CYBER SECURITY - TOP TIPS

Allianz

1 Update software/browsers

Any software/browsers used by your company should be the latest version. Old applications are more susceptible to a cyber attack because they are not updated with the latest security protection. This will help minimise your exposure to associated vulnerabilities. Cyber-attacks can steal information, penetrate networks, and cause severe damage.

2 Watch out for Phishing emails

Phishing is when a cyber attacker uses email (that appear to come from a legitimate source) to trick or fool you into taking an action, such as clicking on a malicious link, opening an infected email attachment or inputting sensitive data.

Protect yourself by looking out for:

- Messages requiring immediate action or urgency
- Spelling & grammar mistakes
- Messages directed to “Dear Customer”
- Suspicious links. Hover over any links – are they familiar or are they mismatched?
- The sender’s email address. Is it familiar and does it match with the content of the email?
- Are you expecting to receive this email?

If you receive a suspected phishing email, do not respond to it.

3 Secure your physical environment

Do not leave confidential material where others, who do not have access, are able to view. It is also essential that only people with the correct authority are let into the building.

4 Supplier landscape

Understand the type of data that you will send to a supplier and understand the impact if the data was compromised, corrupted, intercepted or changed in some way and if the data/service wasn’t available.

5 Information security education & awareness

Security is everyone’s responsibility so advise your staff how they can protect the company, employees and customers information.

Read more about the Government-backed, industry supported Cyber Essentials scheme to help organisations protect themselves against common online threats.