Tech Solutions INC. Managed Services Computer Consulting Network Administration

TechPoints

August 2014 *IT Tips and TechSolutions News* Vol. 4 No. 8

In This Months TechPoints

- What Makes a Mailbox a Big Mailbox?
- 5 Common Security Breaches
- Looking at Android Work for Android
- Reducing Desktop Clutter

What Makes a Mailbox a Big Mailbox?

By Rich Kenney, Vice President, TechSolutions, Inc.

Have you ever had someone from tech support or a system administrator tell you that you have entirely too much email? Or that you need to delete some of your email because your mailbox is too big? Most people in the business world have had that experience at least one time. So what's the big deal and how much mail is too much? In this article I'll attempt to enlighten you as to why size matters and help you determine the difference between a large mailbox and a small mailbox. To be clear, the term mailbox here refers to the location where all your email folders (INBOX, DELETED, SENT ITEMS, etc.) are accessed.

The two main reasons that system administrators get concerned over large mailboxes are 1) hard drive space utilization and 2) performance.

Regarding hard drive space utilization, in some ways your mailbox represents a dollar figure to a system administrator. Every email that you save in your inbox that has, for example, a 5 MB attachment represents 5 more MB of hard drive space consumed. In terms of individual emails, that number is not cause for alarm, however let's multiply that one email by 5,000 and assume that multiple people within your organization have been recipients of those very same emails. Suddenly we are talking about a substantial amount of hard drive space that is required on a mail server to store all of those emails.

For example, based on the numbers above, 4 people, each retaining 5,000 emails with 5 MB attachments, would require over 100 GB in hard drive space to store these emails and attachments. On top of that, many backup products nowadays would require 1 to 3 times additional, separate hard drive space to backup those emails. After some quick addition, that single 5 MB email from above, including backup space requirements, is now consuming up to 20 MB of hard drive space within your organization and, using the example of 4 people with 5,000 emails, up to 400 GB in total. It doesn't take long before additional hard drive space is needed to keep up with the ever-growing size of everyone's collective mailboxes – and that results in more money being spent translating to fewer profits.

In terms of performance, system administrators continually strive to keep systems operating at peak performance, which isn't always easy to achieve due, in part, to how users manage their mailboxes. Certain folks out there (you know who you are) are email hoarders. Others are so inundated with incoming mail that they simply cannot keep up with the reading, filing and deleting of emails. Either of those scenarios results in quantities of email that simply seem to grow exponentially The problem with that is that the number of emails, more so than the size, are the enemy of email application performance. So for example, if you have say 43,000 emails in your INBOX, that could negatively impact performance.

You're probably wondering, "Well how big is too big?" The short answer is "it depends." In an Outlook/Exchange environment, which many companies are in, there are lots of different technical configurations to account for in determining the answer to that question. The version of software that is being used on workstations (for example Outlook 2003 vs. Outlook 2007 vs. Outlook 2010 vs. Outlook 2013) as well as what is installed on the server side of things (Exchange 2003 vs. Exchange 2007 vs. Exchange 2010 vs. Exchange 2013) makes a huge difference in determining what "too big" is.

To complicate things further, there are no hard set limits to go by … just guidelines. In general, Microsoft's stance is that the collective size of the entire organizations mailboxes is basically limited by the financial expense of storage. Even so, their recommendation is that a mailbox be no more than 15 GB or so for people using Outlook 2010 or Outlook 2013, about 5-7 GB in Outlook 2007 and less than 4 GB in Outlook 2003.

The real performance inhibitor in working with email is more so the total number of items in any one folder. Microsoft recommends the fewer the better, especially in the critical path folders such as INBOX and SENT ITEMS. As long as the version of Exchange server software being used is 2007 and above, a general rule of thumb would be to keep the quantity of items in any one email folder to less than 20,000 (less than 5,000 if working with Exchange 2003). This is not to say that having 20,001 items in your INBOX will cause your email to stop working because these are general guidelines only.

Regarding mailbox size verses number of emails, in the eyes of Microsoft, working with an Outlook 2010 INBOX containing 2,000 items and totaling 5 GB is perfectly fine. Whereas working with an Outlook 2010 INBOX containing 21,000 items but only totaling 1.5 GB is borderline and could result in performance issues and complaints from the end user.

