2022/10

Инструкции за сигурност при използване на KBC Online Bulgaria

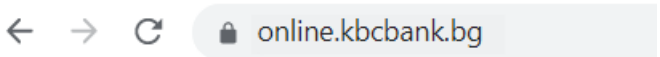
Кей Би Си Банк България ЕАД използва най-съвременни методи и средства за защита на своето интернет банкиране – KBC Online Bulgaria, като ефективно пази Вашите парични средства и Ви дава удобството да банкирате навсякъде. Съветваме Ви да спазвате правилата за сигурност, описани в настоящия документ, за да допринесете за повишаването на тази защита. Това ще доведе и до значително намаляване на риска от измама при извършване на разплащания по електронен път.

Достъп до сайта за интернет банкиране KBC Online Bulgaria

- Не използвайте споделени компютри за достъп до KBC Online Bulgaria. Ограничете максимално броя на устройствата, които използвате за влизане в интернет банкирането. Използвайте проверени и защитени с актуализиран антивирусен софтуер устройства.
- Избягвайте използването на KBC Online Bulgaria в присъствието на други хора или на публични места.
- Ако използвате безжична мрежа (Wi-Fi), уверете се, че е защитена със съвременен протокол за изграждане на сигурна връзка (WPA2 или по-нов). Избягвайте публични Wi-Fi мрежи. Свързването Ви към общодостъпни и отворени мрежи може да осигури достъп на злонамерени лица до въведената от Вас информация в интернет, в т.ч. потребителско име и парола.
- Достъпвайте KBC Online Bulgaria директно чрез набиране на адреса https://online.kbcbank.bg или от официалния сайт на Кей Би Си Банк България ЕАД https://www.kbcbank.bg. Не използвайте функции за автоматично допълване на адреси.
- Не включвайте сайта на KBC Online Bulgaria в предпочитаните връзки (Bookmarks, Favorites) на Вашия браузър, тъй като съществува риск от манипулиране на запазените по този начин връзки от неоторизирани лица (хакери).
- Винаги проверявайте дали уеб страницата, която отваряте, за да достъпите KBC Online Bulgaria, е автентична и комуникацията с нея е подсигурена. След зареждането на страницата направете проверка на сесията от Вашия уеб браузър, преди да въведете потребителско име и парола. Проверката се прави по следния начин:

Google Chrome

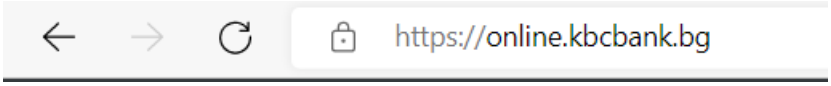
- В лявата част на полето за адрес трябва да видите заключен катинар



- Кликнете върху него
- Уверете се, че виждате статус “Connection is secure”.

Edge

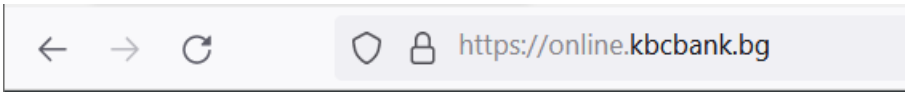
- В лявата част на полето за адрес трябва да видите заключен катинар



-
- Кликнете върху него
- Уверете се, че присъства статус „Connection is secure"

Mozilla Firefox

- В лявата част на полето за адрес трябва да видите заключен катинар



- Кликнете върху него
- В прозорчето, което се отваря се уверете, че присъства статус "Connection is secure"

- Винаги, след като приключите банкирането с KBC Online Bulgaria, използвайте бутона (Изход) в горния десен ъгъл на екрана преди да затворите браузъра.

