Мерки за сигурно користење на онлајн платформите ССВ Online и ССВ Mobile на

ЦКБ АД Скопје

Вашата одговорност како корисник на онлајн банкарството е да ги чувате Вашите персонални средства за идентификација согласно барањата во Општите услови на ЦКБ АД Скопје. Придржувањето кон наведените мерки во голема мера ја зголемува сигурноста при користење на онлајн платформите, како и на пристапот до информациите и износот на средства на Вашите банкарски сметки.

При користење на дигитален сертификат на усб токен, поврзувајте го усб токенот со компјутерот само при користење на услугата и не го оставајте токенот поврзан на компјутерот кога не го користите електронското банкарство или кога компјутерот го користи друго лице!

Пристап до веб страната за електронско банкарство ССВ Online

- Избегнувајте користење на јавни компјутери како на пример во интернет кафе, библиотеки итн. за пристап до ССВ Online.

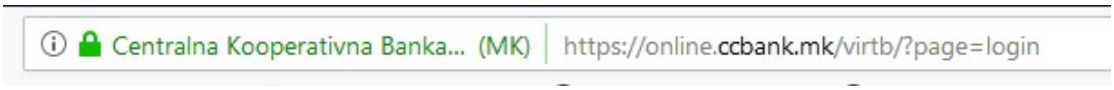
- Ако користите безжична мрежа (Wi-Fi), уверете се дека истата е заштитена. Поврзувањето со јавни и отворени мрежи може да ве изложи на ризик од злоупотреба на податоците кои ги внесувате, вклучително и корисничкото име и лозинка.

- Поврзувајте се со ССВ Online директно преку адресата https://online.ccbank.mk/virtb/?page=login или од официјалниот сајт на ЦКБ АД http://www.ccbank.mk. Не користете функции за автоматско дополнување на адреси.

- Секогаш проверувајте дали веб страната што ја отварате за да пристапите до ССВ Online е автентична и комуникацијата со истата е безбедна.

- При отварање на веб страната на ССВ Online полето за веб адреса треба да биде зелено или со зелен катанец, во зависност од Вашиот пребарувач:

  Mozilla Firefox

  Google Chrome

- Откако ќе завршите со работа во ССВ Online, секогаш излегувајте со копчето „Излез” и исклучете го пребарувачот.

Интернет пребарувачи

- Не ги меморирајте Вашето корисничко име и/или лозинка за влез во ССВ Online во Вашиот пребарувач.

- За пристап до ССВ Online користете интернет пребарувач којшто поддржува 256-битно криптирање – верзии на Microsoft Edge, Mozilla Firefox, Safari, Opera, Google Chrome, коишто редовно добиваат нови верзии и имаат тековна поддршка од нивните производители.

- Пребарувачите коишто може да ги користите за оптимална работа и максимална безбедност се Microsoft Edge, Mozila Firefox, Google Chrome.

- Активирајте автоматска инсталација на нови верзии и Phishing филтри на пребарувачот којшто го користите.

- Не инсталирајте дополнителни ленти со инструменти (toolbars – ASK toolbar, Google toolbar и др.) во пребарувачот којшто го користите за пристап до ССВ Online, освен ако не Ви се неопходни. Слични дополнувања (Addons, Extensions) кон пребарувачите често се користат за распространување на злонамерен софтвер.

Корисничко име и лозинка

- Користете лозинки со минимална должина од 8 симболи и комбинација од мали и големи букви, бројки и специјален знак . Лозинки со должина помала од 8 симболи или само букви или само цифри, лесно може да бидат откриени.

- Периодично менувајте ја Вашата лозинка за пристап до услугата ССВ ССВ Online, како и PIN кодот на токенот што го користите.

- Запомнете ги Вашето корисничко име и лозинка за ССВ Online и не ги запишувајте никаде, ниту на хартија, ниту во меморијата на мобилниот телефон или на Вашиот компјутер.

- Избегнувајте да користите за лозинка имиња на членови од семејството, имиња на фирми, датуми на раѓање или телефонски броеви.

- Привремено заклучување на профилот во траење од 15 минути при погрешно внесена лозинка последователно пет (5) пати.

Пристап до ССВ Mobile

- Внимавајте на Вашиот кориснички ПИН, не го соопштувајте на никого и чувајте го на безбедни места недостапни за трети лица.

- Внимавајте на сигурноста на Вашиот мобилен уред каде е инсталирана апликацијата за мобилно банкарство на банката.

- Користете ги стандардните механизми за безбедност на оперативниот систем на мобилниот уред, како биометрија или код за влез којшто не треба да се совпаѓа со избраниот ПИН за пристап до мобилната апликација.

- Чувајте ги Вашите корисничко име, лозинка и ПИН за токен коишто се неопходни за влез во системот за електронско банкарство, преку кој може да се управува со услугата мобилно банкарство.

- Секогаш инсталирајте ги најновите ажурирања на оперативниот систем на Вашиот мобилен уред.

- Не користете „jailbroken" и "rooted" уреди кај кои механизмите за сигурност на оперативниот систем се уништени.

- Препорачливо е да користите антивирусна програма за заштита од вируси и не е препорачливо да инсталирате и користите сомнителни мобилни апликации, кои можат да ја компромитираат сигурноста на Вашиот мобилен уред.

- Во случај на губење или кражба на мобилниот уред, поврзете се со корисничка и техничка поддршка на телефон 3 249 331 или посетете експозитура на Банката.

- Заштитете го мобилниот уред со лозинка и активирајте автоматско заклучување на екранот кога уредот не се користи.

- Инсталирајте ја мобилната апликација само од официјалните продавници за апликации – Apple Store, Google Play Store.

- Користете го копчето „Излез" при излегување од системот.

- Се препорачува да не се користат јавни безжични мрежи, за да не се изложува мобилниот уред на ризик.

Фишинг и е-маил известувања

- Фишингот (phishing) претставува измама, која поттикнува корисници на компјутери и други уреди поврзани со интернет да откријат свои лични или финансиски информации во е-маил порака или на веб сајт. Корисникот се насочува кон измамнички веб сајт, кадешто се бара да достави лични и финансиски податоци. Тој веб сајт личи на вистинскиот, но всушност е негова лажна копија. Воведените информации подоцна се користат за кражба на идентитет или неовластен пристап до електронското банкарство.

- Некои од интернет пребарувачите имаат вградени филтри за спречување на фишинг, а други ја даваат таа можност преку дополнителни алатки (add-ons).

- ЦКБ АД Скопје НЕ испраќа по електронска пошта известувања кои бараат од Вас да внесете податоци за Вашата лозинка, корисничко име, број на банкарска сметка, број на платежна картичка и др.

- ЦКБ АД не разменува информации за електронското банкарство по електронска пошта.

- ЦКБ АД не испраќа по електронска пошта известувања, коишто содржат линкови кон веб страници на Банката.

- Ако се сомневате во вистинитоста на добиено известување не се двоумете да не контактирате.

Доколку имате прашања или сомнежи за злоупотреби за ССВ Online или ССВ Mobile контактирајте не на:

Телефони	3 249 331
E-mail	ibank@ccbank.mk