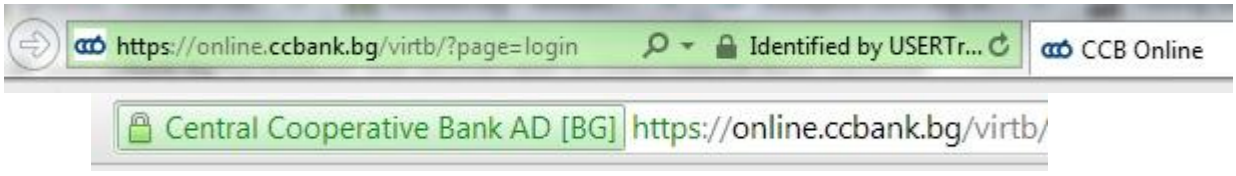
Мерки за сигурност при използване на онлайн платформите за отдалечено банкиране на ЦКБ АД

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/ ССВ Lite

- Избягвайте използването общодостъпни компютри (интернет зали, библиотеки и т.н.) за достъп до **ССВ Online/ССВ Lite**.
- 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.
- Достъпвайте **ССВ Online** директно чрез набиране на адреса https://www.ccbank.bg/bg/ccb-online-login или от официалния сайт на ЦКБ АД https://www.ccbank.bg. Не използвайте функции за автоматично допълване на адреси.
- Достъпвайте **ССВ Lite** директно чрез набиране на адреса https://www.ccbank.bg/bg/ccb-online-lite-login 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/ ССВ Lite**, е автентична и комуникацията с нея е подсигурена.
- При отваряне на станицата на ССВ Online полето за уеб адрес трябва да бъде зелено или със зелен катинар, в зависимост от Вашия браузър:



В долния десен ъгъл на браузера трябва да се вижда червен триъгълник с катинар:

Ако кликнете на картинката, можете да проверите автентичността на страницата.

- След като приключите работа с **ССВ Online/ ССВ Lite** , винаги излизайте с бутона „Изход” и затваряйте браузъра.

Интернет браузъри

- Не запаметявайте Вашето потребителско име и/или парола за достъп до **ССВ ССВ Online/ ССВ Lite** във Вашия браузър.
- За достъп до **ССВ Online/ ССВ Lite** използвайте интернет браузър, който поддържа 256-битово криптиране – версии на Internet Explorer, Mozilla Firefox, Safari, Opera, Google Chrome, които получават редовни актуализации и не са със спряна поддръжка от разработчиците им.
- Браузърите, които може да използвате за оптимална работа и максимална сигурност са: Internet Explorer: версия 9.0 или по-висока версия, Mozila Firefox: версия 52.8 ESR, Google Chrome: версия 42.
- 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/ ССВ Lite**, 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 и големи букви и цифри. 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 ССВ Online/ ССВ Lite**, както и PIN кода на използвания от Вас КЕП.
- Запомнете Вашето потребителско име и парола за **ССВ ССВ Online/ ССВ Lite** 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 Lite** за един астрономически час при въвеждане на пет грешни пароли.

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 – Apple Store, Google Play Store.
- 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

- Фишингът (fishing) представлява измама, която подканва потребителя на компютри и други устройства свързани с интернет да разкрие своя лична или финансова информация в имейл съобщение или уеб сайт. Потребителят бива насочен към измамнически уеб сайт, където се изисква да предостави лични и финансови данни. Този уеб сайт прилича на истинския, но всъщност е негово фалшиво копие. След това въведената информация се използва за кражба на самоличност или неоторизиран достъп до интернет банкирането.
- Някои от интернет браузърите имат вградени филтри за предотвратяване на фишинг, а други предоставят тази възможност чрез допълнителни добавки (add-ons), които да правят тази филтрация.
- ЦКБ АД не изпраща по електронна поща съобщения, които Ви приканват да предоставите данни за Вашата парола, потребителско име, номер на банкова сметка, банкови карти и др.
- ЦКБ АД не разменя този тип информация по електронна поща.
- ЦКБ АД не изпраща по електронна поща съобщения, съдържащи връзки към уеб страници на Банката.
- Ако се съмнявате в истинността на дадено съобщение не се колебайте да свържете се с нас.

При възникнали въпроси и съмнения за злоупотреби – връзка с

CCB Online, CCB Lite и CCB Mobile

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