactly how to do something.