Email File Storage

Tim Clarkin

One of the more overlooked aspects of data management in today's business environment is how email is stored and managed. Depending on your business, you may only need to refer back a few days for email, or you may need to go back months or years, at times. By following a few simple tips, you can help to make sure that you have access to the email you need without having unwanted and unneeded messages taking up extra space and hurting the performance of your email software.

The first practice that is often prone to error is how users keep data in the "Deleted Items" folder. With any mail client, whether it's Microsoft Outlook, Outlook Express, Mozilla's Thunderbird, or the Mac-only Microsoft Entourage, when you first hit the delete key to remove a message, it is moved to this folder. The idea behind it is great, since it allows users to have an extra layer of protection against acci-

dentally deleting a message and having no way to recover it. There are two problems this can create. First, users forget or fail to properly clean out their deleted items folder with any frequency. Some users can go weeks, even months, without emptying out the deleted items folder. This can lead to a situation where unwanted mail sits in a mailbox folder, taking up space and negatively impacting the performance of your computer. At a minimum, the deleted items should be cleared out once every two weeks. This way, you're allowed a little bit of time to make sure you don't accidentally delete a message or attachment you might need without having the messages continue to unnecessarily take up space for indefinite periods of time after they're no longer needed.

The second problem that can occur with the deleted items folder is that users will sometimes use the "Deleted Items" folder as a place to store important messages they might want to refer back to. When this problem occurs, it usually is the result of a user who likes to keep

his or her inbox as lean as possible. Logistically, this would be like storing documents you may want or need in a trashcan in the name of keeping them off your desk. All you're really doing is inviting a scenario where messages you may need are going to be accidentally deleted. So instead of simply soft-deleting a message that you don't need in your inbox, it makes much more sense to simply create separate folders on your email client where you can file messages to keep your inbox as neat and tidy as possible. We often suggest creating folders labeled by date or by closed or open business. You can then also have sub-folders by company name for further organization.

As always, if you have any questions regarding this or any technology issue, please do not hesitate to ask M&H for help. Our techs are all very familiar with best standards and practices for this type of work and you can certainly ask us during regular Tech for a Day maintenance appointments. You can also send us an email to support@mhconsults.com.

How to clean a laptop

Use the following information to keep your notebook looking shiny and new.

Cleaning the cover of your computer

Occasionally clean the exterior of your computer as follows:

1. Prepare a small mixture of a gentle kitchen-use detergent (one that does not contain abrasive powder or strong chemicals such as an acid or alkaline). Use 5 parts water to 1 part detergent.

2. Absorb the diluted detergent into a sponge or lint-free, soft cloth and squeeze out the excess liquid from the sponge or cloth.

3. Wipe the cover, using a circular motion and taking care not to let any excess liquid drip then wipe the surface to remove the detergent.

4. Wipe the cover with the clean sponge or lint-free, soft cloth and wipe the surface again with a dry, lint-free, soft cloth. Wait for the surface to dry completely and then remove any fibers left from the sponge or cloth.

Cleaning your computer keyboard

1. Absorb some isopropyl rubbing alcohol on a lint-free, soft cloth.

2. Wipe the key top surface with the cloth, ensuring no liquid drips on or between the keys.

3. Allow to dry.

Notes:

•*Never spray or pour any liquid cleaner directly on the LCD display or the keyboard.*

•*You can use compressed air to remove any crumbs and dust from beneath the keys.*

Cleaning your computer LCD display

1. Gently wipe the display with a dry, lint-free, soft cloth.

2. If stains remains, moisten a lint-free, soft cloth with water or a 50-50 mixture of isopropyl alcohol and water that does not contain impurities. Wring out as much of the liquid as you can. Wipe the display; do not let any liquid drip onto the computer.

3. Dry the display before closing the lid.

Notes:

•*Anti-static LCD cleaning cloths and Kim Wipes are also acceptable alternatives.*

•*Isopropyl Alcohol is a flammable liquid. Do not use this cleaner near an exposed flame or when the system is on.*

M&H CONSULTING

THE M&H MONITOR

Principle of Least Privilege

Tim Clarkin

The battle against viruses and malware infections can be a constant struggle for businesses and their employees. You can make sure you have up to date quality security software, are keeping up to date with all security updates from Microsoft and 3rd party software vendors and still you can end up with machines getting infected by malware and compromising your system. Malware and virus infections cause lost productivity, compromised security on your network, and can be costly to remove, so what extra steps can be taken to prevent infections from costing your business time and money?

The answer may lie in a recent study which analyzed every Microsoft Security patch released in 2009 and found that a large percentage of all security issues which Microsoft patched last year were issues that could have been avoided by simply exercising something known as the "Principle of Least Privilege", where computer users in a domain office environment have limited access to install programs and modify their own system under their main user account. Currently, most offices have all users set up as local administrators on their own machines, which gives the user full reign to

install programs as they see fit, but it can also leave them vulnerable to malicious software hijacking their system and using those same privileges to infect their system. Well designed malware usually doesn't take more than a few errant clicks to start infecting a system when a user is logged on with Administrator rights, but if you have users start logging on as standard users without the ability to modify their systems, you'll be protected from an overwhelming majority of the inherent software vulnerabilities that exist in various Microsoft programs before they even get patched by Microsoft.

There are some drawbacks to the principle of least privilege. For starters, you're limiting the functionality for users who might be used to (and perfectly capable of) installing software and updates all on their own. By taking away local administrator rights, you do create an extra hoop to jump through for getting software installed and updated on each system. In addition, some software will simply require users to be logging in with administrator rights in order to run properly, such as QuickBooks. There is also the simple risk of alienating your

users. While it is certainly not your responsibility as an employer to give each employee free reign over their computer, many business owners struggle with locking down computers with extra security policies (whether it's limiting user rights or blocking specific web traffic) when it may frustrate and alienate the end users.

Ultimately, the decision on how to handle user's access rights is up to each individual business owner, but rethinking current access policies can certainly go a long way in proactive prevention of virus and security related problems. With the new data privacy laws in Massachusetts, it is now more important than ever to make sure you're considering every possible way to keep your systems safe and secure. If you have any questions about what could be changed in your office set up, feel free to contact M&H Consulting at support@mhconsults.com