Protecting your firm and your clients

One way to help protect your firm and your clients is to understand the ways in which you might be targeted. Criminals use many tactics to try and steal information or money, but the most common ones are:

- Phishing – an email is sent from an ostensibly trustworthy source in an attempt to trick the recipient into providing sensitive information. This approach can also be used in text messages and phone calls.
- Malware – the criminal may distribute malware (malicious software) via email or compromised websites. The malware can then be used to capture sensitive information such as banking details and card numbers.
- Social engineering – the criminal will try to manipulate their intended victim psychologically. They may pretend to be a trusted source (as seen in phishing) and create a sense of urgency as a way of getting the recipient to act quickly and send over sensitive information.

Phishing scams

Phishing attempts can take place via email, text message, phone call and social media. Attackers target the recipient by tricking them into falling for the attacker's desired action; this could include revealing financial information, system login details, or other sensitive information.

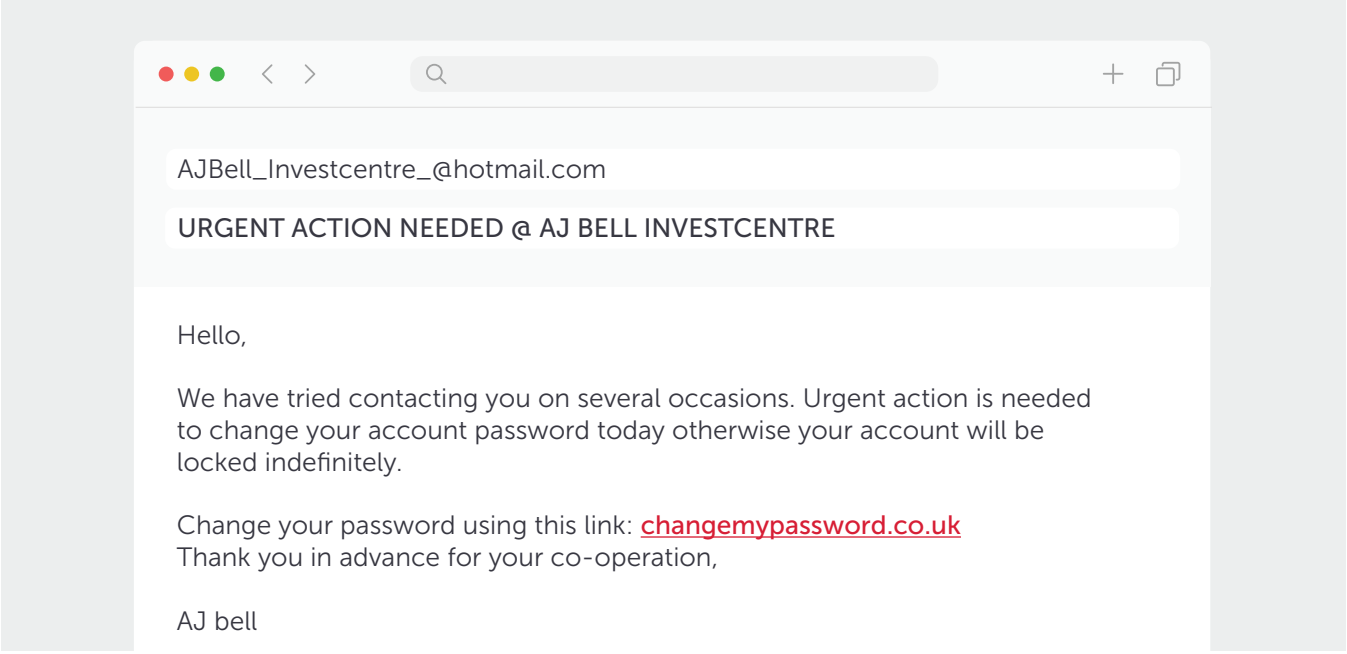
Phishing involves psychological manipulation and deception whereby attackers present themselves as reputable people or businesses in order to entice you into taking action such as clicking links to fake websites, downloading and installing malicious files, or divulging private information, like bank account numbers or credit card information.

Scammers target people using this technique because it is simple to navigate, affordable and highly effective. If you or your clients fall victim to a phishing scam you are susceptible to malware infections, identity theft and data loss.

Phishing techniques

Email phishing

Email is the most common phishing tactic. A phishing email might ask you to open an attachment, call a fake customer care number, or click on a website link. These emails usually present a sense of urgency.



