Основным инструментом злоумышленников для хищения денег остается использование приемов и методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит деньги или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение. Проблема мошенничества актуальна как в отношении физических, так и в отношении юридических лиц.

На протяжении последних четырех лет Банк России фиксирует ежегодное увеличение объема операций, совершенных без добровольного согласия клиентов. В 2023 году злоумышленники похитили 15,8 млрд руб. По сравнению с 2022 годом объем похищенных денег вырос более чем на 11,4 %. Количество мошеннических операций увеличилось на 33% и превысило 1,1 млн.

В 2023 году: банки отразили 34,8 млн попыток кибермошенников похитить деньги у граждан, сохранив 5,8 трлн рублей.

В 2023 году количество мошеннических операций с использованием платежных карт было самым высоким среди остальных типов операций. Использование злоумышленниками чувствительных данных увеличивает риск хищений как собственных накоплений граждан, так и полученных под влиянием мошенников кредитных средств.

Телефонный звонок – ключевой инструмент мошенников, которые занимаются хищением денежных средств. Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы заполучить доступ к деньгам. Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. Приведем некоторые распространенные способы обмана:

1. **Якобы сотрудник Пенсионного фонда, соцслужбы.** Мошенники сообщают, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда. Причем для получения этой выплаты никуда ходить не надо: все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.
2. **Якобы сотрудник поликлиники, аптеки, медицинского центра.** Мошенники соотносят информацию о проблемах со здоровьем гражданина и сообщают ему о появлении дефицитного и дорогого лекарства по специальной цене, которое надо срочно выкупить. Злоумышленники объясняют, что человек платит полную стоимость, а разницу в цене по скидке вернут ему на карту, реквизиты которой необходимо сообщить звонящему.

3. **Якобы сотрудник банка** (как правило, представителя службы безопасности). Сценарии могут быть разные: от классического «с вашей карты пытаются перевести деньги» до пугающего «по карте замечены подозрительные операции, и она заблокирована». В любом случае итогом будет просьба сообщить информацию по карте или счету, код из СМС-сообщения.
4. **Якобы друг, родственник.** Мошенник может представиться родственником/другом, попавшим в неприятную ситуацию, или ее случайным свидетелем, а также представителем правоохранительных органов, который готов помочь гражданину с решением проблемы. Схема довольно старая, но мошенники продолжают ею пользоваться, так как страх за близкого человека – это очень сильная эмоция.

Мошенники очень часто представляются якобы сотрудниками Центрального банка (Банка России). Гражданам звонят и от имени Центробанка сообщают, что по их карте зафиксирована подозрительная активность: пытаются перевести все деньги за рубеж. Чтобы сохранить свои деньги и подтвердить, что это не сам человек совершает данную операцию, ему необходимо открыть в Центробанке «защищенный/безопасный/специальный» личный счет. Для этого уточняют паспортные данные, просят подтвердить данные по счету/карте, а для открытия счета просят подтвердить небольшой перевод на этот счет, который Центробанк якобы совершает для своих клиентов, то есть сообщить код из СМС. Следует помнить, что Банк России не работает с физическими лицами. При поступлении телефонного звонка от Банка России немедленно прервите разговор.

Также иногда злоумышленники представляются сотрудниками правоохранительных органов. Такие мошенники долго и подробно рассказывают об обстоятельствах уголовного дела, участником которого, по их словам, гражданин является. Далее для уточнения информации они просят сообщить личную и финансовую информацию. Это и является признаком того, что гражданин разговаривает с мошенником: правоохранительные органы не просят назвать по телефону финансовую информацию. Помните, что настоящие сотрудники полиции никогда не запрашивают личные и финансовые данные по телефону.

Социальная инженерия – введение в заблуждение путем обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа (банковские карты, онлайн-банк) или побуждения владельцев самостоятельно совершить перевод денежных средств с целью их хищения.

Основные проявления социальной инженерии:

1. Обман или злоупотребление доверием (например, мошенники представляются сотрудниками банков, правоохранительных органов или родственниками).
2. Психологическое давление.
3. Манипулирование.

Действительно, мошенники оказывают психологическое давление (торопят, сознательно пугают или, наоборот, приводят в состояние эйфории) и, используя вызванные положительные или отрицательные эмоции, манипулируют действиями граждан. Существуют различные методы социальной инженерии. Телефонное мошенничество – это один из основных инструментов, которым активно пользуются злоумышленники.

В чем заключается «успех» мошенников?

Формула «успеха» телефонных мошенников: неожиданность+ сильные эмоции (положительные и отрицательные) + психологическое давление и создание паники + актуальная тема = вы готовы сделать все, что от вас просят мошенники (перевести деньги, совершить финансовые операции, сообщить личную или финансовую информацию).

Распространенные мошеннические схемы, а также способы противодействия им Банк России публикует на своем официальном сайтев разделе «Противодействие мошенническим практикам».

Как действуют мошенники, что человек, отбросив все свои знания, все равно идет у них на поводу?

Прежде всего злоумышленникам играет на руку эффект неожиданности. Застав Вас врасплох, они подключают к действию эмоции:

Мошенники воздействуют на основные базовые эмоции. Задача киберпреступников – вывести человека из спокойного состояния и отключить у него критическое мышление.

