3 WAYS TO CHECK YOU'RE NOT PAYING A SCAMMER

#1 CHECK IF YOU CAN COMMUNICATE OR PAY ONLINE SECURELY.

- Look for the closed padlock symbol in the address bar of your web browser.
- Make sure the URL begins with https instead of http because 's' means secure.
- Check if the email address uses the company's domain name eg: @asic.gov.au @Xero.com.au
- See if the web address is correctly spelled and truly from the official website. Don't click links in emails unless sure.

#2 VERIFY IF THE SOURCE IS LEGITIMATE.

- Use their official contact details.
- Check if their ABN number is real.
- Look for the company on ASIC's Australian Financial Services licensee register.
- Research about the business online.

#3 LOOK OUT FOR RED FLAGS.

- Unsolicited emails asking you to open an attached file.
- Bogus invoices from vendors or suppliers you never made business with.
- Calls or emails asking for upfront payment through untraceable international wire transfer.
- Directions to deposit payment into a personal bank account.
- Instructions to pay via vouchers, prepaid cards or gift cards.
- Requests for you to download software that will allow remote access to your computer.
- Demands that you buy anti-virus/malware software because your computer is infected, even if it's not.
- Instructions for you to call a premium number (starting with 19) to claim a prize from a raffle you didn't join or an inheritance from a relative you don't recognise.
- Threatening phone calls claiming that you will be arrested by the ATO unless you pay money.
- Requests for your Tax File Number (TFN), credit card number or other personal information.

Report Scammers To SCAMwatch
Website: https://www.scamwatch.gov.au/report-a-scam
Twitter: @scamwatch_gov

RB RESTAURANT BOOKKEEPERS AUSTRALIA