ПАМЯТКА О БЕЗОПАСНОСТИ

В последнее время наблюдается рост числа попыток совершения мошеннических действий в отношении средств клиентов, размещенных на банковских счетах, во вкладах и по операциям с банковскими картами.

Для того, чтобы эффективно противостоять попыткам мошенничества, необходимо понимать основные цели, преследуемые преступниками:

- Получение доступа к денежным средствам, размещенным на банковских счетах и картах
- Сбор персональных данных для получения доступа к Вашим активам обманным путем

МЕТОДЫ МОШЕННИКОВ

Для того, чтобы усыпить Вашу бдительность, мошенники могут использовать различные методы психологического давления и социальной инженерии:

1. Создание обстановки повышенной срочности
   - Звонок о компрометации банковской карты или паролей доступа к Интернет-банку, мобильному банковскому приложению или личному кабинету клиента и необходимости срочно сообщить звонящему персональные данные для блокировки счета во избежание неправомерного списания денежных средств
   - Звонок с предложением какого-либо продукта или услуги на особо выгодных условиях с очень коротким периодом действия 2 (только сегодня) и просьбой сообщить свои персональные данные якобы для проверки доступности этого предложения для клиента или для подготовки заявки или документов для оформления сделки
2. Создание видимости рутинного характера происходящего
   - Звонок с просьбой сообщить свои персональные данные или содержимое смс-сообщения, мотивированное проверкой работоспособности ИТ-систем Банка, сверкой данных о клиенте, оценкой качества работы Банка и т.д.
   - Звонок с предложением пройти опрос об используемых клиентом банковских и инвестиционных продуктах и услугах

ТИПИЧНЫЕ ФРАЗЫ ТЕЛЕФОННЫХ МОШЕННИКОВ

(Если вас просят назвать что-то из перечисленного, завершите разговор и обратитесь в банк самостоятельно!)

«СМС нельзя называть обычным сотрудникам, а мне скажите…»

«Для вас есть выгодное предложение, давайте я зайду в Ваш НВ-Виртуоз…»

«Скорее подойдите к банкомату, я вам продиктую Ваши действия…»

«Мне код называть не нужно, озвучьте его роботу…»

«Или наберите код в тональном режиме…»

«Если вы не назовёте мне логин и пароль, перевод будет совершён…»

«Если вы сейчас же не назовёте мне цифры из СМС, операция пройдёт…»

«Чтобы я перевёл вам деньги, скажите срок действия и CVV/CVC…»

«Давайте скачаем и установим приложение для телефона, чтобы настроить ваш НВ-Виртуоз…»

«Я старший менеджер по безопасности всего Центрального аппарата Центрального Банка Центрального региона…»

КАКИЕ МЕРЫ НЕОБХОДИМО ПРЕДПРИНЯТЬ?

Банк на постоянной основе осуществляет мероприятия, направленные на защиту активов и персональных данных своих клиентов. Наши сотрудники в любой момент окажут содействие в случае попытки осуществления мошеннических действий. Тем не менее, рекомендуется руководствоваться следующими правилами в случае поступившего телефонного звонка с предложением передать Банку какую-либо информацию:

• Не сообщайте какие-либо данные Вашей банковской карты (в т.ч. CVC/CCV-код), коды подтверждения по СМС и персональную информацию, даже в случае, если звонок поступил с официального телефона Банка. Перезвоните в Банк самостоятельно. Код из СМС – только для вас! Не разглашайте никому, в том числе «роботу в тональном режиме», Кодовое слово понадобится назвать только если вы САМИ звоните в банк.

• Не скачивайте никаких программ и приложений в случае, если программы Вам не известны и/или эти программы на находятся в официальных магазинах приложений App Store и Google Play. Ссылки на эти приложения есть на сайте Банка. Скачивайте их только там. Сотрудники банка никогда не просят установить дополнительные программы на ваш телефон или ПК.

