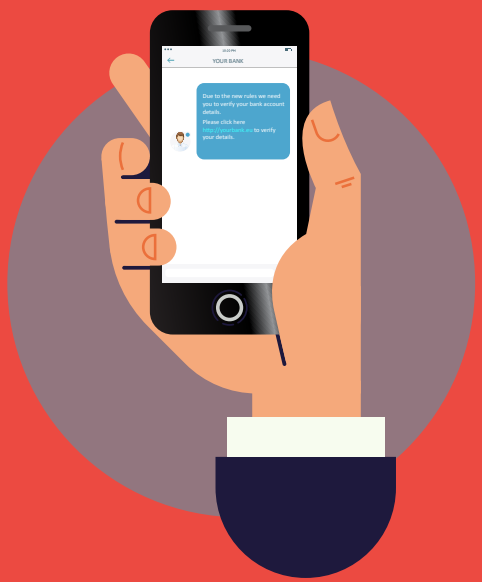
BANK SMISHING SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- **Don't click on links, attachments or images** that you receive in unsolicited text messages without first verifying the sender.
- **Don't be rushed.** Take your time and make the appropriate checks before responding.
- **Never respond to a text message** that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, **contact your bank immediately**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

#CyberScams