ClickRegion.

WHAT ARE SOME OF THE SIGNS I SHOULD LOOK OUT FOR WHEN LOOKING FOR SCAM EMAILS?

A scam email usually has a weird email disguised behind an address that looks genuine. To find out if there's a scammer behind what looks like a genuine sender, use your mouse to hover the cursor over or right-click on the sender name and you should see the email address behind it. Does this email match the company name they are contacting you from?

Are they trying to rush you or giving you a false sense of urgency? "this needs to be actioned immediately" "failure to do so will result in ...."

Does the email sender use poor grammar and spelling?

An impersonal greeting "Hi" not addressing you correctly or "Greetings".

Asking for personal information like banking details or passwords.

Scammers might also try too hard to make the email sound official. They will do this in a number of ways, including using the word ‘official’. You are unlikely to see messaging about 'how official a company is' in an authentic email.

Does this email also contain information such as account numbers and IDs designed to trick you into thinking the email is genuine. Check any of these against your records to see if they match.

If you're still unsure whether a scammer is behind the email you received, get in touch with the brand or company featured in your email directly via social media or their 'contact us' page via googling them. DO NOT use the email for their contact us page, call them instead.

Remember to check the brand or company's help and customer services pages. Often big companies are aware of scams circulating and have published advice for customers on what to watch out for.

And, if you do accidentally click on something in the email DO NOT PANIC.
Call your bank and tell them.
Change your passwords on your email accounts from another device,
notify the real entity of the scam and alert police if required.

BUILDING
DIGITAL
CONFIDENCE