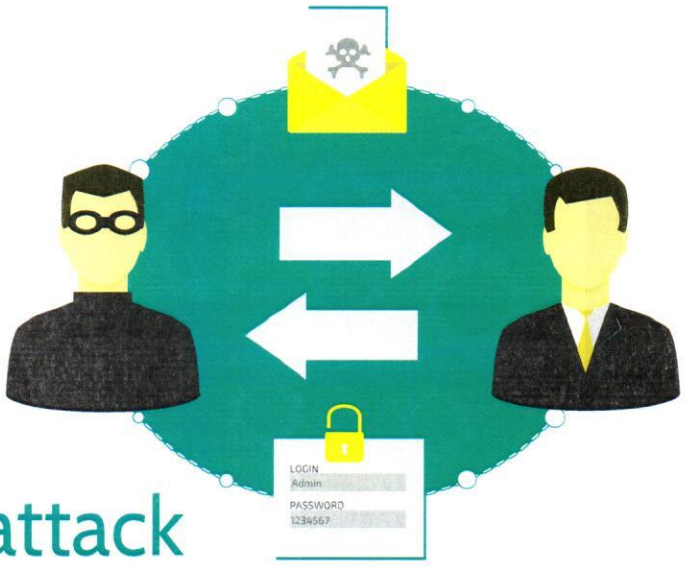
Don't take the bait

on a spear phishing attack



By now, most lawyers are familiar with phishing attacks. For those who are not, phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email. They take the form of a message, allegedly from your bank or an online retailer you deal with, that suggests your account has been compromised or that payment is overdue. Phishing scams are usually bulk emails sent to large numbers of people. Even if only two or three per cent of recipients fall for them, hundreds or even thousands of people can be victimized.

Like convincing bait, these messages include the same layout, logos and links as legitimate emails from these companies. Phishing messages try to create a sense of urgency and ask you to login to reset your password or verify a payment was made, etc. However, the link you click takes you to an imposter website that looks much like the familiar company site, but when you login you are actually giving your password or other personal information to the hackers. They will use your information for malicious purposes such as ID theft or credit card fraud.

Spear phishing attacks take phishing to a higher level. They are a concern to LawPRO as Ontario firms have been targeted as have firms elsewhere.

The "spear" in spear phishing alludes to the fact that messages are targeted to specific individuals. Spear phishing messages are more convincing because they are personally addressed, appear to be from someone you already know, and may include other detailed personalized information.

In one case, a senior accounting staff member at a large firm received a request on an active file, purportedly from the firm's managing partner, to send a bank account number and account signatures to a person in Europe so they could verify a certified cheque was from the firm. While spear fishing scammers will sometimes use public information from social media or the web to personalize the message, in this case, the fraudster seemed to know details about the matter that were not public. The email was even followed up with a phone call.

Thankfully, the person receiving the email noticed some irregularities: the email opened with an honorific and surname, notwithstanding that these two people had worked together for more than two decades and always addressed each other using their first names; the message used odd phrasing; and, on the call, the person had an accent that was incongruous with the ethnicity of the name used in the email.

Stay off the hook

Educate the lawyers and staff at your firm to make sure they will not fall for a spear phishing scam. Follow firm processes and procedures for the review and approval of financial transactions – and don't bypass them due to urgent circumstances. Never share confidential client or firm information without being sure it is appropriate to do so by getting confirmation from someone familiar with the file. Be on the lookout for and question any last minute changes on fund transfers or payments. ■

Dan Pinnington is Vice President, Claims Prevention & Stakeholder Relations at LawPRO.

For more advice on keeping your data safe and secure, see the Cybercrime and Law Firms issue of *LawPRO Magazine* (practicepro.ca/cybercrimemag)