State Privacy Office
April Privacy Tip

Spring Clean Your Online Life

A sloppy digital life can make your data harder to find and leaves your personal information vulnerable to bad actors. With a few steps, you can keep yourself and your family safe online with a squeaky clean digital life. While you don't have to clean your digital workspace and online presence in the spring, it is wise to declutter at least once a year.

1. CLEAN UP YOUR PASSWORDS AND FIND A PASSWORD MANAGER

Chances are you have some old, unsecured passwords that need to be cleaned up or you are using the same password for multiple accounts. If the idea of going through every website you use seems overwhelming, download a password manager. Not only do password managers store passwords and suggest strong ones, but the best options alert you if you're using a duplicate or weak password, and prompt you to change it. Even better, many are free. Firing up a password manager is a great way to toss out unsecured passwords and replace them with fresh, strong ones.

Get started:

Check out reviews of popular password managers from Consumer Reports, Tom's Guide, CNET, or your preferred review site, to find the right password manager for you.

2. ENABLE MULTI-FACTOR AUTHENTICATION

Guarding your key accounts with multi-factor authentication (MFA) is a quick and easy way to stay safe online. MFA is a security feature that requires two types of credentials when logging into an account; such as a facial scan or a unique, one-time code sent through an app on another device. MFA builds another layer of protection to your accounts and alerts you if someone tries to log in. This ensures your data is protected, even in the event of a data breach.

Get started:

Ensure multi-factor authentication is set up on accounts with very sensitive information, including: email accounts, bank accounts, credit card accounts, and social media accounts. Consider enabling MFA on any account that permits it, especially ones that store personal information or credit card data. This includes retail accounts and delivery apps.

3. CHECK APP PERMISSIONS

Review privacy and security settings on all accounts you use. Consider shutting down accounts on any app you don’t use. Check to see if your apps and services have access to information that is not required or relevant for the services they are offering, such as your location, contacts, and photos.

Get started:

Check out NCA’s Manage Your Privacy Settings page to check the settings of social media accounts, retail stores, apps and more.

To find a list of downloaded apps on your phone, follow these steps:

For iOS users:
Go to your settings app -> Scroll to the bottom to see a list of all downloaded apps
To check which apps have access to your camera, microphone and location, go to Settings -> Privacy for complete lists of apps

For Android users:
Go to your settings app
Select Apps & Notifications -> See All Apps
To check which apps have access to your camera, microphone and location, go to Settings -> Privacy -> Permission Manager for complete lists of apps
Don’t need it? Delete it. While reviewing your apps, delete apps you don’t need. Uninstalling apps from your phone not only declutters your home screen but ensures that your data is not being shared with apps you no longer use.

4. UPDATE YOUR SOFTWARE AND SET AUTOMATIC UPDATES

Software updates shouldn’t be ignored because they usually include important security improvements that protect your devices against the latest cybercriminal tactics.

Get started:
Check your browser, laptop, phone and other devices for available software updates. Step away from the “Remind Me Later” button. You can usually change your settings to automatically install updates.

5. BACK-UP YOUR DATA

Protect your data by making copies of your important files and storing them in a separate, secure location. Back up photos, videos, documents and any other file you don’t want to lose in case a device is lost, stolen or breaks down. You should back up your data frequently, ideally at least once a week.

Get started:
Use the 3-2-1 rule to help guide you:

Keep 3 copies of your important data (this includes the original copy and two backup copies)

Save your backup copies on 2 different media types (such as the cloud, a USB, or an external hard drive)

1 of those media types should be kept in a separate location, either online in the cloud or secured in another room or building

6. SECURELY DISPOSE OF OLD DEVICES

When you're cleaning, take any old devices and electronics to an e-waste recycling location. Don't throw your electronics in the trash – not only is it bad for the environment, but you also don't know who will find them once you get rid of them.

Get started:

Take an inventory of any electronics you don't need. Some recyclable items include laptops, phones, tablets, hard-drives, TVs, appliances, printers, gaming consoles.

Your old tech probably contains a lot of old data and personal information. It's not enough to just delete your data. You must wipe it from your devices. Perform a factory reset on your phone or other devices where applicable. Remove any memory cards or hard drives. Consider using disk cleaning software on your computer. Learn more from the Cybersecurity and Infrastructure Security Agency

Once you've wiped all data from your devices, use the following resources to find local recycling centers: Best Buy, Environmental Protection Agency Guide, and many local governments run e-waste recycling programs. Check with your municipality to see if they have any upcoming recycling events.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*