Приложение 1 к приказу
от «13» марта 2020 г. № 126-од/1

РЕКОМЕНДАЦИИ

по обеспечению необходимого уровня безопасности при работе в системе дистанционного банковского обслуживания «СНГБ Онлайн» Акционерного общества «Сургутнефтегазбанк»

г. Сургут

СОДЕРЖАНИЕ

Статья 1. ОБЩИЕ ПОЛОЖЕНИЯ

АО БАНК «СНГБ» (далее – Банк) использует современные механизмы безопасности системы дистанционного банковского обслуживания посредством системы «СНГБ-Онлайн» (далее – система ДБО), обеспечивая при этом высокий уровень ее надежности. Вместе с тем, наибольшая эффективность данных механизмов зависит также от соблюдения клиентом разработанных Банком Рекомендаций по обеспечению необходимого уровня безопасности при работе в системе дистанционного банковского обслуживания «СНГБ Онлайн» Акционерного общества «Сургутнефтегазбанк» (далее - Рекомендации).

Придерживаясь Рекомендаций, клиент минимизирует свои риски. Вместе с тем, даже надлежащее соблюдение Рекомендаций не гарантирует абсолютную безопасность системы ДБО от действий злоумышленников, в том числе по причине того, что каналы передачи информации через интернет, используемые при получении услуг посредством системы ДБО, не всегда являются безопасными.

Клиенту следует руководствоваться нижеследующими рекомендациями.

Статья 2. ПРИЛОЖЕНИЕ ДЛЯ РАБОТЫ В СИСТЕМЕ ДБО

Приложение к устройству, с которого планируется работа в системе ДБО (далее - Устройство).

Перед работой в системе ДБО на Устройство необходимо установить соответствующее приложение.

К атрибутам, подтверждающим то, что приложение размещено именно Банком, относятся следующие:

- приложение распространяется бесплатно;
- приложение размещено только в официальных репозиториях производителей мобильных платформ: App Store и Google Play (информация об актуальных версиях публикуется на сайте Банка в сети интернет по адресу: www.sngb.ru, в разделе «СНГБ-Онлайн»);
- авторами приложения указаны АО БАНК «СНГБ», либо Qulix Systems (разработчик Приложения, официальный сайт: http://www.qulix.ru);
- каждая версия приложения оснащается специальным электронным сертификатом, который можно проверить.

В случае если клиент обнаружил ложное приложение, имитирующее программный интерфейс официального приложения Банка, необходимо немедленно прекратить работу в системе ДБО и закрыть используемое приложение, а также сообщить в Банк по телефонам: 8 (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04.

Статья 3. УСТРОЙСТВО И ПОРЯДОК РАБОТЫ С НИМ

На Устройство необходимо установить лицензионное и легальное антивирусное обеспечение, а также своевременно обновлять антивирусные базы и периодически осуществлять полное антивирусное сканирование операционной системы Устройства. (Для платформы Android рекомендуются бесплатные приложения: Dr.Web Light и Kaspersky Mobile Antivirus: AppLock & Web Security (доступны для загрузки из Google Play). Для персонального компьютера: Kaspersky, Dr.Web, Symantec, Avira, ESET NOD 32, McAfee и др.).

Запрещено взламывать операционную систему Устройства (например, через Jailbreaking, реинжиниринг, принудительное получение root-прав), так как это отключает защитные механизмы, заложенные производителем соответствующей платформы. В результате Устройство становится уязвимым к заражению вирусным ПО.

Запрещено отключать и взламывать встроенные механизмы безопасности Устройства.

Необходимо использовать только актуальные версии браузеров, полученные с официальных сайтов производителя, без плагинов сторонних разработчиков.

Запрещено устанавливать и запускать в Устройстве сомнительные программные приложения, в подлинности которых Вы не можете убедиться.

При наличии технической возможности необходимо включить шифрование данных на Устройстве.

Необходимо установить парольную защиту на Устройстве.

Запрещено оставлять Устройство в разблокированном состоянии без присмотра.

Запрещено передавать Устройство с установленной системой ДБО в пользование другим лицам.