This subject matter is complicated and full of IF's and BUT's, hopefully though I've shed a little light on how to decipher a poorly-performing "large mailbox" from a quick and responsive "small mailbox". Of course we are here for you as well, so if you have any questions, give us a call at (302) 656-8324 and we can help you understand how all of the puzzle pieces fit together.

5 Common Security Breaches

These days, the security of various technology based systems is constantly being called into question. From attacks on mobile devices to ever increasing types of malware, many businesses are struggling to stay on top of their security. One of the best ways to help ensure your systems are secure is to be aware of common security issues. To that end, here are five common ways your security can be breached.

1. You are tricked into installing malicious software

One of the most common ways a system's security is breached is through malware being downloaded by the user. In almost every case where malware is installed the reason is because the user was tricked into downloading it.

A common trick used by hackers is to plant malware in software and then place this software on a website. When a user visits the site, they are informed that they need to download the software in order for the site to load properly. Once downloaded, the malware infects the system. Other hackers send emails out with a file attached, where only the file contains malware.

There are a nearly limitless number of ways you can be tricked into downloading and installing malware. Luckily, there are steps you can take to avoid this:

- Never download files from an untrusted location - If you are looking at a website that is asking you to download something, make sure it's from a company you know about and trust. If you are unsure, it's best to avoid downloading and installing the software.

- Always look at the name of the file before downloading - Many pieces of malware are often disguised with file names that are similar to other files, with only a slight spelling mistake or some weird wording. If you are unsure about the file then don't download it. Instead, contact us as we may be able to help verify the authenticity or provide a similar app.
- Stay away from torrents, sites with adult content, and movie streaming sites - These sites often contain malware, so it is best to avoid them altogether.
- Always scan a file before installing it - If you do download files, be sure to get your virus scanner to scan these before you open the apps. Most scanners are equipped do this, normally by right-clicking on the file and selecting Scan with….

2. Hackers are able to alter the operating system settings

Many users are logged into their computers as admins. Being an administrator allows you to change any and all settings, install programs, and manage other accounts.

If a hacker manages to access your computer and you are set up as the admin, they will have full access to your computer. This means they could install other malicious software, change settings or even completely hijack the machine. The biggest worry about this however, is if a hacker gets access to a computer that is used to manage the overall network. Should this happen, they could gain control over all the systems on the network and do what they please on it.

In order to avoid this, you should ensure that if a user doesn't need to install files or change settings on the computer, they do not have administrator access. Beyond this, installing security software like anti-virus scanners and keeping them up to date, as well as conducting regular scans, will help reduce the chances of being infected, or seeing infections spread.

3. Someone physically accesses your computer

It really feels like almost every security threat these days is digital or is trying to infect your systems and network from the outside. However, there are many times when malware is introduced into systems, or data is stolen, because someone has physically had access to your systems.

For example, you leave your computer on when you go for lunch and someone walks up to it, plugs in a USB drive with malware on it and physically infects your system. Or, it could be they access your system and manually reset the password, thereby locking you out and giving them access.

What we are trying to say here is that not all infections or breaches arrive via the Internet. We recommend that you password protect your computer so that you need to enter a password in order to access it. You should also be sure that when you are away from your computer it is either turned off, or you are logged off.

Beyond that, it is a good idea to disable drives like CD/DVD and connections like USB if you don't use them. This will limit the chances that someone will be able to use a CD or USB drive to infect your computer.

4. It's someone from within the company

There have been a number of infections and security breaches that were carried out by a disgruntled employee. It could be that they delete essential data, or remove it from the system completely. Some have even gone so far as to introduce highly destructive malware.

While it would be great to say that every business has the best employees, there is always a chance a breach can be carried out by an employee. The most effective way to prevent this, aside from ensuring your employees are happy, is to limit access to systems.

Take a look at what your employees have access to. For example, you may find that people in marketing have access to finance files or even admin panels. The truth is, your employees don't need access to

everything, so take steps to limit access to necessary systems. Combine this with the suggestions above – limiting admin access and installing scanners – and you can likely limit or even prevent employee initiated breaches.

