Cyber Spring-Cleaning Tips

Neighbors! Spring is here and many of us are putting away our cold weather gear and organizing what we will put up for sale on the next neighborhood yard sale. While you’re taking the time to clean up your living environment take a few moments to focus on your digital life. This list is an aggregate of best practices from some of the top security organizations and things I do periodically to maintain my devices and accounts:

* **BACKUP your Data**. Find a trusted cloud storage platform/off site backup for your sensitive files (digital and hard copy).
* **Update Device FIRMWARE/Drivers/OS.** Your computer and mobile device receive periodic updates to maintain security and functionality but did you know your home router, Smart TV and other internet of things (smart devices) need to be updated? Check your device user guide or consult the company on steps needed to keep your smart devices secure!
* **Change your passwords!** It’s a good idea to change your passwords from time to time. Security organizations such as SANS recommends 90 days while others recommend 180 days. Data breaches happen all the time and without warning. Check out <https://haveibeenpwned.com/> to see if any of your accounts have been compromised. ***Also…DO NOT USE THE SAME PASSWORDS FOR DIFFERENT ACCOUNTS!!!*** Each account should have a unique strong password. Check out a password manager such as LastPass to help organize the multitude of passwords you have to memorize.
* **Secure your accounts.** While changing your passwords look to see if there are advanced login options such as multifactor authentication.
* **Refresh/update Social Media Settings.** Updates to Facebook, Twitter, LinkedIn, Instagram, etc can change privacy /account settings on your account. Go through your settings to make sure you’re not exposing sensitive data to the public or your contacts. For example, turn off all location-based settings and opt out of any marketing/advertisements.
* **Refresh your Social Media Presence.** While you’re modifying your settings go ahead and fine tune your social media profiles. Delete contacts you no longer keep up with and remove questionable pictures/posts. Some employers do a deep dive on candidates and make final decisions based on their social media presence.
* **Check App Permissions.** Go through your mobile apps and verify permission settings have not been altered. Give apps the bare minimum features to function. For example – Facebook does not need access to your contacts, camera, or gallery for it to work.
* **Delete accounts you no longer use.** If you have an old/dormant account that you no longer use, your data (Personally Identifiable Information, credit card, etc) is still being managed by that organization – Just delete the account to minimize your exposure to a data breach.
* **Delete apps you no longer use**. We often download apps for a specific use such as travel, shopping, etc. If you don’t need it – delete it! (just delete the information in that account before you delete the app)
* **Update /clean your internet browser.** Purge browsing history, delete cookies, remove autofill data, and remove stored passwords or payment information.
* **Maintain your antivirus software.** All devices (MAC, iOS PC, Android, Linux) can be hit by malware. Find a reputable antivirus suite (do your research and don’t pick the free ones) and make sure your devices are secure.
* **Delete/Purge old files.**  Go through your PC, Laptop, Mobile Device and delete files you no longer use. ***The same goes for your email inboxes*** – backup what’s important and delete old emails. Make sure you purge the trashcan. Also take note on what your company policy is on deleting work related data. Some companies have data retention policies – do not violate those!

**John Higgins, CEH**