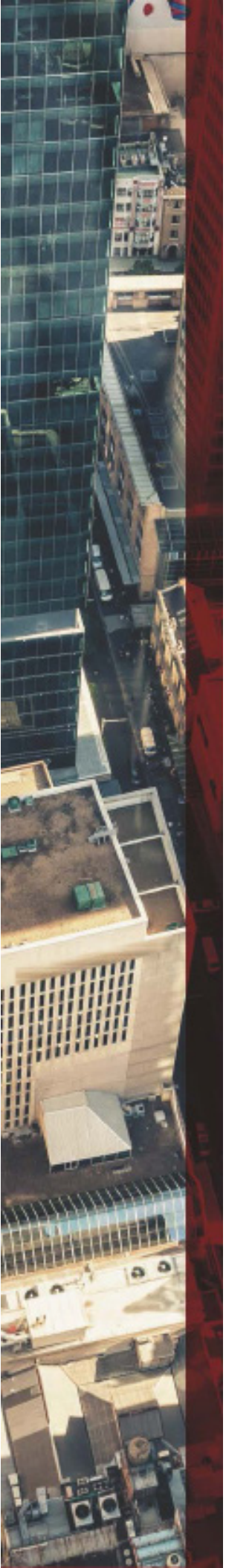

WARNING! EOFY SCAM ALERT

The Federal Government has recently released alerts regarding a sophisticated and well-designed scam aimed at obtaining banking details from unsuspecting taxpayers.

These alerts serve as a timely reminder to be vigilant regarding the sensitive information you share online or via email.

The scam in question follows the below pattern:

1. A phishing email claiming to be from Medicare asks you to update your EFT details to allow you to receive Medicare claims;
2. Clicking the link within the email directs you to a replica Medicare website, including myGov and Medicare branding. Note the URL includes '.net' instead of '.gov.au'. Australian Government domains always include the latter;
3. Targets are then required to enter their login details and security questions and answers;
4. You are then taken to a new page where you are asked to input you bank account details.

The Government has issued the follow reminders regarding cyber safety:

- myGov and Medicare will never send you a text, email or attachment with hyperlinks or web addresses;
- exercise caution in opening unexpected messages, especially from unknown senders;
- be wary of suspicious messages that aren't addressed to you directly;
- any legitimate messages from Medicare will appear on your official myGov account, which can be accessed by typing the web address into your browser;
- if in doubt contact the organisation separately to confirm the message is legitimate.

Hall Chadwick Qld advises caution when supplying or transmitting sensitive information online or via email.

Should you receive any suspicious correspondence claiming to be from the ATO or any related department please don't hesitate to contact our office for confirmation.

The original Government alert can be found here.

Find out how we can help, contact our office.

QUEENSLAND
LEVEL 4, 240 QUEEN STREET
BRISBANE ,QLD, 4000
general@hallchadwickqld.com.au
(07) 3221 2416