Положительные: радость, желание быстрее получить деньги или выгоду (как правило, такие эмоции человек испытывает после таких фраз, как: «Вам положены социальные выплаты», «Вы выиграли крупную сумму денег» и другие похожие истории).

Отрицательные: страх, испуг, желание помочь, спасти или родного человека, или свои сбережения (эти эмоции проявляются у человека после таких фраз, как: «Ваш сын попал в аварию», «С Вашей карты пытаются украсть деньги»).

Они активируют базовые эмоции, обеспечивая быструю и необдуманную реакцию жертвы.

Одной из распространенных мошеннических схем является ситуация, когда мошенники представляются сотрудниками Банка России или правоохранительных органов. С целью сохранения денежных средств они настаивают на выполнении процедуры обновления единого лицевого счета в Банке России. Чтобы гражданин окончательно поверил в реальность лжеситуации, мошенники могут прислать целый пакет якобы подтверждающих документов: сканы официальных документов с подписями и печатями, фотографии удостоверений сотрудников и другие документы на официальных бланках органов государственной власти. К сожалению, такие документы могут содержать фамилии реальных работников — эти сведения злоумышленники могут брать с сайта Банка России (или с сайта той организации, сотрудниками которой они представляются). Высылая фальшивое удостоверение или документы, они надеются убедить человека в правдоподобности своих мошеннических действий, чтобы в дальнейшем лишить его денег или оформить на него кредит. На самом деле сотрудники Банка России не звонят людям и не направляют никому копии каких-либо документов, не запрашивают персональные и банковские сведения, не предлагают совершить какие-либо операции со счетом.

Еще один вид мошенничества – это фишинг. Злоумышленники подделывают популярные сайты (к примеру, органов власти и различных ведомств). Аферисты также подделывают сайты известных магазинов, маркеплейсов, туристических компаний и др. Например, на слайде представлен сайт, замаскированный под официальный сайт «Госуслуги». Несмотря на то что внешне он очень похож на настоящий, при внимательном рассмотрении можно заметить, что наименование сайта в адресной строке отличается от официального домена. Настоящий сайт «Госуслуги», а также официальные сайты финансовых организаций в популярных поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Заметьте, что тематика фишинговых сайтов, как и сценарии телефонных звонков, также соответствует актуальным событиям: когда основной новостной повесткой была новая коронавирусная инфекция, злоумышленники всячески использовали ее в качестве поводов для выманивания денег у граждан. Для чего мошенники создают фишинговые сайты? Имитируя интернет-ресурсы популярных компаний, они рассчитывают, что пользователи не заметят подделку и оставят на поддельной фальшивой странице важную информацию: личные или финансовые

данные, логин и пароль, контактные сведения (номер телефона и электронную почту). Заполучив чувствительную информацию, мошенникам будет легче обмануть человека.

Существуют общие правила поведения с кибермошенниками. Следуя им, вы сможете себя обезопасить:

−не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

−установите антивирусные программы на все свои гаджеты. Данное ПО предупредит вас в случае установки подозрительного продукта на ваш гаджет. Важно регулярно обновлять антивирусную базу.

−не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, звонки на неизвестные пропущенные телефонные номера могут быть чреваты как минимум списанием значительной суммы с вашего мобильного счета, а как максимум − быть поводом для мошенников активизировать против вас мошенническую схему;

−не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету;

−заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получат доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.

В случае если вам позвонили и представились якобы сотрудником банка, положите трубку и самостоятельно позвоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка. Не нужно перезванивать на номера, с которых вам звонили, – вы рискуете попасть на мошенников. Чтобы связаться с банком, самостоятельно наберите номер, указанный на обратной стороне вашей банковской карты или на официальном сайте кредитной организации.

Для того чтобы обезопасить свои данные, установите двухфакторный способ аутентификации (например, логин и пароль, а также подтверждающий код из СМС) –

это, как правило, бесплатно. Пользуйтесь только проверенными и официальными сайтами финансовых организаций в поисковых системах (Яндекс, Mail.ru), помеченными цветным кружком с галочкой.

Как противостоять телефонным мошенникам?

Ни в коем случае не отвечайте на звонки с незнакомых номеров. Как правило, если вам звонят с работы или из другой организации, от которой вы ожидаете звонка, вам дополнительно напишут СМС-сообщение или сообщение в мессенджере. Никогда не перезванивайте по незнакомым вам номерам.

Если разговор касается финансовых вопросов, не продолжайте разговор и положите трубку. Сотрудники банков или правоохранительных органов не запрашивают Ваши личные и финансовые данные по телефону.

Не торопитесь принимать решение, ведь мошенники добиваются именно того, чтобы вы приняли быстрое и необдуманное решение. Они используют методы социальной инженерии: торопят Вас, пугают, создают чувство паники. Не стоит поддаваться такому давлению: проверьте информацию в Интернете или обратитесь за помощью к близким родственникам.

Прежде чем принять какое-то решение, связанное с финансами, позвоните близкому человеку, в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий. Важно получить подтверждение информации именно из официального источника, контактные номера при этом берите из своей записной книжки или с официальных сайтов организаций.

Не торопитесь принимать решение: всегда лучше проконсультироваться у специалиста, которому Вы доверяете, или посоветоваться с близкими и родственниками.

Будьте бдительны и оставайтесь в безопасности!