Fraud awareness

The number of attempts at fraud affecting financial services customers is growing all the time. If you understand the threats and how to spot the possible warning signs, you stand a better chance of keeping both your clients and your business safe.

Two techniques used by fraudsters it is important to be aware of are phishing and email hacking. These can be used to gain control of a client's email account, which the fraudsters then use to send out a withdrawal request. This withdrawal request is generally accompanied by new bank account details, along with 'proof of account documents', like bank statements.

Is that email really from a client?

When you get an email from a client, ask yourself the following questions – the answers could offer clues as to whether the email has actually been sent by a fraudster.

- Does this client usually communicate with you by email? If not, bear in mind that fraudsters often prefer to communicate by email, and will generally make excuses to explain why they cannot be contacted by phone.
- If the email purports to be from a client you have a well-established relationship with, does it seem uncharacteristically blunt?
- Does the email contain terms or expressions which the client would not normally use?
- Is there a lot of bad grammar, unusual language or poor spelling? Does the tone of the email seem different to normal?
- Are there any mistakes or inconsistencies in terms of the information given?
- Is the email asking for something to be done urgently? Does it set any unrealistic timescales?
- If you try to verify any requests made in the email, do you get a satisfactory answer? Bear in mind that if a customer states they haven't received a particular email or emails from an intermediary, it is possible that fraudsters have intercepted the email and created a new folder for all subsequent emails, making them invisible to the client.
- Is there a time difference which suggests the email was sent from abroad?
- Is the email requesting you to do something which is outside your customer's usual pattern of behaviour, like making a withdrawal?
- Have they requested a withdrawal that exceeds the current value of funds held?
- Does the email request that you forward on a prepopulated withdrawal form?
- Have they provided new bank details for funds to be sent to? Is this bank anywhere near where the client actually lives?
- Are they suddenly willing to pay a fee, such as a CHAPS payment fee, in order for you to send the funds quickly?

Other things to look out for

If the 'client' forwards you any documents or completed forms, bear the following in mind.

- Fraudsters may choose to forward any completed documents by scanning and emailing them to you, in keeping with the urgent nature of the request.
- They might provide bank statements or other documents to 'prove' the bank account receiving any funds is genuine, but these documents could be faked. Check the colours and typeface are correct.
- Ask yourself if the transactions shown on any bank statement provided match up with what you know about the client, e.g. why does that vegetarian lady keep eating out in steak houses?
- Fraudsters often request partial withdrawals from just one wrapper – usually the biggest. Does the choice of wrapper requested seem strange to you?

Foil the fraudsters – follow these tips

- If you are sent an instruction via email, make sure you get verification from another channel before acting.
- Only use a registered contact number to reach clients, and verify their identity before confirming any instruction.
- Never email out prepopulated withdrawal forms.
- Always use original documents to validate bank account details. Do not rely on electronic documents.
- Keep all anti-virus software up to date and ensure firewalls are robust.
- Look out for 'voice phishing' (or 'vishing'). This is when fraudsters call up and impersonate clients in order to access personal information.
- If you suspect that an email is fraudulent, tell your colleagues as they may have received it too.

AJBIC/FA/20210413