Интернет браузъри

- Не запаметявайте Вашето потребителско име и/или парола за достъп до KBC Online Bulgaria във Вашия браузър.
- За достъп до KBC Online Bulgaria използвайте интернет браузър, който поддържа протокол за изграждане на сигурна връзка TLS версия 1.2 или по-нова и версии на Edge, Mozilla Firefox, Safari, Opera, Google Chrome, които получават редовни актуализации и не са със спряна поддръжка от разработчиците им.
- Обръщаме внимание, че производителят на браузъра Internet Explorer преустанови неговата поддръжка на 15.06.2022 г. Това означава, че след тази дата потребителите на този браузър няма да получават актуализации, които да коригират установени проблеми със сигурността или програмни грешки. С цел сигурност и безпроблемна работа с KBC Online Bulgaria е необходимо за достъп до Вашето онлайн банкиране да ползвате браузърът Edge, който заменя Internet Explorer или друг браузър, чиято поддръжка не е преустановена.
- 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 KBC Online Bulgaria, освен ако не са Ви от абсолютна необходимост. Някои допълнения към браузърите могат да се използват за разпространяване на зловреден софтуер.

Потребителско име и парола за достъп

- Още при първоначалната промяна на паролата - винаги избирайте „силна" парола, която е с минимална дължина от поне осем символа, съдържаща малки и главни букви, цифри и специални символи (*,!,&, и др.).

- Сменяйте редовно паролата си (минимум веднъж на два месеца). Паролата за Вашето интернет банкиране трябва да е различна от тези, с които достъпвате Вашите имейли, регистрации в социални мрежи и други, както и да е различна и да не съдържа част от Вашето име за интернет банкиране. Ако използвате софтуер за безопасно съхранение и управление на пароли, уверете се, че ползвате такъв с висок рейтинг и репутация.
- Запомнете Вашето потребителско име и парола за KBC Online Bulgaria 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. Избягвайте да използвате за парола речникови думи.
- Не споделяйте потребителското име и паролата си с никого, дори и с членове на семейството или колеги. Те са строго лични, еднозначно Ви определят в системата като потребител. Това е Вашата самоличност пред системата за онлайн банкиране. Ако някой се сдобие с потребителското Ви име и парола, той ще добие достъп до системата от Ваше име.
- Ако е необходимо служители на фирмата Ви или членове на семейството Ви да имат достъп до сметките Ви, Вие като титуляр е необходимо да заявите отделен достъп за тях като посетите офис на Кей Би Си Банк България ЕАД.
- При промяна на посочения телефонен номер за връзка с Вас, винаги информирайте за промяната Кей Би Си Банк България ЕАД. По този начин, при нужда от потвърждаване на платежно нареждане, ще можем да Ви предоставим по-бързо и качествено обслужване. Не посочвайте телефон на Ваш близък или колега.

Допълнителни средства за сигурност при активно банкиране

- KBC Online Bulgaria предоставя на потребителите си допълнителни средства за сигурност, които се използват за потвърждаване на активните операции – парола MTAN, която се изпраща чрез SMS съобщение или код, генериран от хардуерно устройство или токен (хардуерно устройство или специализирано приложение за мобилни устройства – софтуерен токен)
- Парола MTAN чрез SMS съобщение – При оторизиране на плащания чрез парола MTAN, като SMS съобщение получавате детайли за превода – парола MTAN, сума на превода и последните 10 цифри и букви от IBAN номера на сметката на получателя. Ако получите MTAN без да сте инициирали плащане или има разминаване на последните 10 цифри и букви от IBAN номера в SMS съобщението с тези на IBAN номера, по който желаете да наредите средства – НЕ въвеждайте MTAN кода за оторизиране на операцията и веднага сигнализирайте на Кей Би Си Банк България ЕАД. Не предоставяйте мобилния си телефон, на който получавате SMS съобщения за оторизиране на преводи на други лица.
- Хардуерно устройство (token) – Съхранявайте токен устройството на сигурно място под Ваш контрол. Запомнете отключващия ПИН и не го съобщавайте на никого, не го записвайте на физически носител или на гърба на токена.
- Потвърждаване с токен - При оторизиране на плащания чрез токен устройство на дисплея на устройството (софтуерен или хардуерен) получавате детайли за превода – последните 10 цифри и букви на сметка на получател, сума на превода и валута. Винаги сверявайте последните 10 цифри

