CYJAX

Cyber Security In the workplace

01 **PASSWORDS**

Use a screenlock for all your devices, and two-factor authentication (2FA) – such as a code sent to your smartphone – to protect your accounts. Do not use work account passwords for other websites, and never share passwords with anybody.

02 **PHISHING ATTACKS**

Look out for suspicious emails. Don't be fooled into clicking on links or downloading infected attachments. Provide regular awareness training to staff to ensure they are equipped to identify these emails.

03 **BUSINESS EMAIL COMPROMISE**

These emails appear to come from a senior person in your company and involve financial transactions. Don't send requests for financial transfers over email and verify suspicious transactions with a phone call.

04 **RANSOMWARE**

A ransomware attack starts when someone clicks on an infected attachment, and all documents on the PC or the network will be locked. Back up your data, preferably to offsite storage.

05 **SOCIAL ENGINEERING**

Be aware of the information you are sharing on social media. Your posts can provide a rich source of data for cybercriminals.

06 **PATCHING AND SOFTWARE**

Keep all software up to date. Apply patches as quickly as possible and follow a patch management process.

07 **THIRD-PARTY SUPPLIERS**

Who is storing and processing your data? Make sure you have carried out due diligence on your third-party suppliers and their information security policies.

IF YOU WOULD LIKE ANY FURTHER INFORMATION AND ADVICE ON CYBER SECURITY IN THE WORKPLACE, PLEASE CONTACT US AT INFO@CYJAX.COM OR VISIT OUR WEBSITE CYJAX.COM