

Stay Safe Online

Cristina Graur
Student ID: 2332971



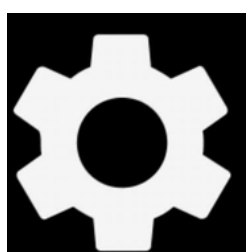
ENSURE YOUR PASSWORDS ARE UNIQUE.

Always use passwords that are long and not easy to guess, and keep them safe using a password manager or write them down in a safe place.



BEWARE WHAT YOU CLICK WHEN ON LINE.

Don't download any information from websites that cannot be trusted. These may contain viruses and malware. Check website credibility on <http://check.getsafeonline.org>



CHECK AND TURN ON PRIVACY SETTINGS.

Be the one in control of your data and how you want to be used by others by enabling privacy feature



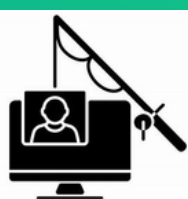
THINK TWICE BEFORE YOU POST SOMETHING ON SOCIAL MEDIA.

Don't share sensitive personal information online.
Oversharing information may expose you to physical harm.



ALWAYS USE AN ANTI-VIRUS PROGRAM ON YOUR COMPUTER.

Make sure you turn on your anti-virus software and you keep it up to date so it can detect any potential malware in your system.



ALWAYS REPORT PHISHING.

Don't disclose your personal details such as usernames, bank details and passwords by email, don't open any links sent by email from unknown recipients and report any phishing immediately.

References:

Reedy, K. and Parker, J. (eds.) (2018) Digital literacy unpacked. London: Face
<https://staysafe.org/10-tips-to-stay-safe-online>
<https://check.getsafeonline.org>
www.bing.com/images
www.cyber.gov.au;
<https://www.canva.com>; <https://www.gov.uk/guidance/phishing-scams-how-you-can-avoid-them>