Government of **Western Australia**
Department of **Finance**
Office of State Revenue

Protecting your online data and Revenue Online account

The Office of State Revenue is vigilant in ensuring that our customers' Revenue Online data remains secure from online fraud and encourages all customers to take the necessary steps to stay cyber-secure.

We do not issue emails that contain links to login pages or that ask for personal information, account details, PINs or passwords.

If you receive emails like this that appear to come from us, please follow the tips below and contact us as soon as possible.

For more information on Revenue Online or protecting your details when using Revenue Online please contact the Office of State Revenue on 08 9262 1300.

See below for some security tips to keep your online data safe.

Use complex passwords

Protect your Revenue Online (ROL) account by creating a strong and secure password that makes sense to you, but not to others. Be aware of scamming tactics such as phishing, email spoofing and spamming (explained below).

To minimise the risk of password security breaches, the Department recommends that you:

- create a strong password containing alphabetic and numeric characters with a combination of upper and lower case letters;
- do not share your password with anyone; and
- regularly update your password.

For guidelines of what your password must contain, see the online services password policy.

You can change your password by logging into your ROL account and clicking on the 'Change Password' link in the top right-hand corner of the homepage.

It's important to know about the following hacking methods used by scammers, commonly via email, so you don't get caught out.

Avoid spam

Spam emails can consist of advertising emails, chain letters as well as other forms of non-commercial mailing.

Types of spam

- Intentional spam comes from spammers soliciting products or attempting to commit fraud.
- Unintentional spam comes from computers that have been infected with a virus or worm. The virus or worm sends bulk messages from the infected computer without the computer owner knowing.

Be aware of phishing

Phishing is a form of spam intended to trick you into entering your personal or account information so scammers can breach your account and commit identity theft or fraud.

How it works

- Typically, a false email message is delivered to you that appears to come from a legitimate source. This email can appear to be sent from a company's email address, often containing a legitimate logo.
- The message may ask you to update your account, or run a software program to upgrade your computer.
- Normally you are then asked to enter personal information such as your name, date of birth, place of birth, social security number, mother's maiden name, bank account number and bank PIN. This information may then be used to steal your credentials.

See below for tips to protect yourself and to assist you to combat phishing.

Look out for email spoofing

Spoofing is the forgery of an email header so that the message appears to have come from a legitimate source. It is often used by spammers and can be accomplished by changing the 'From' email address when composing the message.

How it works

- A user receives an email that appears to have originated from one source when it was actually sent from another. A spoofer could send an email that appears to be from you with a message that you didn't write.
- The spoofing email tries to trick the user into making a damaging statement or releasing sensitive information (such as a password).

Tips to protect yourself

- Don't open emails which look like spam. If unsure contact your ICT provider, otherwise delete them immediately.
- Never click on web links within your emails from senders you're not familiar with.
- Don't open attachments from anyone you don't know.
- If you receive a message from a friend with a link, ask them before opening the link to confirm it's not a spoofer (infected machines send random messages with links).
- Be wary of visiting unsafe or unreliable sites.
- Be aware that fraudulent email messages often use names similar to popular services to try to trick you into providing information or downloading an attachment with a virus.
- Ensure your antivirus and threat protection are up to date.