Online Security Update: Business Email Compromise

DRUMMOND LAURIE
CHARTERED ACCOUNTANTS

With the seemingly unstoppable move to email as the primary form of business communication, there is the growing risk of fraud and theft from malicious emails apparently sent from someone inside your organisation, or from a supplier or contractor, that have actually been sent from an impostor attempting to extract money from you.

These emails usually take the form of a request from a senior official in your organisation requesting that an urgent payment be made (often with an instruction not to discuss the matter with anyone else) or a request from a contractor or supplier to send all future payments to a new bank account as they have changed their banking arrangements.

It can sometimes be quite difficult to identify these fraudulent emails as the perpetrator will often go to great lengths to make the email appear as genuine as possible, but sometimes some simple checks will often catch them out.

If you are using certain email clients, then they will display the email address of a sender beside their name at the top of the email. This is often enough to identify a suspicious email as the email address will not match the supposed sender of the email.

For example, an email that was received recently here at Drummond Laurie was supposedly from NatWest stating that changes had been made on a credit card, and giving a link to click on to check the changes. The email was from NatWest, but the email address displayed was Natwest_creditcard@btconnect.com. As its highly unlikely that an organisation such as Nat West bank would use a generic email address like this, especially a non natwest.com one with no clear links to them, then this was enough to set alarm bells ringing.

Similarly, when reading an email, quite often if you put the mouse pointer over any links, but don't actually click on them, then they will display the address that the link leads to, which again can be compared with the contents of the email and can identify a fraudulent one. In the same example as above, the link to check the changes on the credit card actually led to daddytom.net which appeared to be nothing at all to do with Nat West and therefore raised suspicions immediately.

Despite the above, suspicious emails may not be detected, or an actual email account may have been hacked into and thus the email will appear 100% genuine. Therefore it is important to also have procedures in place to prevent this sort of attempted fraud / theft from succeeding.

Firstly, make any relevant staff aware of this type of fraud / theft so that they can look out for it and recognise the risks involved.

Additionally look at putting technical and other measures into place to reduce / eliminate the chances of such fraud occurring, such as:

- If you can, set your email system to reject all emails seemingly from someone in your organisation but sent from out with your network. For example, any drummondlaurie.co.uk

emails can only be sent using our server, so therefore anything that is received from outside with a drummondlaurie.co.uk email address is automatically rejected.

- Always confirm any changes to bank or other sensitive information with the contractor / supplier directly, using contact details from your existing systems rather than anything in the email.

- Have a system in place that ensures that any changes to bank account details etc. are not entered by the same person that is responsible for entering any payments, i.e. involve at least two people in the process, with one of them preferably being someone at a more senior level.

- Have clear procedures in place for payments being made from your own organisation, with recognised levels of authority and the steps that must be followed before changing / adding any bank details. These procedures should clearly cover what should happen if a one-off or urgent payment needs made, and should be followed by **everyone** no matter what their level of seniority. If your staff get used to seeing them being followed, even by the managing director, then they are much more likely to question something, even if the email is seemingly from the MD and instructs them not to discuss the matter.

- Finally, work with your IT department or adviser to put technical measures in place to identify suspicious links and block emails from known fraudulent email addresses. Whilst no system will ever completely eliminate such emails, by reducing them to a lower level it will make it easier to pick out the ones that do get through.

Whilst the above is a guide to dealing with these kinds of emails, the internet is fast-paced and always changing and therefore it is recommended you seek advice from your own IT department or adviser for more specific options for your organisation.

For any general queries, please contact ross.nicol@drummondlaurie.co.uk