МОРСКОЙ БАНК

РЕКОМЕНДАЦИИ

для клиентов по информационной безопасности при работе с системой дистанционного банковского обслуживания МОРСКОГО БАНКА (АО)

2019 г.

МОРСКОЙ БАНК

1. БЕЗОПАСНОСТЬ СЕРВИСА

1.1. Система дистанционного банковского обслуживания «Клиент-Банк» и «Интернет-Банк» (далее - ДБО) МОРСКОГО БАНКА (АО) (далее – Банк) реализована с использованием надежных механизмов безопасности. Для обеспечения безопасной работы в ДБО используются, в частности, следующие средства:

- защищенный канал соединения с Банком, позволяющий клиенту удостоверяться в том, что он работает именно с Банком;
- идентификация клиента посредством указания логина для входа в систему;
- авторизация клиента посредством указания пароля для входа в систему;
- авторизация клиента посредством ввода одноразового сеансового пароля;
- средства криптографической защиты информации (криптографические ключи) для подтверждения авторства, обеспечения неизменности и конфиденциальности направляемых в Банк распоряжений клиента (для юридических лиц);
- информация о посещении системы, позволяющая клиенту обнаружить факт использования системы без его ведома;
- функционал по информированию клиента о проведенных от его имени операциях в системе посредством SMS-сообщений.

1.2. Однако, несмотря на применяемые в ДБО защитные механизмы, использование ДБО влечет за собой риск несанкционированного списания денежных средств. Существенным условием для минимизации данного риска и обеспечения безопасной работы клиента в ДБО является соблюдение клиентом определенных правил и рекомендаций Банка, представленных в данных Рекомендациях.

2. ОРГАНИЗАЦИЯ РАБОЧЕГО МЕСТА

2.1. Для работы в системе ДБО используйте отдельный выделенный компьютер, для доступа в Интернет-банк отдельное выделенное мобильное устройство.

2.2. На компьютере с установленной системой ДБО исключите, либо минимизируйте работу в сети Интернет (особенно с такими сайтами как социальные сети, форумы, игры, файлообменники, сайты с нелегальным и подозрительным содержимым (программы, музыка, видео, книги, порнография и пр.)). Исключите работу с электронной почтой, минимизируйте установку программ, включайте компьютер только на время сеанса с системой ДБО, в остальное время компьютер должен быть выключен.

2.3. Обязательно используйте антивирусное программное обеспечение (антивирусы) и регулярно обновляйте антивирусные базы. Компьютерные вирусы могут быть направлены на предоставление злоумышленнику дистанционного доступа к компьютеру пользователя, либо осуществлять сбор информации (идентификаторы, пароли, ключи, наличие систем ДБО, бухгалтерских программ, посещаемые сайты и пр.).

2.4. Используйте программное обеспечение для борьбы с вредоносными программами (malware, spyware). Вредоносные программы могут быть направлены на сбор

конфиденциальной информации на компьютере пользователя (персональные данные, банковская тайна). Антивирусы зачастую не способны выявить такие вредоносные программы.

2.5. Используйте только лицензионное программное обеспечение, официально приобретенное (полученное) у поставщиков (разработчиков) данного программного обеспечения. Это относится к операционной системе, к антивирусам и прочему программному обеспечению, используемому на компьютере. В официально приобретенном (полученном) программном обеспечении гарантируется отсутствие специально внедренных злоумышленником вредоносных недокументированных возможностей, а также осуществляется своевременное устранение разработчиком найденных уязвимостей и несоответствий.

2.6. В операционной системе, а также в другом программном обеспечении, используемых на компьютере, должна быть активирована функция (в случае ее наличия) автоматического получения обновлений от разработчика. Это позволит устранять обнаруженные уязвимости и несоответствия в данных программах до того момента, когда этими уязвимостями сможет воспользоваться злоумышленник.

2.7. Используйте межсетевой экран (firewall) с соответствующими настройками, исключающими доступ на компьютер по сети. Возможно использование как аппаратных межсетевых экранов, так и программных.

2.8. Не используйте удаленное управление и удаленный доступ к компьютеру. Отключите возможность доступа к компьютеру через удаленный рабочий стол, не используйте и не устанавливайте программы для удаленного доступа аналогичные Radmin, TeamViewer, AmmyAdmin и т.п.

2.9. Для работы в ДБО используйте WEB-браузер «Windows Internet Explorer» версии не ниже 11. Использование других WEB-браузеров может вызвать проблемы совместимости и безопасности.

2.10. Отключите в WEB-браузере сохранение форм, а также имен пользователей и паролей в формах. Для этого в WEB-браузере «Windows Internet Explorer» нужно снять соответствующие отметки в меню «Сервис» (Tools) -> «Свойства обозревателя» (Internet Options) -> «Содержание» (Content) -> «Автозаполнение» (AutoComplete).

3. ПРАВИЛА БЕЗОПАСНОСТИ

3.1. Ключевые носители информации, логины и пароли необходимо хранить в недоступном для посторонних лиц месте. В случае подозрения на доступ к ним посторонних лиц незамедлительно сообщить об этом в Банк по тел. +7(495)777-1177 с целью их блокирования.

