safe on social
education and consulting

www.safeonsocial.com

Essential Cybersecurity Tips

Be cautious when clicking on links or opening attachments. Even if an email appears from someone you know, exercise caution with attachments. Take that extra moment to avoid entering a potentially harmful digital situation. Don't reply to the email, as the sender's identity could have been compromised.

Confirm requests for personal information. Whenever you're asked to provide personal information (yours or someone else's), verify the identity of the requester—even if they seem to be someone you know. Scammers are skilled in gathering information to steal identities. Regularly check your financial statements and credit reports, even if you believe you're safe.

Safeguard your passwords. Never disclose your passwords to anyone. Make them lengthy, robust, unique and utilise multi-factor authentication (MFA) where possible. Consider using a password manager like LastPass or RoboForm. Create distinct passwords for various accounts. Use separate passwords for work and home. Avoid allowing apps and websites to remember your passwords.

Secure your belongings! Keep a close watch on your possessions when in public areas. Lock items up or take them with you before departing, even if it's only for a brief moment. At work, lock your computer screen and secure your space before leaving your desk. Bring your phone and other portable items with you.

Update your devices, browsers, and apps regularly. At home, set up automatic software updates and occasionally restart your devices to make sure updates are fully installed.

Back up crucial files. Store backups in a physically separate location from the original files and periodically test them. Consider using a reputable cloud storage service.

Report anything suspicious! Learn to recognise potential scams and other dubious activities. At work, forward suspicious emails as attachments to your organisation's IT security team.

Be wary of public Wi-Fi networks. Avoid using public Wi-Fi networks, such as those found in cafes or airports, for sensitive tasks like online banking or accessing confidential information. Public networks can be easily exploited by hackers. Instead, use a virtual private network (VPN) to encrypt your internet connection and protect your data.

Enable device encryption. Enable encryption on your devices, such as smartphones, tablets, and laptops, to protect your data in case of theft or unauthorized access. Consult your device's user guide or manufacturer's

website for instructions on how to enable encryption.

www.safeonsocial.com

Regularly review privacy settings. Regularly check and adjust the privacy settings on your social media accounts, apps, and online services to control who can see your personal information. Limit the amount of information you share publicly and be cautious about accepting friend or connection requests from unknown individuals.

Be cautious with online shopping. When shopping online, only use reputable websites and look for HTTPS (the padlock icon) in the address bar to ensure a secure connection. Be wary of deals that seem too good to be true, as they may be scams or phishing attempts.

Educate yourself about phishing and social engineering. Phishing and social engineering attacks are designed to trick you into revealing sensitive information or performing actions that compromise your security. Learn to identify common tactics, such as urgent requests or threats, and verify the legitimacy of any unexpected communication.

Install antivirus and anti-malware software. Protect your devices with reputable antivirus and anti-malware software. Keep the software updated and run regular scans to detect and remove threats.

Use two-factor authentication (2FA) for online accounts. Enable two-factor authentication (2FA) for your online accounts whenever possible. This adds an extra layer of security by requiring a second form of verification, such as a one-time code sent to your mobile device, in addition to your password.

Be prepared for a potential security breach. Develop a plan for dealing with a security breach, including steps for reporting the incident, changing passwords, and monitoring accounts for signs of unauthorised activity. Being prepared can help you respond quickly and minimise the impact of a breach.

No part of this e-book/cheat sheet or its associated modules may be reproduced or transmitted by any person or entity in any for by any means, electronic or otherwise including photocopying, recording or scanning or by any information storage without prior permission from Safe on Social Media Pty Ltd other than the licensor who is licensed to use this information in newsletters and in print and has been granted permission from the publisher under an annual license. The publisher, authors, licensee, licensor and their respective employees or agents will not accept responsibility for injuries or damage, physical or emotional occasioned to any person as a result of a social media use or any other activities described in this e-book/cheat sheet. very attempt has been made to ensure that the information in this e-book/cheat sheet is accurate, it is the nature of social media to be constantly changing. Therefore, Safe on Social Media Pty Ltd gives no guarantees and accepts no responsibility to the completeness or accuracy of the contents of this guide.