5. Your password is compromised

Your password is the main way you can verify and access your accounts and systems. The issue is, many people have weak passwords. There has been a steady increase in the number of services that have been breached with user account data being stolen. If a hacker was to get a hold of say your username, and you have a weak password, it could only be a matter of time before they have access to your account.

If this happens, your account is compromised. Combine this with the fact that many people use the same password for multiple accounts, and you could see a massive breach leading to data being stolen, or worse – your identity.

It is therefore a good idea to use a separate password for each account you have. Also, make sure that the passwords used are strong and as different as possible from each other. One tool that could help ensure this is a password manager which generates a different password for each account.

If you are looking to learn more about ensuring your systems are secure, contact us today to learn about how our services can help.

Published with permission from TechAdvisory.org

Looking at Android Work for Android

Google's mobile operating system Android has become one of the most popular systems installed on phones. While the system is feature heavy, many businesses are wary about the overall openness of the system. Earlier this year, Google announced the next version of Android – Android L – which will have a number of business-specific features called Android Work.

What exactly is Android Work?

Android Work is a program that is being developed by Google that will be introduced in the next version of Android – Android L. Because of the overall open and somewhat fragmented nature of Android, many businesses have been struggling to manage devices. In an effort to attract business customers, device manufactures have come up with their own business-centric suite of features that boost device security and manageability.

While there are a number of options out there, Samsung has had the most success with KNOX. This is essentially a secure version of Android that can be managed by businesses. With devices running KNOX, administrators can separate personal and work features, as well as manage and secure business apps and content on a user's device.

The best way to think of this program is that it enables a completely separate business profile, that can be managed by a company, on a personal device. Users with a system like this will be able to separate work and personal apps, content, and data, but still be able to use the same device. This is what mobile experts refer to as containerization – business apps and data are essentially stored in a container that is kept within the overall Android system.

Google found this idea of being able to separate personal lives and work on the same device to be something worth investing in, and have subsequently developed Android Work based on the KNOX platform. This will allow all Android users, not just users with Samsung devices, to take advantage of this program.

When launched there will be a number of key business oriented features beyond just the KNOX support. Here are two of the most talked about.

Seamless transition between personal and work data

Containerization is usually referred to as creating a separate system on one device, kind of like having a work and personal profile on your computer. While this is great, it can be annoying to switch between profiles on your device. So, Google has decided to modify the way containers work, making them more seamless.

With Android Work, IT will be able to install and manage apps on a user's device – they have to agree to this of course. Only, these apps will appear on the device beside personal apps and will be useable just like any other app. In the background however, the Android Work managed apps will sit in their own container. This container will apply heavy encryption to related data going in and out of the device, and restrict what users can do with the app (based on whatever rules the IT admin has set).

The key here is that while the apps and security are separate, the user will not notice any major difference and will be able to interact with both personal and business apps from the same profile. They will be able to tell the difference between work and personal apps as apps installed, managed or related to Android Work will have an identifying badge on the icon.

Easier deploying and managing of apps

With Android Work, IT admins or managers will be able to bulk purchase apps from the Google Play store and have them automatically installed on user's devices. If you use separate apps, or have developed apps for use in-house, you will also be able to push these to devices.

Beyond that, there will be admin panels that can push updates to apps on all devices, or even bulk manage existing apps. While the user will see no real difference, the apps in the Work container are managed by the administrator, not the user.

Will Work be useful?

Many business owners have been asking this question over the past few months, and the answer really depends on how you use devices in the office. If you support BYOD (Bring Your Own Device), you will be able to easily manage the apps, data, and security of just the business related apps, while still allowing personal apps and data to be installed on the same device.

Companies who provide their employees with mobile phones or tablets will also find Android Work useful as it will enable easier management and enhanced security across a variety of Android devices.

When will Android Work be available?

As of now, Android Work is still in development, but Google has noted that it will be released as a feature of the next version of Android, which is slated to be released this fall.

If you are looking to learn more about Android Work, or how to manage Android devices, contact us today to see how we can help.

