МБ РУС
БАНК

Памятка о мерах по обеспечению безопасности при работе в системе ДБО для физических лиц

В целях минимизации рисков и для обеспечения безопасности своих денежных средств просим Вас соблюдать следующие рекомендации:

- при использовании системы электронного дистанционного банковского обслуживания Банка (далее – системы ДБО) проверьте правильность указания доменного имени сайта Банка в строке браузера и наличие сертификата безопасности (https в адресной строке браузера и наличие значка «Замочка»), используйте только официальный сайт Банка https://www.mbrus-bank.ru.

- в случае обнаружения подозрительных сайтов, доменных имен и стилей оформления, сходных с именами и оформлением страницы сервиса ДБО Банка, а также при отсутствии возможности подключения к системе ДБО Банка, сообщите в Банк по электронной почте или по контактным телефонам, указанным на официальном сайте Банка https://www.mbrus-bank.ru.

- никому не сообщайте и не передавайте смс-коды, свой логин, пароль, коды от входа в систему интернет-банк/в мобильное приложение или для подтверждения операций в нем (одноразовые коды приходят на указанный вами номер мобильного телефона в виде смс-сообщения или push-сообщения), не вводите данные на подозрительных сайтах и в приложениях.

- для разблокировки мобильного устройства, предназначенного для работы с системой ДБО, включён максимально возможный из доступных на данном мобильном устройстве способ защиты от несанкционированного доступа к функциям устройства и хранящихся на нём данным (в порядке убывания стойкости защиты): средство распознания радужки глаза, средство распознавания отпечатка пальца или лица, пароль длиною не менее 6 символов (включая буквы и цифры), графический ключ, пин-код.

- обеспечьте защиту компьютера, с которого выполняется работа с системой ДБО: установите лицензионное антивирусное программное обеспечение и не реже одного раза в день обновляйте его, обеспечьте своевременную установку обновлений операционной системы и прикладных программ; отключите встроенные учетные записи «Администратор» и «Гость»; отключите службы «Удаленный реестр» и «Удаленное управление Windows»; работайте на компьютере с правами «Пользователь»; используйте только лицензионное программное обеспечение, полученное из доверенных источников; устанавливайте/обновляйте мобильное приложение только с официального сайта Банка или из магазинов приложений, перечень которых указан на информационных стендах в операционных залах Банка и на официальном сайте Банка, не устанавливайте и не сохраняйте подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, отключить автозапуск любых внешних носителей, не отвечайте на подозрительные письма электронной почты, смс-сообщения, иные сообщения, направленные по другим каналам связи, с просьбой выслать/сообщить/передать логин, пароль, пин-код мобильного банка и другие конфиденциальные данные.

- не храните логин, пароль, пин-код для входа в мобильное приложение (систему ДБО) непосредственно на мобильном телефоне, планшете или компьютере, на котором установлено приложение системы ДБО, а также не храните логин, пароль, пин-код на бумажных носителях, доступных другим лицам.

- регулярно, не реже одного раза в три месяца, производите смену пароля доступа в компьютер, с которого осуществляется работа в системе ДБО, пароля доступа в систему ДБО, пин-кода для входа в мобильный банк. Пароль должен отвечать следующим требованиям: длина не менее десяти символов, должен состоять из строчных и (или) заглавных букв латинского алфавита, как минимум одного специального знака и одной цифры, не должен состоять из легко подбираемых комбинаций (qwerty,

12345678, admin, password) или их вариантов (!qwerty, 12348765, @dmin, passw0rd), не должен совпадать с паролем на вход в компьютер и в личные сервисы сети Интернет, не рекомендуется использовать в паролях последовательность одинаковых символов, а также персональную информацию (например, имя, дату рождения клиента, членов его семьи, номера телефонов), имя учетной записи или другие общедоступные данные, избегайте присутствия третьих лиц при вводе логина и пароля или регистрации в мобильном приложении, включая момент формирования логина и пароля; исключите доступ к Вашему мобильного устройству со стороны третьих лиц.

- при утрате логина/пароля, при подозрении об их компрометации, при утрате мобильного устройства необходимо срочно обратиться в Банк для временной блокировки доступа к системе ДБО; при восстановлении доступа на новом мобильном устройстве проверить все действия и операции в системе ДБО за период отсутствия доступа в систему ДБО.

