

OUCH!

The Monthly Security Awareness Newsletter for You

Digital Spring Cleaning

Overview

Most of us are so looking forward to spring! The landscape starts to take shape, flowers start to bloom, and, for many, there's a desire to spring clean. While it might be easy to see the need to purge and tidy up, realizing the need to also digitally declutter isn't so apparent. Here are some quick tips to get your digital life in order and establish new digital habits:



BACKUPS: We listed this step first because, in the long run, it's one of the most important and a step you want to take before moving on to the others. No matter how safe or secure you are, at some point, you will most likely need backups to recover your important information. Reasons can include having a hard drive fail, losing a device, and becoming infected with malware such as ransomware. Creating and scheduling automatic backups ensures you can recover your most important information.



DELETE: Delete any unused programs or apps on your mobile devices and computers. Some apps require large amounts of storage, can introduce new vulnerabilities, and may even slow things down. The fewer apps you have, the more secure your system and your information. Many devices show you how long it has been since you've used an app—if it has been more than a few months, chances are you don't need the app!



UPDATE: Update all of the devices and apps you do have, and enable automatic updating whenever possible. This way, your devices and apps stay current, not only ensuring they run faster but making it much harder for anyone to hack into them.



PASSWORDS: Review your passwords. If you are using the same passwords for multiple accounts, change them so each account has a unique password. Can't remember all your unique passwords? Consider using a password manager. Finally, enable two-factor authentication (2FA) whenever possible, especially for any email or financial accounts.



FINANCIAL ACCOUNTS: Make sure your bank accounts, credit card accounts, and retirement accounts are configured to alert you whenever a transaction is made, especially for large purchases or money transfers. The sooner you spot fraudulent activity, the sooner you can stop it. Depending on what country you live in, a credit freeze can be one of the most effective ways to protect your identity.

...

BROWSER: Review any and all add-ons or plugins installed in your browser. Review the permission settings; do the plugins really need access to your location, passwords, or contact lists? If you are no longer using certain plugins, or have privacy concerns about them, delete them.



SOCIAL MEDIA: Check out your online presence and own it. Review your privacy settings and delete any photos and videos that are no longer accessed or needed. You can also search for yourself on a search engine and see what information is out there about you. Remember, it's fine to limit how much information you share, and even with whom you choose to share it with.



DESK: Clean out your desk drawer, wipe any old hard drives and USBs, and perhaps even destroy any sticky notes with too much information. Consider investing in a document shredder if you don't have one.



EMAIL: Perform an email file purge, delete what you don't need, and organize what you do. Pay particular attention to any sensitive documents, such as those with your date of birth or Social Security number, and get those out of your inbox!

While this may appear to be a daunting task, rest assured your devices and information will be far more protected. If this seems like a lot to do, consider choosing just a few items, or try to check off one item per day or week. Every little step goes a long way in protecting you.



Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.

Do you think you've got what it takes to get into the cyber security industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

Guest Editor

Katie Nickels ([@LiketheCoins](https://twitter.com/LikettheCoins)) is a Principal Intelligence Analyst with Red Canary as well as a SANS Instructor for FOR578: Cyber Threat Intelligence. She has worked in network defense, incident response and cyber threat intelligence for over a decade.



Resources

- Got Backups: <http://www.sans.org/u/ZVr>
- Making Passwords Simple: <http://www.sans.org/u/ZVw>
- Search Yourself Online: <http://www.sans.org/u/ZVB>
- Disposing of Your Mobile Devices: <http://www.sans.org/u/ZVG>

OUCH! is published by SANS Security Awareness and is distributed under the [Creative Commons BY NC ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley