

Basic Digital Safety

Zallio and Clarkson (2022) highlighted that digital safety is the only way to stay safe online. Some essential tips to stay safe online can be found here.

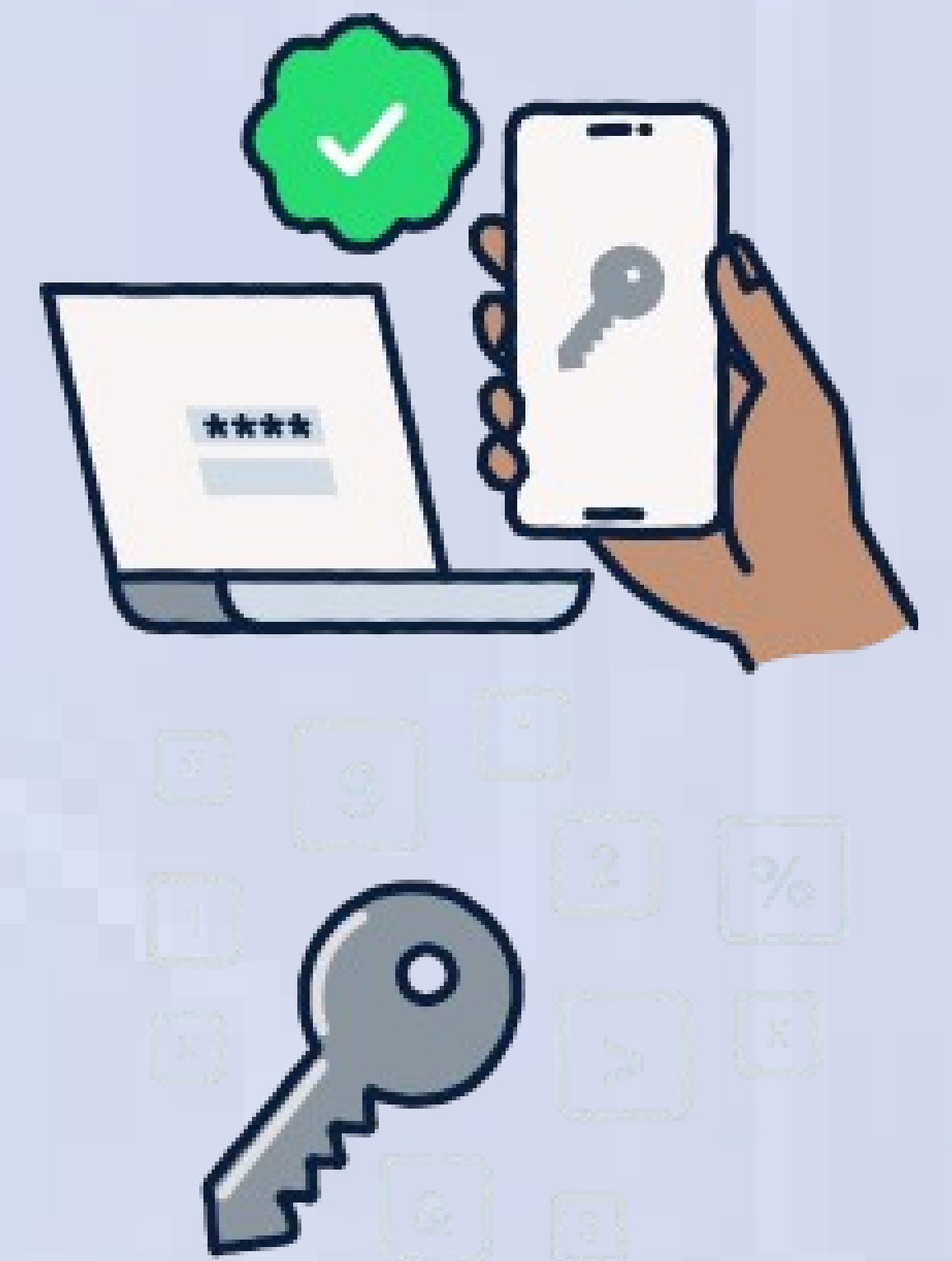
Passwords & 2 Factor Authentication

1. Use Strong and Unique Passwords:

According to Yildirim and Mackie (2019), using mixed letters, numbers, and special characters to create passwords is the most fundamental way to ensure digital safety. Never use something like a birthday or name. A good practice is to use a password manager to store and secure unique passwords for every account, which can be used in an organised way.

2. Enable Two-Factor Authentication (2FA):

Enabling 2FA also adds another layer of security, adding a second follow-up verification step, such as sending a code via phone or email. It decreases the risk of unauthorised access (Amft, 2024).



Phishing Scams & Regular Updates

3. Beware of Phishing Scams:

Do not click suspicious links in emails or messages from unknown senders. Share personal information only after you verify the source.

4. Update Software Regularly:

Keep operating systems, apps, and antivirus software updated. Most updates that are installed contain security patches to prevent the newest threats.



Limit Public Wi-Fi Use

5. Limit Public Wi-Fi Use:

Sombatruang et al.'s (2018) discussions suggest not opening sensitive accounts or conducting financial transactions on a public Wi-Fi network. Occasionally, a secure connection can be established using a virtual private network (VPN).



Account Monitoring and Social Media Involvement

6. Be Cautious on Social Media:

Set the privacy settings so that people can see or not see your posts and personal information. Guard the digits before sharing sensitive details online.

7. Monitor the Accounts:

It is essential to regularly check your bank statement and online accounts for unauthorised activity and immediately report any suspicious transactions.



These practices, when adopted and used properly, help one protect the digital presence and diminish the threat of cyber-attacks.

References:

- Amft, S.M., 2024. On the usability of authentication security communication.
- Sombatruang, N., Kadobayashi, Y., Sasse, M.A., Baddeley, M. and Miyamoto, D., 2018, August. The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In 2018 16th annual conference on Privacy, Security and Trust (PST) (pp. 1-11). IEEE.
- Yildirim, M. and Mackie, I., 2019. Encouraging users to improve password security and memorability. International Journal of Information Security, 18, pp.741-759.
- Zallio, M. and Clarkson, P.J., 2022. Designing the metaverse: A study on inclusion, diversity, equity, accessibility and safety for digital immersive environments. Telematics and Informatics, 75, p.101909.