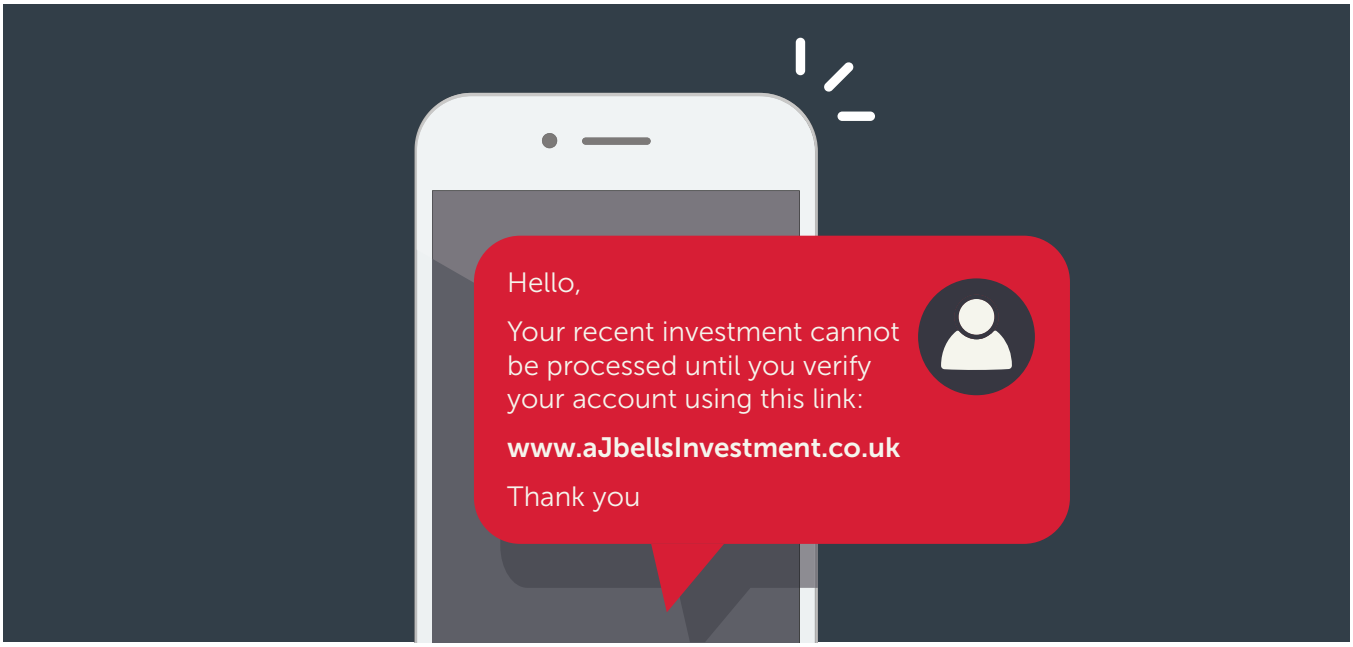
Impersonation

A client or associate's email is hacked and used to communicate instructions to transfer or withdraw funds. The fraudsters can access template payment instructions from previous emails within the hacked address, which include signatories, and change only the account number.

Or, instruction is sent from clients to make payments or change bank details from an email address that appears to be from a recognised client – we encourage you to always call a client before making any exchange of money or personal details, to confirm a request.

