к Правилам дистанционного банковского обслуживания
с использованием системы Интернет-Банк для физических лиц
в КБ «РТБК» (ООО)

ПАМЯТКА ПО БЕЗОПАСНОСТИ

1. Общие положения

1.1 Использование средств для дистанционного банковского обслуживания (банковские карты, интернет-банкинг и т.п.) всегда связано с повышенными рисками. Для того, чтобы работа в Системе Интернет-Банк была удобной и защищенной, ознакомьтесь с рекомендациями по безопасности до начала работы.

1.2 Распечатайте для себя памятку по безопасности, чтобы иметь ее под рукой.

1.3 Для обеспечения безопасности проводимых операций в Системе Интернет-банк используются следующие средства защиты:

1.3.1 Защищенное соединение (SSL-шифрование)

Соединение и работа с Системой Интернет-банк осуществляется через общедоступную сеть Интернет, поэтому для защиты канала, по которому компьютер пользователя соединяется с сервером, используется защищенный режим SSL.

Признаком установки защищенного соединения является то, что адрес Интернет-банка начинается с https:// (обязательно символ s), а в браузере появляется изображение замка (справа или слева от адресной строки, либо справа вверху/внизу браузера).

Кликнув по замку, можно убедиться в подлинности сертификата.

1.3.2 Одноразовые пароли для проведения операций.

Разовый пароль используется для проведения платежных операций в Системе Интернет-банк. Для получения одноразового пароля необходим мобильный телефон, номер которого был указан Вами при подключении услуги Интернет-банк.

После ввода всех необходимых платежных данных, система предложит ввести разовый пароль для совершения операции. Для получения Разового пароля нужно нажать на кнопку «получить пароль» пароль будет доставлен в SMS-сообщении на Ваш мобильный телефон (порядок получения Разового пароля подробно изложен в Руководстве пользователя).

Текст SMS-сообщения, которое содержит Разовый пароль, также содержит краткую информацию о реквизитах платежа.

2. Требования по обеспечению мер безопасности при использовании системы дистанционного банковского обслуживания Интернет-Банк

2.1. Обновляйте операционную систему и другие программы на Вашем компьютере.

2.2. Используйте лицензионную операционную систему.

2.3. Своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемые компанией-производителем. Копируйте обновления только с официальных сайтов компаний-производителей.

2.4. Используйте дополнительные средства безопасности.

2.5. Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»-рассылок и пр.

2.6. Установите и обновляйте антивирус на Вашем компьютере. Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Используйте современное, лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.

2.7. Установите парольную защиту на вход в АРМ.

2.8. Регулярно проводите смену Паролей.

2.9. При установке Пароля рекомендуется придерживаться следующих правил:

2.9.1. Длина Пароля – не менее 8 символов.

2.9.2. Пароль не должен совпадать ни с одним из последних трех Паролей, ранее использованных Клиентом.

2.9.3. В Пароле должны присутствовать символы из разных регистров (большие и маленькие буквы) и цифры. Для предотвращения возможных осложнений, связанных с различной кодировкой, рекомендуется использовать «латиницу».

2.9.4. Пароль не должен целиком состоять из комбинации символов, несущей смысловую нагрузку. Не рекомендуется использовать имена, названия, общепринятые аббревиатуры, адреса или другие общеизвестные слова и их сочетания, в том числе русское слово, набранное в латинской транскрипции (например: ФАМИЛИЯ - AFVBKBZ);

2.10. Если у Вас есть подозрение, что Ваши Логин и Пароль украдены или стали известны третьим лицам, как можно быстрее смените Ваш пароль в Интернет-банке или заблокируйте доступ в Интернет-банк по телефону +7(495)787-58-70.

2.11. Для входа в систему Интернет-банк нужен только Логин и Пароль. В Интернет-банке не должно быть никаких дополнительных полей для ввода такой информации, как Разовый пароль, номер Вашей карты и другие реквизиты (CVV/CVC код, срок действия карты, имя владельца). Если появились такие поля – сообщите об этом по телефонам, указанным выше, либо по телефону Банка, указанному на Вашей карте.

