Инструкции за сигурност при използване на Райфайзен ОНЛАЙН и RaiMobile

Райфайзенбанк България (ЕАД) използва най-съвременни методи и средства за защита на своето интернет банкиране – Райфайзен ОНЛАЙН, 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 злоупотреба, когато плащате с банкови карти в интернет.

Достъп до сайта за интернет банкиране Райфайзен ОНЛАЙН

- Не използвайте общодостъпни компютри (интернет зали, библиотеки и т.н.) за достъп до Райфайзен ОНЛАЙН.
- 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 Райфайзен ОНЛАЙН директно чрез набиране на адреса https://online.rbb.bg или от официалния сайт на Райфайзенбанк https://www.rbb.bg. Не използвайте функции за автоматично допълване на адреси.
- Не включвайте сайта на Райфайзен ОНЛАЙН 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 Райфайзен ОНЛАЙН, 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 зелен катинар

  - Кликнете върху него
  - Кликнете върху опцията “Details”
  - Кликнете върху бутона “View certificate”
  - Изберете таб „Certification path”
  - Проверете дали йерархията на сертификата (Certification path) има последователност "COMODO RSA Certification Authority" -> "COMODO RSA Extended Validation Secure Server CA" -> "online.rbb.bg" и статуса на сертификата (Certificate status) е “OK”.

  Internet Explorer

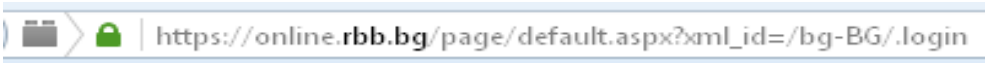
  - В дясната част на полето за адрес трябва да видите катинар

  - Кликнете върху него
  - Кликнете върху бутона “View certificates”
  - Изберете таб „Certification path”
  - Проверете дали йерархията на сертификата (Certification path) има последователност "COMODO RSA Certification Authority" -> "COMODO RSA Extended Validation Secure Server CA" -> "online.rbb.bg" и статуса на сертификата (Certificate status) е „OK”.

Mozilla Firefox

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



- Кликнете върху него
- В прозорчето, което се отваря кликнете върху стрелката сочеща в дясно
- Натиснете бутона „More Information"
- В прозореца, който се отваря натиснете бутона "View certificate"
- Изберете таб "Details"
- Проверете дали йерархията на сертификата (Certificate Hierarchy) има последователност "COMODO RSA Certification Authority" -> "COMODO RSA Extended Validation Secure Server CA" -> "online.rbb.bg" и датата на валидност (Validity Not After) е актуална.

- Винаги след като приключите да банкирате с Райфайзен ОНЛАЙН, използвайте бутона „Изход" преди да затворите браузъра.

Интернет браузъри

- Не запаметявайте Вашето потребителско име и/или парола за достъп до Райфайзен ОНЛАЙН във Вашия браузър.
- За достъп до Райфайзен ОНЛАЙН използвайте интернет браузър, който поддържа 128 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.
- 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 Райфайзен ОНЛАЙН, 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

- Още при първоначалната промяна на паролата - винаги избирайте „силна" парола, която е с минимална дължина от 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.
- Запомнете Вашето потребителско име и парола за Райфайзен ОНЛАЙН 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. 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 можете да заявите отделен достъп за тях като посетите офис на Райфайзенбанк.

Допълнителни средства за сигурност при активно банкиране

- Райфайзен ОНЛАЙН предоставя на потребителите си две допълнителни средства за сигурност, които се използват за потвърждаване на активните операции – парола MTAN чрез SMS съобщение и токен (хардуерно устройство или специализирано приложение за мобилни устройства – софтуерен токен).
- Парола MTAN чрез SMS съобщение – При използване на това средство за сигурност, потребителят своевременно ще бъде информиран (получавайки SMS с парола и детайли), в случай на злонамерен опит за извършване на активни операции от негово име, които реално не е инициирал. Не предоставяйте мобилния си телефон, на който получавате SMS съобщения за оторизиране на преводи на други лица.
- Хардуерен и Софтуерен токен – Съхранявайте Вашия токен на сигурно място под Ваш контрол. Запомнете отключващия ПИН и не го съобщавайте на никого, не го записвайте на физически носител или гърба на токена.
- Райфайзенбанк разпространява мобилната апликация софтуерен токен „Райфайзен Токен“ само чрез официалните маркети - използвайте за инсталиране на приложенията Google Play Store (за Android) и iTunes (за iOS).
- Райфайзен ОНЛАЙН 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 лични или 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 недобронамерени лица да използват „пробиви“, чрез които да се сдобият с Ваша лична информация.

- Различни видове софтуер, инсталиран на компютъра, с който банкирате с Райфайзен ОНЛАЙН, може да се отрази 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 Райфайзен ОНЛАЙН. 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 WindowsXP (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 апликацията RaiMobile

- Интернет банкирането на Райфайзенбанк – Райфайзен ОНЛАЙН може да бъде достъпвано и чрез специализираното мобилно приложение RaiMobile за смарт устройства – телефони, таблети и др. Приложението е достъпно за операционните системи Android и iOS.
- Райфайзенбанк разпространява апликацията RaiMobile за смарт устройствата само чрез официалните маркети - Google Play Store (за Android) и iTunes (за iOS).
- Достъпът до RaiMobile се извършва със същите потребителско име и парола както и за стандартното интернет банкиране. За по-удобен и бърз вход в RaiMobile, мобилното приложение предлага възможността за настройка на ПИН и/или биометричен отпечатък – 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 меню „Моят профил" да избере желания от него начин на достъпване. 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.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 RaiMobile.

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

  Райфайзенбанк 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 нотификации от меню „Известия". Нотификациите се получават на последното устройство, от което потребителят се е вписал в своя профил в RaiMobile.
  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 отново от меню „Известия".
- Допълнителните средства за сигурност, които могат да се използват за активно банкиране чрез мобилната апликация са MTAN парола чрез SMS или специализирано приложение - софтуерен токен („Райфайзен Токен"). 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 и имейл нотификации

- Фишингът (fishing) 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. 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 Ви.
- 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.
- Райфайзенбанк не изпраща по електронна поща съобщения, които Ви приканват да предоставите данни за Вашата парола, потребителско име, номер на сметка, банкови карти и др.
- Райфайзенбанк не разменя този тип информация по електронна поща.
- Райфайзенбанк не изпраща по електронна поща съобщения, съдържащи връзки към уеб страници на Банката.
- Райфайзенбанк не изпраща по електронна поща съобщения, които Ви приканват да се обадите на посочен в съобщението телефон, за размяна на информация свързана с акаунта Ви в Райфайзен ОНЛАЙН.
- 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 Контактния център

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