Приложение №2 к Приказу
от 29.03.2018 №96/1

Рекомендации по обеспечению безопасной работы в системе дистанционного банковского обслуживания «РУСНАРБАНК-Онлайн»

Уважаемые клиенты, до начала работы в системе дистанционного банковского обслуживания «РУСНАРБАНК-Онлайн» просим Вас ознакомиться с нижеуказанными рекомендациями по безопасности.

Распечатайте для себя эти рекомендации, чтобы в любой момент иметь их под рукой.

Для обеспечения безопасности проводимых операций в системе «РУСНАРБАНК-Онлайн» используются следующие средства защиты:

Защищенное соединение (SSL-шифрование)

Соединение и работа с системой «РУСНАРБАНК-Онлайн» осуществляется через Интернет, поэтому для защиты канала, по которому компьютер клиента соединяется с сервером, используется защищенный режим SSL. Признаком установки защищенного соединения является то, что адрес для входа в систему «РУСНАРБАНК-Онлайн» 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.

SMS-коды для проведения операций

SMS-код используется для подтверждения операций в системе «РУСНАРБАНК-Онлайн». Для получения SMS-кода необходим мобильный телефон, номер которого был указан Вами при подключении системы «РУСНАРБАНК-Онлайн». Код будет доставлен в SMS-сообщении (или PUSH-сообщении) на Ваш мобильный телефон, и будет содержать также краткую информацию о реквизитах подготовленного документа.

Минимальные меры безопасности, которые необходимо соблюдать при работе в системе «РУСНАРБАНК-Онлайн»:

Обновляйте операционную систему и другие программы на вашем компьютере

Используйте лицензионную операционную систему. Своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемые компанией-производителем. Устанавливайте обновления только с официальных сайтов (репозиториев) компаний-производителей.

Используйте дополнительные средства безопасности

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

Установите и обновляйте антивирус на Вашем компьютере, в целях защиты от вредоносного кода

Вирусные программы могут запоминать и отсылать 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.

Если у Вас есть подозрение, что Ваши учетные данные (логин/пароль) для входа в систему «РУСНАРБАНК-Онлайн» украдены или скомпрометированы, как можно быстрее смените Ваш логин/пароль для доступа в систему «РУСНАРБАНК-Онлайн» или обратитесь в Банк и выполните блокировку доступа в систему.

Помните, что для входа в систему «РУСНАРБАНК-Онлайн» нужны только логин и пароль, а также SMS-код, полученный в SMS-сообщении или PUSH-сообщении

На странице входа в систему «РУСНАРБАНК-Онлайн» не должно быть никаких дополнительных полей для ввода такой информации, как номер Вашей карты и/или другие ее реквизиты (CVV2 код, срок действия карты, имя владельца). Если у Вас на экране появились такие поля – срочно сообщите об этом в Банк.

Никому не сообщайте Ваши логин/пароль, значения SMS-кодов

Логин и пароль – 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.

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

При каждом входе в систему проверяйте адрес сайта системы «РУСНАРБАНК-Онлайн»

Система «РУСНАРБАНК-Онлайн» доступна только по адресу: https://online.rusnarbank.ru . Вас могут пытаться обмануть, предлагая оставить Ваши логин, пароль, SMS-код или код, полученный в PUSH-сообщении, на поддельном сайте (например, http://online.rusnarbank.com.org). Если Вы обнаружите подобный сайт, обязательно сообщите об этом в Банк!

Внимательно проверяйте сумму и реквизиты операции в SMS-сообщении или PUSH-сообщении, содержащем SMS-код

Информация в нем должна совпадать с данными совершаемой Вами операции в системе «РУСНАРБАНК-Онлайн», которую вы хотите подтвердить. Если эта информация не совпадает, не вводите SMS-код и сообщите об этом в Банк!

Используйте для звонков в Банк только номера телефонов, указанные на официальном сайте Банка https://www.rusnarbank.ru

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 сообщите об этом в Банк только по номерам, указанным на официальном сайте Банка!

Проверяйте, используется ли защищенное соединение – https://online.rusnarbank.ru

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.

Корректно завершайте работу в системе «РУСНАРБАНК-Онлайн»

Завершение работы с системой выполняйте путем выбора соответствующего пункта меню - это удалит из браузера информацию о параметрах работы в системе «РУСНАРБАНК-Онлайн».

Защитите свой мобильный телефон

Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения или PUSH-сообщения с кодом, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email - сообщения.

При утрате мобильного телефона, на который Банк отправляет SMS-сообщения или PUSH-сообщения с кодом подтверждения, Вам следует, незамедлительно обратиться к своему оператору сотовой связи и заблокировать телефонную SIM-карту.

При наличии возможности, не заходите в интерфейс «РУСНАРБАНК-Онлайн» с того же мобильного телефона, на который приходят SMS-сообщения или PUSH-сообщения с кодом.

Что делать, если вам пришло SMS или PUSH на подтверждение операции, которую вы не совершали:

Вам следует незамедлительно обратиться в Банк для блокировки учетной записи в системе «РУСНАРБАНК-Онлайн». Не используйте этот SMS-код, 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 интерфейсу системы «РУСНАРБАНК-Онлайн».

О факте такого SMS или PUSH незамедлительно сообщите в Банк.

Что делать, если есть подозрение на мошенничество:

Если Вы получили подозрительное письмо или SMS-сообщение, необходимо обратиться в Банк и сообщить о данном факте.

Если есть подозрения, что Ваши логин и пароль стали известны кому-либо, обязательно смените пароль самостоятельно на незараженном компьютере или получите новый пароль в Банке.