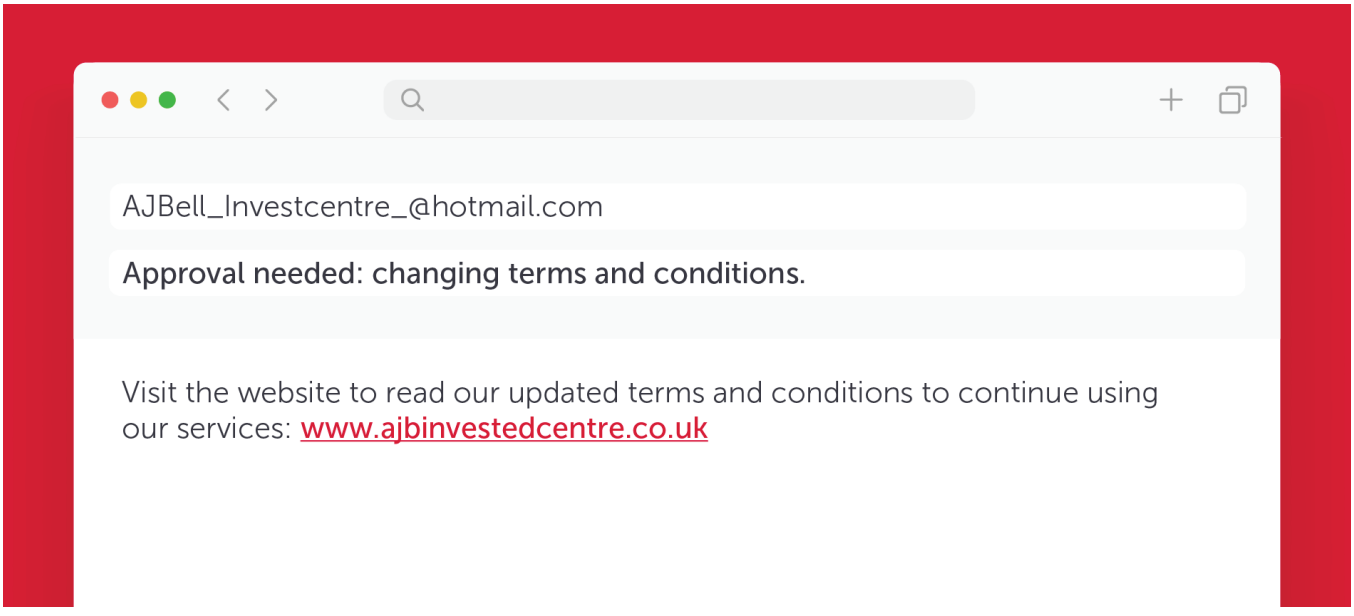
Fake texts

They will give you a link or a number to call and include a message that invokes a sense of urgency.



Fake websites

Fake websites generally work with phishing emails. An email will give you the link to a fake website and when you click on it, it might ask for your password or bank information. In some cases, clicking on the link may even install malware on your device.



Spear phishing

Where most phishing attacks cast a wide net, spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customised, making them particularly effective at bypassing basic cybersecurity.

How to prevent phishing attacks

Know what to look out for – it's important that your organisation and your clients are aware of the different types of phishing tactics as the first way of keeping yourselves safe.

Internal training resources for staff are key, as well as carrying out various phishing tests.

Email security and anti-spoofing – invest in software that makes it difficult for fake emails to be sent from your organisation's domain. Details of the types of software can be found on the National Cyber Security website.

Avoid clicking links – if you are unsure about a link, instead of clicking it, type the official domain into a browser and authenticate directly from the manually typed site.

Change passwords regularly – we'd encourage you to change your passwords every 30-45 days to reduce an attacker's window of opportunity. Leaving passwords active for too long gives an attacker indefinite access to a compromised account.

If you, your firm or a client suspects they have fallen victim to a phishing scam we encourage you to report it via the details on the GOV.UK website.

