

## Phishing

**[Voiceover]** Phishing scams, also known as email scams, are when fraudsters create the illusion that they're your bank or a trusted organisation.

They'll try and trick you into clicking fake links, to revealing your personal information.

They'll probably tell you your account is at risk, say your password is about to expire or convince you a recent payment wasn't received.

The links in the email aren't as they seem...

...They'll lead you to a website that might download malware.

Then as if by magic, the fraudsters have direct access to your personal information.

You can stay one step ahead of fraudsters tricks by hovering your mouse over the links so it shows you the real destination.

Checking the email address is spelt correctly and is coming from who they claim to be, watching out for generic greetings.

Most official emails will contain your name...

...Thinking twice about emails that ask you to act quickly.

And remember, HSBC will never ask you for your personal information via email, convince you to share your one time codes or Secure Key Code, scare you into giving away your personal information or email you a link that takes you directly to a login page.

HSBC will only ever send you links that lead to [www.hsbc.co.uk](http://www.hsbc.co.uk) or [www.hsbc.com](http://www.hsbc.com)

If you have doubts, don't reply or click any links and report it to [phishing@hsbc.co.uk](mailto:phishing@hsbc.co.uk)

If you think you've been a victim of fraud, call the number on the back of your card.