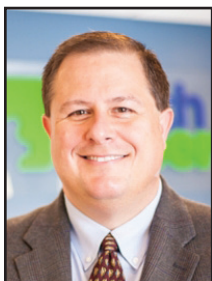# Six Tips For Dealing With Email Overload

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

Most, if not all, small business owners are barraged by the large number of emails they receive on a daily basis. As a consequence, way too much time is spent on email that actually slows down productivity.

Email has become a 'disruptive' technology that could take you on a tangent and eat up your time fast. So, it is important to take charge of your inbox and filter unwanted emails. Here are some ways you could do that:

Prioritize incoming emails

As a rule, not every email you receive requires immediate attention. Filtering out the most important messages allows you to prioritize the emails you should answer and saves you valuable time.

Most email software have a few good filters that make this possible.

Set specific times to respond to your emails

Giving in to the temptation of checking and responding to your emails is actually an issue of inefficiently dealing with emails rather than the abundance of emails.

Instead of continuously checking your email from multiple devices, set specific times throughout the day to check your email and refrain from checking email outside these times. It is actually more efficient to respond to your emails in bulk rather in piecemeal.

Use the search function

Organizing your emails in folders are important; however, if you are searching for an old email, use the search function, the advanced search operators, and filters to quickly find what you are looking for.

Unsubscribe from unwanted lists

To eliminate the many emails that are not spam but which are still cluttering your inbox, take some time and unsubscribe from newsletters or services which you no longer read or use. Look into using a mass unsubscribe tool if you don't want to unsubscribe from each list.

Use filters

Most email systems allow filtering, which you can assign to any type of email that you get regularly. For instance, a filter makes it possible to forward emails which contain particular keywords to your assistant or have a particular automated response to certain emails. This significantly reduces the amount of time you spend on email.

Turn off notifications from social media sites

You really don't need to get an email each time someone responds to your Facebook comment or tweet. Since you'll eventually see such updates once you actually visit those sites, they shouldn't be allowed to clutter your inbox. In fact, such notifications are just distractions that could cut on your productivity.

We're proud to partner with the computer industry's leading companies:

Microsoft Partner

Microsoft® Small Business Specialist

Business Partner IBM®

Why Is Network Security Important For Your Small Business?

Michael Menor is Vice President of Support Services for Tech Experts.

Network security is very important to all networks big or small. The purpose of network security is to prevent loss, through the misuse of data.

There are a lot of issues that can arise when network security is not properly implemented and maintained, a few issues include, but are not limited, to the following: data destruction, data manipulation, and breach of confidentiality.

The most important layer of security is physical security, this should be the first line of defense for any network. An organization can have all the access rules, logical security policies, and Intrusion Detection Systems (IDS) in place, but nothing beats being protected at the physical level.

One of the simplest steps is to lock the door, for example the server room or network closet should have a physical door and lock that secures it. This can also include any items that may be vulnerable to theft or physical damage.

Another form of physical security can be having surveillance cameras monitoring the premises. This gives an organization that extra sense of security, especially after hours. Earlier we discussed ways to secure

the physical network, but what about the logical network? You do not want to be on a network that does not challenge you for logon credentials to access systems.

This is where authentication and password security comes into play. Securing a network with usernames and passwords can prevent unauthorized access to data and also provide measures that prevent unauthorized changes of systems.

System administrators can also implement a password complexity policy, which requires users to have passwords that are of a certain length, and contains a combinations of alphanumeric and special characters. It is also wise for users not to use any personal identifying characters in their passwords because this is usually the first things hackers look into.

The Internet is not a secure place, viruses pose a big security risk to a computer network because there are so many out there. Without antivirus protection, a computer can get infected and may even infect other computers on the same network.

Depending on the purpose, or payload, of the virus, the viruses' creator may have designed the virus to steal or delete information,

render a system useless by using all resources, or even use the computer as part of a botnet. Antivirus software provides protection against most, but not all viruses.

Not only should users frequently update and scan their computers for viruses, but they must also be smart when browsing the Internet because many viruses can disguise themselves as legitimate software.

Firewalls are a great way to control the internal network traffic and also incoming traffic from the Internet.

While antivirus protection helps to protect a computer from potentially unwanted programs and viruses, a firewall can help to control network access into a computer system.

There are two types of firewalls: software- and hardware-based firewalls. Both provide similar functions, but it is best to implement a hardware firewall because it gives a system administrator the ability to make changes to a system as a whole, rather than at individual systems, or endpoints.

Within the firewall there are policies which allow or deny traffic based on the needs of the network. The most secure policy is a restrictive policy which denies all network traffic, this policy only allows essential network traffic to traverse the firewall.

If you have any questions about your network security give us a call at the office, (734) 457-5000, or email info@mytechexperts.com.

Windows 8 - WOW Does It Look Different!

Scott Blake is a Senior Network Engineer with Tech Experts.

Microsoft's venture into a truly mobile operating system, that can be spread spectrum across all of their platforms, was in theory a great idea.

What went wrong was underestimating the public's attachment to the look and feel of their Windows XP and Windows 7 (we'll just forget about Vista) operating system.

