DRAFT

BANK PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.



HOW DOES IT WORK?

These emails:

may look identical to the types of correspondence that actual banks send.



replicate the logos, layout and tone of real emails.

ask you to download an attached document or click on a link.

use language that transmits a sense of urgency.

WHAT CAN YOU DO?

- **Keep your software updated,** including your browser, antivirus and operating system.
- Be especially **vigilant** if a 'bank' email requests sensitive information from you (e.g. your online banking account password).
- **Look at the email closely**: compare the address with previous real messages from your bank. Check for **bad spelling and grammar.**
- **Don't reply to a suspicious email,** instead forward it to your bank by typing in the address yourself.
- **Don't click on the link or download the attachment,** instead type the address in your browser.
- When in doubt, **double check** on your bank's website or give the bank a call.

Cybercriminals rely on the fact that people are busy; at a glance, these spoof emails appear to be legitimate.

Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet.

#CyberScams



EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

DRAFT - NOT FOR PUBLIC USE

DRAFT

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**.

DRAFT

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.



WHAT CAN YOU DO?

- **Beware** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank.**



EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

DRAFT - NOT FOR PUBLIC USE #CyberScams