Paying attention to the fraud behind the curtain:

Don't get fooled by spoofed email addresses

We have previously written about the dangers associated with email spoofing and phishing schemes, where fraudsters will send fabricated emails purporting to be from a trusted colleague or third party in an effort to trick a lawyer or staff member into clicking on a dangerous link or downloading a dangerous attachment. These fraudulent schemes continue to evolve as lawyers and firms become aware of various red flags and danger signs. Here are recent examples of cyber-fraud and practical advice on how to avoid similar attempts in the future.

One firm's close call during an attempted fraud

It began with multiple members of the firm – staff and lawyers – receiving an email, ostensibly from the firm's receptionist. The address of the sender, as contained in the "From" line of the email, was an exact duplication of the receptionist's work address – it contained no misspellings or other obvious signs of being a spoof. The body of the email simply said "please see attached invoice," and contained an attachment labeled "invoice."

One of the recipients of this email was the firm's bookkeeper, who, in the habit of receiving invoices from the staff and lawyers at the firm, opened the attachment. Upon doing so, and unbeknownst to the bookkeeper, spyware was downloaded onto their computer. The spyware gave the fraudsters access to, among other things, the bookkeeper's email history.

Later that day, the bookkeeper attempted to log into the firm's online-banking service and found that they were unable to do so. Soon after making that discovery, the bookkeeper received a telephone call from an individual claiming to be an employee of the firm's bank. In reality, the individual on the phone was the fraudster. The fraudster gained the bookkeeper's trust during their conversation by referencing details gleaned from the bookkeeper's email history as to the firm's banking relationship, including

referencing the firm's account manager at the bank by name.

Once the fraudster gained the bookkeeper's trust, the fraudster "explained" that the bookkeeper's online banking credentials would need to be resubmitted. Doing so required not only a username and password, but also the use of two separate token-generated, one-time-use codes (these are numerical codes generated by a key-fob device possessed by the staff and lawyers at the firm, which are valid for a limited time and cannot be reverse-engineered by outside parties – for example, an RSA SecurID mechanism). When the bookkeeper entered the required credentials, including the token-generated codes, the fraudster was able to surreptitiously acquire the information being entered into the bookkeeper's computer and simultaneously use those credentials to access the firm's online-banking account from the fraudster's location. The fraudster then initiated a transfer of a large amount of money from the firm's trust account into an account controlled by the fraudster.

Luckily, the bookkeeper noticed the unauthorized transfer soon after it occurred. The firm's bank was immediately notified of the fraud attempt, and the bank was able to halt and reverse the transfer before the fraudsters were able to remove the funds to a place where they could no longer be retrieved.

Although this story had a happy ending, not every firm targeted by a phishing scheme will be so lucky. Even though the firm had taken steps to ensure cybersecurity – such as using two-factor authentication with token-generated, one-time-use codes – these steps were circumvented through clever deception on the part of the fraudster.

What's clear is that, in this case, the unfortunate course of events was put in motion by the bookkeeper's failure to realize that the initial "invoice" email was a spoof. Had that mistake been avoided, the attempted fraud would have been unsuccessful.

Tips on how to avoid falling for spoofed email addresses

Most lawyers are now aware that fraudsters may send fraudulent email that erroneously appears to be from a colleague or trusted third party. Sometimes these phony emails are sent from an email address that can be identified as phony upon closer inspection (such as when the domain of the address is slightly misspelled, e.g. lawyer@lawwpro.ca). However, many otherwise tech-savvy lawyers are unaware that a sender's email address appearing in the "From" line can be identically spoofed. That is, a fraudster can send an email to an individual or individuals from the fraudster's server, but the email will appear to be from a trusted party, with no way to distinguish the phony email from one actually sent by the trusted party by reviewing only the sender's address as it appears in the "From" line.

However, there are a few relatively simple things that can be done to reduce the chance of being fooled by spoofed emails in these circumstances.

