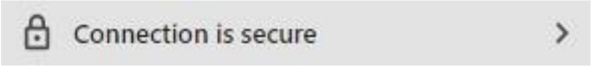
Security measures upon using the online platforms for remote banking of CCB Plc

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

- Avoid using generally accessible computers (Internet rooms, libraries, etc.) for an access to **CCB Online.**
- 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.
- For optimal performance and maximum security, use computers with the following operating systems: **Windows 10** or **11**; **Linux** (Ubuntu 20.04 or higher)
- Access CCB Online directly by dialing https://www.ccbank.bg/bg/ccb-online-login or https://online.ccbank.bg/virtb/ or from the official CCB plc website https://www.ccbank.bg. Do not use address autocomplete features.
- Always check that the web page you are opening to access CCB Online is authentic and communication with it is secure.
    - The page address must begin with https;
    - You should see a locked padlock icon in your browser's address bar or status bar;



Connection is secure

    - The CCB plc online banking page is certified by Sectigo Limited, to verify click on the icon - locked padlock and view the certificate;

- Always log out of CCB Online using the "Logout" button before closing your browser.

Internet browsers

- Do not save your username and/or password for access to **CCB Online** in your browser.

- Updated (always up to date) browsers: Edge, Firefox, Chrome, Safari;

  Internet Explorer 11, which will be supported until 31.12.2025.
- 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**, unless they are absolutely necessary for you. Such addons 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 Online**, as well as the PIN of your QES.
- Remember your username and password for **CCB Online** 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 Online** for one hour upon the entry of 5 wrong passwords and/or use an invalid or incorrect certificate.

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

The phishing attack prompts you to update your personal or banking information such as your PIN (personal identification number), phone number, account number (IBAN), bank card details, username, mobile or internet banking password through messages sent by senders impersonating the bank. Please note that these messages are not sent by CCB plc. Messages with fraudulent content may be received through various channels (email, SMS, Viber, Messenger, Telegram, Whatsapp, etc.) under false pretext of updating your details as a customer. If you receive such a message, we ask that you do not take any action described in it, do not open the attached links or attachments, and do not reply to the sender. If you have any suspicion that you have entered your login details on an illegitimate page, please notify us immediately on *5050.

Upon any questions and suspicions of abuses – contact

CCB Online and CCB Mobile

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