и букви на сметката на получателя със сметката, по която желаете да наредите средства – в случай на разлика НЕ въвеждайте генерирания от токена код за оторизиране на операцията и НЕ потвърждавайте превода чрез онлайн режим на подпис и веднага сигнализирайте на Кей Би Си Банк България ЕАД.

- KBC Online Bulgaria предоставя възможност за използване на групов подпис, при който активните операции могат да бъдат потвърждавани от няколко потребителя с различни допълнителни средства за сигурност. По този начин се повишава сигурността при активните Ви операции. Преценете възможността от използването на групов подпис за корпоративни цели.

Операционна система и допълнителен софтуер

- Винаги използвайте максимално обновена операционна система и софтуерни продукти. Днес повечето операционни системи и софтуерни продукти могат да бъдат настроени да се обновяват автоматично. Ако такава опция е налична, активирайте я. В случай, че опцията за автоматично обновление не е налична, използвайте обновявания за операционната система и софтуерните продукти само от страниците на производителите им. Хакери често използват електронната поща за разпространяване на фалшиви обновявания за различни софтуерни продукти, които съдържат зловреден софтуер. Чрез използването на актуализирана операционна система и софтуерни продукти, намалявате възможността недоброномерени лица да използват „пробиви“, чрез които да се сдобият с Ваша лична информация.
- Различни видове софтуер, инсталиран на компютъра, с който банкирате с KBC Online Bulgaria, могат да окажат влияние на сигурността на Вашето онлайн банкиране. Следете информацията, предоставяна от производителите на инсталираните от Вас програми за „пропуски“ или „бъгове“ в техните продукти.
- Използвайте персонална защитна стена (firewall) на компютъра, с който банкирате електронно. По този начин се защитавате по време на престоя Ви в интернет от нежелана намеса от трети лица. Защитните стени могат да бъдат конфигурирани да Ви алармират при опит за атака отвън. Активирайте опцията за автоматично обновяване на програмите – персонални защитни стени.
- Инсталирайте антивирусна програма на персоналния компютър, който използвате за банкиране с KBC Online Bulgaria. Антивирусният софтуер сканира файловете и електронната Ви поща за вируси. Той предпазва и от „троянски коне“, които позволяват на външно лице да придобие отдалечен контрол над личния Ви компютър.
- Използвайте утвърдени марки антивирусен софтуер. Проверете за препоръчан от производителят на операционната Ви система. В интернет се предлагат голям брой свободни антивирусни програми под различни наименования от неизвестни производители. В голяма част от случаите тези програми са създадени от хакери и се разпространяват чрез спам или тактики за сплашване (интернет страница Ви съобщава, че компютърът Ви е заразен с вирус и Ви приканва да свалите съответната програма, за да го изчистите – scareware). Често подобни програми съдържат вируси, „троянски коне“ и друг зловреден софтуер. В други случаи тези програми правят компютъра, на който са инсталирани неизползваем, докато потребителят не заплати лицензионна такса за тях (ransomware).
- Повечето антивирусни програми се обновяват автоматично, за да предпазват от постоянно изникващите нови заплахи в интернет пространството. Винаги използвайте актуализиран антивирусен софтуер.

- Не инсталирайте и не използвайте софтуер със съмнителен произход. Използването на „кракнати“ програми от торент сайтове също носи голям риск. Тези програми са с пробита защита, като могат да послужат за инсталирането на зловреден софтуер и „троянски коне“.
- Обръщаме Ви внимание за изтеклата поддръжка на операционната система Windows XP (http://windows.microsoft.com/bg-bg/windows/end-support-help) и мерките, които трябва да предприемете, за да запазите нивото си на сигурност.

