МЕРКИ ЗА СИГУРНОСТ
ПРИ ИЗВЪРШВАНЕ НА ПЛАТЕЖНИ ОПЕРАЦИИ

Централна Кооперативна Банка
Важният си ти.

Централна Кооперативна Банка предлага различни услуги, чрез които лесно, бързо и сигурно може да оперирате със своите парични средства в реално време, без да посещавате офис на Банката.

Предоставяме на Вашето внимание информация, съвети и препоръки относно Вашата сигурност при извършване на разплащания.

СРЕДСТВА ЗА ИДЕНТИФИКАЦИЯ И СИГУРНОСТ ОНЛАЙН

CCB ONLINE

- Идентификацията на потребителите в системата се извършва с потребителско име, парола и Квалифицирано удостоверение за квалифициран електронен подпис;
- При въведено грешно потребителско аиме и/или парола е необходимо и въвеждането на четирицифрен код, генериран от сайта на Банката;
- Допълнителна защита с SMS авторизация при извършване на превод към нов контрагент;
- Продължителност на сесия – 10 /десет/ минути;
- Забрана за ползване на услугата при ползване на интернет връзка с динамичен IP адрес.

CCB ONLINE LITE

- Идентификацията на потребителите в системата се извършва с потребителско име и парола;
- Допълнителна защита с SMS авторизация при извършване на преводи;
- Заключване на акаунта за един астрономически час при пет последователни опита за вход с грешно въведена парола;

- Продължителност на сесия – 5 /пет/ минути;
- Забрана за ползване на услугата при ползване на интернет връзка с динамичен IP адрес;
- Максимален дневен лимит за преводи и покупко-продажба на валута между собствени сметки до размера на левовата равностойност на 15’000 (петнадесет хиляди) евро (29’337.45 лв. по фиксинга на БНБ);
- Максимален лимит за преводи към предварително зададени контрагенти и плащания на битови сметки – 5’000 лв. за 24 часа;
- Максимален лимит за преводи към произволни получатели – 500 лв. за 24 часа.

CCB MOBILE

- Осигурено е криптиране на информацията, която се предава от приложението на мобилния телефон до сървърите на Банката чрез използване на https (ssl) протокол;
- Идентификацията на потребителя се осъществява посредством комбинация от регистрираното мобилно устройство, обвързано с потребителско име, парола и персонален потребителски ПИН код;
- Временно заключване на приложението за един астрономически час при въвеждане на три последователни грешни ПИН кода;
- Деактивиране на приложението при въвеждане на шест последователни грешни ПИН кода;
- Авторизацията на ниво трансакция се извършва за всяка една трансакция посредством вградени криптографски методи, които осигуряват най-високо ниво на сигурност както от външни, така и от вътрешни заплахи;
- В инфраструктурата на системата се използват хардуерни секюрити устройства (HSM), чрез които се гарантира сигурността на извършваните криптографски изчисления;
- Създадени са изключително богати възможности за задаване на права, лимити и управление на системата за мобилното банкиране посредством системата за Интернет банкиране CCB Online;
- Всеки превод, нареден през CCB Mobile, се потвърждава чрез въвеждане на ПИН код или чрез използване на Face ID/Touch ID (Fingerprint);

» Дневен лимит на всички операции, извършвани чрез услугата ССВ Mobile, е в размер на левовата равностойност на 15’000 (петнадесет хиляди) евро (29’337.45 лв. по фиксинга на БНБ);

» Максимален лимит за преводи към предварително зададени контрагенти, плащане на битови сметки и плащания към държавата– 10’000 лв. за 24 часа;

» Максимален лимит за преводи към произволни получатели – 4’000 лв. за 24 часа;

» Денонощен контактен център *5050 за блокиране на устройство в случай на загуба или кражба.