В случае работы в системе ДБО с Устройства, с которого осуществляется доступ в социальные сети и/или работа с электронной почтой, необходимо проявлять осторожность при открытии сообщений от неизвестных отправителей и не переходить по неизвестным web-ссылкам.

Запрещено использовать функцию браузеров по сохранению паролей к сайту.

Не рекомендуется использовать на Устройстве программное обеспечение для удаленного администрирования (например, TeamViewer, Radmin, Ammyy Admin и др.)».

Внимание!!!

Необходимо избегать работы в системе ДБО с использованием «недоверенных» Устройств, таких как компьютеры в интернет-кафе или другие общедоступные устройства, «чужие» устройства, временно используемые вами и т.п.

Недопустима работа с системой ДБО из публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользуйтесь «мобильным интернетом». В вышеописанных случаях существенно повышается риск кражи Ваших конфиденциальных данных и, как следствие, денежных средств.

Запрещено оставлять без присмотра Устройство, с использованием которого осуществляется работа в системе ДБО, с активной сессией работы в системе ДБО.

Завершать работу в системе ДБО необходимо через завершение сессии (кнопка (Выход).

В случае осуществления работы в системе ДБО с использованием iPhone, желательно отключить возможность использовать голосовое управление Siri на заблокированном экране.

Помните!!!

Банк не рассылает своим клиентам ссылки или указания на установку приложений через sms/mms/e-mail сообщения.

Статья 4. ИНТЕРНЕТ - АДРЕС СИСТЕМЫ ДБО

До ввода логина и пароля на странице входа в систему ДБО (страница авторизации) необходимо проверить адрес первоначальной страницы авторизации системы ДБО, он должен быть таким: **https://online.sngb.ru.**

Другие адреса, например, **https://online-sngb.ru** или **http://onlinesngb.ru** (возможны варианты), а также адреса, содержащие кириллические символы, например, снгб-онлайн.рф, **являются ложными** и свидетельствуют о наличии мошеннических действий.

Без внимательной проверки адреса страницы системы ДБО отличия от верного адреса страницы системы ДБО трудно заметить ввиду его возможной схожести с адресом ложной страницы системы ДБО.

Внешний вид ложной страницы системы ДБО может ничем не отличаться от оригинальной страницы системы ДБО, за исключением адреса.

В случае, если клиент обнаружил, что адрес страницы системы ДБО не соответствует оригинальному адресу страницы системы ДБО (т.е. https://online.sngb.ru), необходимо немедленно прекратить работу в системе ДБО, закрыть используемый интернет-браузер и

сообщить о данном факте в Банк по телефонам: 8 (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04.

Внимание!!!

Ссылка на подлинный сайт системы ДБО всегда находится на основной странице сайта Банка в сети интернет по адресу: www.sngb.ru.

Статья 5. ПРОВЕРКА БЕЗОПАСНОСТИ СОЕДИНЕНИЯ

После осуществления проверки адреса первоначальной страницы системы ДБО по адресу https://online.sngb.ru, перед вводом логина и пароля необходимо убедиться в безопасности соединения.

Для этого необходимо нажать на значок. В отобразившемся окне необходимо выбрать строку «Просмотр сертификатов». Поле «Кому выдан» обязательно должно содержать сведения о принадлежности сертификата АО БАНК «СНГБ» - online.sngb.ru.

Срок действия этого сертификата должен быть действительным на дату текущего входа в систему ДБО.

Рекомендуем осуществлять указанную проверку не только при входе в систему ДБО, но и при выполнении операций, прежде чем ввести Код подтверждения.

Статья 6. ПАРОЛЬ К СИСТЕМЕ ДБО

Для работы с системой ДБО необходимо использовать только сложные пароли.

Пароль должен соответствовать следующим обязательным критериям:

- длина пароля должна быть не менее 8 символов;
- в пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) символы, цифры, а также специальные символы (например, #, %, ^, * и т.п.); примеры паролей (hjf#48Dft, 5$ma(fQ5er, %dER*2fvw2);
- в качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие связанные с Вами данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
- в качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;
- пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля;
- при смене пароля новый пароль не должен совпадать с ранее используемыми паролями.

Статья 7. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

Сохраняйте в тайне информацию о логине и пароле к системе ДБО. Не сообщайте информацию о логине и пароле к системе ДБО даже сотрудникам Банка.

