2022/10

KBC Bank
Part of KBC Group

Security Instructions for usage of KBC Online Bulgaria

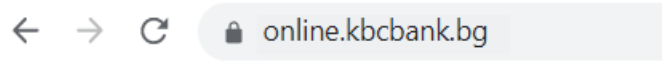
KBC Bank Bulgaria EAD uses state-of-the-art methods and tools to protect its online banking platform - KBC Online Bulgaria and effectively protecting your funds and gives you the convenience of banking everywhere. We advise you to comply with the security policies described in this document to help increase this protection. This will also lead to a significant reduction of the risk of fraud when making payments electronically.

Access to the Internet banking platform KBC Online Bulgaria

- Do not use public computers (PCs in Internet cafes, libraries, etc.) to access KBC Online Bulgaria.
- Avoid using KBC Online Bulgaria in the presence of other people or in public places.
- If you are using wireless Internet (Wi-Fi), make sure the connection is encrypted. Any connections to public and free Internet can result in compromised user credentials (username and password).
- Access KBC Online Bulgaria directly by typing the web address https://online.kbcbank.bg or the official site of KBC Bank https://www.kbcbank.bg. Do not use automatic address completion features.
- Do not include the KBC Online Bulgaria site in your browser's bookmarks or favorites because in this way there is a risk of manipulating the saved links by unauthorized contacts (hackers).
- Always check if the KBC Online Bulgaria web page you access is the authentic one and communication with it is secured. After loading the page, make a session security check in your browser prior to entering your username and password. The check is done as follows:

Google Chrome

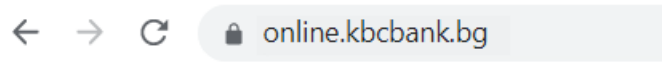
- In the left part of the address bar you should see a green locked padlock



- Click on it
- Click the "Connection is secure"
- Verify that there is a status “Certificate is valid”.

Edge

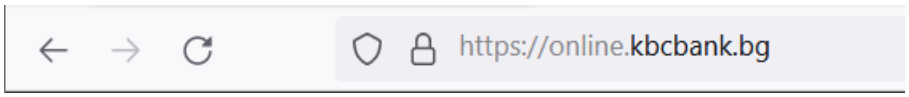
- In the left part of the address bar you should see a locked padlock



- Click on it
- Verify that there is a status “Connection is secure”.

Mozilla Firefox

- In the left part of the address bar you should see a locked padlock



- Click on it
- Verify that there is a status "Connection is secure".

- Whenever you have finished banking with KBC Online Bulgaria, use the Exit button in the upper right corner of the screen before closing the browser.

Internet browsers

- DO NOT save your username and password for KBC Online Bulgaria in your browser.
- Use an Internet browser that supports a secure connection protocol TLS version 1.2 or later and versions of Edge, Mozilla Firefox, Safari, Opera, Google Chrome that receive regular updates and are not suspended from their developers to access KBC Online Bulgaria.
- Please note that the official manufacturer support of Internet Explorer has ended since 15.06.2022. This means, that after this date the users of this web browser shall not receive updates, which can correct security vulnerabilities or bugs. For security reasons and trouble-free work with KBC Online Bulgaria is necessary to use the Edge browser, which has replaced Internet Explorer or different browser, which technical support is up to date.
- Activate the Automatic updates and the Phishing filters in your browser.
- Do not install additional toolbars – ASK toolbar, Google toolbar, etc. in the browser you are using to access KBC Online Bulgaria unless necessary. There are many cases of toolbars being used by hackers for distributing malware.

Username and password for authentication in KBC Online Bulgaria

- Even when changing the password for the first time always choose a "strong" password, which has a minimum length of eight characters, containing lowercase and uppercase letters, numbers and special characters (*,!, &, etc.).
- Change your password regularly (at least once every two months). The password for your internet banking must be different from and should not contain parts from the ones you use for access to your emails, accounts in social networks and others and from your name for internet banking. Should you

be using software for safe password storage and management, make sure that it is has high rating and good reputation.

- Remember your username and password for KBC Online Bulgaria. DO NOT write them down on paper, in your mobile phone or in the computer.
- Your password should not contain names of family members, pets and company names. Do not use birthdates for a password. Do not choose dictionary words for passwords.
- Do not share your username and password with anyone, not even family members or colleagues. These are strictly personal and unambiguously define you in the system as a user. This is your identity in front of the online banking system. If someone obtains your username and password, they will gain access to the system on your behalf.
- If it is necessary that employees from your company or family members need to have access to your accounts, you as an account holder can request a separate access profile by visiting a KBC Bank Bulgaria branch.
- If you change your specified contact telephone number, always inform KBC Bank about the change. In this way, if you need to confirm a payment order, we will be able to provide you with faster and better service. Do not give the phone number to a relative or colleague.