3.2. Подключайте ключевые носители к компьютеру непосредственно перед их использованием. Сразу после окончания их использования необходимо отсоединить их от компьютера и хранить в недоступном для посторонних лиц месте. Если оставить ключевые носители в компьютере, то получивший доступ к компьютеру злоумышленник сможет беспрепятственно воспользоваться ими.

3.3. Используйте надежные пароли для доступа. Надежный пароль должен содержать в себе цифры, заглавные и прописные буквы, а также желательно специальные символы. Длина пароля должна быть не меньше 8 знаков. Пароль не должен

представлять собой связанную с Вами информацию, имена, телефоны, даты рождения, клички домашних животных, а также не должен состоять из простой последовательности типа 12345678, qwertyui, 1234qwer и т.п.

3.4. Не используйте одинаковые пароли для работы в ДБО и на других ресурсах, таких, как электронная почта, регистрация в социальных сетях, интернет-магазинах, форумах и т.п.

3.5. Никому не сообщайте и не передавайте логины, пароли, ключевые носители для работы с системой ДБО. Любой человек, который будет знать эту информацию, сможет получить доступ к вашему счету в Банке.

3.6. Не записывайте и не храните логины и пароли в местах, где с ними могут ознакомиться посторонние лица.

3.7. При вводе логина и пароля используйте безопасную авторизацию посредством экранной клавиатуры (при наличии такой возможности). Это снизит вероятность перехвата пароля злоумышленником при помощи специальных программ и устройств.

3.8. Выключайте компьютер после завершения работы в ДБО и при отсутствии необходимости работы в ней. Не оставляйте компьютер с включенной системой ДБО.

3.9. Всегда завершайте работу в ДБО нажатием на кнопку «Выйти из системы», а не просто закрывайте окно WEB-браузера. В этом случае сеанс связи будет немедленно прекращен.

3.10. Не работайте в ДБО с посторонних компьютеров (в интернет-кафе, у друзей и т.п.) и через общедоступную сеть Wi-Fi. В данных случаях безопасность работы может быть не обеспечена.

3.11. При каждом подключении к ДБО убедитесь, что осуществляется соединение с официальным WEB-сайтом Банка в защищенном режиме (SSL), согласно раздела 5 настоящего документа.

3.12. При входе в ДБО всегда обращайте внимание на дату и время предыдущего сеанса работы. Вспомните, действительно ли работали в это время.

3.13. В случае возникновения подозрения на то, что кто-то кроме Вас имел (имеет) доступ ДБО, немедленно сообщите об этом в Банк по тел. +7(495)777-1177.

3.14. Пользуйтесь услугой Банка по SMS-информированию о проводимых операциях. Это позволит оперативно узнать о появлении несанкционированной операции и приостановить ее, оперативно связавшись с Банком.

4. ПРОТИВОДЕЙСТВИЕ МОШЕННИКАМ

4.1. Всегда проверяйте в Банке поступившую к Вам (посредством электронной почты, SMS и т.п.) от неизвестных лиц подозрительную информацию касательно ДБО, банковских карт, счетов.

4.2. Банк никогда, ни при каких обстоятельствах, не запрашивает в обращениях к клиенту (посредством телефонного звонка, электронной почты, SMS и т.п.) конфиденциальную информацию, такую как пароли доступа в ДБО, одноразовые пароли, ключевую информацию, номера и PIN-коды банковских карт и т.п. Также

эту информацию не уполномочены запрашивать никакие другие службы и ведомства (служба безопасности, центральный банк, полиция, ФСБ и пр.). Если такая информация запрошена у клиента (в том числе от имени Банка), то это действия злоумышленников. Телефонные звонки мошенников могут осуществляться с использованием программы подмены номера или с номера, похожем на телефонный номер Банка. О всех случаях телефонного мошенничества просьба сообщать в банк.

4.3. Никогда не звоните по неизвестным телефонным номерам, указанным в письмах, либо SMS, даже если эти сообщения пришли якобы от имени Банка. С большой вероятностью это могут быть телефонные номера мошенников, целью которых является выведать под любым предлогом конфиденциальную информацию, или вынудить выполнить определенные действия, которые могут навредить клиенту. Связывайтесь с Банком только по официально установленным телефонным номерам Банка.

4.4. В случае появления изменений в работе ДБО (например, для входа в систему запрашивается информация, которая ранее не запрашивалась, либо наоборот не запрашивается информация, которая ранее запрашивалась и т.п.) обязательно уточните эти изменения, позвонив в Банк по тел. +7(495) 777-1177.

4.5. Для входа в ДБО, на официальном WEB-сайте Банка клиенту необходимо ввести только логин, одноразовый и/или постоянный пароль доступа. Если запрашиваются дополнительные сведения (номера телефонов, банковских карт и т.п.), то вероятнее всего Вы попали на WEB-сайт злоумышленников. Не вводя никакой информации, незамедлительно сообщите об этом в Банк.