Мобилно банкиране чрез специализирани апликации

- Интернет банкирането на Кей Би Си Банк България ЕАД – KBC Mobile Bulgaria може да бъде достъпвано и чрез специализираните мобилни приложения за смарт устройства – телефони, таблети и др. Приложенията са достъпни за операционните системи Android и iOS.
- Кей Би Си Банк България ЕАД разпространява апликациите за смарт устройствата само чрез официалните маркети - използвайте за инсталиране на приложенията Google Play Store (за Android), AppGallery (за Huawei) и App Store (за iOS).
- Достъпът до мобилното приложение на KBC Mobile Bulgaria се извършва със същите потребителско име и парола, както и за стандартното интернет банкиране. За по-удобен и бърз вход в KBC Mobile Bulgaria, мобилното приложение предлага възможността за настройка на ПИН и/или биометрични данни – когато устройството го поддържа (пръстов отпечатък за Android, FaceID и пръстов отпечатък за iOS).
  За целта потребителят трябва да се впише със своето потребителско име и парола, след което от настройките на профила (меню „Моят профил“) да избере желания от него начин на вписване. В случай на забравен ПИН или при проблем с разчитането на биометричния отпечатък, потребителят винаги може да избере опцията да се впише със своето потребителско име и парола. При получаване на нов пин плик за достъп от офис на Банката в случай, че преди това на устройството е било активирано вписване чрез биометрия или ПИН, то тази настройка се деактивира автоматично. За да се активира отново бърз вход с биометрия/ПИН, е необходимо приложението да се преинсталира и да се достъпи с данните за вход от новия пин плик.
  Само по един потребител на устройство може да ползва опцията за вписване с ПИН и един за вписване с биометричен отпечатък. Например:
  - потребител „А“ използва опция за вписване с ПИН, потребител „Б“ опция за вписване с биометричен отпечатък,
  - потребител „А“ използва опциите за вписване с ПИН и биометричен отпечатък. В този случай потребител „Б“ няма да може да настрои нито една от двете опции за бърз достъп, но може да използва потребителско име и парола.
- За да може да се използва опцията за вписване чрез биометричен отпечатък, потребителят трябва предварително да е направил настройката на своето устройство.
  - Когато устройството работи с операционна система Android, след всяка промяна – добавяне или премахване на биометричен отпечатък в настройките на устройството, потребителят трябва да изчисти данните на мобилното приложение, след което отново да направи съответните конфигурации за вход с ПИН или биометричен отпечатък.
  - При операционна система iOS добавянето или премахването на биометричен отпечатък в настройките на устройството не налага каквито и да било нови настройки в мобилното приложение на KBC Mobile Bulgaria.

Обръщаме внимание, че при използването на биометричен отпечатък за вписване в KBC Mobile Bulgaria, когато операционната система е iOS, всяко лице, имащо достъп до устройството чрез биометричен отпечатък, ще получи достъп до профила за KBC Mobile Bulgaria, който е конфигуриран да работи с биометричен отпечатък на въпросното устройство!

Кей Би Си Банк България ЕАД не съхранява и не обработва въпросните биометрични отпечатъци!

