CRAIG MCDONALD - *CEO & Founder, MailGuard*
https://www.linkedin.com/in/craigmcdonaldcybersecuritysocialimpact/

(Cybersecurity Expert, Published Author, Board Advisor, Speaker and Mentor)
After an email-borne virus wreaked havoc on his company, Craig founded MailGuard in 2001 in the hopes of protecting other businesses from cyber threats. MailGuard is a world leader in stopping fast-breaking email threats in real-time with speed, up to 48 hours ahead of competitors.

TIP 1 IMPLEMENT STRONG PASSWORD POLICIES AND ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Using complex passwords or passphrases, which frequently change, and using a password manager for secure storage can help to reduce the risk of unauthorised access to your systems. Enabling MFA on your accounts can also help to reduce cyberattacks by 80-90%. While one-time passwords may be more convenient, we encourage you to use biometric signatures, like fingerprints or facial recognition for increased security.

TIP 2 ENSURE ALL SOFTWARE AND SYSTEMS ARE REGULARLY UPDATED WITH THE LATEST SECURITY PATCHES

Outdated software often contains known vulnerabilities that can be exploited by malicious actors to gain unauthorised access to sensitive information, or a business's systems. Regularly updating software with the latest security patches can help prevent these types of attacks. Better yet, turn on automatic updates where possible.

TIP 3 REGULARLY BACK UP IMPORTANT FILES

Backing up to a cloud is a good start, but it's important to ensure that at least one back up is offline on an external device. The 3-2-1 strategy recommends having at least three copies of your data, two local (on-site) but in different storage formats, and at least one copy off-site to assist with disaster recovery.

TIP 4 BUILD A HUMAN FIREWALL

95% of cybersecurity breaches are due to human error, so continuously developing your team's cyber awareness and preparedness is a critical last line of defence against cyber threats. By being aware of and vigilant against potential security risks, such as phishing, ransomware, and BEC, employees can prevent data breaches and protect sensitive information from falling into the wrong hands.

TIP 5 BE WARY OF SHARED FILES AND LINKS

Scammers use links and attachments in emails to share malware or phishing sites. If the link or attachment has come from an untrusted source, or someone you weren't expecting to hear from, proceed with absolute caution. You can also hover over links in emails to check where it will actually direct you.

TIP 6 DON'T OVER-SHARE IN YOUR 'OUT OF OFFICE' (OOO) REPLIES

OOO replies are useful for letting your team, or other essential contacts, know you're away and your responses will be delayed but oversharing by saying you're on holidays or at a conference can leave you vulnerable to business email compromise attacks. Keep it simple – say you're unavailable and you'll reply when able to and, if necessary, add a general company email or phone number in case of emergencies.

TIP 7 AVOID USING BUSINESS EMAILS FOR PERSONAL USE

If you're using your professional email address when creating accounts, subscribing to newsletters, or making purchases online for personal use, it may make it harder to distinguish between a legitimate email and a phishing attempt. Additionally, the more your professional email is used online, the greater chance there is that it could be sold to a third-party or compromised in a data breach, putting your business at risk.

TIP 8 PERFORM PERIODIC RISK ASSESSMENTS

They can help your business identify its cyber strengths and weaknesses and can help you to get your systems back online quicker if you're attacked. They will also help you to stay ahead of rapidly evolving threats and technologies to ensure your defences are up-to-date.

TIP 9 DON'T FORGET ABOUT PHYSICAL SECURITY

Make sure to lock your computer when you're away from it, never write usernames and passwords down, be wary of who can see your screen, and lock away any confidential documents. It may sound simple but cyberattacks don't have to start online.

TIP 10 INVEST IN MULTI-LAYERED EMAIL SECURITY

The best defence is to boost your company's cyber resilience levels to avoid threats landing in your inboxes in the first place. Even if you're using Microsoft 365 or Google Workspace, you should also have a third-party email security specialist in place to mitigate your risk.