Рекомендации для клиентов физических лиц, использующих мобильные приложения, по мерам снижения риска получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, а также рекомендации по защите информации от воздействий вредоносного кода.

В целях выполнения требований Положения Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», рекомендаций, изложенных в письмах от 7 декабря 2007 г. № 197-Т «О рисках при дистанционном банковском обслуживании», от 30 января 2009 г. № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга», от 25 июня 2009 г. № 76-Т «О рекомендациях по информированию клиентов о размещении на Web-сайте Банка России списка адресов Web-сайтов кредитных организаций», от 23 октября 2009 г. N 128-Т «О Рекомендациях по информационному содержанию и организации Web-сайтов кредитных организаций в сети Интернет», от 5 августа 2013 г. № 146-Т «Рекомендации по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети « Интернет» АКБ «АКТИВ БАНК» (ПАО) (далее - Банк) доводит до своих Клиентов информацию о существующих рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, 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 (далее – НСД) вследствие которых осуществляются операции перевода денежных средств с использованием устройств мобильной связи – смартфоны, планшеты и т.п. (далее – УМС) без согласия лиц, обладающими правом распоряжения этими денежными средствами.

Не рекомендуется сообщать посторонним лицам свою персональную информацию (ФИО, логин, пароль, номер карты, счета, паспорта и т.д.). Сотрудник Банка имеет право уточнять у Клиента подобную информацию только в случае, если Клиент самостоятельно обратился в Банк.

Банк не направляет своим Клиентам электронные письма, за исключением деловой переписки, инициированной обращением Клиента, по вопросам, связанным с функционированием системы дистанционного банковского обслуживания физических лиц «Мобильные платежи» или «Handybank» (далее – Система), и SMS-сообщения с просьбой уточнить их персональную информацию.

К несанкционированным операциям по переводу денежных средств относятся (включая, но не ограничиваясь ими):

- операции по оплате товаров и услуг при осуществлении доступа к сети Интернет через УМС Клиента, в том числе по реквизитам платёжных карт;
- операции по переводу денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»;
- операции, осуществляемые с использованием приложения Системы, предоставляемого Банком и установленного Клиентом на УМС;
- операции по оплате товаров и услуг с использованием иных приложений, установленных на УМС Клиента.

Несанкционированный перевод денежных средств проводится 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, 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 перевод денежных средств, в том числе в виде SMS-сообщений на «короткие номера»;
- формирует и отправляет от имени Клиента распоряжения на перевод денежных средств с использованием приложений Системы и иных приложений, предназначенных для оплаты товаров и услуг;
- перехватывает SMS-сообщения с кодами подтверждения, приходящие на УМС в целях подтверждения операции.

Наибольший риск таких операций связан с тем, что в ряде случаев вредоносный код скрывает от Клиента приходящие от Банка уведомления о списании денежных средств. Таким образом, Клиент, не зная о несанкционированной операции с его банковским счетом, не может направить в кредитную организацию в определённые законодательством сроки уведомление о переводе денежных средств без его согласия.

Также злоумышленники, используя методы социальной инженерии, могут вынудить Клиента сообщить данные для проведения операции – коды доступа, коды SMS-подтверждения и осуществить несанкционированные операции.

В случае обнаружения списания денежных средств необходимо в сроки, установленные законодательством РФ, обратиться в Банк или к оператору связи (если произошло списание денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»).

