Инструкции за сигурност при използване на Райфайзен ОНЛАЙН

Настоящият документ описва правилата за сигурност при работа с Райфайзен ОНЛАЙН, които следва да се прилагат при използване системата за интернет банкиране на Райфайзенбанк. Спазването им ще ви осигури и сигурност при разплащане с карти в интернет пространството.

Достъп до сайта за интернет банкиране Райфайзен ОНЛАЙН

Не използвайте общодостъпни компютри (интернет зали, библиотеки и т.н.) за достъп до Райфайзен ОНЛАЙН.

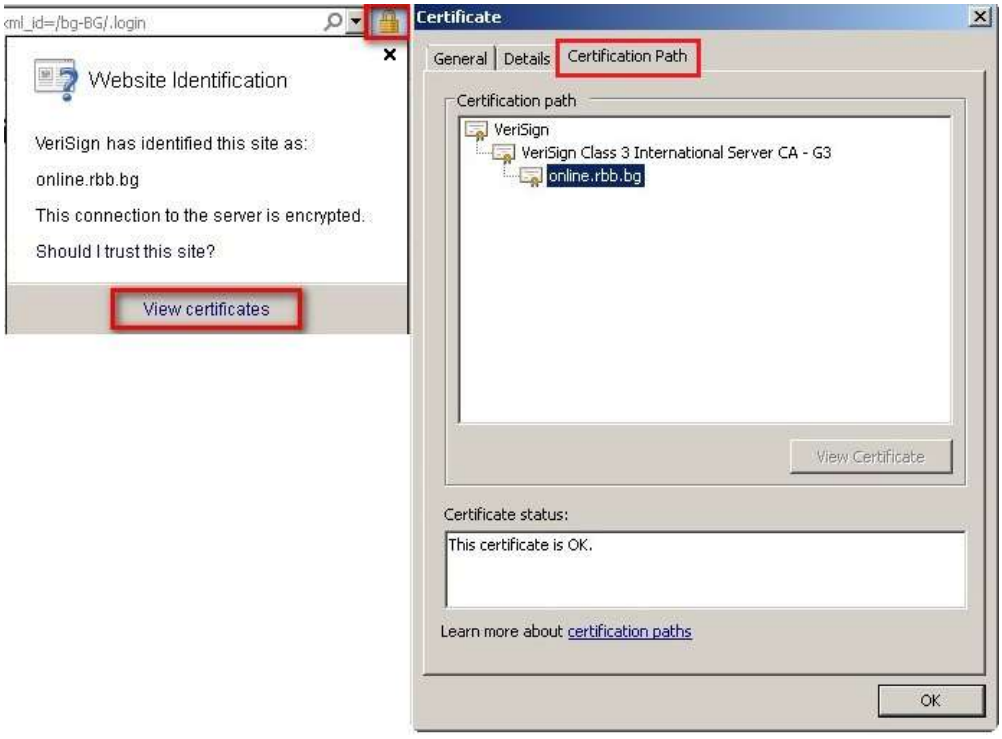
Ако използвате безжична мрежа (Wi-Fi), уверете се, че е криптирана. Свързването Ви към общодостъпни и отворени мрежи могат да осигурят достъп на злонамерени лица до въведената от Вас информация в интернет, в т.ч. потребителско име и парола.

Достъпвайте Райфайзен ОНЛАЙН директно през адреса https://online.rbb.bg или от официалния сайт на Райфайзенбанк http://www.rbb.bg.

Винаги проверявайте дали уеб страницата, която отваряте за да получите достъп до Райфайзен ОНЛАЙН е автентична и комуникацията с нея е подсигурена.

След зареждането му направете проверка на сесията от Вашия браузър преди да въведете потребителското име и парола.

- Кликнете на жълтия катинар в лентата с адреса
- Изберете опцията "View certificates"
- Изберете таб „Certification Path"
- Проверете статуса дали се изписва „This certificate is OK."
- Проверете дали "Certification Path" съдържа VeriSign Class 3 Primary CA "VeriSign Class 3 Secure Server CA - G3" online.rbb.bg



Винаги след като приключите да банкирате с Райфайзен ОНЛАЙН, използвайте бутона „Изход“ и затворете браузъра.

Интернет браузъри

Никога не запаметявайте Вашето потребителско име и/или парола за достъп до Райфайзен ОНЛАЙН във Вашия браузър.

Не включвайте сайта на Райфайзен ОНЛАЙН в предпочитаните връзки (Bookmarks, Favorites) на Вашия браузър, тъй като съществува риск от манипулиране на записаните по този начин връзки от неоторизирани лица (хакери).

За достъп до Райфайзен ОНЛАЙН използвайте интернет браузър, който поддържа 128 битово криптиране – актуални версии на Internet Explorer, Mozilla Firefox, Safari, Opera, Google Chrome.

Активирайте автоматично обновяване и Phishing филтрите на браузъра, който използвате.

Не инсталирайте допълнителни ленти с инструменти (toolbars – ASK toolbar, Yahoo 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.

Сменяйте редовно паролата си (минимум веднъж на два месеца). Не използвайте една и съща парола за достъп до различни акаунти за интернет банкиране, имейли 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 банката.

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 хардуерно устройство (token).

Парола MTAN чрез SMS съобщение – SMS съобщението съдържа освен еднократна парола за потвърждение на транзакции, така и детайли за тях. . При използване на това средство за сигурност

потребителят ще получи информация, ако злонамерен извършител се опита да потвърди активна операция.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.

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 гърба на токена.

Не оставяйте отворен прозореца на браузъра след изход от банкирането.

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. 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.

Операционните системи и повечето от програмните продукти могат да бъдат конфигурирани да се обновяват автоматично. Ако такава опция съществува, активирайте я.

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 „дупки" 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 известни 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 неизвестен производител. 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..

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 специализирани апликации

Интернет банкирането на Райфайзенбанк – Райфайзен ОНЛАЙН 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.

Райфайзенбанк разпространява апликациите за смарт устройствата само чрез официалните маркети - използвайте за инсталиране на приложенията Google Play (за Android) и iTunes (за iOS).

Достъпът до Райфайзен ОНЛАЙН се извършва със същите потребителско име и парола както и за стандартното интернет банкиране. За допълнителна сигурност приложенията не запаметяват Вашите потребителско име и парола за достъп.

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.

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. 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. 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 предоставят допълнителни добавки (add-ons), които предоставят възможност за филтриране на подобни фишинг измами.

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 все пак смятате, че дадено съобщение е истинско, не отговаряйте на мейла и не кликайте на хипервръзката в него, а отидете директно на корпоративния сайт.

В случай на фишинг (phishing) атака, насочени към Вас или при съмнения за такава атака, молим да ни уведомите своевременно на е-мейл адрес phishing.report@rbb.bg

При възникнали въпроси и съмнения за злоупотреби – връзка с Райфайзен Директ

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