2.12. Никому не сообщайте Ваш пароль и одноразовый секретный пароль.

2.13. Пароли в Интернет-банк (на вход и на подтверждение операции) – это Ваша личная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте никому свои пароли, включая сотрудников Банка. Сотрудники Банка никогда не просят сообщить или ввести куда-либо конфиденциальную информацию (Пароль или Разовый пароль по SMS).

2.14. Не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других электронных носителях информации, потому что это может привести к его краже и компрометации.

2.15. Проверяйте адрес Интернет-банка, он должен быть https://elf.faktura.ru/app/?site=rtbk. Наш Интернет-банк всегда доступен только по адресу https://elf.faktura.ru/app/?site=rtbk. Вас могут пытаться обмануть, предлагая оставить Ваши Пароль и Логин на поддельном сайте. Если Вы обнаружите такой сайт, обязательно сообщите об этом по телефонам, указанным выше!

2.16. Разовый пароль по SMS действует только на подтверждение платежа. Отменить операцию в Интернет-банке невозможно! Никто никогда не попросит у Вас ввести одноразовый пароль для отмены операции.

2.17. Внимательно проверяйте параметры операции в SMS-сообщении, содержащем Разовый пароль. Информация в нем должна совпадать с Вашей операцией в Интернет-банке, которую Вы хотите подтвердить. Если эта информация не совпадает, не вводите Разовый пароль и сообщите об этом по телефонам, указанным выше!

2.18. Используйте для звонков в Банк номера телефонов, указанные на Вашей карте либо в данной памятке. Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть недоступны или по ним ответит оператор, который будет пытаться Вас обмануть. В случае подозрения на мошенничество звоните в Банк только по номерам, указанным на Вашей карте либо в службу поддержки Интернет-банка по телефонам, указанным в этой памятке!

2.19. Проверяйте, используется ли защищенное соединение – https://elf.faktura.ru/app/?site=rtbk . Проверяйте, действительно ли соединение происходит в защищенном режиме SSL – справа или слева от адресной строки, либо справа вверху/внизу браузера должен быть изображен значок закрытого замка.

2.20. Корректно завершайте работу в Интернет-банке Завершение работы с системой выполняйте путем выбора соответствующего пункта меню «ВЫЙТИ» - это удалит из браузера информацию о параметрах работы в Интернет-банке.

2.21. Защитите свой мобильный телефон. Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения с подтверждающим Разовым паролем, приложения, полученные от неизвестных вам источников. Помните, что банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email – сообщения.

2.22. При утрате мобильного телефона, на который Банк отправляет SMS-сообщения с подтверждающим Разовым паролем, Вам следует незамедлительно обратиться в офис Банка или по телефону +7(495) 787-58-70 для временной блокировки доступа к Системе Интернет-Банк (до восстановления SIM-карты) или изменения номера мобильного телефона (при личном обращение Клиента в офис Банка).

2.23. Не заходите в Интернет-банк с того же мобильного телефона, устройства, на которое приходят SMS-сообщения с подтверждающим Разовым паролем.

2.24. Если Вам пришло SMS с Разовым паролем для подтверждения операции, которую Вы не совершали, скорее всего, ваш компьютер заражен вирусом. Не используйте этот Разовый пароль, даже если Вам позвонил человек, представившийся сотрудником банка, и попросил сделать это.

- Установите или обновите антивирус. Выполните полную проверку компьютера на вирусы.

- Проверьте SSL-сертификат при доступе к Интернет-банку (сделать это можно нажав на иконку замка в Вашем браузере). Сертификат должен быть действительным для www.fakrura.ru (поле «Кому выдан).

- Заходите в Интернет-банк с этого компьютера только после того, как Вы выполнили все рекомендации, перечисленные выше.

- О факте такого SMS обязательно сообщите по телефону+7(495)787-58-70

2.25. Если у Вас есть подозрение на мошенничество, например, если Вы получили подозрительное письмо или sms-сообщение, необходимо обратиться в службу поддержки по телефону +7(495) 787-58-70

2.26. Если есть подозрения, что Ваши Логин и Пароль стали известны кому-либо, обязательно смените пароль самостоятельно на незараженном компьютере.