With many users still looking sideways at the new stylish Windows 8 interface, and even with the slight upgrades and changes in looks (ha, I laugh at the new start button) that Windows 8.1 has brought on since its release.

For many users out there, this still is not a big enough change to truly bring enjoyment to their personal computer experience.

If you are in "ever search mode" to locate and regain that look and feel of operating systems of yesteryear, there are two great programs that allow anyone of any level of computer experience to install and customize to regain that feeling of comfort.

Classic Shell, a freeware program, can enable a legacy-style Start menu and Windows Explorer interface. You can even have the

Windows 7 menu back! But why stop there? Windows XP and Windows Classic menus are available as well. The Classic style will be a comfort to anyone upgrading from Windows 98.

The classic Explorer settings can also transport you into the way-back machine, and users can now have the simple Windows XP style back that they know and love.

A small low impact application that gives you a true look and feel of a Windows 7 interface, while still maintaining the complete functionally of the Windows 8 operating system.

Classic Shell, gives you a true start button and brings back that all too familiar look and feel of your dearly departed Windows XP or 7 systems.

Check it out, it even offers a "Shut Down" button. Classic Shell also allows for customization of the new start menu.

Created by Stardock, a company that's been making Windows user interface mod's for years, Start8 comes as a free 30-day-trial. After that, you can "unlock" the third-party software for just $4.99.

Start8 does not re-enable the Windows Start menu. Instead, it creates a new menu that looks similar to it. Because of this, Stardock provides a great deal of customization.

Users can make the menu appear Metro-like by giving it square edges, or can stick with the Windows 7 look by giving it rounded edges. It's also possible to change color, add or remove translucency, and give the Start menu button a custom icon.

And that's just the beginning. There's a plethora of options available in the app's configuration and control menus for users to explore and customize.

Considering its low price and the large number of options, I think this software is a good deal. I even like the optional faux-Metro style.

However, Start8 doesn't add any new functionality, so users are essentially paying $5 to have what was bundled with Windows 7.

So there you go. Two great choices, it just all comes down to "to pay or not pay, that is the question." Remember the technicians at Tech Experts are always ready to lend a hand.

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.

Spring Cleaning Tips for Your Home and Office Computers

Spring is a good time to get some cleaning done in your home as well as your office. Here are few tasks and tips you should check off your list, if you own a small business or if you simply are a computer user:

Back up your files

You should make it a routine and regularly back up your important files to the cloud or into an external hard drive. Delete old unnecessary emails and archive important ones. This will make it easier to locate specific email chains and will open up the storage space in your computer.

Update your security settings

You may assume that your home or small business or PC is too small a target for hackers, but that is simply not the case.

Internet security statistics show that hackers are targeting businesses with fewer than 250 employees due to the fact that it's generally easier to hack into small businesses and home users.

As a rule, assume that any valuable information you have is at risk, and ensure you install the latest security patches and updates whenever they become available.

Take advantage of mobile technology

Research indicates that small businesses that do not accept mobile payments could be losing up to 1 trillion dollars annually. Many small business owners realize the potential of mobile technology, but 91% of them still don't have mobile-optimized websites. If your business is not yet mobile friendly,

it is important to start thinking about upgrading your services.

Go paperless

Going paperless will significantly reduce paper clutter and will minimize the time needed for spring cleaning. There are many affordable solutions you could adopt which allow you to maintain and organize critical business documents.

Manual clean-up

Your hardware and peripherals also need to be cleaned, so take some time to clean your keyboards, screen monitors and to check the batteries in your mouse or wireless keyboards. Also, remember to clean your printer and check whether or not you have installed all the required updates from the manufacturer and that all its parts work seamlessly.

Effective Ways To Increase Your Privacy Online

With the increased hacking and account infiltration attempts, protecting people's privacy has become extremely important.

While online, you can minimize your exposure by browsing privately or completely anonymously.

Private Browsing

You can browse the internet privately, by turning on the private browsing feature. It will prevent the history tracking of pages you visit. The feature is found in the main browser menu.

In Internet Explorer, the feature is called 'Private Browsing,' in Firefox, it is called 'Private Window' and in Google Chrome, it is called 'Incognito mode.'

However, there are limits to private browsing: Any files you save or

websites you visit will have your IP address as well as unencrypted data you send.

For greater privacy, there is Sandboxie, an application which prevents other programs from saving any data to your disk.

Protect Personal Data

It is good practice to use unique usernames and passwords for each computer user, including guests.

This will help to reduce unwanted access to your files. You could also encrypt your hard drive by enabling Bitlocker which will encrypt your entire drive, making it inaccessible to anyone without your Windows user password.

In case you don't have Bitlocker built into your OS, TrueCrypt is another free alternative that will

secure your files. When you need to completely delete your files, use a utility like Eraser which will ensure they can never be recovered.

Use a Private OS

The best way to ensure complete anonymity and privacy, you could work in an entirely different operating system from your regular OS through virtualization.

A wall is set up around the virtual computer to prevent anything you do from leaving files on your normal Windows file system.

This is an entire operating system devoted to privacy, and is installed on a DVD or USB to run on any computer.

Nothing is written to the computer's main drives and your browsing activity is completely anonymous.