- если мобильное приложение установлено на устройстве, которое не используется ежедневно, то необходимо периодически проверять работоспособность SIM-карты и самого мобильного устройства. Если SIM-карта или устройство перестали работать, обратитесь в Банк для блокировки доступа в систему ДБО. Доступ в систему ДБО считается заблокированным с момента обращения в Банк. При переустановке мобильного приложения проверьте все действия и операции в системе ДБО в период неработоспособности мобильного устройства.

- не выполняйте операции по повышению привилегий или взлому операционной системы Вашего мобильного устройства (получение root-прав для Android, установка jailbreak для iOS), на котором установлено или планируется установка мобильного приложения. Не устанавливайте мобильное приложение на устройство, которое уже получило такие привилегии, исключите использование средств удаленного администрирования.

- в личном кабинете на сайте вашего сотового оператора Банка, через мобильное приложение или в офисе своего сотового оператора подключите услугу запрета обслуживания и/или совершения действий от имени абонента по доверенности.

- используйте современное антивирусное программное обеспечение (предпочтительно российского производства) и следите за его регулярным обновлением для своевременного обнаружения вредоносных программ.

- по рекомендации компании-производителя мобильного устройства своевременно обновляйте его операционную систему, обеспечьте использование исключительно лицензионного программного обеспечения и операционной системы.

- при прекращении использования мобильного устройства удалите установленное мобильное приложение, личные данные и финансовую информацию с устройства.

Рекомендации по противодействию злоумышленникам и безопасной работе в Интернете

Злоумышленники постоянно совершенствуют методы для обмана граждан и получения их персональных данных с целью хищения денежных средств. Основные способы получения таких данных в настоящее время следующие:

- ✓ ***Телефонный звонок***

Злоумышленники могут представляться работниками Банка, различных финансовых, правоохранительных, налоговых органов, их номер может определяться в мессенджерах как номер Банка. Основная цель звонящих — запугать, ввести в заблуждение и получить доступ к конфиденциальной информации или вынудить Вас установить на мобильное устройство сторонние программы для удаленного управления вашим телефоном для того, чтобы совершать операции от вашего имени. Помните, что по телефону запрашивать информацию об одноразовых паролях из push/смс-уведомлений или кодах

доступа могут только злоумышленники. Сотрудники Банка никогда не запрашивают такие данные, а также не дают советы по немедленному снятию наличных или срочному «безопасному» переводу денежных средств и не предлагают установку приложений на мобильное устройство для защиты текущих счетов клиента.

При ответе на входящий звонок обращайте внимание на следующие признаки попыток воздействия со стороны злоумышленников, которые представляются сотрудниками Банка, Сбербанка, Банка России или других банков, следователями органов полиции, Следственного комитета, прокуратуры, инспекторами налоговой инспекции, специалистами Росфинмониторинга, сотрудниками вашего мобильного оператора или других муниципальных, государственных, правоохранительных, налоговых органов с целью запугать вас, побудить срочно снять и перевести денежные средства на другие счета, указанные злоумышленниками, или совершить иные срочные действия для исправления какой-либо чрезвычайной ситуации:

сообщение о возникновении некоей проблемной ситуации, касающейся лично Вас (например, в банк обратился человек, предоставил Ваш паспорт и ему одобрили кредит; либо с Вашей банковской карты пытаются перевести некую сумму денег; либо сообщают о неких подозрительных финансовых операциях, якобы совершенных Вами; либо уведомляют о завершении договора с мобильным оператором на Вашу сим-карту).

предложение невероятно привлекательных условий по кредитным, депозитным, инвестиционным продуктам, обещающим огромную доходность.

попытка Вас напугать: говорят о том, что Вам придётся выплачивать взятый мошенником кредит, либо, что если немедленно не принять необходимые меры, о которых они скажут, с карты спишут все Ваши деньги, или же о том, что Вам грозит серьёзная ответственность за якобы совершенные Вами финансовые операции, сотрудники мобильных операторов угрожают, что Вам заблокируют сим-карту и отключат связь, если не продлить договор.

