PEXA responds to cyber attacks

GRANT FEARY, DEPUTY DIRECTOR, LAW CLAIMS

Highly publicised cyber breaches involving conveyancing practitioners have highlighted the importance of maintaining robust cyber security controls and practices. Our advice? Be vigilant. Inform all relevant parties (including staff) of proper procedures. Verify. Act.

This Riskwatch again concerns cyber-security. We make no apology for the recent proliferation of articles on this topic because it is highly topical and of critical importance.

PEXA ISSUES

In recent highly publicised incidents an unknown party gained unauthorised access to a (conveyancing) practitioner's email account. Through access to the practitioner's email account, the unknown party used the password change email link sent from the PEXA platform to allow access to the Subscriber's PEXA profile. With access to the practitioner's PEXA profile, the unknown party was then able to create a new User account and with the new User account was able to fraudulently change the destination account details in the respective settlement schedules.

The practitioner subsequently digitally signed (or re-signed) the financial settlement schedule, confirming the account details that were entered, allowing settlement to proceed. It appears in both of these instances the practitioners did not check the settlement schedule they were signing off on which resulted in the misdirection of funds.

In both instances, the misdirected funds were sent to bank accounts and the banks involved were quickly contacted. While it is believed that all the money from one transaction and a substantial proportion of the money from the other transaction have been recovered, besides the stress involved, one of the cases attracted national media attention as the funds belonged to a TV celebrity. The prospect of reputational damage for PEXA and the conveyancing practitioners involved is, no doubt, very significant.

PEXA have said that they will make the following additions to the system:

- **Increased monitoring of PEXA Workspaces:** PEXA has been monitoring all Workspaces for several activities including identifying unusual activity surrounding password resets, new user creations and changes to BSB and account numbers. PEXA has been actively contacting practitioners to confirm any such activity is legitimate. PEXA say that new instances of this fraud have been found and these continue to be isolated incidents.
- **Creation of new users within existing accounts:** PEXA will only allow new users to be created to existing Subscriber accounts in an "inactive" status, and PEXA will be required to activate them.
- **Workspace time stamps:** PEXA will add a feature to the system which highlights the date, time and specific user that last updated the settlement schedule. This will provide an additional method to validate the details prior to signing and will be displayed on the signing screen.
- **Multi-factor verification:** PEXA will introduce additional two factor authentication. All Subscribers will be required to confirm their identity through this additional verification layer when logging into PEXA.

EMAILS: THE WEAKEST LINK?

In many cyber fraud incidents to date the initial problem has been the susceptibility of emails to hacking. Emails are simply not a secure form of communicating sensitive information.

In a recent article in the Australian Financial Review (3rd July 2018), Peter Moon, a technology lawyer at Cooper Mills, made the following comments:

> *"Email wasn't designed as a secure messaging platform and almost everything about it is the opposite of how a secure communication system should work.*
>
> *Email was conceived as a short messaging tool. "Meet at the cafeteria at 1pm to talk about the results?" "Sure. See you then." It didn't matter that it travelled over the network encrypted, or that copies might sit indefinitely on servers that third parties could access, or that there was minimal proof of the sender's identity.*
>
> *If it appeared to come from Fred, it probably was from Fred.*
>
> *It was later generations who decided to apply this handy but insecure chat system to serious business and high value transactions.*
>
> *Most of us simply choose to trust email, against overwhelming evidence that it doesn't warrant it."*

For better or worse, however, email is now part and parcel of how business is done and it appears that isn't going to change any time soon.

Many law practices now have security gateways to detect malicious emails but they are unlikely to be a complete defence to criminal activity. For example, a criminal scammer can gain access to a client's or practitioner's account via a weak password or where a password has been copied while the user has accessed an insecure (often free) wi-fi network. More sophisticated forms of access are by targeted computer network hacking (and law practices are a high-profile target) or via malware which has enabled a scammer to gain access.

Where this has occurred the fraudulent email is likely to come from the sender's actual email account. In other instances, the email comes from an entirely different account but with an email address that is nearly identical to the apparent sender's (this is called "spoofing").

Regardless of the method by which the email is sent, it is likely to be the recipient's response to the email that will determine if the fraud is successful or not.

ADDRESSING THE RISKS

The following are the steps we suggest you implement:

Vigilance

- Adopt a less trusting and more critical mindset as requests by email regarding money transfers may be fraudulent.
- Develop secure cyber fraud prevention policies and procedures for managing emails, especially requests for money transfers or change of bank account details.

Inform

- Train your staff in the prevention procedures and ensure they are complying with them.
- Let relevant parties (e.g. clients, other law practices, real estate agents) know that you will not –
  - change your account details by email; or
  - request by email that they provide you with account details, and that they should inform you if they receive an email to the contrary.
- Tell all relevant parties that you will seek verification of any emails apparently from them that seek to change account details or request the transfer of money to other than verified accounts.

Verify

- When an email contains instructions to transfer funds or change account details call the apparent sender using a credible number, such as from original instructions (not from the suspect email), and verify all relevant information.
- Consider also verifying the identity of the person you are speaking to by one other valid piece of information (try to ensure the information would not have been contained in any email exchange).

Act

- If the verification process is correct, proceed as instructed.
- If the verification fails, you need to consider:
  - Informing the apparent sender of the suspected fraud, particularly if it appears they have been hacked
  - Investigating the incident if it appears your email has been compromised
  - Conducting a "*lessons learned*" review, amending your prevention procedures if necessary and letting staff know what has happened and why the procedures are so important.

Acknowledgements:

- Peter Moon "*PEXA hack shows antiquated email is a fraudster's best friend*" (Australian Financial Review 3rd July 2018)
- Law Cover (NSW) "*Cyber Fraud Aware and Prepared*"
- Law Mutual (WA) – Risk Alert "*Is email "The Weakest Link"?*"

It was later generations who decided to apply this handy but insecure chat system to serious business and high value transactions.