# Spring into Action: A cybersecurity checklist

**Image:** Included in toolkit.

**Suggested Alt Text:** Woman using a laptop and the screen showing a padlock.

Consider de-cluttering your digital life this spring with these tips and resources. Taking a few of these proactive steps can help safeguard you from cybercriminals.

* **Lock Down Your Login.** One of the first things everyone needs to do is to ensure that [passphrases for each account are lengthy, unique, and safely stored](https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/). Enable 2-factor authentication on all accounts that offer it.
* **Update Your Software.** Don’t postpone critical software updates. Having the most current security software, web browsers, and operating systems are some of the easiest ways to protect your data.
* **Back IT Up.** Protect your data by making copies – or [backups](https://staysafeonline.org/resources/back-it-up/) – of your most important files. Use the 3-2-1 rule to help guide you: 3 backup copies, 2 different media types, 1 offline, and in a separate location.

**Your Digital De-Clutter Checklist**

* Uninstall software and apps you are no longer using.
* Establish and communicate records retention guidelines for your digital and physical records. Permanently and securely dispose of all old or unnecessary data.
* Unsubscribe from newsletters, email alerts, and updates you no longer read.
* Securely dispose of any old devices, including hard drives, laptops, tablets, copy machines, fax machines, etc. Check to see if there is a Secure Your ID Day or similar event in your area. Many “Shred Day” events include the safe destruction of electronic equipment and files as well. The Cyber Security and Infrastructure Security Agency has prepared some [specific tips for the secure disposal of electronic devices.](https://www.cisa.gov/uscert/ncas/tips/ST18-005)
* Do a data assessment. [Analyze what data your business collects and stores](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business). Assess whether you actually need that information for a legitimate business purpose. If you don’t, then safely dispose of the information and stop collecting it.

**Clean Up Your Online Presence**

* Own your Online presence by reviewing the privacy and security settings. You should do this for both business and personal accounts. Delete old or unnecessary media and accounts that are no longer in use.
* Control your role by reviewing and limiting who has administrative access to your Online accounts. Grant access only to individuals who absolutely need it.

**Stay Cyber Aware**

* Beware of Phishing. Phishers try to trick you into clicking a link that may result in a security breach.
* Think before you click. More than 90 percent of successful cyber attacks start with a phishing e-mail. Commonly leading to identity theft, malware, and ransomware attacks.

**Make a Security Plan**

Take the time to develop your own cybersecurity strategy. Always review and update the strategy to remain cyber-safe.

**Additional Resources**

* [US Department of Veterans Affairs Phishing Awareness](https://digital.va.gov/security-excellence/hook-line-and-sinker/)
* [National Cybersecurity Alliance’s CyberSecure My Business website](https://staysafeonline.org/programs/cybersecure-my-business/)
* [The Better Business Bureau’s 5-Steps to Better Business Cybersecurity](https://www.bbb.org/article/news-releases/20833-the-5-step-approach-to-cyber-security)