

KEEP IT PRIVATE!

STAYING SAFE ONLINE: TOPS TIPS



STRONG PASSWORD

A strong password reduces the risk of unauthorized access to your accounts, remember to avoid using the same password for multiple accounts and change it every three months.



PHISHING ATTACKS AND SCAMS

Fake emails may appear to be legitimate at first glance, maybe a business communication or even a message from your boss. In some cases, they may promise you an offer. If you have any doubts reach out to IT department never share your personal details!



SOCIAL MEDIA

Be mindful of the information you share on social media platforms. Ensure that the content you post is only visible to people you know. Sharing personal information can potentially compromise your privacy and security. Keep it private!



PROTECTION

It is essential to ensure that you regularly perform software updates and operate reliable antivirus software. By doing so, you can enormously enhance the security of your devices and protect your personal information. Make sure you are connected to a secure wifi network.

Reference List:

- Lyons, S. (2021) *National Cyber Security Center*, British Government, Available at <https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available> (Accessed: 21 November 2023)
- Guest, D. (2010) *University of Sussex*, Available at: <https://www.sussex.ac.uk/its/help/guide?id=100> (Accessed: 22 November 2023)
- Harrison, R. (2016) *Cyber insecurity: navigating the perils of the next information age*, p. 46 p.67, Rowman & Littlefield Publishers, Available at: <https://www.vlebooks-com.ezproxy.uwtsd.ac.uk/Product/Index/936923?page=0&startBookmarkId=-1> (Accessed: 22 November 2023)