

1

00:00:02--> 00:00:08

Smishing is a fraudulent text message that tricks you into sharing confidential bank account details.

2

00:00:08 --> 00:00:10

Here's how it works:

3

00:00:10 --> 00:00:16

You receive a text message with a link claiming to be from HSBC or another organisation.

4

00:00:16 --> 00:00:20

Some messages might instruct you to call a fraudulent phone number.

5

00:00:20 --> 00:00: 27

You're then taken to a fake website or voice call asking you to share your personal or banking details.

6

00:00:27 --> 00:00:28

Protecting yourself is simple:

7

00:00:29 --> 00:00:30

Don't click.

8

00:00:30 --> 00:00:31

Don't call.

9

00:00:31 --> 00:00: 32

Don't reply.

10

00:00:32 --> 00:00:36

Stay alert and when in doubt call us directly to verify.