ЗАЩИТА НА БАНКОВИТЕ КАРТИ, ПРЕДЛАГАНИ ОТ ЦКБ АД

» Банковите карти на ЦКБ АД са снабдени с чип технология, гарантираща високо ниво на сигурност на плащанията при търговци и теглене на пари в брой;

» При заплащане в търговски обект на ПОС терминал и при теглене на пари в брой от банкомат се въвежда ПИН код за потвърждаване на плащането. За да бъдат сигурни и защитени безконтактните трансакции с Вашата карта, издадена от ЦКБ АД, Ви уведомяваме, че съгласно „Втората европейска директива за платежни услуги – (PSD2)“ въвеждане на ПИН код при безконтактно картово плащане ще бъде необходимо и след извършване на пет поредни безконтактни трансакции без ПИН – на шестата трансакция ще Ви бъде изискан ПИН код или следва да извършите трансакция с прочитане чипа на картата;

» При извършване на онлайн плащане посредством банковата карта, потвърждаване на плащането се извършва чрез CVC/CVV код, отпечатан на гърба й. При плащания при търговци, регистрирани за допълнителни програми за защита **Mastercard Identity Check** и **Visa Secure**, потвърждаване на плащане се извършва с допълнителни пароли благодарение на услугата на ЦКБ АД **E-Secure**;

» ЦКБ АД Ви осигурява допълнителна защита за картите, като предоставя възможност да блокирате своята карта и да я разблокирате непосредствено преди извършване на плащане или теглене на пари в брой чрез мобилното приложение ССВ Mobile;

» Банката осигурява мониторинг на трансакциите, извършени с картите на ЦКБ АД, и в случай на съмнение за злоупотреба блокира използването на картата Ви;

» На разположение е 24-часов център за обслужване, чрез който имате възможност да блокирате своята карта в случай на загуба, кражба или съмнение за злоупотреба;

» Чрез допълнителна SMS услуга на Банката може да получавате SMS нотификации както за всяка авторизация, извършена с картата, така и за проверка на наличност;

» В секция “Карти” на ССВ Mobile, чрез бутон „Текуща наличност“, имате възможност да проверявате наличността по картата си по всяко време;

» В секция „Карти“ в ССВ Mobile и ССВ Online Lite чрез бутон „Текуща наличност“ клиентите имат възможност да проверяват наличността по картата си по всяко време.

Препоръчваме Ви да използвате допълнителните услуги, които Ви предлагаме за по-голяма защита на Вашата карта:

» **ССВ Mobile** – чрез мобилното приложение на ЦКБ АД имате възможност да получавате информация за наличност и движение по Вашите банкови карти, както и да извършвате действия по тяхното управление – блокиране/разблокиране на регистрираните във Вашия профил Карти;

» Услугата **SMS Детектив** Ви осигурява защита от измами и злоупотреби с Вашата карта. Получавате SMS веднага след използване на картата Ви, в момента на плащане в търговски обект, в интернет или при теглене на пари в брой. Ако получите SMS за трансакция, която не е извършена от Вас, незабавно се обадете на денонощните телефони на Банката, за да бъде блокирана картата Ви, или блокирайте картата си в профил “Карти” на ССВ Mobile;

» Чрез услугата **E-Secure** на ЦКБ АД получавате допълнителна защита при пазаруване в Интернет с Вашата карта. Регистрацията и ползването на E-Secure са напълно безплатни. Услугата се осъществява съвместно с картовите организации Visa и Mastercard, като при двете организации има различни наименования: **Mastercard Identity Check/Mastercard SecureCode** при Mastercard; **Visa Secure/Verified by Visa** или **VbV** при Visa.

Услугата използва 3-D Secure протокол, осигуряващ допълнително ниво на сигурност при онлайн трансакции с кредитни и дебитни карти;

Услугата „Сигурни плащания в Интернет“ (E-Secure) включва двуфакторен модел за автентикация на картодържатели чрез съчетаване на два отделни компонента **динамична парола** и **статична парола** за плащания в Интернет, които се въвеждат от оправомощения ползвател за потвърждение на платежни операции с банкова карта;

Предстои въвеждането и на мобилна автентикация (автентикация чрез биометрични характеристики) чрез интеграция на Mastercard Identity Check Mobile (IDCM) в мобилното банкиране на ЦКБ АД ССВ Mobile. В зависимост от устройството, на което използвате ССВ Mobile при извършване на трансакции в интернет, ще Ви бъде предоставена възможност да потвърждавате своето плащане чрез лицево разпознаване (Face ID), пръстов отпечатък (Fingerprint) или Touch ID.

