IMPORTANT INFORMATION

Fraudsters can use reliable institutions names like banks, public institutions, telco operators, widely used software companies like Apple, Microsoft etc.

They may send SMS or e-mails on behalf of such companies/institution with links to update customer data like card numbers, card expiry date,
CVV of card, pin of card, social security number, e-banking/ mobile banking password, e-mail, windows passwords, mother maiden name etc.

Such institutions never ask such kind of information via e-mail, SMS or any other channel of communication. Don't share your personal information with anyone.

BKT
BANKA KOMBETARE TREGTARE

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.

use language that transmits a sense of urgency.

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

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.

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.

#CyberScams

BANKA KOMBETARE TREGTARE

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 IT WORKS?

The seemingly legitimate message will ask you to click a link or call a phone number because:

- You have won a gift
- You must “verify”, “refresh” or “reactivate” your account
- You need to "update" your phone number
- You need to "learn more" about an issue that concerns you

The link actually directs you to a website and phone number of the scammer pretending to be a bank or a government institution.

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**.

Note: The ownership and responsibility of the credentials and sharing the credentials with third unverified parties belongs to the customer.

BKT
BANKA KOMBETARE TREGTARE

#CyberScams