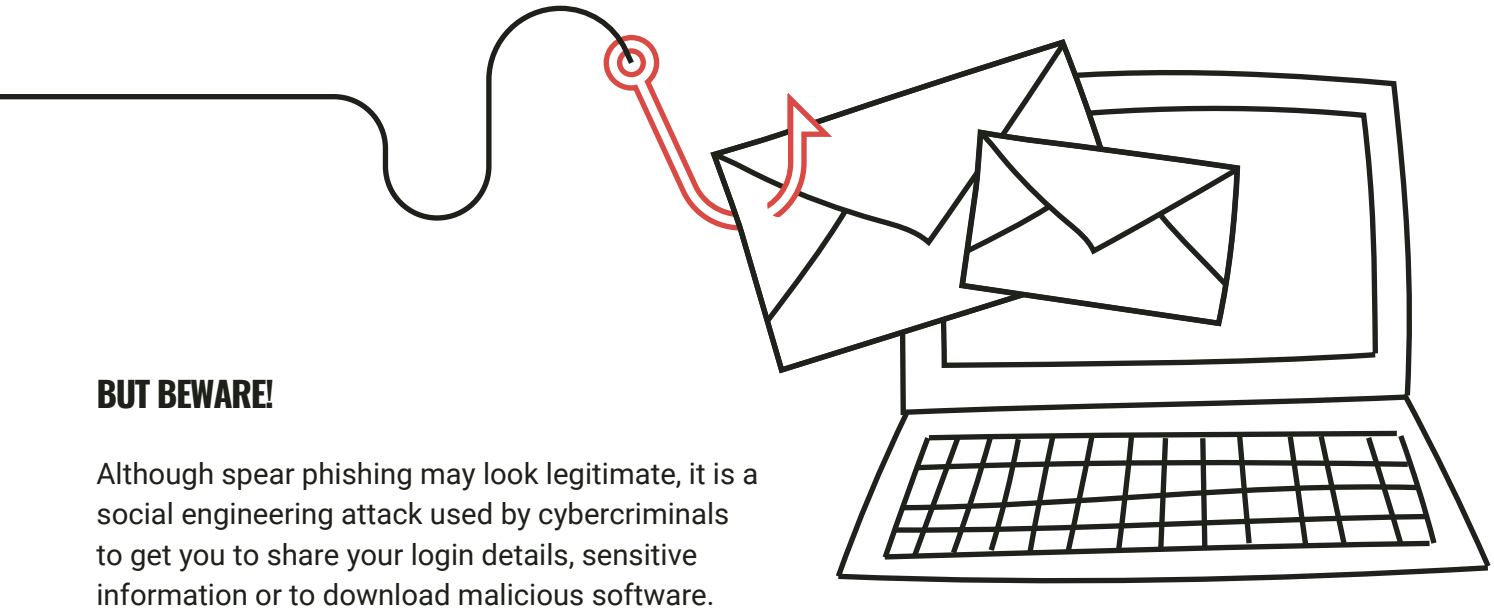
CRIMINAL MINDS

DON'T BE AN EASY TARGET FOR SPEAR PHISHING

You may receive an email that looks like it was meant for you, contains details related to you or your interests and looks like a legitimate person or organisation could've sent it.



BUT BEWARE!

Although spear phishing may look legitimate, it is a social engineering attack used by cybercriminals to get you to share your login details, sensitive information or to download malicious software.

Spear phishing attacks include an email with an attachment or a link. The email often uses language that plays on your emotions to entice you to open the link or download the attachment.

For these scams to be successful, the cybercriminals gather information — via fake ads, looking at out-of-office notifications and using the information found on social media.

DON'T TAKE THE BAIT!

- Verify any links or attachments you were not expecting
- Don't take action when your emotions are heightened
- Be careful not to overshare on social media
- Report any suspicious messages

WATCH CRIMINAL MINDS - SPEAR PHISHING TO SEE WHAT CAN HAPPEN IF YOU OVERSHARE ON SOCIAL MEDIA.

Popcorn Training