Cyber Byte

Cyber Spring Clean Your Personal Accounts

This year is first time since 1896 that spring has started so early. So why not continue with some early Cyber spring cleaning and de-clutter your data whilst improving your online security.

A digital spring clean can help keep your devices and information safe and secure. It can also help improve the performance and speed of devices and reduce the risk that a hacker could access old information that you've forgotten about.

Here are a few tips to support your Cyber spring clean.

Review your online accounts.

- ✓ Delete accounts you no longer use.

- ✓ Remove information in any of your current accounts that isn't needed anymore, such as saved credit cards which are expired or old documents in cloud storage.

Update your devices.

- ✓ Update the apps and operating system on your internet-connected devices – including PCs, smartphones, tablets, home wi-fi routers, smart TVs – to reduce risks from malware and viruses.

- ✓ Deleting unused apps is another positive thing to do and will also free up storage space.

Refresh browsers.

- ✓ Check your browser settings. Clear out old data, such as stored passwords and old autofill information.

- ✓ Delete unused browsers and browsing history.

Throw out your trash.

✓ Many of us forget to empty trash or recycling bin on our devices. The recycling bin is a storage area all of its' own which, if not cleared out, also takes up valuable storage space. So when you clean out your old emails, files and downloads, always empty the trash or recycling bin when you're done. Also remember your spam folder – delete filtered mail from there as well.

✓ Unsubscribing from newsletters, email alerts and mailing lists you no longer require also contributes towards decluttering your email inbox.

Lock down your login.

✓ Use a password, passcode, fingerprint, or facial recognition to log into all of your devices.

✓ Turn on 2SV (two-step verification) or two-factor authentication – on critical accounts like email, banking and social media where available. Setting up 2-Step Verification (2SV) - NCSC.GOV.UK

✓ Review your passwords. Are they strong? Change any that aren't and use a unique password for each account using "Three random words". Three random words - NCSC.GOV.UK

Review your online presence.

✓ Review and update your online profiles on social media sites and include a review of your privacy and security settings on these and other sites you use. Set them at your comfort level for sharing.

> ✓ Delete old photos, posts, etc. that are embarrassing or no longer represent who you are.
>
> ✓ Review friends and contacts on social media platforms. Does everyone still belong to your group?
>
> ✓ Actively manage your location services and access that apps ask for such as photos, microphone and camera – make sure apps use them appropriately or consider only allowing apps to use your location when you are using the service the app provides.

Back up your files.

- ✓ Make a complete backup of important files. Copy important data to a secure cloud site, another computer or external encrypted hard drive where it can be safely stored. You should also password protect your back-ups.

- ✓ Back up your files before disposing of a device and ensure all data is deleted.

- ✓ Be sure you can restore the files from your backup; a backup that you can't use isn't very helpful!

Dispose of electronic devices securely.

Make sure you know where all your devices and media are, especially those you don't use anymore but which might still contain your personal data and take the following steps:

- ✓ 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, networking equipment, copiers and printers.

- ✓ Erasing devices - NCSC.GOV.UK

Doing a refresh of your data and devices will take you a bit of time to attend to. So, take your time and carefully consider what you are keeping and deleting.

If you need support with this, ask a trusted friend or seek independent advice.

Additionally the following link will take you to the Cyber Scotland Partnership website; Cyber Aware – Cyber Scotland for further supporting guidance.