UniCredit Bulbank

UniCredit Bulbank takes professional care to protect its customers by using the latest global practices and technologies in the area of Internet security and electronic banking channels.

However, your behavior online and the means you use to protect your computer and the devices for online access are equally important.

Security recommendation

Choose a category to find out more

Recommendations
What do I need to know and do for my safety?

Checklist
Do I follow the necessary security measures?

Fraud prevention
How can I protect myself against current fraud attempts by cybercriminals?

More about security
What else do I need to know for my safety?

UniCredit Bulbank

Security recommendations

WHAT DO I NEED TO KNOW AND DO FOR MY SAFETY?

Information security is of utmost importance for online and mobile banking. UniCredit Bulbank takes professional care to ensure the security of its computer network, a part of which is the website of Bulbank Online. The measures that you take – on your computers, computer networks and Internet access, are no less important for the security of the online banking that you use.

UniCredit Bulbank allows access to Bulbank Online through the usual means of identification - username and password, and for active operations - through an additional means of authorization (QES, digital certificate, mobile token). If the security of your computer gets compromised, malicious individuals can gain access to your means of identification and, through them – to online banking on your behalf. In this way, access can be obtained to bank information regarding your accounts, as well as to the funds on them.

Your responsibility as a user of online and mobile banking is to protect your personal means of identification in accordance with the requirements set out in the General Terms and Conditions for the electronic banking services Bulbank Online and Bulbank Mobile.

- **Do not use public computers or software of obscure origin.**
- **Check the sender of emails and do not provide confidential information.**
- **Check the security indications on the websites.**
- **Avoid saving usernames and passwords in your web browser and on your computer.**
- **Use licensed antivirus software, anti-spyware and firewall. It is recommended that they be maintained by a specialist.**
- **When giving physical access to your computer to third parties, delete all means of identification and authorization from it.**
- **Update your software, web browser and operating system, follow the manufacturer's security recommendations.**

Bulbank Online

- **Do not reveal your username and password to anyone, change them often. Do not provide SMS passwords and M-token codes to third parties.**
- **Check the access to Bulbank Online on your behalf, always use "Exit" after using the site.**
- **It is recommended that you use a Qualified Electronic Signature or a digital certificate on a hardware cryptographic device.**
- **For corporate clients – consider the possibility of a combined signature.**
- **In case of doubt about unauthorized access to Bulbank Online on your behalf, you must immediately inform UniCredit Bulbank.**

Bulbank Mobile

- **Always lock your phone and set an access PIN/ password. Do not record passwords for access on your phone, do not share your access to the phone, as well as the phone itself with third parties.**
- **The phone has to be updated to the latest available version of the operating system.**
- **In the absence of communication services with your number, please immediately request the status from your mobile operator and in case of declaration for requesting a change or re-issuing of a SIM card, you must request immediate blocking. Immediately inform UniCredit Bulbank and request blocking of the mobile banking by the bank.**
- **Do not use programs that provide remote access to your phone.**
- **Install applications on your phone only from the official application stores: AppStore / Google Play.**

Security checklist

DO I FOLLOW THE NECESSARY SECURITY MEASURES?

Review the listed security measures and make sure you comply with each of them.

By answering all the questions with a positive answer "**YES**", you can rest assured that you have done everything necessary for your security when using the electronic channels for online and mobile 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 PASSWORD FOR THE ELECTRONIC BANKING CHANNELS AT LEAST ONCE A MONTH.
- THE BROWSER I USE FOR BANKING IS SET AT THE HIGHEST LEVEL OF DATA PROTECTION.
- I USE THE LATEST VERSIONS OF SYSTEM SOFTWARE, WEB BROWSER, OPERATING SYSTEM AND FIREWALL.
- WHEN LOGGING IN TO THE ELECTRONIC BANKING CHANNELS, I ALWAYS MAKE SURE THE PAGE IS GENUINE BY CHECKING WHETHER THE ADDRESS BAR IS COLOURED IN GREEN AND WHETHER THE WEB PAGE ADDRESS STARTS WITH HTTPS://.
- I DO NOT DISCLOSE MY USERNAME AND PASSWORD AND DO NOT SAVE THEM IN THE INTERNET BROWSER.
- I DO NOT INSTALL PROGRAMMES OF OBSCURE 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 APP STORES – APP STORE, GOOGLE PLAY.
- I DO NOT KEEP MY UNIVERSAL ELECTRONIC SIGNATURE (IN CASE I USE SUCH) ALWAYS ACTIVE ON MY COMPUTER WHEN I DO NOT NEED IT.

