Памятка о мерах по обеспечению безопасности при работе в системе дистанционного банковского обслуживания физических лиц

В целях минимизации риска переводов денежных средств без добровольного согласия клиента при использовании Системы ДБО Банка необходимо соблюдать следующие рекомендации:

- установить на SIM-карту телефона, используемого в процессе управления денежными средствами (установлено мобильное приложение или получаются СМС коды подтверждения), PIN-код и включить в телефоне запрос PIN-кода при включении телефона;
- установить антивирусную программу на всё оборудование, используемое в процессе управления денежными средствами (телефон, планшет, компьютер);
- самостоятельно устанавливать мобильное приложение Банка на свое мобильное устройство только из официальных магазинов приложений (App Store, Google Play);
- незамедлительно поменять пароль, получаемый от Банка при регистрации в системе ДБО;
- не записывать и не хранить пароль для входа в мобильное приложение или систему ДБО;
- для доступа в систему ДБО использовать сложный пароль: не менее восьми символов, заглавные и прописные буквы латинского алфавита, цифры. Не использовать последовательность одинаковых символов, персональную информацию (например, имя, дату рождения, номер телефона);
- при утрате пароля или подозрении на его компрометацию необходимо срочно сообщить в Банк о необходимости блокировки доступа к Системе ДБО. К случаям компрометации относятся в том числе следующие происшествия с оборудованием, используемым в процессе управления денежными средствами (телефон, планшет, компьютер):
    - утрата с последующим возвратом или без такового;
    - установка недоверенного программного обеспечения (приложений);
    - утрата работоспособности оборудования (в т.ч. с последующим восстановлением);
    - раскрытие пароля, кода подтверждения Системы ДБО;
    - выявление наличия вредоносного программного обеспечения;
    - выявление факта доступа или совершения операций в Системе ДБО, которые Вами не совершались;
- при утрате мобильного устройства или утрате его работоспособности необходимо срочно обратиться в Банк для временной блокировки доступа в Систему ДБО;
- обеспечить использование и хранение мобильного устройства способом, исключающим доступ к нему третьих лиц;
- проверять работоспособность SIM-карты и устройства, на которые осуществляется доставка кодов подтверждения системы ДБО. Если SIM-карта или устройство перестали работать, обратитесь в Банк для блокировки доступа в Систему ДБО;
- не выполнять операции по повышению привилегий или взлому операционной системы мобильного устройства (получение root-прав для Android, установка jailbreak для iOS), на котором установлено или планируется установка мобильного приложения;
- по рекомендации компании-производителя мобильного устройства своевременно обновлять его операционную систему;
- при прекращении использования мобильного устройства удалить установленное мобильное приложение, личные данные и финансовую информацию, а при отсутствии необходимости использования ДБО Банка – заблокировать доступ к нему;
- связываться с Банком только по официальному телефону, размещенному на официальном сайте в сети Интернет www.mcbankrus.ru или через чат мобильного приложения;

- немедленно прерывать телефонные звонки (особенно поступившие с использованием мессенджеров), игнорировать сообщения в мессенджерах, СМС-сообщения, содержащие запрос о вашей конфиденциальной информации (пароль, одноразовые пароли (Push/СМС-пароли), данные о банках, услугами которых вы пользуетесь, и так далее);
- внимательно просматривать текст приходящих на ваше мобильное устройство сообщений системы ДБО, чтобы убедиться, что вы подтверждаете выполнение именно той операции, которую собирались совершить;
- не входить в Систему ДБО с недоверенных устройств, а также с использованием публичных точек доступа Wi-Fi-сети;
- не устанавливать на оборудование, используемого в процессе управления денежными средствами (телефон, планшет, компьютер), сомнительные приложения;
- не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.