Информация за наличността по картата Ви и извършените операции с нея можете да получите чрез:

- **ССВ Online** – интернет банкиране с КУКЕП на ЦКБ АД, чрез което може сигурно и бързо да извършвате левови и валутни плащания в страната и чужбина, да нареждате масови плащания и преводи към бюджета. Имате възможност да получавате информация за движения и салда по Вашите сметки и карти в Банката, да договаряте курсове при покупко-продажба на валута, да получавате информация за състоянието по кредитните си продукти, да плащате битови сметки;
- **ССВ Online Lite** – мобилно банкиране за Вашия смартфон, таблет или компютър, чрез което по всяко време следите движението по своите сметки и проверявате без такса каква е наличността по Вашите карти и всички трансакции, извършени с тях;
- **ССВ Mobile** – приложение за мобилно банкиране на ЦКБ АД, чрез което може сигурно и бързо да извършвате левови и валутни плащания в страната и чужбина, а също да нареждате и бюджетни преводи. Имате възможност да получавате информация за движения и салда по Вашите сметки и карти в Банката, да управлявате банковите си карти, да договаряте курсове при покупко-продажба на валута, да получавате информация за състоянието по кредитните си продукти, да плащате битови сметки;
- **SMS наличност** – можете да проверите по всяко време и навсякъде с каква сума разполагате по картата си. Получавате информацията чрез SMS до мобилния Ви телефон.

ПРЕПОРЪКИ ЗА СИГУРНОСТ ПРИ ИЗПОЛЗВАНЕ НА ИНТЕРНЕТ БАНКИРАНЕ

ССВ ONLINE

Осъществявайте достъп до услугата 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;

- Премахвайте Вашия КУКЕП от компютъра при приключване на работа в услугата ССВ Online;
- Избягвайте използването на общодостъпни компютри (интернет зали, библиотеки и т.н.) за достъп до услугата ССВ Online;
- Избягвайте използването на общодостъпни безжични мрежи (Wi-Fi) с цел ограничаване на риска от достъп на злонамерени лица до въведената информация в интернет, в т.ч. потребителско име и парола;
- Осъществявайте достъп до услугата ССВ Online директно чрез набиране на уеб адреса на портала за вход в услугата от официалния сайт на Банката. Избягвайте ползването на функции за автоматично допълване на уеб адреси;
- Проверявайте автентичността на уеб страницата и сигурността на комуникацията с нея чрез клик върху иконата катинар в адресната лента на браузъра;
- Използвайте бутон „Изход“ и затваряне на браузъра при приключване на работа в услугата ССВ Online;
- Използвайте пароли за достъп с дължина поне 6 /шест/ знака, съдържащи задължително главни и малки латински букви, цифри и специални символи;
- Периодично променяйте паролата за достъп до услугата ССВ Online и ПИН кода на електронния подпис;
- Не запаметявайте потребителското име и парола в браузъра на

компютъра;

» Избягвайте използването на имена на членове от семейството или фирмени имена, рождени дати или телефонни номера за парола за вход в ССВ Online;

» Използвайте интернет браузъри, които поддържат 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;

» За оптимална работа и максимална сигурност използвайте браузъри – Internet Explorer ver. 11, Mozilla Firefox ver.27, Google Chrome ver.38 или по-нова, Microsoft Edge, Safari ver.7 или по-нова, Opera ver.17 или по-нова;

» Активирайте автоматично обновяване на браузъра, вкл. Phishing филтрите на браузъра;

» Избягвайте инсталирането на допълнителни ленти с инструменти (toolbars – ASK toolbar, Google toolbar и др.) в браузъра – подобни допълнения към браузърите често се използват за разпространяване на зловреден софтуер;

» Своевременно уведомявайте Банката при промяна на GSM номера за

получаване на SMS-кодове за потвърждаване на платежни операции и промяна на права и лимити.

