Мерки за сигурност при използване на онлайн платформите за отдалечено банкиране на ЦКБ АД

Вашата отговорност като потребител на онлайн банкирането е да опазвате персоналните Ви средства за идентификация, съгласно изискванията в Общите условия на ЦКБ АД. Придържането към изброените мерки в голяма степен повишава сигурността на използваното от Вас онлайн банкиране, както и достъпът до информацията и средствата по Вашите банкови сметки.

При банкиране с квалифициран електронен подпис (КЕП) свързвайте КЕП-а с компютъра само при вход и не оставяйте КЕП-а свързан към компютъра, когато не работите с услугата и не е под Ваш контрол!

Достъп до сайта за интернет банкиране ССВ Online

- Избягвайте използването общодостъпни компютри (интернет зали, библиотеки и т.н.) за достъп до **ССВ Online**.
- Ако използвате безжична мрежа (Wi-Fi), уверете се, че е криптирана. Свързването Ви към общодостъпни и отворени мрежи могат да осигурят достъп на злонамерени лица до въведената от Вас информация в интернет, в т.ч. потребителско име и парола.
- За оптимална работа и максимална сигурност използвайте компютри със следните операционни системи: **Windows 10** или **11**; **Linux** (Ubuntu 20.04 или по-висока версия)
- Достъпвайте **ССВ Online** директно чрез набиране на адреса https://www.ccbank.bg/bg/ccb-online-login или https://online.ccbank.bg/virtb/ или от официалния сайт на ЦКБ АД https://www.ccbank.bg. Не използвайте функции за автоматично допълване на адреси.
- Винаги проверявайте дали уеб страницата, която отваряте, за да достъпите **ССВ Online** е автентична и комуникацията с нея е подсигурена.
    - Адреса на страницата трябва да започва с https
    - В адресната лента или в лентата на състояние на браузъра трябва да виждате иконка - заключен катинар;

      

    - Страницата за онлайн банкиране на ЦКБ АД е сертифицирана от Sectigo Limited, за проверка кликнете върху иконката - заключен катинар и разгледайте сертификата;

- Винаги излизайте от ССВ Online с бутон "Изход" преди да затворите браузъра си.

Интернет браузъри

- Не запаметявайте Вашето потребителско име и/или парола за достъп до **ССВ Online** във Вашия браузър.
- Актуализирани (always up to date) браузъри: Edge, Firefox, Chrome, Safari;

  Internet Explorer 11, чиято поддръжка ще бъде до 31.12.2025 г.
- Активирайте автоматично обновяване и Phishing филтрите на браузъра, който използвате.
- Не инсталирайте допълнителни ленти с инструменти (toolbars – ASK toolbar, Google toolbar и др.) в браузъра, който използвате за достъп до **ССВ Online**, освен ако не са Ви от абсолютна необходимост. Подобни допълнения към браузърите често се използват за разпространяване на зловреден софтуер.

Потребителско име и парола за достъп

- Използвайте пароли с дължина поне 6 символа, задължително малки, големи букви на латиница, цифри и специални символи. Пароли с дължина, по-малка от 6 символа или само букви или само цифри, лесно могат да бъдат открити.
- Периодично променяйте Вашата парола за достъп до услугата **ССВ Online**, както и PIN кода на използвания от Вас КЕП.
- Запомнете Вашето потребителско име и парола за **ССВ Online** и не ги записвайте никъде, нито на хартия, нито в паметта на мобилния телефон или на компютъра си.
- Избягвайте да използвате за парола имена на членове от семейството или фирмени имена, рождени дати или телефонни номера.
- Временно заключване на профила в **ССВ Online** за един астрономически час при въвеждане на пет грешни пароли и/или при използване на невалиден или грешен сертификат.

Достъп до ССВ Mobile

- Пазете своя потребителски ПИН от неоторизиран достъп, като не го съобщавате, съхранявайте го на сигурни и недостъпни за трети лица места.
- Пазете физически устройствата, на които е инсталирано приложението за мобилно банкиране на банката.
- Използвайте стандартните механизми за сигурност на операционната система на мобилните устройства, като код за достъп, който не трябва да съвпада с избрания ПИН за достъп до мобилното приложение.
- Пазете потребителското име, парола и персоналния идентификационен номер (ПИН) за КЕП (квалифицирания електронен подпис), които са необходими за достъп до системата за Интернет банкиране, чрез която може да бъде управлявана услугата мобилно банкиране.
- Осигурявайте сигурността на операционната система на мобилното устройство, чрез инсталиране на последните й обновления.
- Не използвайте „jailbroken” и “rooted” устройства, при които механизмите за сигурността на операционната система са унищожени.
- Препоръчително е да използвате антивирусна програма за защита от вируси, както и не е препоръчително да използвате съмнителни мобилни приложения, които могат да компрометират сигурността на мобилното Ви устройство.

- В случай на загуба или кражба на устройството в системата за Интернет банкиране се свържете с Центъра за обслужване на клиенти на телефон *5050 или посетете офис на Банката.
- Защитете мобилното устройство с парола и задайте автоматично заключване на екрана, когато не използвате мобилното устройство.
- Инсталирайте антивирусен софтуер в смартфона и редовно го актуализирайте.
- Инсталирайте приложения само от официални магазини за приложения – App Store, Google Play или Huawei AppGallery.
- Използвайте бутон „Изход” при излизане от системата.
- Деактивирайте функцията „Запомняне на пароли” в браузъра.
- Не използвайте случайни безжични връзки с интернет, за да не излагате устройството си на риск.

Фишинг и имейл нотификации

Фишинг атаката Ви подканя да актуализирате Ваша лична или банкова информация като ЕГН, телефонен номер, номер на сметка (IBAN), данни за банкова карта, потребителско име, парола за мобилно или интернет банкиране чрез изпратени съобщения от податели, представящи се за банката. Моля да имате предвид, че тези съобщения не се изпращат от ЦКБ АД. Съобщенията с измамно съдържание може да получите по различни канали (имейл, SMS, Viber, Messenger, Telegram, Whatsapp и т.н.), под фалшив претекст за обновяване на Вашите данни като клиент. При получаване на подобно съобщение Ви молим да не предприемате никакви действия, описани в него, да не отваряте приложените линкове или прикачени файлове, както и да не отговаряте на подателя. В случай, че имате съмнение, че сте въвели своите данни за вход в нелегитимна страница, незабавно ни уведомете на телефон *5050.

При възникнали въпроси и съмнения за злоупотреби – връзка с

ССВ Online и ССВ Mobile

Телефони	***5050 и 02/92 66 666**
E-mail	**front@ccbank.bg**