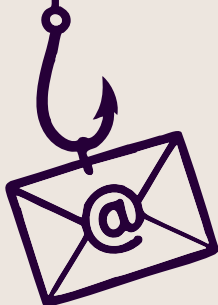


Don't get hooked this holiday season!

Our top five tips to help you spot suspicious phishing emails this festive season:



1 Double check who it's from



Look out for sneaky email addresses that mimic trusted ones but have small changes (e.g. `contact@supplier.com.au` vs `contact@supplier-express.com.au`). If something looks off, don't click it.

2 Don't let urgency steal your festive cheer



Scammers love to use phrases like "Your account will be closed today!" or "Immediate action required" to make you act without thinking. Don't let urgency steal your festive cheer, take a breath and check twice before you click.

3 Hover to uncover



Before you click any links, hover to preview the URL. If it looks suspicious or doesn't match the sender's organisation, it's best to leave it unopened just like a dodgy gift.

4 Look out for spelling mistakes and poor grammar



Watch for subtle spelling or grammar mistakes, even small errors can be a sign something's off. If in doubt, verify the message by contacting the organisation using details you've found yourself, like from their official website.

5 Keep your information to yourself



No reputable company will ask for your passwords or credit card details via email, text or phone. If in doubt, check through official channels and always access secure portals or apps directly, never via email links.



CAPRICORN

At Capricorn, we're committed to supporting you to keep your business safe online.