Additional security devices for users with active profiles

- KBC Online Bulgaria provides system users two additional security means for transaction authorization – MTAN via SMS messages or code generated by token (hardware device or native mobile application – software token)
- Password MTAN sent with SMS message – When you authorize payment with MTAN password, you receive SMS message, containing details for the transaction – password MTAN, amount of the payment and the last 10 digits and characters from the IBAN of the payee. If you receive MTAN without initiating a payment or there is difference in the last 10 digits or letters of the IBAN of the payee in the SMS message – DO NOT use this MTAN password to authorize the transaction and immediately contact KBC Bank Bulgaria. Do not give your mobile phone which you use for payment authorizations to other people.
- Token confirmation - When authorizing payments via a token device on the device display (software or hardware) you receive details about the transfer - the last 10 digits and letters on the recipient's account, the amount of the transfer and the currency. Always check the last 10 digits and letters of the recipient's account with the account to which you want to transfer funds - in case of difference DO NOT enter the code generated by the token to authorize the transaction and DO NOT confirm the transfer via online signature and immediately report KBC Bank.
- Hardware Token – keep the token in a safe place and in a secure manner. Remember the unlock PIN and do not share it with anyone. Do not write it down on paper or on the back of the token.

- Native application for mobile devices – software token - KBC Token application is available for Android and iOS operating systems. KBC Bank distributes the applications for smart devices only at official stores Google Play Store (for Android) and App Store (for iOS). Do not let the phone you use for banking to be used by others without supervision. In case you use software token with PIN do not share the last one with others and do not write it down.
- KBC Online Bulgaria provides the opportunity to use a group signature, in which active transactions can be confirmed by several users with various additional security tools. This increases the security of your active operations. Consider using a group signature for corporate needs.

Operating system and additional software

- Always use up-to-date operating systems and software. Today most operating systems and software products can be set to automatically update. If this option is available, activate it. If the auto-renewal option is not available use only patches and updates for your operating system and software that are published on the official vendor sites. Hackers often use e-mails and fake update pages to distribute fake security patch/update announcements urging you to download patches/updates, which are malware. By using an updated operating system and software products, you reduce the chance for ill-intentioned persons to use "breakthroughs" to access your personal information.
- Different types of software that you have installed on the computer you use to access KBC Online Bulgaria may affect the level of security of your online banking usage. Follow the information provided by vendors of the software you have installed for reported bugs and security holes in their products and apply the relevant patches, updates and fixes according to their recommendations.
- Install a personal firewall on the computer you are using for online banking to protect from unauthorized manipulations. Firewalls can be configured to send out alert message when they detect an attack from the Internet. Use automatic updates options for your personal firewall.
- Install antivirus/antimalware software on the computer you use for banking with KBC Online Bulgaria. The antivirus software scans your files and electronic mails for viruses, Trojans and other types of malware that may allow for unauthorized users to gain control over your personal computer.
- Consider antivirus software recommended by the operating system vendor. You can find many free downloadable antivirus/antimalware programs on the Internet under different names and from unknown vendors. It is very common that such programs are developed by hackers/malicious users and are distributed by spam mails or other scare tactics – as you browse a web page a pop-up or the page itself claims that it has detected that your PC is infected and you should download a specific antivirus tool in order to clean it – scareware. Very often such programs contain viruses, Trojans or other malware themselves. In other cases, the program locks all the programs rendering the PC unusable until you pay some kind of license fee – ransomware.

- Most antivirus programs are automatically updated so that the new threats on the Internet are mitigated. Always use updated antivirus software.
- DO NOT install any software with unknown origin. Using cracked programs from torrent sites is also a big risk. These programs have breakthrough protection and can be used to install malware and Trojan horses.
- We would like to draw your attention on the discontinued maintenance of the operating system Windows XP (http://windows.microsoft.com/bg-bg/windows/end-support-help) and the measures you should undertake to keep safe and secure.