- Мобилното приложение поддържа известия в реално време (push notifications). Потребителят може да активира желаните от него известия от настройките на своя профил (меню „Известия"), след вписване в мобилното приложение.
  Нотификациите се получават на последното устройство, от което потребителят се е вписал в своя профил в KBC Mobile Bulgaria.
  В случай че се е наложило да се впишете от друго устройство, единственото, което трябва да направите, за да продължите да получавате известия, е да се впишете отново в профила си от Вашето лично устройство.
  За да прекратите получаването на известия, може да деактивирате абонаментите от меню Известия.
- Допълнителните средства за сигурност, които могат да се използват за активно банкиране чрез мобилните апликации са MTAN парола чрез SMS и хардуерно устройство (token). При използване на MTAN парола чрез SMS, е удачно да заявите получаването на оторизиращия код на друг телефонен номер, различен от този, който е в устройството за мобилно банкиране.
- Обмислете поставянето на допълнителна защита на смарт устройството като парола за отключване, разпознаване на лицеви черти, пръстов отпечатък, жестове и други в зависимост от модела и функционалностите на мобилното устройство. По този начин ще увеличите сигурността си при физическа кражба на устройството. Не позволявайте телефонът, от който банкирате, да се използва от други лица без надзор.
- Инсталирайте антивирусен софтуер предоставен от надеждни производители на антивирусни програми. Използвайте официалните маркети за инсталирането му.
- Винаги актуализирайте операционната система на смарт устройството до последната възможна версия. Чрез тези актуализации производителите отстраняват откритите уязвимости в по-ранните версии на системата. Използвайте инструкциите на производителя.
- Не банкирайте активно от смарт устройства, които са руутнати (root) или jailbreak. Root и jailbreak са действия, които позволяват да се използват заключени от производителя функции на телефона и придобиване на администраторски права. Получаването на администраторски права предоставя възможност от злонамерени лица да получат пълен и неоторизиран достъп до цялото Ви устройство.

Фишинг, социално инженерство, имейл нотификации, съобщения в чат и телефонни обаждания

- Фишингът (phishing) представлява измама, която подканва потребителите на компютри и други устройства, свързани в интернет да разкрият своя лична или финансова информация в имейл съобщение или уеб сайт. Потребителят бива насочен към измамнически уеб сайт, където им се поисква да предоставят лични данни (например) тяхното потребителско име и парола за достъп до KBC Online Bulgaria. 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 му. **Кей Би Си Банк България ЕАД никога не изпраща линкове, които Ви подканват да въведете потребителско име и парола за вход в KBC Online Bulgaria**. Винаги въвеждайте собственоръчно адреса на KBC Online Bulgaria в уеб браузъра – само така можете да бъдете сигурни, че въвеждате данните си за вход без да ги споделяте с трети лица.

- 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.

Социално инженерство (опит за подвеждане) представлява действия от лица, представящи се за служители на обслужващата Ви банка, с които се стремят да Ви накарат да споделите в телефонен разговор, чат съобщение или имейл поверителна информация, чието разкриване може да Ви навреди. Също така, под претекст, че информацията е необходима, за да Ви се окаже съдействие, да Ви насърчат да инсталирате софтуер на Ваше мобилно устройство или компютър, чрез който да добият достъп и контрол над него.

Кей Би Си Банк България ЕАД не изпраща по електронна поща или чат съобщения, които Ви приканват да предоставите данни за Вашата парола, потребителско име, номер на сметка, банкови карти и др. Служители на Кей Би Си Банк България ЕАД няма да поискат такава информация и в телефонен разговор с Вас.

- Кей Би Си Банк България ЕАД не разменя този тип информация по електронна поща, чат или в телефонен разговор.
- Кей Би Си Банк България ЕАД не изпраща по електронна поща или чат съобщения, които Ви приканват да се обадите на посочен в съобщението телефон, за размяна на информация свързана с акаунта Ви в KBC Online Bulgaria.
- Кей Би Си Банк България ЕАД няма да поиска от Вас да инсталирате софтуер за отдалечен контрол като Team Viewer, AnyDesk, VNC и др. с цел отдалечено съдействие.
- Ако се съмнявате в истинността на дадено съобщение, получено чат съобщение или телефонно обаждане, не се колебайте да свържете се с нас на официалният ни телефонен номер или имейл адрес.

При възникнали въпроси и съмнения за злоупотреби – връзка с Контактния център

Телефони	0700 10 000 (Vivacom); 17 21 (A1 и Yettel)
E-mail	call.center@kbcbank.bg