ССВ ONLINE LITE

Осъществявайте достъп до услугата ССВ Online 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;

» Избягвайте използването на общодостъпни компютри (интернет зали, библиотеки и т.н.) за достъп до услугата ССВ Online Lite;

» Избягвайте използването на общодостъпни безжични мрежи (Wi-Fi), с цел ограничаване на риска от достъп на злонамерени лица до въведената информацияв интернет, в т.ч. потребителско име и парола;

» Осъществявайте достъп до услугата ССВ Online Lite директно чрез набиране на уеб адреса на портала за вход в услугата от официалния сайт на Банката;

» Избягвайте ползването на функции за автоматично допълване на уеб адреси;

» Проверявайте автентичността на уеб страницата и сигурността на комуникацията с нея чрез клик върху иконата катинар в адресната лента на браузъра;

» Използвайте бутон „Изход“ и затваряне на браузъра при приключване на работа в услугата ССВ Online Lite;

» Използвайте пароли за достъп с дължина поне 6 /шест/ знака, съдържащи задължително главни и малки латински букви, цифри и специални символи;

» Периодично сменяйте паролата за достъп до услугата ССВ Online Lite;

» Избягвайте да запаметявате потребителското име и парола в браузъра на компютъра;

» Избягвайте използването на имена на членове от семейството или фирмени имена, рождени дати или телефонни номера за парола за вход в ССВ Online Lite;

» Използвайте интернет браузъри, които поддържат 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;

» За оптимална работа и максимална сигурност използвайте браузъри – Internet Explorer ver. 11, Mozilla Firefox ver.27, Google Chrome ver.38 или по-нова, Microsoft Edge, Safari ver.7 или по-нова, Opera ver.17 или по-нова; Активирайте автоматично обновяване на браузъра, вкл. Phishing филтрите на браузъра;

» Избягвайте инсталирането на допълнителни ленти с инструменти (toolbars – ASK toolbar, Google toolbar и др.) в браузъра – подобни допълнения към браузърите често се използват за разпространяване на зловреден софтуер;

» Своевременно уведомявайте Банката при промяна на GSM номера за получаване на SMS-кодове за потвърждаване на платежни операции и промяна на права и лимити.

CCB MOBILE

» Опазвайте и съхранявайте мобилното устройство и ПИН кода за вход в мобилното приложение на сигурни и недостъпни за трети лица места;

» Използвайте стандартните механизми за сигурност на операционната система на мобилното устройство – използвайте код за достъп до мобилното устройство, различен от избрания ПИН код за вход в мобилното приложение;

» Поддържайте сигурността на операционната система на мобилното устройство чрез инсталиране на последните й обновления;

» Избягвайте използване на „jailbroken” и “rooted” устройства, при които механизмите за сигурността на операционната система са унищожени;

» Инсталирайте антивирусен софтуер в мобилния телефон и редовно го актуализирайте;

» Избягвайте използването на съмнителни мобилни приложения, които могат да компрометират сигурността на мобилното устройство;

» Защитете мобилното устройство с парола и задайте автоматично заключване на екрана, когато не използвате мобилното устройство;

» Инсталирайте приложения само от официални магазини за мобилни приложения – App Store, Google Play и Huawei App Gallery;

» Използвайте бутон „Изход” при излизане от мобилното приложение;

» Избягвайте използването на общодостъпни безжични мрежи (Wi-Fi) с цел ограничаване на риска от достъп на злонамерени лица до въведената информация в интернет, в т.ч. потребителско име и парола;

» Периодично сменяйте Вашия ПИН код за достъп до мобилното приложение;

В случай на загуба или кражба на мобилното Ви устройство с достъп до системата за Интернет банкиране, се свържете с Центъра за обслужване на клиенти на денонощен телефон *5050 или посетете офис на Банката.