Mobile banking through native applications

- Users can access the mobile banking system of KBC Bank – KBC Mobile Bulgaria through native mobile applications for smart devices – phones, tablets, etc. The applications can be used by smart devices running on Android and iOS operation systems.
- KBC Bank distributes the applications for smart devices only at official stores Google Play Store (for Android), AppGallery (for Huawei) and App Store (for iOS).
- The authentication for the mobile KBC Mobile Bulgaria is carried out with the same credentials (username and password) used for the online banking system. For a more convenient and quicker login, the mobile app offers the ability to set up a PIN and / or biometric login when the device supports it (fingerprint for Android, FaceID, and iOS fingerprint). For this purpose, the user has to login with the username and password and then choose the preferred login method from the profile settings (My Profile menu). In case of a forgotten PIN or a biometric fingerprint reading problem, users can always choose to enter with their username and password. When a new pin envelope was issued and if the quick login with biometrics or PIN was activated on the device earlier, the option is going to be deactivated automatically. In order to activate again quick login with biometrics/PIN the user has to reinstall the application and to login with the credentials from the new pin envelope. Only one user per device can use the PIN login option and one for biometric login. For example:
  - User "A" uses the PIN login option, user "B" uses biometric login
  - User "A" uses the PIN login and biometric login. In this case, user B will not be able to set up quick login but can use a username and password. In order for the biometric login to be used, the user must have the device set up beforehand.
- In order to use the biometric fingerprint option, the user must have pre-configured their device.
  - When the device is running an Android operating system, after each change - adding or removing a biometric data in the device settings, the user must clear the mobile application's data, then re-make the appropriate PIN or biometric input configurations

- For iOS, adding or removing a biometric data in device settings does not impose any new settings in KBC Mobile Bulgaria mobile app. Note that when using a biometric login and the operating system is iOS, anyone who has access to the device through biometrics will gain access to the KBC Mobile Bulgaria profile that is configured to work with biometric the device!

KBC Bank Bulgaria EAD does not store or manage the biometric data!

- The mobile app supports push notifications. The users can activate the notifications he wants from their profile settings (the "Notifications" menu) after login into the mobile application. Notifications are received on the last device from which the user has logged into their KBC Mobile Bulgaria account. If you need to sign up from another device, all you have to do to keep receiving notifications is to re-enter your login from your personal device. To stop receiving notifications, you can disable subscriptions from the Notifications menu.
- The additional security devices used for performing active operations through the mobile applications are MTAN via SMS and tokens. We recommend when using MTAN via SMS to receive the authorization code on a different phone number from the one in the mobile device where the application is installed.
- Consider enabling security features on your mobile devices including password, face recognition, fingerprint or other biometrics depending on the functionality of your mobile device. Enabling those features will enhance security in case of mobile device theft. Do not let the phone from which you are banking to be used by others without supervision.
- Install antivirus/antimalware software only from trusted vendors. Use the official markets for installation of antivirus/antimalware products.
- Keep the operating system of your smart device always updated. The patches/updates eliminate security vulnerabilities in operating systems. Consider vendor instructions.
- Do not use rooted and/or jail-broken smart devices for active bank operations. Rooting and jailbreaking are actions that allow you to use phone-locked features and acquire administrator rights. Acquiring administrative rights enables unauthorized persons to obtain full access on your device.

Phishing, social engineering, email notifications, chat messages and phone calls

- Phishing is a scam that encourages users of computers and other devices connected to the Internet to disclose their personal or financial information in an e-mail or website. Users are directed to a fraudulent website where they are asked to provide personal data, for example their username and password to access KBC Online Bulgaria. This website looks like the real thing, but it's actually a fake copy. The information entered is then used for identity theft or unauthorized access to your internet banking. KBC Bank never sends links that invite you to enter a username and password to log in to KBC Online

Bulgaria. Always enter the KBC Online Bulgaria address in the web browser yourself - this is the only way you can be sure that you are entering your login details without sharing them with third parties.

- Some Internet browsers have built-in phishing prevention filters, others provide this opportunity by add-ons which make these filters.
- Social engineering (fraud attempt) means that people presenting themselves for bank employees are trying to force you to share confidential information via phone call, chat message or e-mail. Disclosing this information may be harmful. They may also encourage you to install software on your mobile device or computer which will give them access and control over the device under the pretext that the information is needed to support you.
- KBC Bank DOES NOT send e-mails requesting information about your credentials (username and password), bank accounts, bank cards, etc.
- KBC Bank DOES NOT exchange the above stated information via e-mails.
- KBC Bank DOES NOT send e-mails urging you to call a number stated within the e-mail to exchange information concerning your KBC Online Bulgaria account.
- KBC Bank will not ask you to install remote control software such as Team viewer, AnyDesk, VNC, etc. in order to provide you remote support.
- If you doubt the authenticity of a message, chat or phone call do not hesitate to contact us via the official phone number(s) and website below.

If you have any questions and/or suspect any fraudulent activities, contact us at:

Phones	0700 10 000 (Vivacom); 17 21 (A1 and Yettel)
E-mail	call.center@kbcbank.bg