10 STEPS TO CYBER SECURITY

1 STRONG PASSWORD MANAGEMENT

It may seem like an obvious one, but your password is your weakest link. Stolen credentials are one of the most common causes of a data breach.

Best practice is to use a different password for each login, and use random words with a mixture of lower and uppercase, numbers and special characters. Don't use personal information that could be guessed and always change your password if you think it has been compromised.

2 MULTI-FACTOR AUTHENTICATION

Enable multi-factor authentication on all accounts where you can.

Authentication factors classically fall into three categories:

- **Knowledge –**Something you know such as username, email, and password
- **Possession-** Another device that will verify your identity, such as an SMS code or authenticator app
- **Being-** Something you are, such as a fingerprint, voice, or face ID

3 USE YOUR OWN DEVICES WITH CAUTION

Often organisations have strict own device policies, and rightly so. If your device isn't updated with the latest protection you could put your organisation's data at risk. Ensure you apply all security measures outlined by your company's policy and ask the IT team if you're unsure.

4 ALLOW ALL UPDATES

It can be tempting when you're busy to schedule new updates for your hardware to a later date, but it's important to action these as soon as they're available. Whilst often they take some time and you may be required to reboot your device, it's a good opportunity to work off-screen for a while or take a coffee break to ensure that security patches and fixes are updated as soon as possible.

5 THINK BEFORE YOU CLICK

Clicking links in emails or on unknown sites is a risky habit. Even if the content looks legitimate, a safer habit is to manually type out URLs. This way you're not inadvertently putting your organisation or even your own data at risk. Always check the URLs and email domains of unknown senders too to see if they look genuine.

6 BACKUPS

Backups are key and ensure if something happens to your data for example hardware failures, ransomware attacks and even physical theft, you can retrieve your data. It's important to store backups in a secure location separate from the original files, such as on a cloud system or physical hard drive. Make sure you're aware of any actions required by your organisation so you can play your part in keeping all files secure.

7 LOOK FOR THE PADLOCK

When searching for websites via a search engine, keep an eye on the URL to see if it looks legitimate and matches the company intended (with no typos). Look into the address bar for the padlock icon, this indicates an encrypted connection and identifies the information on the site as safe. This is especially important if you're required to enter sensitive information such as PII or financial information.

8 DON'T USE FREE PUBLIC NETWORKS

If you're out and about working, it may be tempting to use free public networks, but this is a red flag in terms of cyber security. Free WIFI networks are one of the easiest ways cyber criminals can target your device. If you must log in to a free public network, we'd advise not using it for accessing sensitive information and always use a VPN. A VPN improves security and enables users to access a public network as though it was connected directly to the private network.

9 DON'T STORE PASSWORDS OR DATA IN WEBSITES

Convenience is one of the downfalls of cyber security, whilst you may think it's easier to stay remembered on your most used sites to save time, it increases your risk of a hacker accessing your data. Using a password management system is good practice allowing you to create different complex passwords for each site without having to remember them.

10 LOG AND INFORM

If you do suspect a fraudulent website or a phishing scam, notify your colleagues and log within your organisation. Information is key and ensuring all colleagues are aware of potential scams will reduce the risk of them falling victim too.