Short Minutes Transcript: Cyber Fraud – Fake Emails

Lawcover has received a number of notifications regarding suspicious emails being sent to solicitors purporting to be from well-known entities like banks, legal practices or clients, in an effort to gain sensitive information.

This type of cyber scam is known as brandjacking. When the email arrives, it is usually opened because it looks like a legitimate email from a known entity. The email contains appropriate logos and messaging and often includes an attachment like a fake invoice which, when opened, takes the individual to a separate page asking for personal information like user names and passwords. This information is captured and used in identity or bank account theft.

There are a number of ways to spot suspicious emails in your practice:

- The link you are asked to visit is different from the company's usual website
- The senders email address is different to the company's usual address
- The email is unexpected
- Bad spelling or poor grammar
- The email asks for money or sensitive information like user names and passwords

To help minimise the risk and protect the information in your legal practice, relevant software protections should be installed. In addition, staff should be trained to recognise and be suspicious of this type of email.

I'm Malcolm Heath