UniCredit Bulbank

Fraud prevention

HOW CAN I PROTECT MYSELF AGAINST CURRENT FRAUD ATTEMPTS BY CYBERCRIMINALS?

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 who use electronic banking channels.

For us, as a Bank largely focused on our customers' safety, it is important to inform you of the current fraud schemes in the area of electronic channels for online and mobile banking, in order to enable you to identify them in case of occurrence and to protect yourselves.

CURRENT SCAMS AND FRAUD ATTEMPTS BY CYBERCRIMINALS

- A fake message requesting to enter mobile phone data – operating system and phone number
- A fake letter from a contracting party/ partner/ relative or friend regarding a change of their bank accounts
- A fake call or e-mail

A fake message requesting to enter mobile phone data – operating system and phone number

DESCRIPTION

After you log in to the electronic banking channels, a false screen appears, which looks like Bulbank Online. On the pretext of providing additional protection for the customer's mobile phone against 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.

PLEASE, BE AWARE!
This is a fraud attempt which is designed to make the customer install a hacking programme on their phone to divert 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 displays a false screen to the user. Usually, through the virus the hacker has already gained full control over the victim's computer.

REQUIRED ACTIONS

Under no circumstance should you follow the described procedure and the link received on the phone for downloading of the protection programme. You must contact immediately the 24/7 Call Centre of the Bank.

UniCredit Bulbank

Fraud prevention

HOW CAN I PROTECT MYSELF AGAINST CURRENT FRAUD ATTEMPTS BY CYBERCRIMINALS?

A fake letter from a contracting party/ partner/ relative or friend regarding a change of their bank accounts

DESCRIPTION

You may receive a fake letter 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.

PLEASE, BE AWARE!
This is a fraud attempt which is designed to make the customer themselves order a transfer to the fraudster's account.

REQUIRED ACTIONS

Upon receiving information about any change of your contracting parties' data (accounts, address, phone number, etc.), you should always contact them personally in order to confirm the changes with them.

A fake call or e-mail

DESCRIPTION

This fraud scheme involves a phone call or an e-mail from a person introducing 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 pretext of providing assistance – correction of a wrong payment order, an expected delivery, etc., you are requested to provide the code you have received via SMS or other important information.

PLEASE, BE AWARE!
This is a fraud attempt which is designed to make the customer themselves disclose their personal banking information and the confirmation SMS code they have received.

REQUIRED ACTIONS

Never provide personal banking information (SMS codes, passwords for access, numbers of bank cards) to third parties either by phone or in reply to an e-mail. Write down the phone number of the person who is calling or forward the message to the Bank and contact its 24/7 Call Centre.

In case of need for assistance, information or suspicions of unauthorized access to your computer or phone, contact the Bank immediately at **0700 1 84 84** or short number ***1 84 84** from your mobile phone.

UniCredit Bulbank

More about security
What else do I need to know for my safety?

More about security

WHAT ELSE DO I NEED TO KNOW FOR MY SAFETY?

Here you will find general computer security measures as well as measures specific to online banking. Adherence to them will greatly increase the security of your online banking use and, thus – the information and funds on your bank accounts.

