Top Tips for Cyber Security Month

Templar Executives
Cyber Security Resilience For Business

1

Check before you click. Spoofed emails can look just like the real thing. Be careful with attachments and/or links. If you have any doubts about a message contact the sender by other means to check.

2

Be tough to crack.
Use strong passwords, such as three random and unusual words. Consider **Multi-Factor Authentication** (MFA) for accounts with remote access especially seniors'/privileged accounts.

3

Communicate with colleagues securely. When using Microsoft Teams, Zoom and other video conferencing platforms, only send meeting invitations to relevant participants and lock the meeting after all members have joined. Also ensure **that sensitive information is not disclosed** in the chat function.

4

Be careful when downloading apps. Apps should be purchased from a reputable source and any permissions should be appropriate to the purpose of the app. Only company – approved apps should be downloaded at work.

5

Encrypt messages that contain personal and/or sensitive information and use a **Virtual Private Network (VPN)** to securely connect to your organisation's services.

6

Back-up data regularly so that information is safe, up-to-date and can be restored in the event of an IT disruption. Use clear document versions so colleagues know what is current.

7

Pause before you post. Disclosing too much personal information on social media platforms can lead to identity theft, fraud and can potentially cause your organisation reputational damage. Adhere to your organisation's Social Media Policy and 'How to Guides'.

8

Report it. Report all security incidents and breaches to your Line Manager, to the Security team or to IT, in line with company policy.

9

Secure your working area. Change the default password on home Wi-Fi routers and Internet of Things (IoT) devices, and disable any IoT features that are not in use e.g. microphones and camera.

10

Install updates and patches at the earliest opportunity to reduce vulnerabilities from being exploited.

For further information contact us at:
enquiries@templarexecs.com

+44 (0) 203 542 9075 | https://www.templarexecs.com | @templarexecs