Security warning for PEXA users

Recent news reports and emails from PEXA have described a fraud involving the PEXA workspace. Any users of the PEXA workspace need to read this bulletin for tips on how to avoid this happening to them.

The fraudster appears to have gained access to a subscriber's email account and intercepted a change of password email allowing them to change the subscriber's password. This then allowed them to create a new user account which gave them access to the workspace where they changed the bank account details that had already been entered. When the subscriber returned to the workspace to complete the transaction they did not notice the account details had been changed and the transaction was completed with money transferred to the wrong account.

What you must do

- Always double check the payment details entered on the workspace, especially the bank account details, before signing off and locking the workspace. You should not assume that the details will be the same as they were when you entered them.
- If you find you cannot log into the PEXA workspace with your own password, you should be on notice that something may be wrong. Do not simply do a password reset and assume everything is normal. You should:
  - contact PEXA and ask them to check the account and whether any changes to passwords or users have been made
  - check any active workspaces where settlements are pending that all payment details are correct and have not been modified by an unauthorised person.
- Check your PEXA account now to identify any unauthorised users and continue to regularly monitor it.
- Strengthen and maintain your email hygiene and security protocols to minimise the chance of fraudsters gaining access to your email system. This includes:
  - ensure staff have **regular training** on cyber security and fraud prevention
  - develop and implement an **office policy** about cyber security

- use a **business grade** hosted email service that includes quality filtering to block dangerous emails, spam, phishing and malicious content or attachments
- use a **DNS based web filtering** service to block high risk websites
- install a **reputable security software** application on every computer
- **backup** all of your firm's files using an automated daily service that backs up to the cloud
- keep all **software on your computer up to date** by ensuring all updates and security patches are installed
- use only **strong passwords** that have a minimum of eight characters containing uppercase and lowercase letters, numbers and symbols. Change your passwords at least every 12 months

- For more information on cyber security see our Cyber security page on our website and in particular our Cyber security key risk checklist.