Opportunistic cyber attacks - lockdown

The most recent lockdown in Sydney has seen an increase in phishing emails targeting law firms.

Cyber criminals are opportunistic, and lockdown presents a good opportunity to take advantage of vulnerabilities and disrupted communication. Implementing some key risk management measures will ensure that any vulnerabilities in your processes or systems are remedied, minimising your law practice's exposure to this type of cyber-attack.

Make that call

Cyber criminals are known to send fake telephone numbers or create seemingly plausible excuses to explain why it is not possible to confirm account details over the telephone. If you have not already done so, before transferring funds ensure that you, your staff and your clients always confirm bank account details by telephone. This is your best defence against email fraud attacks. Always check client phone numbers held on file before making contact.

Share knowledge and train staff

Your people are the first line of defence. If your staff are aware of what to expect they can react to a potential threat. Ensure that you are consistent in your approach and that processes are clear and concise. Conduct frequent education and training to provide staff with examples of cyber attacks and the appropriate response. Assign roles and responsibilities to ensure accountability and adherence to procedure.

Educating staff is not the only fix but is probably the most important factor in helping to curtail a potential threat.

Slow down, be suspicious

Even in the best practices, lockdown fatigue can cause errors to occur when working from home. Avoid trying to work too quickly and remain vigilant for suspicious emails or unusual requests, especially around email credentials. Don't click on attachments or anything relating to bank details.

Let clients know

Inform clients that you won't accept emailed bank account details from them and will never communicate your bank account details in this way. Let clients know that you will always confirm bank details by telephone and will regularly check the accuracy of telephone details on file.

If your law practice and your clients work together, and there is a shared understanding of cyber security practices, cyber fraud can be managed and prevented.

If you believe you may have received a fraudulent email, you should immediately take steps to ensure that your email system has not been compromised. Contact your IT consultant or Lawcover's cyber incident response team on 1800 BREACH (1800 273 224).

Lawcover provides a complimentary eLearning course, "Cyber Claims in Legal Practice", which contains useful examples of the types of cyber attacks and what you can do to manage risk. Available on our Risk Online e-learning platform - Register for the course.

Candice Perriman
Rick Education Manager