CEO fraud

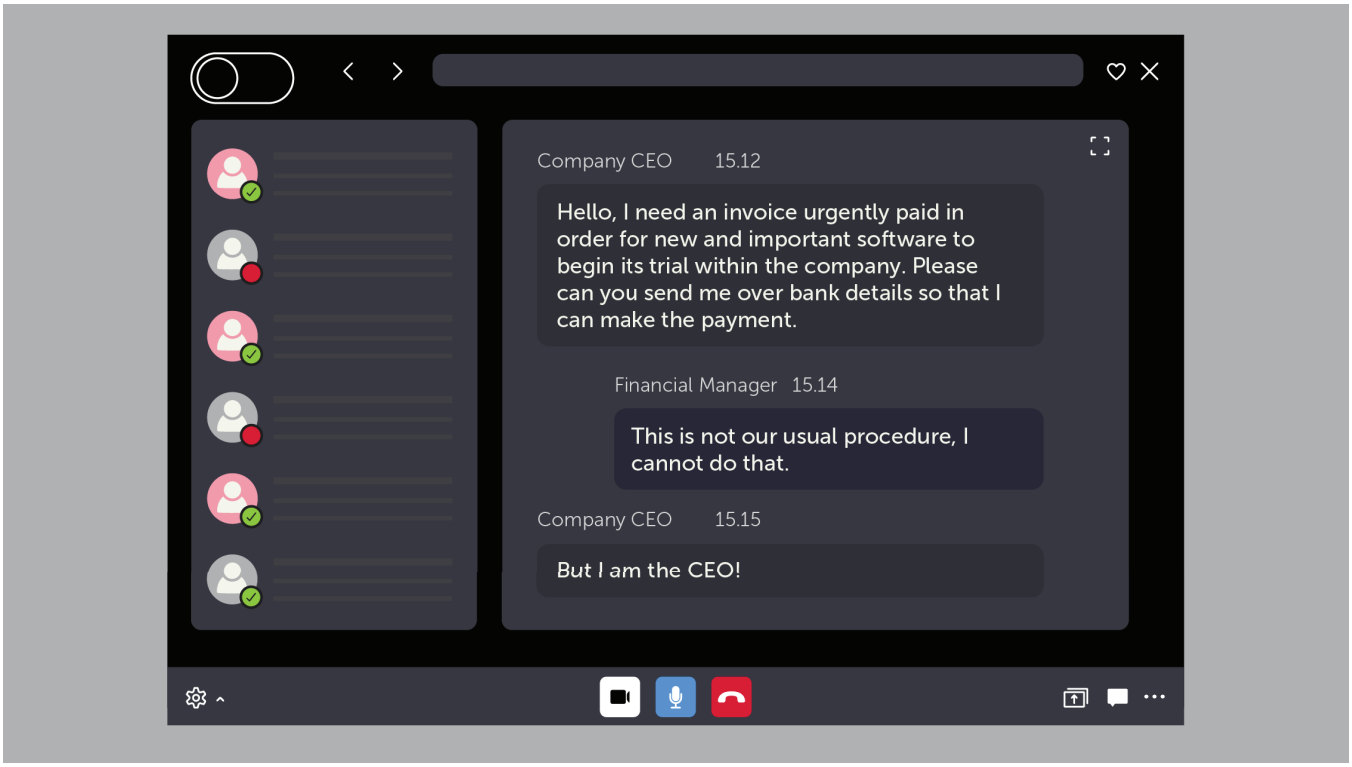
This type of scam can occur when a scammer tries to impersonate your boss or a senior manager, either to make an urgent payment or change payment details for a contract or supplier.

They can access your business' email account by hacking or use spoofing software to email a member of the finance team with what appears to be a genuine email from your boss or a senior manager.

This process can develop over a couple of months as the scammer looks to build a picture of the structure of your firm and the employees responsible for authorising payments. Your website can sometimes reveal information about genuine suppliers that can then be used by criminals.

Identifying a CEO scam

- You're asked to urgently process an out-of-the-ordinary payment by your CEO, a boss or a senior manager.
- The language used in the email isn't consistent with that of the genuine sender.
- You're asked to change the bank details of an existing supplier on your system.



If you believe you've fallen for a scam, contact your bank immediately on a number you know to be correct, such as the one listed on your statement, their website or on the back of your debit or credit card.

Report it to Action Fraud on 0300 123 2040 or via actionfraud.police.uk. If you are in Scotland, please report to Police Scotland directly by calling 101 or Advice Direct Scotland on 0808 164 6000.

Invoice fraud

These scams happen when criminals pose as a regular supplier and persuade you to change the bank account details already on file. You're then tricked into sending money to the account which is controlled by a criminal rather than the genuine supplier.

Criminals carry out extensive research about your business to find out who your suppliers are and when regular payments are due. These scams often involve a criminal intercepting emails, gaining access to your supplier's email account or spoofing their emails.

The fraud is often only discovered when the legitimate supplier of the product or service chases for non-payment. At that point recovery of the funds from the fraudulent account is very difficult.

How do you spot this scam?

- You receive a request out of the blue to change the bank details of an existing supplier.
- You receive more frequent than usual or duplicate invoices for a product or service.

Fake WhatsApp groups

Scammers are now attempting to coax people into sending across money or personal information via WhatsApp.

If you receive an unexpected WhatsApp message, treat it with caution – remember companies are unlikely to contact people out of the blue on WhatsApp without any notice.

Never click on any links in unsolicited WhatsApp messages. You can report the message by selecting it in your conversation list and tapping 'report'. To report the sender on WhatsApp, open up the chat, tap on the sender's contact details and select 'Block and Report'.

Pretexting

Attackers will sometimes use a made-up scenario to gain your trust – have you ever received a phone call claiming to be Microsoft telling you that your laptop is full of viruses? Another example would be somebody pretending to be from the IT team, mentioning names of people they discovered whilst researching your company. They might say that they need to install some updates on your workstation and need to validate a few things.

What do you do?

Stay vigilant. Never provide any information over the phone, online or in person until you have confirmed the identity of the person you're speaking to. Call the person back using the number provided on their organisation's website.

AJBIC/FA-PYFYC/20240201