предложение помощи в решении озвученной проблемы, максимально упростив Вам жизнь. Вам и делать почти ничего не нужно, они всё сделают сами, причем, немедленно, буквально в режиме онлайн! Вам никуда не надо бежать, и главное, не надо поднимать тревогу! Просто нужно перевести деньги с Вашего счета на «безопасный» счёт, который они Вам назовут, и всё, Ваши деньги будут спасены!

для продления договора с оператором мобильной связи Вам просто нужно дать им доступ к Вашему аккаунту на портале Госуслуги, продиктовав цифровой код, который придёт в смс на Ваш мобильный телефон.

Вас постоянно держат на линии, контролируют, переключают на других сотрудников, причем, сотрудник банка может переключить Вас, к примеру, на следователя полиции, или на сотрудника безопасности Банка России (так Вам говорят). При этом Вам задают множество вопросов, к примеру, в каких банках у вас есть счета, карты, просят сообщить персональные данные. Могут спросить также про Ваших родственников.

главное: Вам не дают времени на осмысление происходящего, от Вас требуют немедленного принятия решения (причём, решения, которое они Вам навязывают) и немедленных действий!

- ✓ ***Взлом электронной почты, страниц социальных сетей и аккаунтов мессенджеров (Viber, WhatsApp, Skype, Telegram и другие)***

Взломать могут как Ваш адрес или страницу, так и Ваших родственников и знакомых. Делается это для того, чтобы от Вашего имени или от имени хорошо знакомого Вам человека запрашивать и получать Вашу персональную информацию или похитить Ваши денежные средства.

- ✓ ***Создание поддельных (фишинговых) сайтов, максимально похожих на официальные сайты интернет-магазинов, органов государственной власти или банков***

На таких сайтах злоумышленники могут пытаться получить ваш логин и пароль (push/смс-пароль) для входа в систему ДБО, побуждают оплатить покупку по поддельным реквизитам либо установить приложение, позволяющее дистанционно управлять вашим устройством и действовать от вашего имени. Сайты могут активно рекламироваться, предлагать бонусы от Банка, бесплатные призы, подарки или скидки.

Для того чтобы не стать жертвой злоумышленников, рекомендуется:

- прежде всего, сохраняйте спокойствие и не поддавайтесь панике, потому что когда Вы в панике, Вами проще манипулировать.

- не устанавливайте никаких неизвестных приложений непонятных назначений от незнакомых людей, не проходите по ссылкам в письмах, пришедших от незнакомых адресатов.

- не сообщайте незнакомым людям и не публикуйте в открытом доступе (в соцсетях, на интернет каналах) свои персональные данные, важную информацию о себе, о своём имуществе, данные о банках, услугами которых вы пользуетесь, и так далее.

- не передавайте никому пин-код и секретный код (CVV или CVC) Вашей банковской карты. Любая форма, на любом интернет ресурсе, в которую Вам предлагается ввести номер Вашей карты + секретный код (CVV или CVC), должна вызывать у Вас подозрение!

- относитесь критически ко всему, что Вам говорят и пишут. Кем бы ни представился человек на другом конце линии, он ничем не сможет подтвердить, что он тот, за кого себя выдаёт, а Вы не сможете этого проверить. Поэтому всегда в таких случаях исходите из того, что Вы разговариваете просто с незнакомым человеком и никоим образом не обязаны выполнять того, что он от Вас требует и Вам внушает.

- если позвонивший просит Вас сообщить ему цифровой код из смс-сообщения, пришедшего на Ваш телефон, ни в коем случае этого не делайте! Вы имеете дело с мошенником! Сразу прекращайте разговор и кладите трубку!

- любое сообщение, содержащее просьбу перевести деньги кому бы то ни было, должно вызывать у Вас подозрение! Даже если Вам пишет очень близкий человек, которому Вы безгранично доверяете, не постесняйтесь позвонить ему (именно позвонить, а не написать в мессенджере, который может быть взломан!) и спросить у него лично, отсылал ли он Вам такое сообщение. И только после получения подтверждения лично от него, принимайте решение о переводе денег!

