О противодействии телефонным мошенникам

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: 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.

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 сайте в разделе «Противодействие мошенническим практикам».

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.

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.

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!