Don't immediately click on any links or open any attachments that you are not specifically expecting to receive

Lawyers and staff deal with voluminous amounts of email every day, and it may not be reasonable to take additional steps to ensure the validity of every single email received and reviewed. However, if you receive a link or attachment that you were not specifically expecting, even if it appears to be from a trusted third party or is something you would regularly receive in the ordinary course of business (such as an invoice being received by a bookkeeper), it is always best to take additional steps to confirm the identity of the sender. If the sender is a colleague or someone that can be easily reached by phone, a quick call to the apparent sender can provide assurances as to the email's authenticity.

Check the "return-path" address in addition to the "From" line

Every email is received with two "from" addresses. The first is the address that appears in the "From" line, this is also known as a "header from." It is what we normally think of when we identify the sender of the email. However, the email is also tagged with a "return-path" address, also known as an "envelope from" address, which tells the recipient's server where to send replies. Both the "From" line and the "return path" can be spoofed by fraudsters. However, sometimes the fraudster uses a different address for the return path to ensure that any replies will actually be sent to the fraudster and not the actual trustworthy party whose email is being spoofed.

Although the return path address is not immediately visible to the recipient of the email, it can be identified by bringing up the delivery details and full "header" properties of the email. This can usually be done from a drop-down menu, depending on the email application being used.

Check the geographic origin of the email through the sender's IP address

If a suspicious email originated from an unexpected location – for example, one appearing to be sent from an Ontario-based client, but with an originating IP address located on another continent – this can be a useful warning sign that the email may not be what it appears.

It is possible to trace the geographic origin of some, but not all, emails through the sender's IP address as contained in the email's full "header" properties. Emails sent from domains with public IP addresses can usually be traced to their city of origin by entering the sender's IP address into any of the IP lookup tools available for free online.

Unfortunately, this technique cannot always provide the true geographic origin of the sender. Like the "From" line and "return-path" information, IP addresses contained in the full header can be spoofed by a fraudster, making it extremely difficult to deduce the true originating source. As well, some email domains, like Google's Gmail for example, omit the true sender's IP address from all headers, and instead only provide Gmail's central mail server's information.

A brief explainer of the SPF and DKIM email authentication protocols

SPF: SPF allows the owner of a domain to specify which IP addresses are authorized to send email on behalf of that domain. Essentially, the owner of the domain (the firm) will publish in their Domain Name System (DNS) a record of all IP addresses authorized to send email from that domain. This is done by contacting the DNS provider that handles your firm's email domain. Your email application can then be told to do an SPF-record check on incoming messages. The email application will then check the message's "envelope from" address against the authorized IP address published in the DNS. If the email was actually sent from an unauthorized address (essentially, anyone outside the company), it will be flagged by your email provider as potentially fraudulent.

DKIM: DKIM is a process of cryptographically authenticating the content of an email as originating from an authorized sender. In summary, the legitimate emails sent under your firm's domain would be signed with a code (or "hash") that corresponds to the content of the email. That hash is then encrypted using a private encryption key. A corresponding public key is then published in the DNS, much like the SPF record. When your or anyone else's email provider then receives an email with a DKIM signature, ostensibly from your domain, it will apply the public key to decrypt the signature and recover the original hash string. The process will only work, and the email will therefore only be verified, if the actual sender of the email used the correct private key when "signing" the email. This process assures other members of the same firm or office that the actual sender of an email appearing to be from a colleague is trustworthy.

Authenticate emails sent from your firm's domain

One of the most common phishing techniques in the legal profession is to send a target an email that appears to be from a colleague at the same firm or office, using an address with a domain that is owned by the firm. Often it is the address of a colleague that is temporarily away from the office and is unavailable to immediately confirm the email's authenticity. This danger can be avoided by implementing email authentication protocols for your firm's internet domain. Two authentication protocols to be aware of are the SPF (Sender Policy Framework) and the DKIM (Domain Key Identified Mail). These protocols can be implemented relatively easily at no cost. If your firm does not already have access to IT assistance, many user-friendly guides on how to implement these protocols are available online.

While no security procedure provides complete safety from continually evolving fraud threats, these techniques will provide additional confidence to you and your firm that an email claiming to be from a colleague is trustworthy and not part of a fraudulent scheme. ■

Shawn Erker is Legal Writer and Content Manager at LAWPRO