

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

В последнее время участились попытки неправомерного получения конфиденциальной информации пользователей систем дистанционного банковского обслуживания (далее — Система ДБО) с целью хищения денежных средств.

Телефон Контакт-центра Банка:

[8 800 200 45 67](tel:88002004567)

для бесплатных звонков с территории Российской Федерации

[+ 7 812 603 00 90](tel:+78126030090)

для звонков за пределами Российской Федерации

Для того чтобы сохранить свои денежные средства, не вводите данные на подозрительных сайтах и в приложениях, никому не сообщайте и не передавайте:

- логин, пароль интернет-банка (мобильного приложения) (далее — пароль) или код для входа в мобильное приложение;
- одноразовые пароли (из Push/СМС-уведомлений) для входа в мобильное приложение или для подтверждения операций в нем (коды, которые приходят на указанный вами номер мобильного телефона в сообщениях при входе в мобильное приложение).

Рекомендации по безопасному использованию Системы ДБО

В целях минимизации рисков при использовании Системы ДБО Банк просит клиентов для обеспечения безопасности их денежных средств соблюдать следующие рекомендации:

- в обязательном порядке установить на SIM-карту телефона, с которого планируется пользоваться мобильным приложением, PIN-код и включить в телефоне запрос PIN-кода SIM-карты при включении телефона;
- самостоятельно устанавливать мобильное приложение на свое мобильное устройство только с интернет-сайтов и из магазинов приложений, перечень которых указан на информационных стендах в операционных залах полевых учреждений

и на официальном сайте Банка;

- не хранить код и пароль для входа в мобильное приложение непосредственно на мобильном телефоне, планшете или компьютере, на котором оно установлено;
- использовать сложный пароль: не менее восьми символов, заглавные и прописные буквы латинского алфавита, цифры. Не рекомендуется использовать последовательность одинаковых символов, персональную информацию (например, имя, дату рождения клиента, членов его семьи, номера телефонов);
- при утрате логина/пароля или подозрении об их компрометации необходимо срочно самостоятельно изменить его или сообщить в Контакт-центр о необходимости блокировки доступа к Системе ДБО;
- при утрате мобильного устройства необходимо срочно обратиться в Контакт-центр для временной блокировки карты и доступа в Систему ДБО. При восстановлении доступа на новом мобильном устройстве проверить все действия и операции в Системе ДБО за период его отсутствия;
- менять код для входа в мобильное приложение не реже одного раза в три месяца;
- избегать присутствия третьих лиц при вводе логина и пароля или регистрации в мобильном приложении, включая момент формирования логина и пароля и сканирования отпечатков пальцев;
- обеспечить хранение мобильного устройства способом, исключающим доступ к нему третьих лиц;
- если мобильное приложение установлено на устройстве, которое не используется ежедневно, необходимо периодически проверять работоспособность SIM-карты и самого мобильного устройства. Если SIM-карта или устройство перестали работать, обратитесь в Контакт-центр для блокировки карты и доступа в Систему ДБО. Доступ в Систему ДБО считается заблокированным с момента обращения в Контакт-центр. При активации новой карты и переустановке мобильного приложения проверьте все действия и операции в Системе ДБО в период неработоспособности мобильного устройства;
- 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. Не устанавливать мобильное приложение на устройство, которое уже получило такие привилегии;
- в личном кабинете на сайте, через мобильное приложение или в офисе своего сотового оператора подключить услугу запрета обслуживания и/или совершения действий от имени абонента по доверенности;
- использовать современное антивирусное программное обеспечение предпочтительно российского производства и следить за его регулярным обновлением для своевременного обнаружения вредоносных программ;
- 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.

данных с целью хищения денежных средств, постоянно совершенствуются.

Основные способы получения такой информации в настоящее время:

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 (Team Viewer, Ammyu Admin, AnyDesk, VNC и т.п.) для того, чтобы совершать операции от вашего имени.

Помните, что по телефону запрашивать информацию об одноразовых паролях из Push/СМС-уведомлений, кодах доступа могут только злоумышленники. Сотрудники Банка никогда не интересуются такими данными клиента, 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 обращайтесь внимание на признаки попыток воздействия со стороны злоумышленников:

- звонки якобы от имени Банка, государственных, правоохранительных, налоговых органов с целью запугать клиента, побудить срочно снять и перевести денежные средства на другие счета указанные злоумышленниками или совершить иные срочные действия для исправления какой-либо чрезвычайной ситуации;
- телефонные предложения невероятно привлекательных условий по кредитным, депозитным, инвестиционным продуктам, обещающим огромную доходность;
- постоянные звонки, не позволяющие переключить внимание на иные вопросы.

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 персональную информацию или 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 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:

- связываться с Банком только по телефону Контакт-центра или через чат мобильного приложения. Официальные реквизиты Банка указаны в документах, получаемых непосредственно от него, или иных официальных информационных источниках

(условия ДТС, настоящая памятка и т.п.);

- не отвечать на телефонные звонки (особенно поступившие с использованием мессенджеров), 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). Правоохранительные органы и банки никогда не обращаются с такими просьбами. О факте подобного обращения, в том числе якобы от сотрудника Банка, следует немедленно сообщить в Контакт-центр;
- внимательно просматривать текст приходящих на ваше мобильное устройство одноразовых паролей, чтобы убедиться, что вы подтверждаете выполнение именно той операции, которую собирались совершить, а именно: место проведения операции (указание наименования сервиса/организации (например, ROSTELEKOM.RU, а не, к примеру, ROSTELKOMP2P и т.п.), сумму и вид платежа;
- не входить 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 точках, необходимо 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



Ответственное структурное подразделение: Департамент полевых учреждений

Последнее обновление страницы: 05.04.2023