ИЗПОЛЗВАНЕ НА БАНКОВА КАРТА

СИГУРНОСТ НА КАРТАТА И ПИН КОДА

» Никога не записвайте ПИН кода върху картата или в близост до нея;

» Унищожете плика с ПИН кода веднага след като го запаметите;

» Препоръчваме Ви да промените получения ПИН код веднага след като го получите. Може да смените своя ПИН код на всеки банкомат в България. Не е желателно да използвате поредни цифри, рождени дати или телефонни номера. Сменяйте периодично своя ПИН код;

» Ако при получаването на ПИН плика забележите, че не е запечатан, веднага се обадете в Банката;

» Вашият ПИН е известен единствено и само на Вас. Никога не съобщавайте ПИН кода си на никого, включително и на служител на Банката;

» Не преотстъпвайте, не предавайте и не правете достъпна картата на трети лица, включително и на членове на семейството Ви;

» При получаване на картата от Банката, веднага се подпишете на гърба й, на мястото, определено за Вашия подпис;

» Предпазвайте картата си от механични повреди.

ТЕГЛЕНЕ НА ПАРИ В БРОЙ ОТ БАНКОМАТ

» Пригответе картата си предварително, огледайте се или изчакайте клиента пред Вас, оставяйки разумна дистанция. Ако сте извън страната, предварително проверете дали на банкомата има логото на картовата организация, което е отпечатано и на Вашата карта;

» При въвеждане на ПИН, закрийте с ръка клавиатурата и се убедете, че не сте наблюдавани от някого в непосредствена близост до Вас;

» Не бройте парите пред банкомата, а на друго сигурно място;

» При проблем с трансакцията, никога не се доверявайте на стоящо наблизо лице, което Ви предлага своята помощ;

» Ако Ви се стори, че има нещо нередно, откажете операцията и използвайте друг банкомат;

» Винаги вземайте Вашата разписка и ако нещо Ви притеснява относно остатъчното салдо, може да се обърнете към Банката;

» Преди да използвате банкомат, винаги оглеждайте отвора за картата за нещо съмнително;

» Убедете се, че банкоматът е обозначен с логото на съответния вид карта;

» Когато използвате банкомат, застанете пред екрана и клавиатурата така, че операцията и ПИН кодът Ви да останат скрити. Следвайте инструкциите на екрана. Ако не сте сигурни в операцията, която извършвате, по-добре натиснете бутон „Отказ“;

» Не забравяйте да вземете парите, картата и разписката от извършената трансакция. Имайте предвид че на разписката е записана част от информация за Вашата карта, затова я унищожете преди да я изхвърлите;

» Ако банкоматът задържи картата Ви, незабавно уведомете Банката и блокирайте картата. Препоръчваме Ви да подадете искане за издаване на нова карта с нов номер.

ПЛАЩАНИЯ С КАРТА ЧРЕЗ ПОС ТЕРМИНАЛ В ТЪРГОВСКИ ОБЕКТ

» Уверете се, че даденият търговец е оторизиран да приема плащания с карти;

» Не предоставяйте картата си на други лица. Ако е необходимо да платите с нея в търговски обект, не позволявайте опериране с картата без Ваш надзор;

» Никога не оставяйте Вашата карта без надзор, докато не приключи операцията. Ако е възможно, прекарайте сами картата през четящото устройство на ПОС терминала. Ако Вашата карта е безконтактна и търговецът приема безконтактни плащания, поискайте Вие сами да извършите трансакцията чрез доближаване на картата до ПОС устройството, без да я предоставяте на служител на търговеца;

» Когато плащате с карта в търговския обект, се уверете в точността на сумата, която е изписана на разписката от ПОС устройството.

При въвеждане на ПИН кода закрийте с ръка клавиатурата и се убедете, че не сте наблюдавани от някого в непосредствена близост до Вас.

