UHY Hacker Young
Chartered Accountants

ALERT
Email scam

A guide on how to protect yourself and your business

Make sure you are up-to-date with the latest email scam.

We have recently seen a rise in the number of email scams whereby criminals impersonate a colleague to deceive other employees into transferring money into a fraudulent account.

The scammer will send an email to your accounts department which will appear to be from a senior colleague requesting a payment be made to a third party company. This process is a form of 'spoofing' whereby the scammer creates an email message using a forged sender address.

Many spoof emails can be extremely hard to spot, therefore, it is of upmost importance that your staff are aware of the practical steps they can take in determining whether an email is genuine.

WHAT SHOULD I LOOK FOR?

To assess whether an email is legitimate, you should consider all of the following indicators:

- An internal email, even if sent from a mobile phone, will only display the sender's name in the 'from' field. However, if it is an external email which is using the identity of an internal recipient it will often have inverted commas around it eg. 'Robin Jones'.
- When replying to an email, always check the 'to' field. If it is an internal contact or a contact that you have saved within your address book, then this field should only display the person's name. An email from an outside source impersonating someone will often appear like this:
  Robin Jones <name@fakeemail.com>.
- Is the tone or language of the email normal? Are there lots of spelling errors? Do they fail to use your name? Are they asking you to do something irregular such as bypass a standard policy? All of these factors can indicate a fraudulent email.
- If you have a suspicion about any instruction given by email, speak to the person who gave the instruction, ideally in person or on the phone if you know them well enough to recognise their voice.
- When replying, even if to a regular contact, do not give out any private or confidential information, be wary of anything asked of you and always ask yourself why the information would be needed by that person. If they do not need it, do not divulge it.

Additionally, when dealing with any business relationship, the following should be observed:

- Consider setting up designated single points of contact with companies to whom regular payments are made.
- Any changes to the point of contact for clients or suppliers should be verified with the business' management team.
- Confirm any requested changes in financial instructions using an established contact before making any changes.
- For payments over a certain amount, consider additional checks with the company or colleague requesting payment, and obtain confirmation that the payment will be sent to the correct bank account and recipient.

THE NEXT STEP

If you have any doubts about the validity of an email, we strongly recommend contacting your IT department who can trace where the email originated.

Alternatively, for further information or to discuss any concerns in relation to your specific circumstances, please contact us via email at: marketing@uhy-uk.com or by visiting our website at: www.uhy-uk.com.

www.uhy-uk.com

Helping you prosper