Improving Cybersecurity Awareness

Basic tips for all employees

Top cyber incidents causing disruption for businesses*:

57% PHISHING ATTACK (malicious email)

41% MALWARE (Trojans or worms)

30% SPEAR PHISHING

*Source: BCI Cyber Resilience Report 2017

What can you do to keep your organization safe from cyber-attacks?

Check emails you receive to ensure they are genuine

What might look like a legitimate email address, when examined carefully, can often be false and the email content may contain poor spelling and grammar.

Unless it comes from a trusted source, never:

- Click on a URL in an email
- Enable macros in attachments to emails
- Open email attachments

Make sure that your work is properly backed up

Failure to back up your work means that it could be permanently lost if an attack is successful.

Only download from trusted websites

Poor security on website downloads can lead to malware accessing your computer when browsing. If in doubt check with IT.

Be vigilant

- **Check files on your computer.** If you identify a suspicious file on your computer—for example it has an unfamiliar extension —disconnect your laptop/desktop from the network and report what you have identified.
- **Check any new files you're given before bringing them into your organization's network.** If they have executable code or macros have them checked by IT as they may contain harmful content.
- **Check URLs begin with 'https' or 'shttp'.** This indicates the site is secure and that your data is encrypted.

Report any suspicious activity

- **Suspicious emails:** Don't open it. Create a new message to IT—drag and drop the suspicious email into the new message so it's added as an attachment. Delete it from your mailbox once it's been sent to IT.
- **Suspicious files:** If you experience anything suspicious whilst using business systems or infrastructure, shut down your computer immediately and inform IT. Do not use your account or your computer until advised to do so. If in doubt check with your IT team.

bsi.