HSBC

Video transcript

Smishing

[Voiceover] Smishing scams, also known as text scams, are when fraudsters create the illusion of being your bank or a trusted organisation.

It can be a tough trick to spot as fraudsters are a master of disguise.

Their texts can appear in the same thread as messages from trusted organisations.

They will often pressure you to take urgent action, making you give away your personal information or bank details, verify a new payee, device or transaction, rebook a delivery you never made by paying a fee or click on suspicious links.

If you are suspicious of a message you receive, don't click on any links, download any attachments or reply to the sender.

Stay one step ahead.

HSBC will never coerce you into replying to genuine fraud SMS alerts incorrectly, try to scare you into giving away your personal information, or ask you to share your one-time codes or Secure Key Code. Your PIN, passwords and Secure Key are all for your eyes only.

So keep your cards close to your chest by not sharing it with anyone, whether that's over the phone, by text or in person.

If you think you've been a victim of this scam, call the customer support number on the back of your card.