Общение с сотрудниками Банка

Для минимизации риска телефонного мошенничества обращаем ваше внимание, что сотрудники банка НИКОГДА не попросят:

- Сообщить конфиденциальные сведения: номера карт, пароли из СМС, паспортные данные, последние совершённые операции, кодовые слова, логины, пароли, ПИН-код, любую информацию из чеков,
- Поговорить с «роботом», которому вы якобы должны продиктовать конфиденциальные данные,
- Снимать деньги со счетов и карт,
- Оформлять новый кредит, чтобы «перекрыть мошенническую заявку»,
- Отправлять деньги на «специальные» банковские ячейки, счета, кошельки, телефоны, «карты сотрудников банка» и «карты персональных менеджеров»,
- Проводить любые действия с картой (идти к банкомату, распечатать чеки, привязать карту к телефону или токенизировать чужие карты на ваш телефон,
- Установить на ваше устройство какие-либо программы, например, для настройки защиты телефона или антивирус, а также программы для удалённого доступа,
- Обманывать других сотрудников банка, чтобы якобы «вывести на чистую воду мошенника» или «проверить действия другого сотрудника».

ВАЖНО! Банк не использует для общения с клиентами каналы связи Skype, Viber, WhatsApp и Telegram и прочие мессенджеры.

СМС и коды подтверждений

Внимательно читайте тексты СМС-сообщений с кодами подтверждений, проверяйте реквизиты операции. При поступлении с неизвестных номеров звонков от имени «банковских работников», СМС или иных сообщений от якобы «АО ИШБАНК» (например, «Заблокирована сумма оплаты», «Есть проблемы с проведением операции» и т. п.)
Ни в коем случае не перезванивайте на указанные в сообщениях номера.
Не сообщайте СМС-коды подтверждения, а также персональные сведения: серия и номер паспорта, адрес регистрации и прочие.
В такой ситуации следует считать, что звонки или сообщения приходят от мошенников. Вам нужно прекратить контакт и самостоятельно обратиться в банк по телефонам, содержащимся на сайте банка или в оригинальных банковских документах.

Официальные банковские приложения

Используйте только официальное банковское приложение из магазинов App Store, Google Play. Никогда не пользуйтесь другими неофициальными приложениями во избежание передачи личной информации мошенникам.

Сторонние ресурсы

Не устанавливайте программы для удалённого доступа и управления компьютерами (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin): мошенники могут заразить ваш компьютер или телефон вирусом, получить удалённый доступ к системе ДБО, Вашим личным данным и финансам.
Для использования веб-версии системы ДБО переходите на ресурс по ссылке, размещённой на официальном сайте Банка. При посещении сайта банка обращайте внимание на адресную строку https:// и наличие сертификата безопасности.
При получении электронных писем от банка обращайте внимание на отправителя, наличие цифровой подписи.

Используйте антивирус

Владельцам смартфонов настоятельно рекомендуем использовать антивирусное ПО, которое поможет уменьшить вероятность попадания в устройство вредоносных программ, предназначенных для перехвата приходящих от банка СМС-сообщений, а также кражи персональных данных.

Куда обращаться в случае мошенничества

Если вы получили подозрительное письмо, звонок или обнаружили операцию, которую вы не совершали, а также в случае, когда доступ к вашему компьютеру, смартфону или USB-токену могли получить посторонние лица, немедленно обратитесь к сотрудникам АО ИШБАНК п телефонам 8 (495) 232-12-34 (доб.3333) , 8 (800) 500-19-24.

Как понять, что звонят мошенники

Звонок от сотрудников МВД, ФСБ или Банка России / Центрального Банка
Вам позвонили и сообщили, что на Вас оформлен кредит. В связи с утечкой персональных данных и для сохранения личных сбережений, Вам необходимо срочно перевести средства на безопасный счет. Прекратите разговор и обязательно сообщите о мошенниках, позвонив в Банк.

Звонок сотрудников социальной защиты или Пенсионного Фонда
Вам позвонили и сообщили, что Вам полагается дополнительная выплата от государства. Просят пройти по ссылке, которую направили в СМС-сообщении или мессенджере, затем ввести на сайте или сообщить по телефону данные банковской карты и код для подтверждения. Не переходите по ссылкам и не сообщайте данные карты. Прекратите разговор и обязательно сообщите о мошенниках в Банк.

Блокировка счета/банковской карты
Вам поступило СМС-сообщение или звонок, в том числе через мессенджеры, о подозрительных операциях с деньгами. Прекратите разговор, игнорируйте сообщение. Обязательно сообщите о мошенниках, позвонив в Банк.

Объявление о продаже
Вам позвонили под предлогом покупки товара по Вашему объявлению в Интернете, попросят сообщить реквизиты банковской карты и код из направленного СМС-сообщения для перевода денег за товар. Не сообщайте номер карты и код. Прекратите разговор и обязательно сообщите о мошенниках, позвонив в Банк.

Звонок о несчастном случае
Вам позвонили от имени близкого человека, сообщили о несчастном случае и просят перевести деньги. Прекратите разговор и позвоните близкому человеку. Обязательно сообщите о мошенниках, позвонив в Банк.

Что такое «дропперство»

Телефонные мошенники с помощью методов социальной инженерии выуживают у граждан конфиденциальную информацию для кражи денег со счетов.
Похищенные средства выводят совсем другие люди, их называют «дропперами». То есть «дроппер» — это человек, который вольно или невольно оказывает услуги мошенникам. Именно на карты «дропперов» обманутые люди переводят средства на так называемые «безопасные счета». Дальше эти деньги проходят через цепочку переводов и впоследствии обналичиваются.

Как обезопасить себя от невольного участия в мошенничестве?

Варианты привлечения к «дропперству» могут быть самые разные:

- под видом банков, которым нужно выполнить «план по продажам», предлагают людям оформить любую карту и передать ее неким лицам за вознаграждение.
- предложение «трудоустройства» - быть администратором лотереи и якобы отправлять выигрыш победителям. На самом деле Ваш счет /карта будет использована в схеме вывода похищенных денег, и Вы окажетесь соучастником преступления.

Стоит насторожиться, если предлагают работу вне зависимости от образования и опыта, если обещают быструю и легкую прибыль, связанную с получением денег на ваш счет и последующим переводом по реквизитам.