ПЛАЩАНИЯ С КАРТА В ИНТЕРНЕТ

» Винаги предоставяйте актуален мобилен номер в Банката, за да може да се свържем с Вас;

» Когато в полето за URL адрес най-отпред е изписано https://, “s” означава, че сайтът използва криптирана, защитена комуникация клиент-сървър връзка. Ако сайтът не използва защитена връзка (започва с http://), някой може да проследи или промени информацията, която изпращате или получавате чрез него;

» Следете за икона със заключен катинар в адресната лента на браузъра. Катинарът показва, че страницата използва сертификат за криптиране на комуникацията. Той се издава индивидуално за всяка интернет страница. В него винаги можете да видите какъв е истинският адрес на сайта. За да проверите дали сертификатът действително е издаден на търговеца, от чийто сайт искате да направите плащане с карта, кликнете с мишката върху иконата с катинара. Също така, не забравяйте да обърнете внимание и до кога е валидността на сертификата;

» Ако виждате червен предупредителен надпис на страницата или адресната лента свети в червен цвят, сайтът е означен като опасен. Използването му ще изложи на риск информацията Ви;

» За онлайн покупки ползвайте уебсайтовете на познати търговци или утвърдени марки. Проследете дали търговецът е посочил своята контактна информация – имейл, телефон, адрес. Ако липсва такава, това може да е индикация, че сте попаднали на сайта на някой фалшив търговец, който се интересува единствено от финансовите Ви данни. За да сте спокойни, проверете също какви са условията за доставка и връщане на стоките. Ако липсва секция тип „За нас“/ „Контакти“, както и ясни контакти с екипа, доверието Ви към въпросния сайт трябва да е много ниско;

» Обръщайте повече внимание на офертите, които получавате. Нереално ниски цени на атрактивни стоки може да са сигнал както за предлагането на фалшиви стоки, така и за опит за измама и събиране на данни – имейл адреси, пароли, данни за банкови карти;

» Уверете се в правилното изписване на името на страницата. Някои фалшиви сайтове използват близки имена на популярни домейни, като сменят само някои букви. Целта им е да заблудят потребителите и те да предоставят лична информация;

» Внимавайте, когато отваряте кратки (съкратени линкове), тъй като не е ясно към какъв сайт водят те. За да проверите това, задръжте курсора на мишката върху връзката, но без да кликвате върху нея. По този начин ще Ви се визуализира действителния адрес, към който води връзката;

» Избирайте сайтове, които са включени в програмите за сигурни плащания с банкови карти на Visa и Mastercard – **Visa Secure** и **Mastercard Identity Check**. Ако сайтът не ги поддържа, проверете дали той е защитен – погледнете за икона на ключ или катинар (в името на линка) или най-долу на браузъра Ви. Въвеждайте данните на своята карта само в сигурни интернет страници. Преди извършване на плащане Ви препоръчваме да проверите за отзиви и мнения относно сайта на други потребители;

» Запазете електронната разписка за плащането, имейли или друга кореспонденция с търговеца. Може да Ви е полезна в случай на оспорване на плащането;

» По никакъв повод не бива да въвеждате ПИН кода си в Интернет или да го посочвате в e-mail. ПИН кодът се използва само за потвърждаване на операции банкомати и ПОС устройства;

» Ако търговецът не Ви изпрати или не предостави стоката или услугата в съответния й вид, то е необходимо да се свържете с него и да изясните въпроса. В случай че възникне спор, потърсете Банката за съдействие;

» Избягвайте въвеждането на данните от личните Ви банкови карти на компютри и други устройства с достъп до интернет, които се ползват от повече хора;

» При покупки или резервации в интернет, преди да извършите плащането се убедете, че сте се запознали с всички условия, свързани с него – Общи условия на търговеца, срокове за доставка и политика при връщане на стоки, отказване на резервации и оспорвания и т.н. Бъдете внимателни и се уверете, че давате разрешение на търговеца да задължи сметката Ви само със сумата на конкретната покупка;

» В случай на изгубена, откраднатa карта, на неоторизирано плащане

или съмнение за злоупотреба, е важно веднага да се обадите на денонощен телефон *5050, 02/92 66 500 или 0889 934 694, за да блокирате Вашата карта. Можете да я блокирате и през мобилното приложение на ЦКБ АД – ССВ Mobile.

