Памятка для Клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендации по мерам безопасности при использовании системы дистанционного банковского обслуживания «Мобильный банк» / «Интернет-банк».

1. **Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществляется перевод денежных средств**.

   Пользователям СДБО рекомендуется соблюдать организационные меры по обеспечению информационной безопасности:

   – никому и ни при каких обстоятельствах не разглашать одноразовые пароли, используемые для проведения операций в СДБО;

   – использовать компьютер, предназначенный для работы в СДБО и для выполнения задач, связанных с осуществлением переводов денежных средств;

   – по возможности минимизировать установку стороннего программного обеспечения и использовать только знакомые и проверенные приложения на мобильном устройстве, на котором установлено СДБО «Мобильный банк», не позволяется установка средств удаленного администрирования (Team Viewer, rAdmin и тд.). Установку новых приложений производить только после их предварительной проверки САЗ;

   - исключить работу с СДБО в публичных интернет сетях (общедоступные wi-fi сети, в местах общего пользования, метро и пр.), а также работу с СДБО, с компьютеров, расположенных в библиотеках, интернет-кафе и др.;

   – в случае временного перерыва в работе (совещание, обед и т.д.) на компьютере, используемом для работы с СДБО, необходимо завершить работу в СДБО и заблокировать компьютер путем нажатия комбинации клавиш: «WIN» и «L»; в СДБО «Мобильный банк» - выйти из мобильного приложения СДБО;

   – не записывать и не хранить пароли и данные для входа в СДБО на бумажных листках (или в текстовых файлах на компьютере, в заметках и формах автозаполнения на телефоне и пр.), не оставлять их в легкодоступных местах (на рабочем столе), не передавать их третьим лицам. В случае необходимости хранение паролей следует осуществлять способом, исключающим доступ к таким данным третьих лиц (например, в сейфе или в защищенном паролем приложении);

   – при подозрении на несанкционированный доступ к СДБО неуполномоченных лиц, несанкционированный доступ к компьютеру или мобильному устройству, а также утерю или кражу мобильного устройства с установленным мобильным приложением СДБО «Мобильный банк», паролям или нарушение информационной безопасности СДБО в других случаях следует незамедлительно сообщить об этом в АО МС Банк Рус по каналам связи, указанным в разделе 3.

2. **Рекомендуемые меры по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода**.

   В рамках обеспечения защиты информации от воздействия вредоносного кода пользователям системы дистанционного банковского обслуживания «Мобильный банк» / «Интернет-банк» (далее – СДБО) рекомендуется:

   – постоянно использовать средства антивирусной защиты (САЗ) на компьютерах, используемых для работы в СДБО или мобильных устройствах, на которых установлено мобильное приложение СДБО Банка (далее - СДБО «Мобильный банк»);

– установить настройки, обеспечивающие запуск САЗ в автоматическом режиме, в процессе загрузки операционной системы на компьютерах, используемых для работы в СДБО, а также постоянное функционирование САЗ в фоновом режиме в процессе работы на компьютере, используемом для работы с СДБО, или мобильном устройстве с установленным СДБО «Мобильный банк»;
– регулярно не реже 1 раза в неделю проверять все дисковое пространство и оперативную память компьютеров, предназначенных для работы в СДБО, а также проверять память мобильных устройств с установленным приложением СДБО «Мобильный банк», на наличие вредоносных программ;
– регулярно автоматически (или ежедневно в ручном режиме) обновлять установленные САЗ и антивирусные сигнатурные базы;
– при работе с электронной почтой, онлайн-мессенджерами не открывать письма, сообщения и вложения к ним, полученные от неизвестных отправителей, и не переходить по содержащимся в таких письмах гиперссылкам;
– не производить установку каких-либо программ, загруженных из сети Интернет или из непроверенных источников, кроме лицензионного программного обеспечения по ссылке, полученной от производителя программного обеспечения, Банка или приложений, загружаемых из официального репозитория Банка в Apple Store или Google Play;
– исключить возможность доступа и установки программного обеспечения (в том числе вредоносных программ (вирусов) посторонними лицами (гостями, посетителями) на компьютеры или мобильные устройства, предназначенные для работы с СДБО;
– осуществлять работу на компьютерах, используемых для работы в СДБО от имени учетных записей, не имеющих права администраторов в операционной системе;
– исключить доступ посторонних лиц к мобильным устройствам с установленным мобильным приложением СДБО путем установки специальных паролей, кодов аутентификации или проверки доступа по биометрическим признакам;
– исключить возможность взлома или перепрошивки операционной системы (получение root прав), установленной на мобильном телефоне с установленным СДБО «Мобильный банк»;
– при подозрениях на наличие вредоносных программ (вирусов) на компьютере, предназначенном для работы с СДБО, полностью воздержаться от входа и использования СДБО и проведения платежей до исправления ситуации.

3. **Рекомендации по защите информации при обнаружении в сети "Интернет" ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых АО МС Банк Рус систем СДБО, и (или) использующих зарегистрированные товарные знаки и наименование АО МС Банк Рус, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.**
Пользователям СДБО рекомендуется соблюдать меры предосторожности при использовании сети Интернет для проведения расчетов с использованием СДБО:
- размещение информационных материалов АО МС Банк Рус в сети Интернет осуществляется только по адресу – https://www.mcbankrus.ru/
- в случае обнаружения в сети Интернет ложного веб-сайта АО МС Банк Рус, отличного от https://www.mcbankrus.ru/, программного обеспечения, имитирующего программный интерфейс СБДО, и (или) использующиеся зарегистрированные товарные знаки и наименование АО МС Банк Рус, а также, в случаях, если с Вами пытаются связаться по электронной почте или иным способом лица с требованиями о предоставлении персональных идентификаторов доступа к СДБО или иной информации, необходимо немедленно сообщить об этом в Банк по телефону Горячей линии 8 (800) 770-05-70, через Чат-бот в мобильном приложении или по адресу электронной почты compliance@mcbankrus.ru, помните Сотрудники АО МС Банк Рус **никогда не будут требовать от Вас сообщить или указать где-либо свои учетные данные** .

АО МС Банк Рус не использует WEB-сайт https://www.mcbankrus.ru/ для осуществления расчетных операций в СДБО.