• Не переходите по каким-либо ссылкам в письмах, полученных по электронной почте, и не указывайте никакие персональные данные на Интернет-сайтах.

• Не проводите каких-либо операций через банкомат в случае, если к этому призывает позвонивший по телефону человек, представившийся сотрудником Банка. Не существует переводов в целях «безопасности» ни через мобильное приложение, ни через банкомат или кассу

• Заходя на сайт Банка и страницу авторизации Интернет-банка, обращайте внимание на правильность написания адреса (отсутствие опечаток, перестановки букв и т.д.) и наличие сертификата безопасности и буквы «s» в адресной строке https://. Переходите на страницу авторизации с сайта Банка, а не поисковой выдачи, или сохраните страницу Банка в закладках.

• Не сообщайте персональные данные – только мошенники просят «уточнения» по счетам, вкладам. Не вводите на сомнительных сайтах свои персональные данные, данные банковских карт и данные для входа в НВ Онлайн

ПОПУЛЯРНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

Подборка частных поводов обращения мошенников по телефону, электронной почте и мессенджерах. Подобные схемы позволяют злоумышленникам заполучить персональные данные, данные банковских карт или доступ к вашим аккаунтам в соцсетях и электронным почтовым ящикам или системам дистанционного банковского обслуживания, которые в дальнейшем будут использованы для кражи денег или перепродажи на черном рынке или подключения к рассылке вредоносных сообщений

Если в разговоре присутствуют элементы подобных схем – следует немедленно завершить разговор и самостоятельно обратиться в Банк.

	Ситуация	Что вас могут попросить сделать
Звонок от сотрудников государственных органов	Входящий вызов может выглядеть как звонок с официального номера телефона организации с помощью технологии подмены номера. Легенды могут быть самые разные: — расследование мошеннических действий в отношении вас со стороны сотрудников банка — наличие несанкционированных операций по вашим счетам — зафиксирована попытка оформления кредита на ваше имя На вас могут давить, пугать срочностью вопроса, запрещая под страхом уголовной ответственности или штрафа рассказывать о своих звонках	— поучаствовать в расследовании — перевести деньги «на безопасный счет» — создать «зеркальную» заявка на кредит — снять деньги в банкомате или кассе банка и передать третьим лицам — сообщить полные реквизиты карт
Звонок от «сотрудников службы поддержки оператора сотовой связи»	Звонок поступает под предлогами: — скорого прекращении действия номера абонента — переоформления договора об оказании услуг — смены тарифного плана на более выгодный — отключения платной услуги — блокировки номера телефона	— сообщить логин\пароль для входа в ваш личный кабинет мобильного оператора — подключить переадресацию входящих вызовов и текстовых сообщений или набрать на телефоне комбинацию цифр — установить дополнительную программу
Роботизированные обзвоны	Осуществляя звонки, мошенники имитируют автоматическое голосовое меню банков с помощью технологии роботизации. Робот может сообщить о блокировке вашей карты или о неких действиях со счетом, которые нужно подтвердить. Голосовой помощник может также предложить переключить вас «на оператора»	— набрать в тональном режиме комбинацию цифр — перезвонить на какой-либо номер для выяснения обстоятельств — сообщить полные реквизиты карт и код из СМС или перевести деньги на «безопасный счет»
Ошибочный перевод	Вам поступает сообщение о пополнении счета, имитирующее банковское уведомление. Следом к вам обращаются, сообщая будто бы перевод совершен по ошибке с просьбой перевести средства обратно	— сделать перевод по озвученным реквизитам
Мошенничество на площадках купли-продажи	Вам поступает звонок / сообщение от потенциального покупателя для оплаты / бронирования / оформления курьерской доставки продаваемого вами товара на одной из площадок купли-продажи	— сообщить данные карты, код из СМС и трехзначный код с оборота карты якобы для оплаты товара — перейти по ссылке, присылаемой в сторонний от площадки купли-продажи мессенджер, и ввести реквизиты карты