Protecting you and your money

One way to help protect you and your money 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 you 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 you psychologically. They may pretend to be a trusted source (as seen in phishing) and create a sense of urgency as a way of getting you 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.

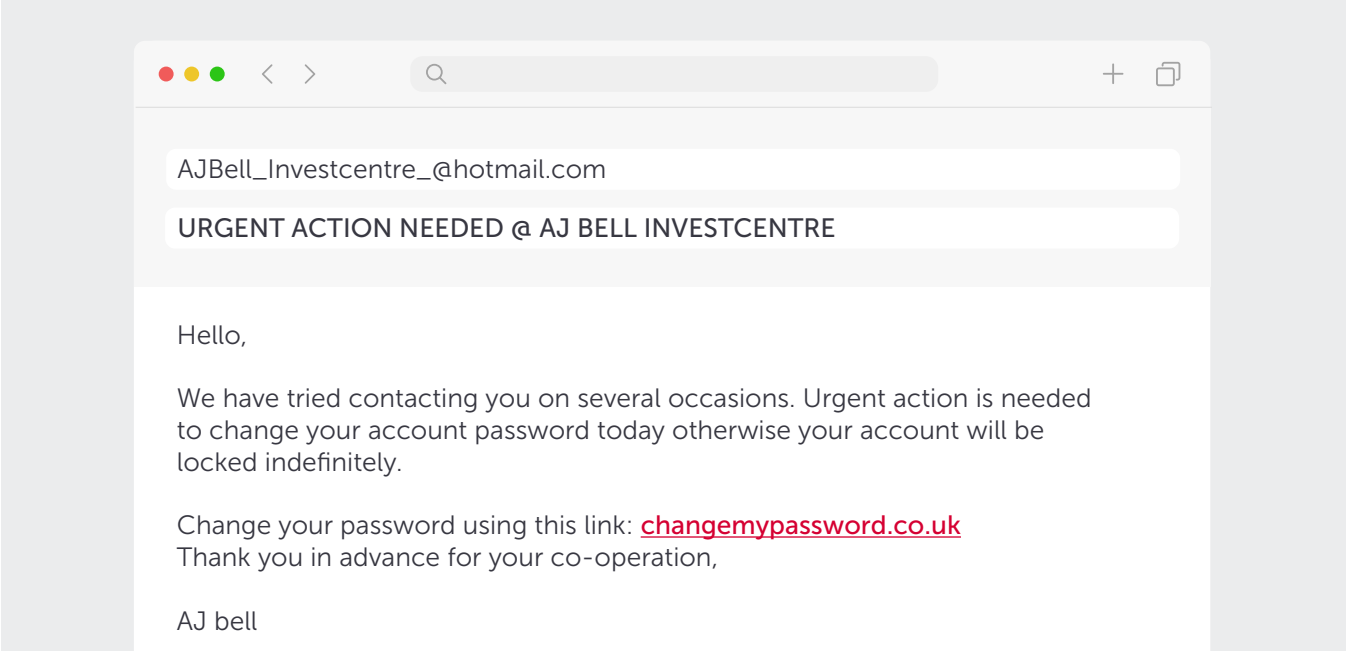
Phishing involves psychological manipulation and deception where attackers present themselves as reputable people or businesses in order to entice you into taking action such as clicking links to fake websites, downloading and installing malicious files, or divulging private information, like bank account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

Scammers target people using this technique because it is simple to navigate, affordable and highly effective. If you fall victim to a phishing scam you are then 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.



