# How to Identify Spam/Scam Emails

> If you are not sure, the email can be forwarded to isthisreal@barweb.com.au, a BarWeb technician will inspect the email along with the email log to ensure the email is safe.

Phishing is an attempt to scam or deceive you into disclosing personal and financial information in an email or online. A hoax email may look like it was sent from a reputable organisation, and may ask you to disclose personal information via return email or by clicking a link. These emails often look genuine, copying a company's branding and email layout, and using an address that's very similar to the real company's URL.

## Hoax emails may:

- Be unaddressed, or addressed generically to Dear Customer
- Be badly written with broken sentences, spelling mistakes and grammatical errors
- Show a sender address that is very close to the real company's address
- Display a suspicious looking URL when you hover over links or buttons you're asked to click
- Contain an unexpected zip file or other attachment
- Ask for your credit card, account details or personal information
- Display account information that doesn't match your real details

## Help protect personal information by following these steps:

- Never trust emails that ask for personal details
- Think twice before giving personal details online - instead, contact the sender using their publicly available contact details
- Visit trusted websites via their URL, rather than clicking a link in the email
- Only provide financial details on secure websites
- Carefully choose and change passwords regularly
- Read the privacy policies of websites and apps you use
- Upgrade your device's security software or apps
- Use a separate email account for subscribing to online services and groups
- Use a spam filter to help block unsolicited and hoax emails

## If you receive a suspicious email:

- Don't click links or reply
- Don't provide any personal information
- Don't open any attachments
- If you click an email link which opens a website, don't enter any personal information
- You can report the incident to ACCC SCAMwatch
- Delete the email as soon as possible
- If you've already provided personal or banking details to a scammer, contact your bank or financial institution immediately (using their publicly available details, not the ones in the email you received) and monitor your bank statements for unauthorised transactions. If you've provided account information, change any passwords you may have disclosed for your account
- If you've already saved or clicked on an attachment, update your anti-virus software and run a complete scan of your computer. Repeat the anti-virus update/scan process again over the next few days. You may also wish to update any online passwords stored on your computer in case they've been accessed

Revision #1

Created Wed, Aug 21, 2019 3:11 AM by Zachary Cash

Updated Wed, Aug 21, 2019 3:12 AM by Zachary Cash