Published with permission from TechAdvisory.org

Reducing Desktop Clutter

Have you ever gone to talk with a colleague and gotten a look at their computer's desktop only to notice that they have files, apps, and folders strewn about in a seemingly random fashion? Or maybe you are guilty of a cluttered desktop. Many

people tend to have somewhat unorganized desktops, especially if they have used the same computer for a number of years. The problem with this is that it can be a chore to find files and folders, and if your desktop has a ton of icons your computer could be more sluggish.

Want to tidy up your desktop? Here are six tips on how you can get your desktop more organized and even reduce virtual clutter too.

1. Before you begin do a bit of recon

Before you go about simply deleting everything off of your desktop, it is worthwhile thinking about what you really want to keep on your desktop. This will vary from person to person, of course, but most people treat their desktop as a place where they put files, folders, and app shortcuts that they want to quickly access.

Take the time to think about what you use the most and which files and folders you really need to access instantly or which you use all the time. An easy way to figure this out is to simply auto-arrange your icons by right-clicking on an empty area of your desktop (where there are no icons) and selecting Auto arrange icons. This will arrange your icons into a grid format that makes them easier to see and work with. Then, right-click on an empty space and hover your mouse over Sort by and select Date modified to order the icons by the date they were last modified, or opened, with the latest at the top.

2. Create holding and app shortcut folders

People often use their desktop to hold files like downloads, photos, screenshots, and even email attachments. This can lead to an incredibly cluttered desktop in a short amount of time.

In truth, you probably don't need all these shortcuts on your desktop. What you can do is create a folder on your desktop where all non-essential files and folders go. A folder like this is great to hold downloads or files that will only be used for a short amount of time.

The key here is this folder is used for non-important, or temporary items. If you don't plan on keeping it, put the file, icon, etc. into this folder. Once you are done with the file, simply go into the holding folder and delete it.

It could help to also create a shortcut folder. When you install new programs on Windows, a shortcut icon is often automatically added to your desktop. However, these desktop shortcuts should be for frequently used programs only. For programs that aren't really used that often, it is best to create a separate folder for the shortcuts. This not only reduces desktop clutter, but puts shortcuts in one central location, making them easier to find.

3. Be ruthless

Once you have your folders set up, it's time to start getting rid of the clutter. As with any clear-out you should be ruthless. If you haven't used a file, folder, etc. in the past two months or so, you should seriously question whether you can get rid of it.

To make this easier, open your desktop via the File Explorer. You can do this by opening any folder and clicking Desktop from the left-hand menu bar. This will make all of the icons and files on your desktop easier to see and work with.

Go through these and uninstall programs you no longer use, delete images you no longer need, move unimportant files, and place files in their relevant folders. Once complete, take a look at your browser to see where it downloads files too. If you have your browser set to download files to your desktop by default, try going into the settings and changing the download location to another file like the Downloads folder.

4. Stick with it

Once you have de-cluttered your desktop, try to stick with the rules you have set. With downloads, ask yourself whether these need to be on the desktop or whether they can go into a folder somewhere else.

Of course, sticking with it won't always be easy, so maybe take time once every month or two to revisit your desktop and clean it up a bit.

5. Use the taskbar or Start for apps, not the desktop

With Windows 8 and 8.1 you can actually pin apps to the Start menu, so when you click it the apps are available in the window that pops up. This is a great alternative to simply having program shortcuts on your desktop. Pin apps to the Start menu on Windows 8 and 8.1 by opening your apps list (clicking the down arrow from the Windows Start screen) and right-clicking on the program you would like to pin. Select Pin to Start to be able to access it when you hit the Windows key on your keyboard.

If you prefer the traditional desktop view of Windows 7, or are using Windows 7, why not pin your important programs to the taskbar at the bottom of the screen? This can be done by right-clicking on an open app and selecting Pin to Taskbar. The programs will remain at the bottom of the screen, and can be opened by simply clicking on them.

6. Strategically pick your wallpaper

An interesting way to minimize clutter is to pick a wallpaper that you enjoy looking at. Be it a favorite picture, slogan, etc., try to frame the image so the focus is in the center of your desktop. Then, place your icons around the image in a way that they still allow you to see the image. If you can't see the image, then you have too many icons and it may be time to get rid of a few.

Also, having an image you like also serves as a reminder to try to keep icons to a minimum in the first place. This could be a proactive solution to keeping desktop clutter down.

Published with permission from TechAdvisory.org.