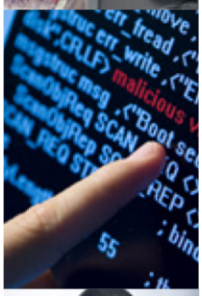
# Crime prevention advice for

# Emails



Emails have become a way of life; they are used at work, home, on the move and transcend geographical barriers. However, this development in communication has also lead to nearly 50% of all emails sent being spam. Below we take a look at some of the vulnerabilities and how these can be protected.

## Dangers of Emails

- **Shoulder surfing** – With the increase in mobile technology, employees can now work from practically anywhere, whether this is with their mobile, laptop or tablet. The danger of this is that when working in a public place, someone nearby may take the opportunity to watch what you are doing. Be careful when opening sensitive emails in a public place. This also applies to working with any sensitive data.
- **Phishing** - Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party (cyber criminal). It is often carried out via email, masquerading as a legitimate source but in fact is looking to steal personal details such as login information.
- **Attachments and spelling mistakes** – If the email is from someone you do not know and is unexpected, you should be cautious about opening any attachments as they could be harmful to your computer. In order to identify a phishing email as well as unusual attachments, you can look out for spelling mistakes or even an unusual email address that sent the email in the first place.
- **Spear Phishing** – These are specific phishing emails targeted directly at your business. They are often harder to detect as they are likely to be from a company you do business with and will seem rather plausible.

## Working Securely

- Secure Email – There are certain email systems that operate much more securely and offer higher levels of encryption so anything passed through them is much more protected.
- Encryption – Encryption is discussed in detail in another Advice sheet but it would essentially mean securing the contents of the email, i.e. attachments before they are sent so that if intercepted, the contents cannot be read.
- Staff training – Human error plays a large part in criminals gaining access to your business via email. It only takes one person to open an attachment or click a link which could jeopardise your whole computer network. It is important that all staff are aware of the risks and are always cautious of unexpected emails.