Чем грозит?

- Полной потерей всех собственных средств.
- В случае оформления кредитов или кредитных карт клиент рискует стать должником перед банками на крупные суммы.
- Непреднамеренное участие по легализации денежных средств в мошеннической схеме.

Что делать?

Никогда, ни при каких обстоятельствах не сообщать:

- Реквизиты карты.
- Коды из смс–сообщений.
- ПИН-коды к картам.
- Логины и пароли к личным кабинетам интернет–банка и т.д.
- Кодовое слово (оно может быть запрошено только работниками банка и только на входящем звонке — от клиента в банк).
- Любые персональные данные — паспортные данные, адреса прописки и проживания, место работы и т. д.
- При любом подозрительном звонке (даже если определяется официальный номер банка, организации и т. д.) перезванивать в организацию самостоятельно.
- Не оформлять кредит по просьбе «работников» банка, службы безопасности и т. д.
- Не устанавливать никакие программы по просьбе звонящих.
- Для предотвращения махинаций с переадресацией тел. номера никогда не набирать по просьбе звонящих никакие комбинации цифр на своем телефоне.
- Не переводить денежные средства на «безопасные счета», «страховые счета», «временные страховые ячейки» и т. д.
- При входящем звонке от «банковского робота» с целью подтвердить перевод — класть трубку.
- При поступлении любых подозрительных смс-сообщений, содержащих какие–либо коды, перезванивать в банк.

Остались вопросы? Позвоните нам!

***1945**

бесплатно по РФ для абонентов
«МегаФон», «Билайн», «МТС» и Tele2

www.finam.ru

127006, г. Москва, пер. Настасьинский, д. 7, стр. 2, комн. 33.

финам

Внимание — социальная инженерия!

Как уберечь себя от социальной инженерии

Главная задача злоумышленников — получить любыми способами доступ к интернет-банку или мобильному банку (счета, вклады, карты) или узнать реквизиты карты, либо вынудить клиента совершить самостоятельный перевод на указанных мошенниками получателей.

От кого поступают звонки?

Чаще всего звонящие представляются так:

«Работники банка» — служба безопасности, финансовый отдел, финансовый мониторинг, техподдержка, в том числе звонок от «робота».

«Социальные службы» — пенсионный фонд, совет ветеранов, «Госуслуги», благотворительные фонды, социальное страхование, управляющие компании и т. д.

«Силовые структуры» — звонки от «МВД, ФСБ, ФСО, СК».

«Брокеры, инвестиционные компании».

«Покупатели или продавцы» — «Авито», «Юла», Авто.ру, «Молоток» и т. д.

С каких номеров звонят?

Чтобы ввести в заблуждение, очень часто мошенники изменяют отображаемый номер входящего звонка на официальные номера банков, фондов, различных служб и т. д.

То есть на экране телефона можно увидеть абсолютно любой официальный номер какой-либо организации. В случае, если получатель звонка сомневается в чем–либо, злоумышленники просят проверить в сети Интернет подлинность номера.

Что говорят?

«Работники банка»

В большинстве случаев поступают звонки под предлогом того, что зафиксирован подозрительный перевод с вашей карты (указывают обычно далекий регион РФ — Якутия, Дальний Восток и т. д.) на карту — вымышленное ФИО. Также звонят с просьбой подтвердить смену номера телефона либо с информацией, что на вас оформлен кредит. Нередки случаи, когда звонящий «работник СБ» просит посодействовать во внутреннем расследовании: для этого клиенту необходимо оформить онлайн или в ближайшем офисе кредит и перевести полученную сумму денег на «безопасные счета», «страховые ячейки» и т. д. Часто «работники СБ» переключают на «следователей», и дальнейшую обработку продолжают уже «работники полиции».

«Социальные службы»

При звонке от таких служб до клиента доводится информация о причитающихся ему выплатах, пособиях и т. д.

Нередки сезонные всплески под различные праздники — День Победы, 23 Февраля: целевая аудитория — пожилые люди.

«Силовые структуры» — звонки от «МВД, ФСБ, ФСО, СК»

В целом разговоры сводятся к следующему:

- Вы — фигурант уголовного дела по факту хищения.
- Необходима помощь в расследовании.
- Мошенничество с вашими картами и счетами.

Нередко «силовики» переключают на «работников ЦБ» и других банков. В своих разговорах часто используют номера статей и частей статей УК РФ.

«Брокеры, инвестиционные компании»

Темы разговоров:

- Выгодно вложить денежные средства.
- Возврат ранее потерянных средств.

«Покупатели или продавцы»

- Купить
- Продать
- Внести предоплату

Что делают?

Если клиент, сообщает реквизиты карты, а также коды из смс–сообщений, злоумышленники могут совершить переводы с карты клиента на сторонние карты, а также осуществить перерегистрацию СДБО (мобильный или интернет–банк).

Далее развитие событий может быть таким:

- Смена номера для смс–информирования — все дальнейшие коды для подтверждения финансовых операций, а также информационные смс–сообщения об остатках денежных средств будут приходить на мошеннический телефонный номер.
- Оформление предодобренного кредита или кредитной карты с последующим выводом денежных средств.
- Изменение ПИН–кода к картам и привязка токена к устройству мошенников и обналичивание денежных средств в банкоматах.
- Закрытие вкладов и вывод денежных средств.

Если клиент сообщает третьим лицам кодовое слово и персональные данные, мошенники осуществляют звонок в банк с «номера телефона клиента», проходят полную идентификацию, снимают дневные, месячные лимиты на расходование денежных средств.

Часто клиенты сами устанавливают переадресацию входящего вызова на телефонный номер мошенников, в таких случаях настоящая служба безопасности банка, увидев подозрительные операции, связывается с клиентом, а разговаривает с мошенниками, которые, зная все персональные данные, подтверждают операции.

Нередко мошенники под видом техподдержки банка убеждают клиентов установить приложения для удаленного доступа (TeamViewer, Anydesk и т. д.), мотивируя данные действия «обновлением банковского ПО», «у вас на устройстве вирус» и пр. После получения полного доступа к устройству мошенники также заходят в СДБО и совершают несанкционированные переводы, закрытия вкладов и т. д.

Мошенники с торговых площадок «Авито», «Юла» присылают поддельные, фишинговые ссылки «для получения денежных средств», после введения реквизитов карты и кодов из смс–сообщений на данных ресурсах третьи лица могут осуществить покупку или перевод.