107 Isabella Drive
Orillia, ON L3V 8K7
705-955-8574

CLEAN YOUR DIGITAL LIFE

Many of us are familiar with the concept of spring cleaning. This year, consider taking some time to spring clean your digital life, too. Just like your home, your digital life can become cluttered; things pile up, get out of date, get lost, are no longer needed or need some care.

A good digital spring cleaning can help keep your devices and information safe and secure year-round. It can also help improve the speed and performance of the devices and services that you use and reduces the risk that a hacker could access old information that you've forgotten about.

Here are a few tips for refreshing, renewing, and reinvigorating your cyber life:

1. **Review your online accounts.**
    1. Delete any you no longer use.
    2. Remove information in any of your accounts that isn't needed anymore, such as saved credit cards or old documents in cloud storage.
2. **Update your devices.**
    1. Update the apps and operating system on all Internet-connected devices – including PCs, smartphones, tablets, home wifi routers, smart TVs, and other internet-connected devices that can be updated – to reduce risks from malware and infections.
    2. Delete unused apps.
3. **Tune up web browsers.**
    1. Check your browser settings. Clear out old data, such as stored passwords and old autofill information, and ensure your browser is set not to store passwords.
    2. Delete unused browsers.
4. **Purge old digital files.**
    1. Clean out your old email, files, and downloads. Always empty the trash when you're done.
        1. **Keep your business retention in mind when purging work files!**
    2. Unsubscribe from newsletters, email alerts and mailing lists you no longer read.
5. **Lock down your login.**
    1. Use a password, passcode, fingerprint, or facial recognition to log into all of your devices. Enable the strongest authentication tools available.

gail@webdezynplus.ca
www.webdezynplus.ca

2. Turn on multi-factor authentication – also known as two-step verification or two-factor authentication – on critical accounts like email, banking and social media where available. Learn more by visiting https://stopthinkconnect.org/campaigns/lock-down-your-login
3. Take an inventory of your passwords. Are they all long and strong? Change any that aren't.
4. Use a unique password for each account.
5. Consider using a password manager to store and protect your passwords.

6. **Refresh your online presence.**
    1. Review and update your online profiles on social media sites.
    2. Review your privacy and security settings on social media sites and other sites you use. Set them at your comfort level for sharing.
    3. Delete old photos, posts, etc. that are embarrassing or no longer represent who you are.
    4. Review friends on social networks and contacts on phones and other devices. Does everyone still belong?
    5. Actively manage your location services, Bluetooth, microphone and camera – making sure apps use them appropriately.

7. **Back up your files.**
    1. Make a complete backup of important files. Copy important data to a secure cloud site, another computer or external hard drive where it can be safely stored. Password protect backup drives.
    2. Back up your files before disposing of a device.
    3. Be sure you can restore the files from your backup; a backup that you can't use isn't very helpful!
    4. Keep UC security requirements in mind if you make your own backups of work files. Contact your IT department for assistance.

8. **Dispose of electronic devices securely.**
    1. Inventory your devices and media, and take the following steps:
        1. Securely dispose of electronic information you no longer need, just as you would shred sensitive paper information. Anything that has the ability to store information can retain that information even after you have deleted it, including ones that aren't obvious, such as phones, wearables, networking equipment, copiers, printers and fax machines.
        2. Thoroughly wipe all electronic devices or have them shredded by a trusted vendor before disposal.
        3. Contact your IT department for information about secure data or device disposal.