Email Spoofing

Email spoofing is the creation of email messages with a forged sender address, i.e. the email appears to come from a trusted source but is actually from a fraudster.

This type of fraud originates with a phishing email which contains an infected attachment. For example, these emails would often include words such as “invoice” in the subject field and an attachment also titled “invoice”. Opening the attachment installs malware onto the computer. This malware provides the criminals with access to the system. With this access the criminals can then employ many methods of gaining access to confidential information.

The criminals often watch and investigate the internal email traffic in the practice to determine who processes electronic banking requests and which individual is most likely to request one. Then the criminal sends an email to the relevant member of staff in the accounts department from a fee earner requesting a transfer of money to a foreign bank account. As the criminal has access to the system they will identify ongoing cases and can include legitimate client references and names in the email.

In other cases, external emails between the solicitor and the client have been intercepted and read by the criminals. When a genuine email is sent with bank account details enclosed, the fraudster intercepts and amends the details of the bank account. This amended email is then forwarded to the appropriate recipient from the spoofed email account.

If the recipients act on the emails in either of the above cases the money will be transferred to the fraudulent account and subsequently dissipated prior to the fraud being identified, making it very difficult to recover the money.

Precautions Specific to this Type of Attack

Ensure your anti-virus software is fully up-to-date and set to automatically update.

Be skeptical of any attachments received in an email, particularly from an unknown source. If in doubt, do not open the attachment.

Be skeptical of unexpected instructions in relation to the transfer of funds, for example, to foreign bank accounts.

Always check the authenticity of the senders address in the “From” field after opening the email, as this may indicate an anomaly.