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

Association of Banks in Bulgaria