Рекомендации для клиентов, использующих устройства мобильной связи, о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода

В целях выполнения требований Положения Банка России от 17 апреля 2019 г. N 684-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций" ООО МКК «Бизнес Кредит» (далее - Компания) доводит до своих клиентов информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации с целью осуществления финансовой операции лицами, не обладающими правом осуществления финансовой операции, а также приводит список рекомендаций по защите информации от воздействия вредоносного кода (компьютерные вирусы, «трояны», «руткиты» и т.п.), о мерах соблюдения информационной безопасности и способах пресечения хищения.

Банк России отмечает участившиеся случаи несанкционированного доступа, вследствие которых осуществляются финансовые операции и/или доступ к защищаемой информации с использованием устройств мобильной связи – мобильные телефоны, смартфоны, планшеты и т.п. (далее – УМС) без согласия лиц, обладающими правом осуществления финансовой операции или доступа к такой информации.

Не рекомендуется сообщать посторонним лицам свою персональную информацию (ФИО, логин, пароль, номер карты, счета, паспорта и т.д.). Сотрудники Компании имеют право уточнять подобную информацию у клиента только в случае, если последний самостоятельно обратился в Компанию. Компания не направляет своим клиентам электронные письма, за исключением деловой переписки, инициированной обращением клиента, и SMS-сообщения (сообщения в мессенджерах) с просьбой уточнить персональную информацию о клиенте.

Несанкционированный доступ к защищаемой информации происходит вследствие заражения УМС клиента вредоносным кодом или посредством удалённого доступа к техническим устройствам клиента. Заражение УМС клиента осуществляется через спам-рассылку SMS или MMS-сообщений, сообщений электронной почты, сообщений в мессенджерах, содержащих ссылки на внешние ресурсы, или при переходе по ссылкам на ресурсы сети интернет. При переходе по таким ссылкам вредоносный код устанавливается на УМС.

Вредоносный код может обладать различными возможностями, в том числе:

- формирует и отправляет от имени клиента распоряжения на осуществления финансовой операции, в том числе в виде сообщений на «короткие номера»;
- перехватывает сообщения с кодами подтверждения, приходящие на УМС в целях подтверждения операции или доступа к защищаемой информации.

Наибольший риск таких операций связан с тем, что в ряде случаев вредоносный код скрывает от клиента приходящие от Компании уведомления. Таким образом, клиент, не зная о несанкционированной операции и/или доступе к защищаемой информации, не может направить в Компанию соответствующие возражения и пресечь несанкционированный доступ.

Также злоумышленники, используя методы социальной инженерии, могут вынудить клиента сообщить данные для проведения операции и/или доступа к защищаемой информации – коды доступа, коды SMS-подтверждения и осуществить несанкционированные действия.

В случае обнаружения несанкционированного доступа и/или совершения финансовой операции следует незамедлительно обратиться в Компанию и дополнительно, при необходимости, к оператору связи для блокировки SIM-карты/УМС/доступа к личному кабинету.

Клиентам, использующие УМС для совершения действий в целях осуществления финансовых операции, необходимо учитывать следующие **рекомендации для предотвращения получения несанкционированного доступа**:

- На УМС следует использовать безопасный способ подключения с помощью специального приложения, а не браузера. Загружать и устанавливать специальное приложение следует только с официальных сайтов – Google Play или Apple AppStore (или с официального сайта Компании в отношении приложений, реализуемых Компанией);
- В случае утери УМС, с установленным специальным приложением, необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи и обратиться в Компанию для блокировки доступа в личный кабинет;
- В случае изменения номера телефона УМС для работы в личном кабинете, обратитесь в Компанию для изменения доступа со старого номера на новый номер телефона. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время;
- Если у Вас неожиданно перестала работать SIM-карта – незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как в отношении Вас третьими лицами возможно проведение мошеннических действий;
- В случае утери (кражи, иного хищения) УМС следует незамедлительно обратиться в правоохранительные органы, сообщить оператору связи об утрате доступа к УМС для дальнейшей блокировки SIM-карты, а также рекомендуется оповестить всех третьих лиц, оказывающих Вам финансовые услуги посредством УМС, об утере (кражи, иного хищения) УМС для последующей блокировки доступа через данное УМС к каналам связи с такими лицами;
- Для работы с личным кабинетом используйте защищенные УМС – не пытайтесь обходить установленные производителем защитные механизмы (например, через джейлбрейк (Jailbreak) или рутинг (Rooting)). Не перепрошивайте свое УМС прошивками сторонних лиц, не являющихся производителями устройства, т.к. это может сделать Ваше устройство уязвимым к заражению вредоносным кодом.
- Не допускается работать в личном кабинете через публичные беспроводные сети (Wi-Fi), незащищенные беспроводные сети. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Для работы необходимо использовать подключение к сети Интернет через мобильного оператора (3G, 4G) или через доверенную защищенную беспроводную сеть;
- Необходимо хранить коды доступа, логины, пароли в тайне и предпринимать необходимые меры предосторожности для предотвращения их несанкционированного использования. Не рекомендуется записывать код доступа там, где доступ к нему могут получить посторонние лица (включая УМС);
- Не сообщайте коды доступа, логины, пароли, SMS-коды, необходимые для проведения операций, ПИН-коды платежной карты и контрольный код, указанный на оборотной стороне платёжной карте (CVV/CVC-код) посторонним лицам, сотрудникам Компании по телефону, электронной почте или

иным способом. Использование SMS-кодов допускается только при работе непосредственно с личным кабинетом, без участия сотрудников Компании. При наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактным телефонам, указанным на официальном сайте Компании;

- Не оставляйте УМС без присмотра. Необходимо установить пароль на доступ к УМС и/или на доступ к SMS-сообщениям. Это затруднит доступ злоумышленникам к УМС в случае его утраты;
- Банк России предупреждает о несанкционированных операциях, совершенных с использованием УМС. Для просмотра сообщения Пресс-службы Банка России пройдите по ссылке http://www.cbr.ru/press/pr.aspx?file=15042015_181850if2015-04- 15T18_12_19.htm.

Рекомендации по защите информации от воздействий вредоносного кода и его своевременному обнаружению:

- Необходимо применять на УМС, с которых ведётся работа с личным кабинетом, лицензионные средства антивирусной защиты, работающие в автоматическом режиме;
- В обязательном порядке обеспечить на постоянной основе автоматическое обновление антивирусных баз;
- Осуществлять регулярный контроль функционирования системы антивирусной защиты;
- Отключение или несвоевременное обновление антивирусных средств, установленных на УМС, используемых для работы в личном кабинете, не допускается. В случае обнаружения на УМС нештатного отключения антивирусных средств – не допускается работа с личным кабинетом на УМС до устранения причины нештатного отключения;
- Необходимо осуществлять проверку УМС на наличие вредоносного кода перед началом работы с личным кабинетом, а также после доступа к Вашему УМС сотрудников технической поддержки различных организаций или любых других частных мастеров, выполнивших работу по установке, обновлению и поддержке различных программ;
- Рекомендуется на постоянной основе регулярно, например, ежемесячно, проводить полную проверку УМС, на котором ведётся работа с личным кабинетом, на наличие вредоносного кода.
- Не рекомендуется передавать УМС для использования третьим лицам, в том числе родственникам, т.к. на оставленном без присмотра УМС может быть совершён ряд действий, направленных на получение доступа к личному кабинету. Например, злоумышленник может установить программное обеспечение с вредоносным кодом, настроить переадресацию SMS-сообщений на другой телефонный аппарат и т.п.;
- Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, SMS и MMS-сообщениях, сообщений мессенджеров, из недостоверных источников, в том числе на известные сайты;
- Не рекомендуется загружать и устанавливать на УМС программное обеспечение, полученное из недостоверных источников: интернет-сайты, ссылки в SMS и MMS-сообщениях и открытках, сообщениях мессенджеров.