THINK BEFORE YOU CLICK THAT LINK

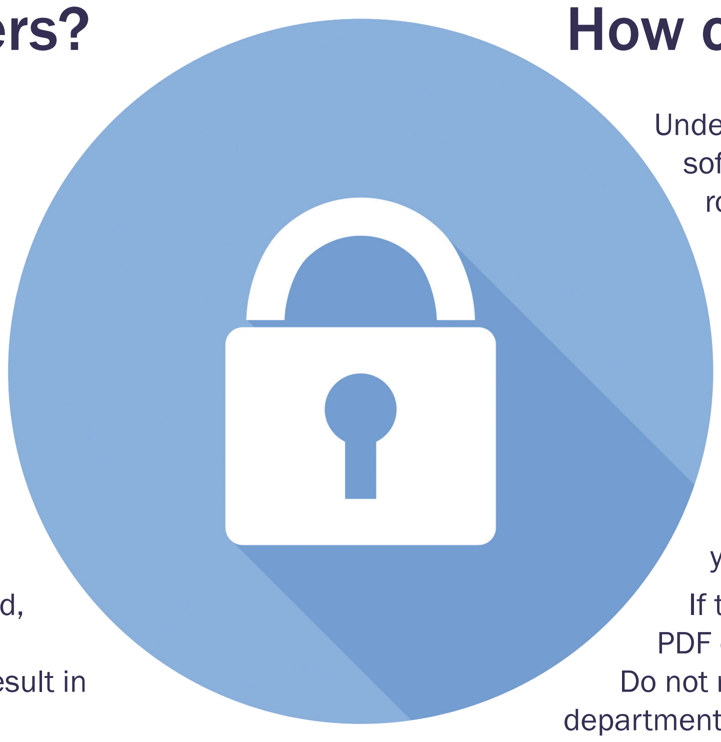
Most people know it's not a good idea to click links or open attachments in unsolicited emails. Fewer might not realise exactly why. **ISO/IEC 27001** addresses the hazards, which can include the installation of viruses – and even demands for cash.

What are the dangers?

If you receive an email containing a link or an attachment – even if sent from someone you know – be wary. Either of these can result in malicious programs being installed on your computer.

Malware can perform a range of tasks, such as encrypting your hard drive, copying passwords or providing an entry point to your network.

An attack can be seemingly random, or targeted at a person or organisation. Another hazard involves ransomware, in which your files are encrypted, and only a cryptocurrency payment to the hacker will result in them being unlocked again.



How can you stay safe?

Under ISO/IEC 27001, our organisation has software controls in place to try to stop rogue emails before they reach you – but occasionally a few get through.

So if you receive a phishing email, how can you tell? It used to be the case that such emails were badly spelled, but this is less often the case today. They will usually not be in response to an email you have sent, although they may look as if they are from someone you know.

If they contain an attachment, such as a PDF or ZIP file, this should ring alarm bells. Do not run them. If in doubt, contact your IT department. And be suspicious at all times.