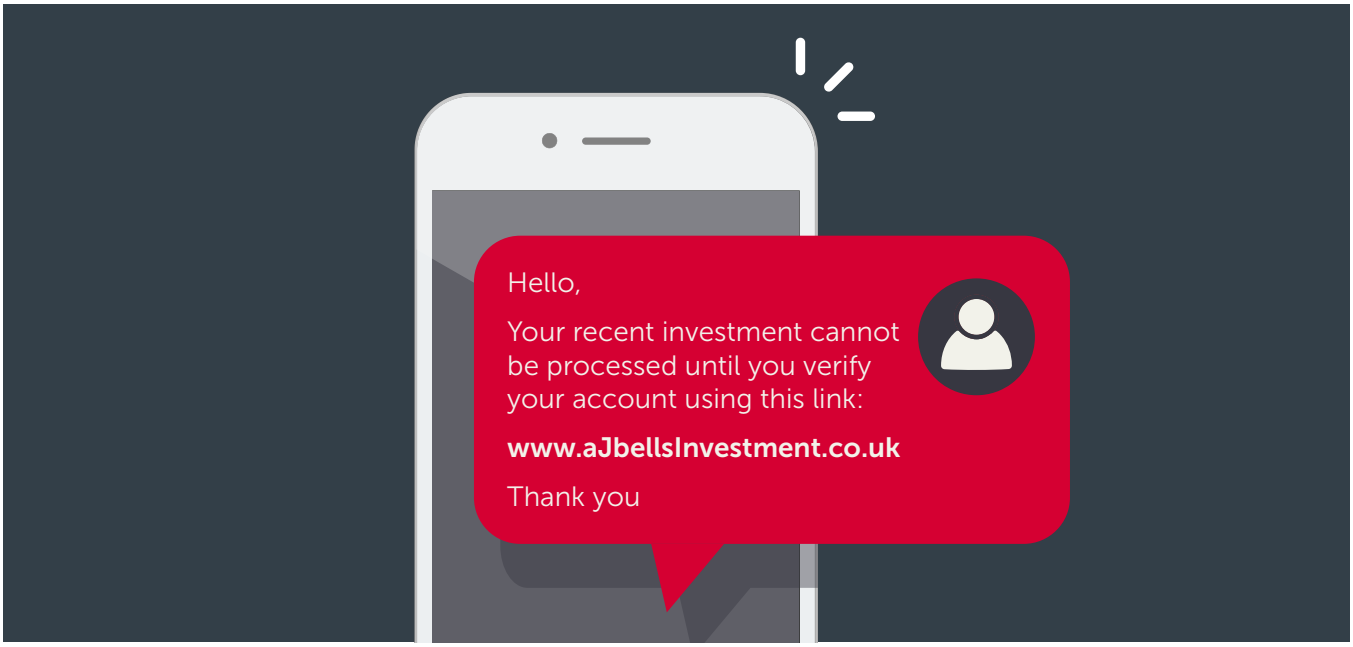
Impersonation

You or your adviser's email is hacked and used to send instructions to your ISA or pension provider 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, an email is sent from what looks to be your address to your adviser, asking to make payments or change bank details – we encourage advisers to always call clients before making any exchange of money or personal details, to confirm a request.

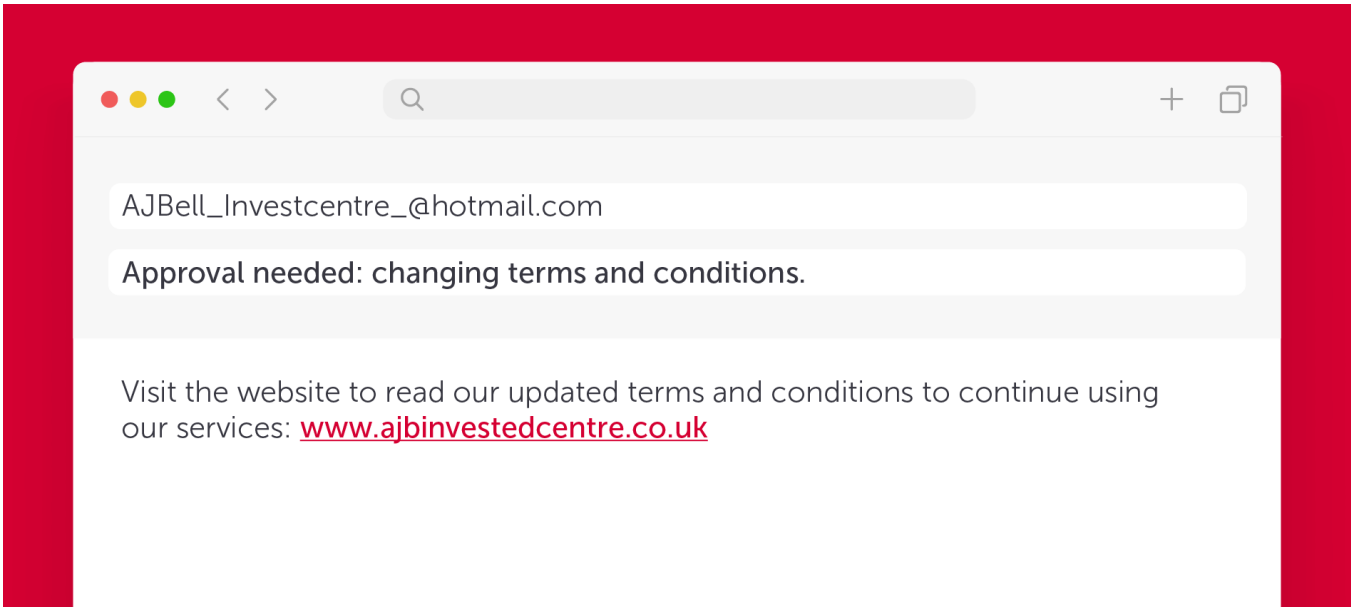
Fake texts

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 you are aware of the different types of phishing tactics as the first way of keeping yourself safe.

Email security and anti-spoofing – if you can, invest in software that makes it difficult for fake emails to be sent from your 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 suspect you have fallen victim to a phishing scam we encourage you to report it via the details on the GOV.UK website.

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 your adviser's firm, mentioning names of people they discovered whilst researching their company. They might say that they 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.