UniCredit Bulbank uses the latest global practices and technologies in the field of Internet security and alternative channels for online banking in order to ensure protection of its customers in a professional manner.

However, your behavior on the Internet is equally important for your security, as are the means of protection and the computers and devices you use to access the Internet.

Recommendations for safe use of alternative channels of banking

- My computer/device has an antivirus software which is updated regularly.
- My antivirus programme has a function for recognition of malware, spyware and trojans.
- I regularly run an antivirus scan on my computer.
- I change my online banking password at least once a month.
- The browser I use for banking is set to the highest level of data protection.
- I use the latest versions of system software, web browser, operating system and firewall.
- When logging in to Internet banking, I always make sure the page is authentic by checking whether the address bar is coloured in green and whether the web page address starts with https://.
- I do not disclose and do not save on the Internet browser my user name and password.
- I do not install programmes of unknown origin and I do not follow links from suspicious messages and emails on the computer I use for banking.
- I download software on my phone/ mobile device only from the official application stores – App Store, Google Play.
- I do not keep my Qualified Electronic Signature (*in case I use such*) always active on my computer when I do not need it.

If you can answer all questions with "YES", you can rest assured that you have done everything possible to ensure your security when using alternative channels of banking

What should we be cautious of – types of online frauds

The more the Internet is used globally, the more active are the criminals who aim at various forms of fraud against the users of the global network, including the customers using alternative channels for online banking.

For us, as a Bank putting a priority on our customers' safety, it is important to draw your attention to the existing fraud schemes in the field of the alternative channels for online banking in order to enable you to identify them in case of occurrence and to protect yourselves.

Current fraud schemes of the cyber criminals

Variant 1:

A FALSE PHONE CALL OR E-MAIL

Description: *This fraud scheme involves a phone call or an e-mail from a person presenting themselves on behalf of a renowned institution (the Bank, a courier service company, an Internet provider, etc.). In the conversation or the e-mail, on the a pretext of need of assistance – correction of a mistaken payment order, an expected delivery, etc., you are requested to provide the code you have received via SMS or other important information.*

REMEMBER! This is an attempted fraud designed to make the customer themselves disclose their personal banking information and the confirmation SMS code received by them.

Necessary actions: Never provide personal banking information (SMS codes, passwords for access, numbers of bank cards) to third parties by phone or in reply to an e-mail. Save the phone number of the person calling or forward the message to the Bank and contact its 24/7 call centre.

Variant 2:

A FALSE LETTER FROM A CONTRACTING PARTY, A PARTNER OR A CLOSE PERSON REGARDING A CHANGE OF THEIR BANK ACCOUNTS

Description: *You may receive a false e-mail from a partner to whom you make regular payments or transfers. With the letter you are informed that your contracting party has new bank accounts which have to be used for any future payments to that contracting party.*

REMEMBER! This is an attempted fraud designed to make the customer themselves order a transfer to the fraudster's account.

Necessary actions: Upon receipt of information about any change of your contracting parties' data (accounts, address, phone number, etc.), always contact them personally in order to verify the necessary data so that the payments can be made accurately.

What should we be cautious of – types of online frauds

Current fraud schemes of the cyber criminals

Variant 3:

A FALSE MESSAGE PROMPTING THE CUSTOMER TO FOLLOW A VERIFICATION PROCEDURE

Description: *When you try to log in to the alternative channels for online banking, a false screen appears, which looks like Bulbank Online. On the pretext of preventing theft of personal data, this screen prompts the user to follow a procedure for generation and sending of an SMS password/ code needed for confirmation and recovery of the normal access.*

REMEMBER! This is an attempted fraud designed to obtain an SMS password! Bulbank Online does not require entering of an SMS password for access to the service. An SMS code is generated only as a result of an active operation performed by the user in the system – such as a transfer, for instance.

Reason for occurrence: The computer is infected with a virus, which manipulates the Internet browser and shows a false screen to the user. Usually, via the virus the hacker has already gained full control over the victim's computer.

Necessary actions: Under no circumstance should you follow the described procedure. Immediately contact the Bank at the phone number of the 24/7 call centre.

Variant 4:

A FALSE MESSAGE REQUIRING THE ENTERING OF DATA OF A MOBILE PHONE - OPERATING SYSTEM AND PHONE NUMBER

Description: *After you log in to the alternative channels for online banking, a false screen appears, which looks like Bulbank Online. On the pretext of providing additional protection of the customer's mobile phone from malware, it requires from the user to follow steps for installation of a mobile antivirus programme through entering of data about the operating system, the phone number, etc.*

REMEMBER! This is an attempted fraud designed to make the customer install a hacker programme on their phone, which programme will redirect the messages received from the Bank to the fraudster's phone number.

Reason for occurrence: The computer is infected with a virus, which manipulates the Internet browser and shows a false screen to the user. Usually, via the virus the hacker has already gained full control over the victim's computer.

Necessary actions: Under no circumstance should you follow the described procedure and the link for downloading of the protection programme. You should contact immediately the 24/7 call centre of the Bank.

Should you need any assistance or information, or in case you suspect any unauthorized access to your computer, please contact the Bank immediately at 0700 1 84 84 or short number *1 8484 for mobile phones.