Помните!!!

Работники Банка никогда не будут спрашивать информацию о логине и пароле к системе ДБО. Если Вам позвонили, представились сотрудником Банка и в ходе дальнейшего разговора попросили сообщить информацию о логине и пароле, прекратите разговор и сообщите о случившемся в Банк.

В случае, если у Вас возникли подозрения в доступности данной информации третьим лицам, необходимо как можно быстрее изменить данные логина и пароля или заблокировать доступ к системе ДБО, позвонив в Банк по телефонам: 8 (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04.

Не передавайте Ваше Устройство в пользование третьим лицам, чтобы исключить возможность изменения настроек Вашего мобильного устройства или приложения.

Не вводите данные логина и пароля на Устройствах третьих лиц.

Не регистрируйте и не сохраняйте на Вашем Устройстве логины и пароли, принадлежащие третьим лицам.

Никогда не сообщайте свой пароль третьим лицам, в том числе родственникам и сотрудникам Банка, вводите пароль только при работе в системе ДБО. Помните, что сотрудник Банка не имеет права запрашивать у Вас пароль, даже если Вы самостоятельно обратились в Банк. Вводите пароль только в системе ДБО, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.

Запрещается хранение на Устройстве (в напоминаниях, SMS и т.п.) логина и пароля для входа в систему ДБО. В случае хищения Устройства или его заражения вирусом злоумышленники могут получить доступ к этой информации.

При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в систему ДБО в порядке, предусмотренном соответствующим руководством пользователя системой ДБО.

Внимание!!!

Если Вы получили SMS-сообщение или PUSH-сообщения с кодом подтверждения для входа в систему ДБО (с информацией о введении неверного пароля при входе в систему ДБО) или SMS-сообщения для совершения расчетной операции, но в этот момент времени не осуществляете работу в системе ДБО, немедленно примите меры по блокированию доступа к системе ДБО, позвонив в Банк по телефонам: 8 (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04.

Если Вы получили SMS-сообщение или PUSH-сообщение от неизвестного Вам абонента, содержащее информацию о блокировании/неисправности банковской карты, о списании/зачислении средств с картсчета, о блокировании/неисправности системы ДБО, другую информацию с просьбой перезвонить по указанному номеру телефона и/или сообщить какие-либо сведения – это действия мошенников. НЕ ВЫПОЛНЯЙТЕ данные указания!

Обязательно проверяйте любую информацию относительно Ваших счетов и получаемых Вами услуг в Банке, поступившую от неизвестных лиц.

Если Вам поступил звонок от, якобы, сотрудника Банка, который сообщает о подозрительной операции с Вашим Счетом (при этом не запрашивая никакой конфиденциальной информации) и который предлагает проверить Устройства, с которых Вами осуществлялся вход в систему ДБО, знайте - это действия мошенников. НЕ ВЫПОЛНЯЙТЕ данные указания!

Для того, чтобы «обезопасить» себя Вас попросят установить на Ваше Устройство стороннее приложение (например: Teamviewer), якобы, для дистанционного завершения работы других, не используемых Вами Устройств, с которых осуществлялся вход в систему ДБО.

Для подключения к Вашему Устройству мошенники попросят Вас сообщить им ID (специальный номер) пользователя, с помощью которого они получают полный контроль над Вашим Устройством.

Помните, что сотрудники Банка НИКОГДА не попросят установить на Ваше Устройство сторонние приложения.

Также будьте крайне внимательны, т.к. мошенники используют технологию подмены номера, т.е. Вам могут звонить с номера Банка, но это будет не Банк. Если Вы подозреваете, что Вам позвонил мошенник, положите трубку и перезвоните сами в Банк, по номерам, которые указаны на Вашей карте.

Если Вы заметили, что Вам приходят SMS/ PUSH-сообщения об операциях, которые Вы не совершали срочно обратитесь в Банк!

О подозрительных действиях сообщайте по телефонам 8 (3462) 39-88-04, 8-800-775-88-04 или 8-800-200-88-04.

Внимание!!! Номер телефона, используемый АО БАНК «СНГБ» для рассылки SMS-сообщений: SNGB.