- если Вы производите оплату не через банковское приложение, а пройдя по ссылке с сайта, внимательно сверьте информацию о банке-эквайере, указанную на интернет странице, с адресом в адресной строке браузера. Убедитесь, что Вы действительно находитесь на сайте указанного банка, а не на фишинговой странице, созданной мошенниками.

- не публикуйте и не отправляйте никому фотографий своих документов (паспорта, СНИЛС и др.), а также фотографий, на которых Ваше лицо и разворот Вашего паспорта находятся в одном кадре.

- не спешите принимать решения и выполнять действия, которые Вам настойчиво предлагают принять и выполнить. При возникновении малейших подозрений, прекращайте разговор и вешайте трубку. Вы всегда можете сами перезвонить в банк и уточнить, одобряли ли кредит на Ваше имя или были ли попытки проведения операций по Вашей карте. Вы также можете позвонить в любой федеральный орган или службу, сообщить, что Вам звонил человек, представившийся их сотрудником, и уточнить, работает ли у них такой. Пока Вы исправно оплачиваете мобильную связь согласно условиям, предусмотренным Вашим тарифом, Вашу сим-карту не имеет права заблокировать ни один оператор.

- внимательно просматривайте текст приходящих на ваше мобильное устройство одноразовых паролей, чтобы убедиться, что Вы подтверждаете выполнение именно той операции, которую собирались совершить.

- не входите в систему ДБО, если ваше устройство подключено к wi-fi-сети в местах, где услуги интернета являются общедоступными, и/или с использованием публичных беспроводных сетей (например, интернет-кафе, сети в публичных местах или общественном транспорте). Если система ДБО

была использована в таких местах, то рекомендуем сменить логин/пароль при первой возможности, не используя публичные беспроводные сети.

- обращайтесь в Банк при возникновении любых подозрений для получения разъяснений и подтверждений полученной информации при обнаружении несанкционированных входов в систему ДБО, а также если Вы получили уведомление об операции, которую не совершали.

В случае обнаружения несанкционированного списания денежных средств

В случае обнаружения несанкционированного списания денежных средств со счёта рекомендуем Вам осуществить следующие действия, в том числе в целях снижения рисков повторного осуществления перевода денежных средств без Вашего согласия:

- немедленно обратиться в Службу клиентской поддержки Банка по телефону 8 (800) 200-08-48 (звонок по России бесплатный) или +7 (495) 797-99-11 (для звонков из-за рубежа) с требованием о блокировке доступа к системе ДБО (в случае её использования), приостановке исполнения платежа и/или с просьбой оказания содействия в возврате несанкционированно списанных денежных средств.

- оформить письменное заявление в Банк о факте несанкционированного списания, с указанием даты, суммы списанных со счёта денежных средств в валюте счёта, других известных Вам обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств. Указанное заявление необходимо представить в Банк на бумажном носителе в срок не позднее 2 рабочих дней с даты устного обращения в Банк в целях оперативного противодействия дальнейшему переводу и обналичиванию денежных средств.

- ознакомиться с рекомендациями по снижению рисков повторного осуществления перевода денежных средств без согласия клиента, размещенных на сайте Банка в разделе «Противодействие мошенничеству» (https://mbrus-bank.ru/anti-fraud).

- клиентам, использующим систему ДБО, также необходимо:

- в случае если в момент несанкционированного списания денежных средств использовались средства вычислительной техники (компьютеры, мобильные или иные переносные устройства) для работы в системе ДБО, то необходимо временно прекратить их использование, отключить их от электрической сети и обесточить. С высокой долей вероятности такие устройства могут быть подвержены воздействию специализированного вредоносного программного обеспечения, поэтому их отключение позволит предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы;

- произвести смену пароля, используемого для работы с системой ДБО;

- по факту несанкционированного доступа к компьютерной информации обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по статьям 272 и 273 Уголовного Кодекса РФ в связи с созданием, использованием и распространением неустановленными лицами вредоносных компьютерных программ, повлекшим неправомерный доступ неустановленных лиц к Вашей компьютерной информации, что, в свою очередь, привело к несанкционированному Вами списанию (переводу) денежных средств с Вашего счёта;

- с копией указанного заявления и с приложением копии талона правоохранительного органа о приёме заявления обратиться в Арбитражный суд города Москвы с исковым заявлением в отношении банка получателя о возврате суммы неосновательного обогащения и с ходатайством об аресте похищенной суммы денежных средств на счете получателя в банке получателя и раскрытии персональных данных получателя в целях привлечения его в качестве соответчика (гл. 60 Гражданского Кодекса РФ). В случае если Вам известны (стали известны) полные реквизиты получателя–физического лица, то указанный иск подается в суд общей юрисдикции;

- копии вышеуказанных обращений в правоохранительные и судебные органы с отметками об их приёме предоставить в Банк для того, чтобы Банк мог оказать содействие в возврате несанкционированно списанных денежных средств.

