Take Time for Digital Spring Cleaning

Spring cleaning is almost a right of passage. With it we celebrate the renewal of life that occurs in nature each spring and eagerly await the exciting fun of summer. Traditionally, spring cleaning means cracking our windows and dusting, mopping, and vacuuming, but this year consider taking a few minutes to spring clean your digital life.

Here are a few tips for home users for refreshing, renewing, and reinvigorating your cyber life:

■ **Online Accounts** — Just like your home, your online accounts can collect clutter and occasionally need a few minutes of care. Start by considering what accounts you have online for both work and home. Chances are your accounts include email, social networks, clubs and organizations, shopping websites, cloud storage accounts, and others. Do you need them all? Is there information in those accounts that isn't needed anymore, such as credit cards saved in your accounts with shops and old documents on cloud storage accounts? Are there accounts that you don't use anymore and can close, like that old email account you never check? Are you using the same password across any of these accounts that you could easily make unique and more secure?

■ **Email Accounts** — Speaking of email, is there information in your accounts that you can archive or delete? Many email providers have limits on mailbox sizes, and for security reasons it's always smart to limit what is available through your email account. On a side note, how many emails are in your inbox – are there any you can file into folders or delete? And when was the last time you cleared out your deleted items or trash folder? Can you set a rule that will automatically empty your deleted items or trash folder on a regular basis? Unsubscribe to recurring emails that no longer interest you.

■ **Social Media** — Just like everything else, it's a good idea to spring clean your social media accounts by taking a few minutes to review your security settings, friends and connections, and posts to make sure you're still comfortable with them. Is the information on your social networking and job websites, including Facebook, Twitter, Instagram, and LinkedIn, current? Do your security settings ensure that only the authorized individuals can view what you post? Do you still use or need all of the social media sites you are registered to?

■ **Devices** — Mobile apps, just like your computer and mobile device operating system, must be updated to stay current. Criminals are constantly searching for and finding weaknesses in apps. They then develop attacks to exploit these weaknesses. The developers that created your app also create and release updates to fix these weaknesses and protect your devices. The more often you check for and install updates, the better. Most devices allow you to configure your system to update mobile apps automatically. We recommend this setting. If this is not possible, then we recommend you check at least every two weeks for updates to your mobile apps. Finally, when your apps are updated, always make sure you verify any new permissions they might require.

■ **Home Networks** — Take another moment to look at what is on your home network and how you're connecting to the Internet. Make sure your home router is secured with a complex and unique password and that it's broadcast name doesn't identify it as belonging to you. Additionally, setting up your wireless router to use a current encryption standard like WPA2 will greatly strengthen your home network security. This would also

be a good chance to see if there are additional security features you can turn on or install, such as firewalls or antivirus software.

■ **Back Things Up** — Whether you save your files to CDs or DVDs, a cloud back-up service, or an external hard drive, spring cleaning is a good opportunity to make sure you have a complete backup of important files. No matter how you're saving those files, make sure you're saving the right files and that you can restore everything from your backup, since a backup that you can't restore from isn't useful at all!

■ **Take Out the Trash** — Last, but certainly not least, take out the trash. Literally. Are there old devices in your house or office that should be recycled? If so, many towns and stores support eCycling initiatives and will help you properly dispose of them. Just make sure to remove and shred/destroy hard drives and other components that may contain sensitive data!

By taking a few minutes to include these digital areas of focus in your spring cleaning plans, you can ensure that your data and devices are that much safer.

Note: Mason employees and students can download free anti-virus software at: antivirus.gmu.edu

The information provided in the monthly newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall information security posture. Mason's IT Security Office brings you these tips produced by the Virginia Information Technologies Agency (http://www.vita.virginia.gov/security/), in coordination with: www.msisac.org and http://www.us-cert.gov/

CYBER SECURITY AWARENESS: "OUR SHARED RESPONSIBILITY"
www.msisac.org | www.staysafeonline.org | www.nascio.org | www.dhs.gov