ACCESS

- **Avoid using Bulbank Online from publicly accessible computers, as well as from those with uncontrolled access.**
- **Do not reveal to anyone and under any pretext your username or password for access to Bulbank Online - they are personal.**
  If you require access for an employee of your company or a family member, as the account holder you can request separate access for them – the Bank will provide a new username and password for them with the requested level of access – for information only, for orders or with a set limit.
- **Never keep your username and password on physical media.**
- **If you suspect that someone is using your username and password, immediately change them using the means provided for this on the Bulbank Online website! If this is not possible, contact the Bank and request that your access be blocked.**
- **If you haven't changed your password recently, take a moment to do so.**
  Use a combination of letters, numbers and symbols. Change your access password more frequently. This reduces the chance that your password will be easy to guess.
- **It is recommended that you avoid the so-called "Automatically save" your credentials or passwords in the browser's memory, on the disk of your personal computer or phone.**

PLEASE, BE AWARE!
The identification codes (access codes and PINs), which are used to access our banking services via the Internet must not be "saved" in the memory of your browser or on the disk of your personal computer. It is a good idea to check that the browser's “AutoComplete” function isn't enabled.

Instruction for deactivation:

INTERNET EXPLORER:

1. *Select the menu “Tools” >> “Internet Options”.*
2. *From “Content” in the section “Personal information”, choose “AutoComplete”.*
3. *Uncheck the checkbox „User names and passwords on forms”, if checked, click on the buttons “Clear forms” and “Clear passwords”.*
4. *Press “OK” to confirm and close the opened menus.*

MOZILLA FIREFOX:

1. *Select the menu “Tools - Options” >> “Security”.*
2. *From “Passwords”, uncheck the checkbox “Remember passwords for sites”, if checked.*
3. *Press “OK” to confirm and close the opened menus.*

UniCredit Bulbank

More about security

WHAT ELSE DO I NEED TO KNOW FOR MY SAFETY?

DIGITAL CERTIFICATE

- **Keep your digital certificate safe**
  If you need to transfer your digital certificate to another computer, always delete it after use - both from the browser and the file through which it was transferred. The transfer of the certificate is desirable to be done personally by the user to whom it is issued. Protect the certificate with a password when transferring it.
- **It is recommended that you use a hardware cryptographic device to store your digital certificate.**
  Digital certificates stored in the browser could be exported from there and used by malicious individuals to create and sign payment orders on your behalf. The certificate from the hardware cryptographic device CANNOT be exported – it is usable only through the device, plus the required PIN for it.
- **The use of a Universal Electronic Signature (UES) is recommended**
  A universal electronic signature is a personal digital certificate on a hardware cryptographic device and means an advanced electronic signature that is created by a device for creating a universal electronic signature and is based on a qualified electronic signature certificate. It is issued by a certification service provider according to the Electronic Document and Electronic Certification Services Act.

INTERNET

- **The suggested sites, especially if they require confidential information or a password, should not be visited even for short periods**
  The link provided in the email may not be what it appears to be, and the files received in most cases carry risks. Do not follow the links in the received emails, as they can lead you to a "dangerous" or "fake" site, which can hardly be differentiated from the original one. Even if the correct address is visible in the address field of the browser, do not trust it - the visualized web address may have been changed by a fraudster. UniCredit Bulbank does not require its customers to enter personal identification data or other confidential information on its official website.
- **When browsing the Internet, avoid giving financial information and especially confidential data (such as passwords or credit/ debit card numbers) on any Internet site without first checking the security of the communication protocol and the authenticity of the website.**
  You have the opportunity to check the communication protocol: 1) "HTTPS://" at the beginning of the web address and 2) a yellow icon depicting a "locked padlock" (which indicates SSL protocol) in the browser status field. As part of UniCredit Group, UniCredit Bulbank uses this secure protocol aimed at protecting and guaranteeing the confidentiality of the information you enter while using the online banking services. To verify the authenticity of the site, double-click on the above-mentioned padlock icon and see the information from the issuer of the certificate on the website.

UniCredit Bulbank

More about security

WHAT ELSE DO I NEED TO KNOW FOR MY SAFETY?