Клиентам, осуществляющим переводы денежных средств с УМС посредством Системы, необходимо учитывать, подготовленные Банком, следующие **рекомендации для снижения риска получения несанкционированного доступа**:

- На УМС для работы с Системой 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. Ссылки для загрузки размещены на официальном сайте Банка. Наши приложения для разных платформ соответствуют требованиям безопасности и периодически обновляются;
- В случае утери УМС, с установленным специальным приложением, используемым для работы с Системой, необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи и обратиться в Банк для блокировки доступа в Систему;
- В случае изменения номера телефона УМС для работы в Системе, обратитесь в Банк 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-карты – незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как в отношении Вас третьими лицами возможно проведение мошеннических действий;

- Для работы с Системой 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 Системе 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;
- Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Банком Системы, и (или) использующих зарегистрированные товарные знаки и наименование Банка, необходимо удостовериться, чтобы при подключении к Системе защищённое SSL-соединение было установлено исключительно с официальным сайтом Системы Handybank - https://aktivbank.handybank.ru/ (в случае использования сервиса Handybank) или Сервиса «Мобильные платежи» - https://www.mpaycard.ru/aktivbank (в случае его использования). Перед началом работы в Системе, необходимо убедиться, что в адресной строке браузера совпадает с вышеуказанным адресом соответствующего сервиса.
- Прежде чем ввести имя пользователя и пароль в системе Handybank, проверьте подлинность сайта aktivbank.handybank.ru по информации из SSL-сертификата. Для этого в адресной строке браузера, например Internet Explorer, щелкните мышкой на символ замка, далее «Просмотр сертификатов», перейти на закладку «Состав», встать на строку «Субъект», в окне просмотра убедитесь в наличии следующей информации: CN = *.handybank.ru, O = JSC HandySolutions. Аналогичным образом можно посмотреть эту информацию и в других браузерах. Центром сертификации, подтверждающим подлинность сайта aktivbank.handybank.ru, является thawte SSL CA - G2. При установке мобильного приложения из репозитория убедитесь, что разработчиком данного программного обеспечения является компания RUCARD Ltd.
- Прежде чем ввести имя пользователя и пароль в сервисе «Мобильные платежи», проверьте подлинность сайта www.mpaycard.ru по информации из SSL-сертификата. Для этого в адресной строке браузера, например Internet Explorer, щелкните мышкой на символ замка, далее «Просмотр сертификатов», перейти на закладку «Состав», встать на строку «Субъект», в окне просмотра убедитесь в наличии следующей информации: CN = www.mpaycard.ru. Аналогичным образом можно посмотреть эту информацию и в других браузерах. Центром сертификации, подтверждающим подлинность сайта www.mpaycard.ru, является thawte DV SSL CA - G2. При установке мобильного приложения из репозитория убедитесь, что разработчиком данного программного обеспечения является компания BelMobileSoft Ltd (при использовании репозитория App Store) или Belmobilesoft (при использовании репозитория Google Play Store).
- При создании паролей придерживайтесь следующих правил. Не допускается использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие системы. Пароль должен соответствовать следующим требованиям – длина пароля должна быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.), пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.);

- Необходимо хранить код доступа в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать код доступа к Системе там, где доступ к нему могут получить посторонние лица (включая УМС);
- Не сообщайте код доступа, SMS-коды, необходимые для проведения операций, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платёжной карте (CVV/CVC-код) посторонним лицам, сотрудникам Банка по телефону, электронной почте или иным способом. Использование SMS-кодов допускается только при работе непосредственно с Системой, без участия сотрудников Банка. При наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактным телефонам, указанным на официальном сайте Банка;
- 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;
- Необходимо корректно завершать работу в Системе, используя для этого пункт меню «Выход»;
- 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:

- Необходимо применять на УМС, с которых ведётся работа с Системой, 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 с которых производятся работы в Системе, не допускается. В случае обнаружения на УМС нештатного отключения антивирусных средств – не допускается работа с Системой на УМС до устранения причины нештатного отключения
- Необходимо осуществлять проверку УМС на наличие вредоносного кода перед началом работы с Системой, 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;
- Необходимо на постоянной основе регулярно, например, ежемесячно, проводить полную проверку УМС, на котором ведётся работа с Системой, 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 Системе. 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 из недостоверных источников, в том числе на известные сайты;
- Не рекомендуется загружать и устанавливать на ПК и УМС программное обеспечение, полученное из недостоверных источников: интернет-сайты, ссылки в SMS и MMS-сообщениях и открытках.