МЕРКИ ЗА ДОПЪЛНИТЕЛНА ЗАЩИТА

- Възползвайте се от услугите, създадени за Вашата сигурност и комфорт, които Банката предлага;
- Преглеждайте ежедневно наличността по картата Ви, извършените с нея операции, и при необходимост се свържете с Банката за съдействие;
- Използвайте антивирусна защита – вирусите могат да повредят Вашия компютър, да унищожат данни или да изпратят лична информация и пароли на неоторизирани лица;
- Използвайте сигурна парола – комбинация от букви, цифри и специални символи като „@“, „!“ и др. Сменяйте паролата си често;
- Важно е да сменяте често паролите си. Препоръчително е паролата да се променя на максимум 3 месеца, това се отнася и за ПИН кода. Не използвайте една и съща парола за достъп до различни акаунти за електронно банкиране, имейли и други;
- Бъдете бдителни – не оставяйте безконтролно личния си мобилен телефон, за да сте сигурни, че не се използва от друг без Ваше знание;
- Не оставяйте без надзор своя КЕП – винаги изключвайте от компютъра Вашия Квалифициран електронен подпис (КЕП) и никога не го оставяйте без надзор;
- Изход от системата – след като използвате ССВ Online Lite и ССВ On-line, прекратете сесията, като натиснете бутона „ Изход“, а не просто да затворите прозореца на браузъра.

ФИШИНГ И ИМЕЙЛ НОТИФИКАЦИИ

Централна Кооперативна Банка не изпраща към своите клиенти електронни съобщения (e-mail), с които да изисква от тях да въвеждат лична информация и данни на посочен интернет адрес. В никакъв случай не предоставяйте Ваши лични данни и информация, свързани с достъпа Ви до интернет банкирането, Вашата банкова сметка, данни от карта и други. Паролите за достъп са персонални и е Ваше задължение и отговорност да ги запазите известни единствено и само на Вас.

Фишингът (phishing) представлява измама, която подканва потребителя на компютри и други устройства, свързани с интернет, да разкрие своя лична или финансова информация в e-mail съобщение или уебсайт. Потребителят бива насочен към измамнически уебсайт, където се изисква да предостави лични и финансови данни. Този уебсайт 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 извършват 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 други. ЦКБ АД не разменя този тип информация по електронна поща;
- Проверявайте какъв е e-mail адресът, а не само името на изпращача. Обикновено в полето „От“ се визуализира името, което изпращачът е избрал да виждате, когато получавате електронно съобщение от него;
- Не отваряйте линкове и прикачени файлове при получаване на съмнителен e-mail и не инсталирайте на компютъра си непознати приложения, преди да проверите техния произход;
- Не отваряйте (кликвайте) върху връзки в имейли, съобщения, уеб страници или изскачащи прозорци от уебсайтове или податели, на които нямате доверие;
- Винаги проверявайте истинността на съобщенията, които получавате на своята електронна поща. Банката комуникира с клиентите си с официални e-mail адреси с домейн: @ccbank.bg.

ПРИ ПОДОБНИ СЛУЧАИ ПРЕПОРЪЧВАМЕ ДА ПРЕДПРИЕМЕТЕ СЛЕДНИТЕ ДЕЙСТВИЯ:

- Проверка на компютърното устройство с лицензиран антивирусен софтуер;
- Редовно обновяване на ползваната система, използване само на лицензиран и закупен софтуер;
- Промяна на паролата за достъп до пощата със сложна комплексна парола (големи и малки букви, числа и специални символи, с не по-малко от 10 символа).

Ако се съмнявате в истинността на дадено съобщение, не се колебайте да свържете се с нас.

- *5050 (Таксуването на разговорите е спрямо тарифите и политиките на използвания от клиента мобилен оператор. Възможно е обажданията към кратък номер да не се включват в пакета безплатни минути, за което ЦКБ АД не носи отговорност);
- 02/9266 500;
- 0889 934 694.

Допълнителна информация и съвети, препоръки и информация за продуктите и услугите за сигурност можете да получите и във всеки офис на Банката, както и на **www.ccbank.bg**

www.ccbank.bg/