

Слайд 1 Заголовок

Слайд 2

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.

С 2019 года по 2022 год количество операций без согласия клиентов выросло в 1,5 раза: 876,5 тыс. ед. в 2022 г. против 576,57 тыс. ед. в 2019 г.

Увеличивается и сумма хищений: в 2022 году у населения было похищено 14,1 млрд руб. Это в 2 раза больше, чем в 2019 году (6,4 млрд руб.) По сравнению с 2021 годом объем похищенных денег в 2022 году вырос на 4,3%.

Важно отметить тенденцию: несмотря на то что в 2022 году произошло снижение числа хищений, связанных с мошенническими действиями, на 15,3% по сравнению с 2019 годом, сумма хищений за этот год выросла на 4,3%. Количество совершенных хищений в 2022 году снизилось по сравнению с 2021 годом на 15,3% и составило 876,6 тыс. случаев.

(СПРАВОЧНО) В 2023 году Банк России ввел для банков новую форму отчетности по операциям без согласия клиентов. Она позволяет видеть соотношение неуспешных операций, заблокированных антифрод-системами кредитных организаций, и фактических незаконных списаний. На основе этого и других показателей в дальнейшем будет оцениваться эффективность систем защиты банков. Так, банки в январе – марте 2023 года отразили 2,7 млн атак кибермошенников на счета клиентов и таким образом предотвратили хищения на 712 млрд рублей. Тем не менее мошенникам удалось провести 252,1 тыс. операций без согласия клиентов, их объем составил 4,5 млрд рублей. Больше всего денег злоумышленники похитили через переводы с помощью онлайн-банкинга, в том числе это были заемные средства.

В прошлом году средний чек хищений, то есть размер денежных средств, приходящийся на одно хищение, по сравнению с 2021 годом вырос на 23%, по сравнению с 2019 – на 19% соответственно. За последние четыре года средний чек ежегодно увеличивался в среднем на 1,68 тыс. руб. Телефонные мошенники провоцируют людей оформлять кредиты, потому что за счет кредитных средств можно существенно увеличить суммы хищений. В том числе по этой причине наблюдается рост среднего чека.

В 2022 году средний чек хищения у граждан составил более 15 тыс. руб., у юридических лиц – практически 177 тыс.руб.

Слайд 3

Телефонный звонок – ключевой инструмент мошенников, которые занимаются хищением денежных средств. Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы получить 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.

Слайд 4

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.

Слайд 5

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.

Слайд 6

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.

Слайд 7

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 сайте в разделе «Противодействие мошенническим практикам».

(СПРАВОЧНО) ТУ и ГУ вправе по данной формуле описать актуальную для региона мошенническую схему.

Слайд 8

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.

(СПРАВОЧНО) ТУ и ГУ вправе в зависимости от целевой аудитории описать актуальную для региона мошенническую схему.

Слайд 9

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 лишиться 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.

Слайд 10

Еще один вид мошенничества — это фишинг. Злоумышленники подделывают популярные сайты (к примеру, органов власти и различных ведомств). Аферисты также подделывают сайты известных магазинов, маркетплейсов, 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.

Слайд 11

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.

Слайд 12

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, а 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, а 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.

Слайд 13

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.

Слайд 14

Что делать, если мошенники все же похитили с вашей карты денежные средства?

Как только вы это обнаружите, сразу же заблокируйте карту, а также сообщите о хищении (не позднее суток с момента получения информации о хищении необходимо написать о несогласии с операцией). Сделать это можно через мобильное приложение банка, а также позвонив в контактный-центр или обратившись в отделение банка.

Затем как можно скорее напишите заявление в полицию, лично обратившись в ближайший территориальный орган внутренних дел с заявлением о возбуждении уголовного дела.

В случае если вы утратили электронное средство платежа и (или) оно использовалось без вашего согласия, банк обязан в течение 30 дней возместить сумму хищения.

Слайд 15

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!

Слайд 16

Фишинг становится все более распространенным явлением. Фишинг – это совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер банковской карты и другую конфиденциальную информацию. Чаще всего мошенники используют поддельные/фишинговые сайты.

Внешний вид таких сайтов неизменен, он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники. Как тогда распознать фишинговый сайт?

Распознать фишинговый сайт можно по нескольким признакам: адрес сайта может отличаться от настоящего лишь парой символов; в адресной строке отсутствует https и значок закрытого замка; дизайн сайта скопирован некачественно, в текстах допущены ошибки, у сайта мало страниц или даже только одна – для ввода данных карты.

Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания.

Слайд 16

Существует довольно много уловок мошенников в Интернете: например, интернет-магазины и аукционы; восстановление кредитной истории; сообщение о крупном выигрыше или выплате от государства; заманчивое предложение о работе; льготные кредиты; туристические путевки со скидкой; сбор «пожертвований» для детей, больных, животных и др.; предложения в высокодоходные инвестиции. Все они используют актуальную новостную повестку, а также воздействуют на базовые эмоции: положительные или отрицательные.

Будьте бдительны. Не верьте слепо предложениям в Интернете – проверяйте информацию на достоверность!