While you’re spring cleaning your physical spaces, make sure you purge your digital spaces of clutter that can make you easy prey to identity theft and cybercrime.

NOTA BENE: These tips are for at-home use only. Refer to official UCOP and UC Davis Health backup, disposal, and retention policies for at-work guidance.

Spring Cleaning: Time to Clear Your Digital Clutter

Just like your home, your digital life can become cluttered: things pile up, get out of date, get lost, or are no longer needed. External hard drives and USBs, phones and tablets, wearables, networking equipment, smart home devices (such as light bulbs, smart plugs, and hubs), and office tools like copiers, printers and fax machines all contain valuable personal information.

A good digital spring cleaning can reduce the risk of cyber criminals accessing old information that could help them figure out how to get to your new information. It can also help improve the speed and performance of the devices and services that you use.

To get started, make a list of all devices where you store personal information. Then perform complete backups on each device. Follow the tips on the next page to make sure that your digital spring cleaning is complete.

Here is a handy checklist to keep you on track.

☐ Back up all locations where you store personal information.
☐ Purge files on desktops, laptops, and hosted/cloud services.
☐ Clean up mobile devices.
☐ Safety-check web browsers.
☐ Review email and other online accounts.

Learn more: https://health.ucdavis.edu/itsecurity/
Purge Files on Desktops, Laptops, and Hosted/Cloud Services

- Perform a thorough review of your digital file locations with a focus on personal records.
- Delete or archive multiple drafts of the same document, outdated financial statements, unused apps, and downloaded files.
- Empty your trash or recycle bin on all devices: Make sure to securely and permanently delete old files.
- Learn more at https://health.ucdavis.edu/itsecurity/.

Clean Up Mobile Devices

- Delete unused apps.
- Update operating system and apps.
- Review location services, Bluetooth, microphone, and camera settings for all apps.

Safety-Check Web Browsers

- Review all browser security settings to make sure that they are still keeping you safe.
- Delete sensitive information from autofill settings and turn off automatic capture of your form entries.
- Remove saved passwords and disable automatic password storage.
- Uninstall seldom-used browser applications. Only maintain one or two browsers that work well with most websites.

Review Email and Other Online Accounts

List all online accounts including Email, social networking services, and other accounts that require a username and password to access them.

- Close accounts that you no longer need.
- Remove outdated credit card and contact information.
- Remove contacts on social networks that you don’t personally know.
- Delete or archive old emails and empty your email trash.
- Unsubscribe from newsletters, email alerts, and other automatic emails that you no longer read.

Backup Checklist

- Wherever you store personal files and information, make sure you have a complete backup before you start purging. The best backup mechanisms have an incremental setting that allows you to return to a specific version of a file even after you have changed or deleted it.
- Regularly test your backup system to make sure that you can access accurate versions of restored files.
- Password protect physical backup drives and store them in a safe deposit box or fire- and water-proof vault for maximum security.
- Maintain copies of important data in a secure cloud site where you can access it if physical drives are destroyed or compromised.
- Configure your backup system to automatically perform regular backups.

NOTA BENE: These tips are for at-home use only. Refer to official UCOP and UC Davis Health backup, disposal, and retention policies for at-work guidance.