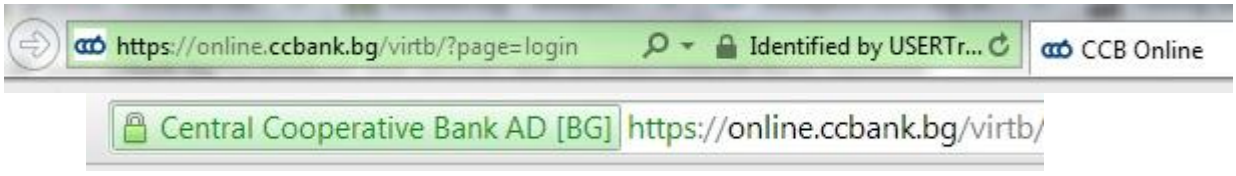
# Security measures upon using the online platforms for remote banking of CCB Plc

Your responsibility as user of the online banking is to keep your personal means of identification, according to the requirements in the General terms and conditions of CCB Plc. Sticking to the specified measures to a great extent increases the security of the online banking used by you, as well as the access to the information and the funds on your bank accounts.

**Upon performing bank operations with qualified electronic signature (QES) connect the QES to the computer only upon entry and do not leave the QES connected to the computer, when you do not work with the service and it is not under your control!**

**Access to the site for Internet Banking CCB Online/ CCB Lite**

- Avoid using generally accessible computers (Internet rooms, libraries, etc.) for an access to **CCB Online/CCB Lite**.
- If you use wireless connection (Wi-Fi), make sure it is encrypted. Your connecting to generally accessible and open networks may provide access to mala-fide persons to the information entered by you on the Internet, including username and password.
- Access **CCB Online** directly via going to https://www.ccbank.bg/bg/ccb-online-login or from the official site of CCB Plc https://www.ccbank.bg. Do not use functions for automatic supplementing of addresses.
- Access **CCB Lite** directly, going to https://www.ccbank.bg/bg/ccb-online-lite-login or from the official site of CCB Plc https://www.ccbank.bg. Do not use functions for automatic supplementing of addresses.
- Always check whether the web site, which you open to access **CCB Online/ CCB Lite**, is authentic and the communication with the web site is ensured.
- Upon opening the web site of CCB Online the field for web address has to be green or with a green lock, depending on your browser:




In the lower right angle of the browser you should see a red triangle with a lock:


If you click on the picture, you may check the authenticity of the web site.

- After you finish working with **CCB Online/ CCB Lite**, always exit with the Exit button and close the browser.

## Internet browsers

- Do not save your username and/or password for access to **CCB CCB Online/ CCB Lite** in your browser.
- To access **CCB Online/ CCB Lite** use Internet browser, which supports 256-bit encryption – versions of Internet Explorer, Mozilla Firefox, Safari, Opera, Google Chrome, which receive regular updates and are supported by the developers thereof.
- The browsers that you can use for optimum work and maximum security are: Internet Explorer: version 9.0 or higher, Mozila Firefox: version 52.8 ESR, Google Chrome: version 42.
- Activate automatic update and Phishing filters of the browser you are using.
- Do not install additional toolbars (toolbars – ASK toolbar, Google toolbar, etc.) in the browser, which you use for access to **CCB Online/ CCB Lite**, unless they are absolutely necessary for you. Such add-ons to the browsers are often used for the distribution of malicious software.

## Username and password for access

- Use passwords with a length of at least 6 characters, you must use small and big letters and digits. Passwords with a length, less than 6 characters either only letters or only digits, can easily be discovered.
- Periodically change your password for access to the service **CCB CCB Online/ CCB Lite**, as well as the PIN of your QES.
- Remember your username and password for **CCB CCB Online/ CCB Lite** and do not write them anywhere, neither on paper, nor in the memory of your mobile phone, nor on your computer.
- Avoid using as password names of members of the family or company names, birth dates or telephone numbers.
- Temporarily lock the profile at **CCB Lite** for one hour upon the entry of 5 wrong passwords.

## Access to CCB Mobile

- Keep your user PIN from unauthorized access, and do not disclose it, keep it at secure places and inaccessible to third persons.
- Keep the physical devices, at which the application for mobile banking of the Bank was installed.
- Use the standard mechanisms for security of the operational system of the mobile devices, such as access code, which should not coincide with the chosen PIN for access to the mobile application.
- Keep the username, password and personal identification number (PIN) for QES (qualified electronic signature), which are necessary for access to the system for Internet banking, via which the mobile banking service may be managed.
- Ensure the security of the operational system of the mobile device, via installing its latest updates.
- Do not use “jailbroken” and “rooted” devices, where the mechanisms for security of the operational system are destroyed.
- It is recommended to use an antivirus program for protection from viruses, and it is not recommended to use suspicious mobile applications, which may expose to risk the security of your mobile application.
- In case of a loss or theft of the device in the system for Internet banking you should contact the Customer Service Centre at *5050 or visit an office of the Bank.
- Protect the mobile device with a password and specify automatic locking of the screen, when the mobile device is not used.
- Install antivirus software on the smartphone and regularly update it.

- Install applications only from official applications shops – App Store, Google Play or Huawei AppGallery.
- Use the “Exit” button upon exiting the system.
- Deactivate the “Saving passwords” function in the browser.
- Do not use chance wireless connections to the Internet, in order not to expose your device to risk.

## Phishing and email notifications

- Phishing is a fraud, which invites the user of computers and other devices connected to the Internet to disclose his/her personal or financial information in an email or web site. The user is directed to a fraudulent web site, where he/she has to provide personal and financial data. This web site looks like the true one, but in fact is a false replica. After that the entered information is used for identity theft or an authorized access to the Internet banking.
- Some of the Internet browsers have built-in filters for the prevention of phishing, and the others provide this possibility via additional add-ons, which make this filtering.
- CCB Plc does not send via email notifications, which invite you to provide data of your password, username, number of the bank account, bank cards, etc.
- CCB Plc does not exchange this type of information via email.
- CCB Plc does not send via email messages, which contain links to web sites of the Bank.
- If you doubt the accuracy of a message, do not hesitate to contact us.

**Upon any questions and suspicions of abuses – contact**

**CCB Online, CCB Lite and CCB Mobile**

| | |
|---|---|
| **Tel.** | ***5050 and 02/92 66 666** |
| **E-mail** | **front@ccbank.bg** |