NEW ZEALAND LAW SOCIETY

NZLS EST 1869

PRACTICE BRIEFING:

HOW TO RECOGNISE AN EMAIL SCAM

INTRODUCTION

Lawyers open lots of emails every day. Increasingly, individual fraudsters and networks of scammers are using hoax emails to trick people into sending money, giving away private information, or exposing their home or organisation's computer network to malicious software and viruses. These fraudulent tactics are often called "phishing scams" – they are designed to "catch" the credulous.

This New Zealand Law Society Practice Briefing is a guide to help lawyers recognise email scams. It is not intended to be legal advice. Lawyers are reminded to always use their professional judgement, and to be vigilant about opening unsolicited emails. If it looks too good to be true, it probably is.

A DEVELOPING PROBLEM

Each time we check our emails and see new messages in our inbox we make judgements:

- Is this email safe to open?
- Should I click on the links inside the email?
- Is this an email I was expecting?
- Is it from someone my organisation knows, or who is familiar?

And we usually get it right. Most emails are not scams.

But there are also some horror stories, where victims of email scams have unwittingly given cybercriminals access to their organisation's entire data store, user account information, client and employee details.

More and more security measures are developed each year to protect internet users from email scams and other cyber-attacks. However, it remains vital that email end-users can recognise messages, attachments and content (hyperlinks) within messages that may be a threat.

Some of this information you're likely to have read before. New, more sophisticated email scams, trends and targeting tactics are constantly being developed, and countered, however, so it's prudent to be vigilant whenever there's something about an email you receive that just doesn't seem right.

These days, it is likely that the scammers have done their homework. They know who you work for, who your colleagues are, what job you do, your position title... Very concerning, not just because of the details cyber-criminals might know about your life, but because knowledge of these details makes it much easier for scammers to convince users that their hoax email is legitimate. "Phishing" is being replaced by "spear-phishing" (targeted phishing).

Before opening any email, ask yourself the following questions:

Who is sending me this email?

Known person

Can you be sure that it is the person known to you who sent the email? Some malicious emails will appear to be sent from someone you know – it is possible their email has been accessed (hacked) or maybe their email address is just being displayed (spoofed) and the real sender's address is hidden.

Be alert for any unusual style in how someone you know addresses you, communicates with you or signs off.

Blank emails with no subject, or something like "check this out" with an attachment, are particularly suspect.

Hackers know you are far more likely to open an email that purports to come from someone you know. More so if that person is your boss, your boss's boss or another partner or director. Remember – the hackers now do their homework. Fortunately it is easy to **verify the sender in these cases – pick up the phone**: "Boss, do you really want me to send my credit card details to that address...?"

There is some malware that appears to be sent from a printer or scanner, so **if you haven't scanned anything, you shouldn't open these**. You should recognise email from your local scanning device.

Unknown person

Is the email from a lawyer? If their email address seems unusual, **look them up on the New Zealand Law Society Register of Lawyers** and check their address. The Register can be found on the home page of the New Zealand Law Society website (www.lawsociety.org.nz – "Search the Register of Lawyers"). If they are from a law firm and their email address is @gmail, consider checking

the Register (although this does not list all email addresses. Many law firm websites now include email addresses). If it looks dodgy because of the content, language, grammar or style, call the lawyer using the phone number from the Register of Lawyers, not the one on the email. **It may be that their email account has been hacked.**

We get emails all the time from people we do not know. Most of them are commercial in nature – they are trying to sell you something. Reputable firms are transparent about who they are, use company domains and always give contact details. Their email address matches their company name and you can visit the company website without using the provided link if you want to. Links will point to the company website and the link shows this when you "mouse-over" the link provided. However, **deals that sound too good to be true probably are.**

Malware often masquerades as email from a parcel tracking service, providing a link to "track a parcel". Be especially wary of such email – especially if you have a parcel in transit somewhere. **Who is really sending this? And where does the link point?** If you have a parcel in transit, only ever use the link provided by the seller.

When you receive an unsolicited email with **little or no explanation of what is being sent to you as an attachment or in a link – be very suspicious.**

What are they asking me to do?

Open a link

When you move the mouse cursor over a hyperlink, the target URL shows up. Is this link pointing to a website that has a **recognisable domain name consistent with the sender's email address?** Is it to a web page to which you would expect to be taken, given the context of the email's contents and subject?

Open an attachment

Sending someone a piece of malicious code (sometimes called a "virus") is a common way to infect a computer. The **code is usually disguised as something** like a .pdf document or Microsoft Word file.

Any email attachment should be regarded as potentially risky. The trust you place in it should be supported by all of the other information in the email. The subject should be consistent with the attachment and the body of the text should explain what the attachment is and why they are sending it to you.

Should I do it?

Are you satisfied that the text of the email provides sufficient reason to think the attachment is safe? Emails with attachments or links with no text in the body of the email should generally not be opened – especially if they come from unknown sources.

Any email that comes from a business entity should have a footer with the contact details of the

sender. Be aware, however, that this is easily forged, and it is now quite common for fraudsters to include nicely-designed footers. Do not rely solely on footers.

WHAT ARE THE RISKS?

To Click - Of opening the link/attachment

Malware infection – eg "Cryptolocker" malware could encrypt your data, preventing you or your organisation being able to access it. "Keystroke logging" software could be installed onto your machine, which could send every keystroke from your keyboard to cyber-criminals who could hold email users to ransom or to steal username and password combinations.

Or Not to Click - Of not opening the link/attachment and deleting the email

Usually the risk of deleting an email is quite small. Certainly smaller than the risk of opening a dodgy email. **If you delete a genuine email by being cautious, you're likely to get a follow-up email or perhaps, a phone call from the sender of the original email.**

If you are unsure whether it is safe to open an emailed file attachment or click on a link, (ie you are inclined to think it is genuine, but you don't have enough information to be sure) then you should either delete the email or respond requesting more information about what is being sent.

April 2016

New Zealand Law Society
Law Society Building
26 Waring Taylor Street
Wellington 6011

PO Box 5041
Lambton Quay
Wellington 6145

04 472 7837