4.6. Никогда не заходите в ДБО посредством ссылок, указанных в электронном письме или SMS. С большой вероятностью эти письма рассылаются злоумышленниками, чтобы заманить клиента на подставной WEB-сайт (внешне похожий на официальный WEB-сайт Банка) с целью получить конфиденциальную информацию клиента (пароли, номера и PIN-коды банковских карт и т.п.). Банк никогда не предлагает клиенту зайти в ДБО по ссылке в письме, либо SMS. Не переходя по такой ссылке, сообщите об этом в Банк. Банк может попросить клиента переслать данное письмо в службу безопасности Банка, с целью анализа и учета фишинговых WEB-сайтов.

4.7. Никогда не открывайте вложенные файлы в подозрительных письмах (в том числе пришедших якобы от имени Банка). Банк не рассылает клиентам письма с вложенными файлами, за исключением выписки по пластиковой карте в архиве с известным только Вам паролем. В случае получения от имени Банка писем с вложенными файлами, не запуская вложенных файлов, сообщите об этом в Банк. Банк может попросить клиента переслать такое письмо в службу безопасности Банка, с целью анализа данной ситуации.

4.8. На мобильном устройстве, предназначенным для работы с системой ДБО, либо на который приходят SMS-сообщения из Банка, устанавливайте приложения только из доверенных источников (Play Market, AppStore). Некоторые программы для мобильных телефонов (смартфонов) специально изготавливаются и распространяются злоумышленниками с целью осуществления перехвата одноразовых паролей и другой конфиденциальной информации, посылаемой Банком клиенту. Лучшим решением в данной ситуации будет использование для приема SMS-сообщений из Банка простого мобильного телефона (не смартфона), на котором отсутствуют доступ в сеть Интернет и установленные сторонние

программы. Банк не рассылает никакое программное обеспечение для мобильных телефонов и не просит клиентов ничего устанавливать на мобильный телефон.

4.9. Будьте осторожны при приглашении компьютерных специалистов из небольших неизвестных фирм (или частных незнакомых специалистов). Некоторые мошенники специально организуют мелкие компьютерные фирмы и распространяют рекламу об оказании услуг компьютерной помощи с целью получения доступа к компьютерам организаций и частных лиц, а в последующем и к их банковским счетам.

4.10. Если Вы подключены к услуге Банка по SMS-информированию и получили сообщение о произведенных от вашего имени действиях в ДБО, которых Вы на самом деле не осуществляли (например, пришло сообщение о направленном распоряжении), незамедлительно свяжитесь по этому поводу с Банком для выяснения ситуации.

4.11. Если в процессе работы в ДБО Вы видите, что в системе начали происходить самостоятельные действия (открываются окна, набирается текст, двигается мышь и т.п.) или компьютер заблокировался (перестал реагировать на команды, погас экран и т.п.) и у Вас есть подозрение на то, что это действия злоумышленников, незамедлительно обесточьте компьютер в обход штатных процедур завершения работы (выдернуть из розетки, а в мобильном компьютере вытащить аккумуляторную батарею), после чего сообщите об этом в Банк. Не производите никаких самостоятельных действий с этим компьютером, пока не получите рекомендаций от Банка.

4.12. Необходимо своевременно информировать Банк об изменении своих контактных данных, так как в целях противодействия мошенникам по несанкционированному списанию денежных средств клиента, Банк оставляет за собой право подтверждать подозрительные операции лично, связываясь с клиентом посредством предоставленной клиентом контактной информации.

5. ПРОВЕРКА ДОСТОВЕРНОСТИ ОФИЦИАЛЬНОГО WEB-САЙТА БАНКА

5.1. Для удостоверения того, что клиент работает по защищенному каналу с официальным WEB-сайтом Банка проверьте, что соединение установлено по протоколу https, а также, что сертификат WEB-сайта является действующим и выдан МОРСКОМУ БАНКУ (АО).

Для WEB-браузера «Windows Internet Explorer 11» это выглядит следующим образом:

- адресная строка WEB-браузера должна начинаться с адреса официального сайта Банка :
  - Интернет-банк: https://ib.maritimebank.com/
- справа от адресной строки WEB-браузера должен отображаться значок защищенного соединения, изображенный в виде закрытого замка;
- рядом с изображением закрытого замка, на зеленом фоне, должно присутствовать название Банка «MARITIME BANK»;
- щелкнув левой кнопкой мышки по значку замка, должна быть следующая информация:

- при нажатии на «Просмотр сертификатов» откроется окно с данными о сертификате WEB-сервера, в котором должна быть следующая информация:
  - Кому выдан: www.maritimebank.com
  - Кем выдан: Thawte RSA CA 2018
  - в окошке с данными о сертификате, на закладке «Путь сертификации» в поле «Состояние сертификата» должно быть указано, что сертификат действителен.
- В случае, если обнаружены несоответствия описанных выше реквизитов, прекратите работу в ДБО (не вводя никаких данных) и сообщите об этом в Банк.

МОРСКОЙ БАНК (АО) заботится о безопасности своих клиентов.