July 2019
Volume 14, Issue 7

Cleaning Out Your Old Data and Devices

WV Executive Branch Privacy Tip

Over the years, many of us have accumulated a mountain of CDs, hard drives, devices, online accounts, and other mediums that store information that are out there and unused. Outside of the key information you kept stored on purpose for long term use or retrieval, it is good to periodically assess and dispose of unneeded storage media and information. These days, information may be split between physical items you have in your possession and online accounts or cloud-based storage. This month's guide will provide some details on how to manage your information and data, as well as how to safely dispose of those pieces you do not need any longer.

Cleaning up Online Accounts and Cloud Storage:

Clean your social media presence: It may have been years since you logged into an old social media platform that you no longer use. If that's the case, consider removing any personally identifiable information like address, date of birth, and other less sensitive details from the account. Furthermore, consider closing the account entirely if you don't think you'll have reason to use it anymore. The fewer places you have personal information stored online, the better!

Keep your social media presence clean: On social media accounts that you still use, minimize the amount of personal information that you display. In particular, minimize how visible your information is to any untrusted individuals. This is especially important as those who are not approved to be your friend or contact on the platform will be less likely to view your personal information. Most sites offer this as a privacy option in the settings for your account.

Close old shopping and rewards accounts: If you do not plan on shopping on a particular site, please consider removing any payment or personal information and closing the account. If you rarely shop on a web site, consider if it's necessary to maintain a user account. Most retail sites have a guest account option for temporary use and lessens the likelihood of your information being saved.

Cloud storage and files: Many of us use cloud storage services of some sort, whether just for storing our photos from our devices, or for backing up and storing important files. Consider clearing out data and information periodically from these storage accounts that you will not need access to in the future.

Physical Storage – Digital and Paper:

CDs, DVDs, Floppy Disks, and other plastic disk media: CD and DVD discs can be shredded in many common household paper shredders (check to ensure your shredder is rated for this). After validating if you need the information or not, consider this best and irreversible method for destroying the unneeded information and the medium. Floppy disks (if you still have any!) can be destroyed by splitting open the plastic casing,

removing the soft disk itself, popping out the metal hub, and then feeding the soft disk without that metal center into a household paper shredder.

Hard disk drives, Solid State Drives, and USB flash drives: When you are looking to get rid of an old computer (or other device with a hard drive) that you perhaps don't use anymore, you should properly clean your data off the device before disposing of it or selling/donating it. You will want to ensure you properly move those family photos, important records, and everything else you want to keep onto a newer device or a disk/thumb drive before beginning the process of cleaning the data off. Next, you will want to either physically destroy the drive or perform the proper process of overwriting by using a utility to permanently erase the data. For physical destruction of drives, either utilize a paid service to properly destroy the device, or follow the US-CERT guidance linked below. For overwriting or permanent erasure of data, there are many software utilities available to perform these operations, some of which may be included with your operating system. US-CERT also provides guidance on some utilities and ways to do this properly. It is important to follow this guidance because simply moving files to the recycle bin or hitting delete doesn't make them permanently as the information can be easily recovered if that's all that has been done! This means your sensitive data is still possibly available to a malicious actor.

Smartphones, Tablets, Gaming Consoles, and other devices: Perform a "hard reset" which will bring the device back to factory settings and remove your data securely. Always ensure no accounts are permanently logged in on the device. You can consult the maker of the device when seeking guidance on how to locate this setting or utility for that particular make and model.

US-CERT Guide on Destroying Devices/Data: https://www.us-cert.gov/ncas/tips/ST18-005

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

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.

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