Ransomware
Reducing the risk

1 Is the email from a trusted source?
Review the "From" address - attackers often impersonate or "spoof" staff by using incorrect spelling of names or domains (i.e. "@y0ur0rg.com") you may be familiar with or in contact with.

2 Review the subject of the mail
Attackers often try to include valid email information in the subject to trick the user into believing the email is legitimate.

3 Review the spelling and content of the mail
Attack emails often contain poor spelling and grammar.

4 *Ask "Is this mail relevant to my job role and responsibilities?"*
Is the nature of the email related to your job function?

5 Does a mail refer to an action you did not take?
Typically attackers will draft these mails as responses to "requests" you may have made. Is there a mail trail of you requesting this information or file? Or is the email a once off?

6 Be vigilant of attachments
Attackers will often include a malicious file as an attachment to a phishing mail.
DO NOT open or interact with any attachments in strange or suspicious emails. Verify that:
- the sender is legitimate,
- the content of the mail includes a legitimate mail history,
- the attached file is one you have requested,
- the attachment is in the correct format (e.g. is this report an xls instead of the usual PDF?)

7 Be vigilant of links
Attackers will also try to include links to malicious content or websites. **DO NOT** click on any links that you do not trust or are not familiar with.

8 Don't forget hyperlinks
Attackers may use URL hyperlinks in the body of an email (e.g. "Click Here").
- Typically, hovering over these hyperlinks will disclose the real destination of the link
- Right-clicking and copy and pasting this into a word processor can also be performed to review the link

SSR Personnel
the face of recruitment

www.ssr-personnel.com