E-MAILS AND MESSAGES

- **Check the sender of emails you have received.**
  Fraudulent emails can be identified by the following:
  - They contain messages requesting personal, confidential data, the reasons for which are not specified (for example: expiration of codes, loss of codes, technical or security issues)
  - they often use a "threatening" tone; they contain, for example, threats to terminate the service in case you do not send a reply - such are never sent through the messages of UniCredit Bulbank;
  - the deadline for sending the requested information is not specified.
- **When receiving suspicious emails:**
  Do not use the links provided in them (the link is a link to a website (site), which is loaded by clicking with the left mouse button on the link). Do not open the files attached to the email.
- **It is recommended to use a universal electronic signature, which certifies the authenticity of the sender and the content of the e-mail.**
  Signing e-mails with a universal electronic signature certifies the authenticity of senders, thus reducing the risks of receiving e-mails sent for illegal purposes.
- **When receiving fraudulent e-mails, it is necessary to report them as quickly as possible to the prosecutor's office or the police, as well as the Bank itself.**
  Do not reply, but immediately inform the Bank through the Call Center or by visiting your servicing branch. Reporting cases that you consider to be criminal to the competent authorities allows them to intervene immediately and the Bank to respond with retaliatory, protective measures to protect its customers.
- **Do not trust any unexpected changes in the way you are required to enter your access codes for the Internet service**
  In case of an unexpected change in the way you enter your access codes for the Internet service, for which you have not been notified, please contact the Bank through the Call Center or by visiting your servicing branch.
- **UniCredit Bulbank, as part of UniCredit Group, does not require codes, access passwords or other confidential information by e-mail.**
  Do not trust an email that requests confidential information, even if it is from known senders. Under no circumstances does UniCredit Bulbank request via email from its customers to provide passwords, user ID, access codes for services (e.g. Bulbank Online), PIN codes, bank card numbers or other confidential information.

UniCredit Bulbank

More about security

WHAT ELSE DO I NEED TO KNOW FOR MY SAFETY?

PROTECTION

- **The use of antivirus software is recommended**
  Fraudulent emails or websites may also contain malicious programs that are designed to intercept and forward sensitive personal information to a malicious person's computer. Antivirus packages are able to detect and alert you to the presence of such dangerous programs. It is recommended that you use an antivirus program from a licensed or free provider, but never from a copy or a compromised source. It is recommended that the antivirus program used be maintained by a specialist.
- **It is recommended to use and maintain an up-to-date personal and corporate Firewall, if available**
  Spyware is a computer program that monitors user actions, records information entered by the user and transmits it to malicious individuals. It can be installed on your computer by malicious software, a website or email. There are combined antivirus/ anti-spyware/ firewall solutions. It is recommended that the solution used be maintained by a specialist.
- **We recommend updating the operating system and all programs used at least quarterly**
  The companies that develop software, operating systems and web browsers periodically provide online updates, which can be downloaded for free (so-called patch) and as improvements they increase the level of security. On the websites of these companies you can check if your browser is updated and, if not, you can install the latest patch.
  Keeping the operating system, browser, e-mail and software used up-to-date generally reduces the so-called application vulnerability that information criminals typically take advantage of. Follow the security instructions provided by the manufacturer of the operating system and other software that you use!
- **Do not install or use software of suspicious or unverified origin**
- **Check the access to Bulbank Online on your behalf through the means provided on the website**
- **If you need support from UniCredit Bulbank, where possible use free messages on the Bulbank Online website, and not the support email address.**
- **When repairing your computer or otherwise providing physical access to it to third parties, including specialists who service your computer:**
  Please export, password protect, store on external media and keep your digital certificate in a safe place, then delete it from the browser you are working with. For this purpose, follow the instructions of the manufacturer of your browser or the instructions of Bulbank Online.
- **For corporate clients it is appropriate to consider the use of combined signing of payment orders. This opportunity is provided by Bulbank Online and can be requested and provided according to your requirements at no additional charge**

UniCredit Bulbank

In case of need for assistance, information or suspicions of unauthorized access to your computer or phone, contact the Bank immediately at **0700 1 84 84** or short number ***1 84 84** from your mobile phone.