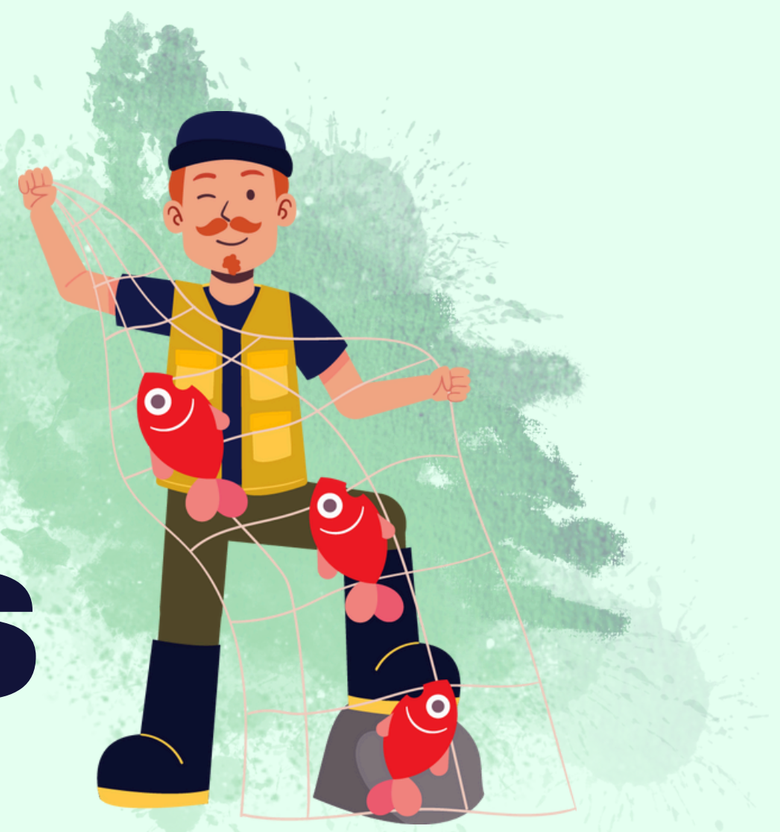
6 PHISHING RED HERRINGS



1 GLANCE AT WHO IT'S FROM

- Make sure the @openroadsins.com domain is spelled correctly for internal emails.
- When looking at external emails, make sure the domain is spelled correctly.

2 LOOK AT WHO IT'S TO

- Long lists of email addresses put the email at a higher likelihood of being spam.
- If it's sent to a group, such as claimsadj@openroadsins.com, it's more likely to be safe.

3 CHECK WHEN IT WAS SENT

- If an internal email is sent outside of business hours, report it.
- Your time outside of work is yours to do with as you please.
- Do not check your email outside of your scheduled work hours.

4 INSPECT ATTACHMENTS

- If there are symbols in the file name, it's best to report the email as phishing.
- Attachments ending in .js or .doc are the most common malicious files.
- Do not download attachments that you were not expecting.

5 READ THE BODY CAREFULLY

- Phishing emails or messages may contain misspellings, grammatical errors, or awkward phrasing.
- When in doubt, read it aloud to yourself so you can hear the errors.

6 HOVER OVER LINKS

- Look for links that are too long or too short.
- Check for common misspellings.
- Hover over links to check their actual destinations, and do not click on suspicious links that you were not expecting.