ABN 92 140 677 792
Property Exchange Australia

Overview

Cyber-security is a key priority at PEXA. In support of our members and the broader property industry, we continue to invest heavily in our infrastructure, support networks and educational resources.

Cyber-crime has long existed in the property industry and is not exclusive to digital settlements. Safeguarding your digital portfolio; your accounts, your devices, your data and your networks, from threats, is vital to ensuring the information of your business and clients remain safe.

There's no individual step, piece of technology or single process that guarantees your cyber-security. A layered approach, with a commitment to shared responsibility between all settlement parties provides the best risk mitigation.

Phishing

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Phishing scams generally instruct recipients to enter personal information at a fake website which matches the look and feel of the legitimate site. 25% of all security breaches involve phishing via email, phone or SMS.

Unfortunately, phishing scams are becoming more complex. No longer do they contain fuzzy, pixelated images and spelling mistakes – they're surprisingly convincing.

Spear phishing

Spear phishing is a highly specialised type of scam that involves the sending of targeted communications towards a specific individual, organisation or business, in order to obtain sensitive information.

In these cases, the cyber-criminal takes the time to 'scout' the potential target, in order to make their attack more precise.

If you receive an email you believe to be suspicious:

- Do not respond.
- Do not click links or download attachments.
- Engage your relevant security administrator or reach out to PEXA's Security team to inspect the email. PEXA would also like to be made aware of any fraudulent emails using our branding.
- Delete the email, once it has been provided for analysis.

If you click on a link within a phishing email:

- Contact the PEXA Support Centre immediately, who will connect you with our Security team.
- Additionally, engage your relevant security administrator.
- Report scams to the ACCC via the Scamwatch report a scam page.

Known scenarios

Some examples that PEXA members have experienced in relation to PEXA are:

- Emails with PEXA branding prompting a password reset.
- Scammers posing as a buyer or seller.
- Sending new bank details as a screenshot from a different number through third party messaging services, such as WhatsApp.
- Robocalls suggesting your settlement has been suspended and you need to provide sensitive information to unlock it.
- Emails being intercepted, modified and sent on with new settlement details, which appear legitimate.

In any of the above instances, it's vital to be certain that the communication you have received is from a legitimate source and if uncertain, verify over the phone with the relevant party.

What PEXA will never do

There is a lot of guidance to support you on what you should or shouldn't do in certain scenarios. However, this list provides you with five simple actions that PEXA will never do.

PEXA will never:

- **Call** you from unverified phone numbers.
- **Ask** for your multi-factor authentication code.
- **Request** files or information from you via a third-party service.
- **Email** you from unofficial addresses (emails that don't end in @pexa.com.au).
- **Send** you an email advising you to click a link to log in to the platform.

How does PEXA support members?

- **World-class security operations:** best in class technology, close collaboration with the security teams of major banks, 24/7 Workspace monitoring and more.
- **Security products designed for industry:** PEXA Key introduced to help securely communicate sensitive details for settlement.
- **Working in partnership with members:** regular community engagement, with a plethora of best-practice content shared.
- **Strict digital identity monitoring:** encrypted digital signing certifications and multi-factor authentication (MFA/2FA).

General security tips

- Keep your devices, applications and operating systems up to date.
- Check the security and privacy settings of all your essential services, including those for personal leisure and make sure they have 2FA/MFA available.
- Keep a backup of your data (it is very easy to backup data now with cloud storage services).

- Be aware of the website and the apps you use. Delete the apps you no longer use or require.
- Be cautious with emails asking to take action, particularly those with a level of urgency.
- Be aware of the ongoing scams so you know when something is not right (Scam Watch has a great list of ongoing scams in Australia and regularly updated).
- Do not use the same password across all your apps/services – use a password manager.
- Do not use public WiFi for work purposes.
- Be wary of parties changing their preferred communication channel ie: if you have been conversing via phone call and there's a sudden shift to WhatsApp.

Helpful resources

- Our team is contactable for security-based issues via security@pexa.com.au.
- We host PEXA and general security advice here: https://www.pexa.com.au/security.
- For our latest network alerts and updates, visit and subscribe in the top right corner: https://community.pexa.com.au/t5/Security/ct-p/Security
- The Australian Cyber Security Centre has published advice for protecting your business at this time. In addition, the Government recommends that you ensure your systems are all patched and to use multi-factor authentication (MFA) where possible.
- The Australian Cyber Security Centre (ACSC) website also has great recommendations for individuals and businesses to gain more information.
    - https://www.cyber.gov.au/acsc/small-and-medium-businesses
    - https://www.cyber.gov.au/acsc/individuals-and-families

If you suspect you've been targeted by a phishing attack or scam, it's important to inform your relevant security contacts immediately. Acting fast ensures the best chance of recovery. There's no need to fear speaking up – we're all human, honest mistakes can happen and we're here to help.