

From the desk of
Michael Aliperti
MS ISAC Chair

2021 Cybersecurity Spring Cleaning Checklist

Spring is not just a good time for cleaning your house or apartment, it's also a good time to clean up your technology and cyber footprint.

Throughout the year, especially around the holidays and during tax season, you extend your cyber footprint by paying bills, shopping, using social media, and many other digital activities whether for business or pleasure. Spring cleaning your space is meant to improve the air quality after having it closed up all winter, and cleaning can improve your mood and remove a year's worth of clutter. Cleaning your technology and cyber footprint can do the same thing; it removes clutter from your life while at the same time protecting you and your loved ones.

While spring cleaning, you often make a list to ensure you don't forget to clean the spots you don't normally think about, like behind the sofa or on top of the fridge. To help you spring clean your technology and cyber footprint, we have developed a checklist to help you through the process. And just like spring cleaning your house, you can assign these tasks to your family.

Passwords

- Review your passwords, updating them as needed, and ensuring they are strong.
- Establish a unique password for each account.
- Consider using a [password manager](#) if you haven't in the past.
- Remember to use Multi-Factor Authentication (MFA) on accounts wherever it is available, especially on accounts that have financial information such as online banking, credit card, and retirement accounts.

Email

- Review all your email accounts.
- Organize folders of emails that you want to keep, delete and purge emails that you no longer need.
- Be sure that there is no personally identifiable information stored in your mailbox.
- Review and update your contacts. Delete contacts that are no longer necessary or current.
- Review and update email filters to send spam and unwanted e-marketing messages directly to trash or another folder.
- Enable MFA whenever possible

Stale Applications

- Review your applications and remove those you no longer use.

Social Media

- Review social media accounts and associated privacy settings.
- Review any photos or videos and delete those that you no longer need or want to make viewable.
- Search yourself online to see what comes up.
- Don't just delete a social media app that you're no longer using, delete your entire profile.
- Be sure you are familiar with the privacy settings in your social media accounts.
- [CISA Social Media Cybersecurity Tips](#)

Closing Accounts

- Close out old application or system accounts that you are no longer using.

Clean Desk

- Shred old and unnecessary paperwork.
- Ensure paper documents that contain personally identifiable information, financial information, or other sensitive information is properly stored and locked up.
- Don't write down passwords or security answers on paper and leave them out.

Backups

- Review your backup routines.
- Review your backup schedule, and what you're backing up.
- Test your backups and validate they are being successfully completed.
- Make sure you can restore from a backup.
- Review your backup location and media.

Update Devices

- Make sure all applications, operating systems, and devices (computers, phones, tablets, smart devices, TVs, etc.) are updated, and are set to update on a regular basis.

Disposal

- Properly shred or destroy all unnecessary paper documents or files.
- Dispose of old electronic equipment (laptops, monitors, phones, tablet, smart devices, etc.)
 - [NIST 800-88](#)
 - Leverage e-recycling programs in your area.

Cleaning can be a very satisfying process. If cleaning is not normally your idea of a good time, we hope that you'll find this technology and cyber spring-cleaning checklist a way to speed up the process. Have fun getting rid of some clutter, and don't forget to have your kids clean under their beds!



The information provided in the MS-ISAC Monthly Security Tips 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 cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.