Что важно помнить

Кибермошеннику, даже если он является самым «продвинутым» хакером или программистом, очень непросто завладеть Вашими деньгами. Банковские сети и приложения достаточно хорошо защищены, а при использовании двухфакторной аутентификации шансы получить доступ к Вашим банковским счетам и картам для любого хакера любого уровня практически равны нулю. Конечно, квалифицированный программист в состоянии написать программу, способную получить доступ и управлять приложением банка онлайн, установленным, скажем, на Вашем смартфоне. Но для того, чтобы установить эту программу на Ваше устройство, ему необходим физический доступ к нему. Либо он должен придумать, как заставить Вас сделать это! Вот почему мошенники всё чаще прибегают к так называемой социальной инженерии, изобретая различные схемы и прибегая к всевозможным ухищрениям и уловкам. Схем придумано великое множество, постоянно появляются новые, но существует несколько базовых схем.

Мошенники пытаются завладеть Вашими персональными данными и затем попытаться их монетизировать через банки или микрофинансовые организации. Для этого мошенники придумывают предлоги для того, чтобы Вы сообщили им интересующую их информацию (например, история с продлением договора на мобильную связь). Идеальный вариант для них – получение доступа к Вашему аккаунту на Госуслугах, но и фотографии Ваших документов тоже подойдут. Также для этого активно используется фишинг.

Мошенники пытаются заставить Вас перевести деньги на их счёт. Для этого Вас выводят из «зоны комфорта». Вам сообщают о якобы грозящей Вам опасности потерять деньги. Это может быть история с одобрением кредита мошеннику, предоставившему поддельные документы на Ваше имя, или рассказ о попытке списания денег с Вашей карты. Также Вам могут рассказать детективную историю о недобросовестном сотруднике банка, которого служба безопасности с Вашей помощью должна поймать за руку. Вам необходимо просто прийти в Банк, получить кредит самому и зачислить его на «безопасный» счёт, или перевести на этот же счёт деньги с Вашей карты. На самом деле, никаких «безопасных» счетов в банках нет (а точнее, в банках все счета одинаково безопасны), а переведя деньги, Вы отдаёте их прямо в руки мошенников. А чтобы Вы не смогли сообразить, что Вас «разводят», Вам не дают времени на раздумье, требуют немедленных действий, всячески подгоняют.

Мошенники активно используют соцсети и мессенджеры. Они взламывают аккаунты, читают переписки, изучают окружение. А затем пишут сообщения от Вашего имени Вашим друзьям, знакомым и близким с просьбой перевести денег, изобретая для этого какой-либо предлог, на который сложно ответить отказом (типа, кто-то попал в беду и срочно нужны деньги). Если повезёт взломать корпоративный чат в мессенджере и вычислить руководителя, то от его имени могут отправить распоряжение срочно перевести деньги на какой-либо счёт, пообещав платёжку сделать завтра. Здесь также может использоваться фишинг. Мошенники могут сделать рассылку Вашим знакомым с просьбой, например, проголосовать за ребенка, который якобы участвует в каком-то конкурсе и ему не хватает несколько голосов для победы в нем и получения желанного первого приза! При этом в сообщении присутствует активная кнопка «Проголосовать» (или что-то вроде этого), нажав на которую голосующий переходит на сайт, принадлежащий мошенникам. На фишинговой странице, как правило, присутствует некая форма, в которую предлагается ввести какие-либо данные, необходимые мошенникам.

Телефоны Контактного центра ООО «МБ РУС Банк»:

8 800 200 45 67 (звонок по РФ бесплатный), +7 (495) 797-99-11 (для звонков из-за рубежа).