

Concise Privacy Tips:

Share With Care

- **What you post can last a lifetime:** Before posting online think about how your post might be perceived now and in the future and who might see it.
- **Own your online presence:** Set the privacy and security settings on web services and devices to your comfort level for information sharing. It's ok to limit how and with whom you share information.
- **Be aware of what's being shared:** Be aware that when you share a post, picture, or video online, you may also be revealing information about others. Be thoughtful about when and how you share information about others.
- **Post only about others as you would have them post about you:** The golden rule applies online as well.

Personal Information Is Like Money. Value It. Protect It.

- **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- **Think before you app:** Information about you, such as the games you like to play, your contacts list, where you shop, and your location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps.
- **Get two steps ahead:** Switch on two-step verification or multi-factor authentication wherever offered to prevent unauthorized access.
- **Lock your devices, like your tablet and phone:** You lock the front door to your house, and you should do the same with your devices. Use strong passwords or passcodes to lock your tablet and phone. Securing your devices keeps prying eyes out and can help protect your information in case your devices are lost or stolen.

Good Technology Practice

- **Keep a Clean Machine:** Having the latest security software, web browser, and operating system is the best defense against viruses, malware, and other online threats.
- **Make Better Passwords:** A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.
- **When in Doubt, Throw It Out:** Links in email, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- **Plug & Scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

- **Encrypt Private Data:** Use encryption to protect laptops, USBs, or external devices that contain private data to protect it in case of theft or loss.

Additional Resources: <https://staysafeonline.org/>