Мошенничество по телефону

Технологии упрощают жизнь не только честным людям, но и преступникам

Ежемесячно со счетов граждан РФ мошенники похищают от 3,5 до 5 млрд рублей.

Одна «удачная» операция в среднем приносит им 8 000 руб. Каждый воровской «колл-центр» делает в сутки 3-7 тыс. звонков, но обмануть удаётся не более 1% абонентов. Тем не менее цифры складываются астрономические.

Как осуществляется мошенничество по телефону

Основой мошеннических схем служит персональная информация, полученная на нелегальном рынке баз данных интернет-магазинов, финансовых учреждений, государственных структур. В том же интервью Станислав Кузнецов рассказал, что нынешние мошенники усложнили методы своей работы. Они могут долго обрабатывать очередную жертву, чтобы убедить её перевести деньги, соблазняя финансовой выгодой и даже предлагая некую должность с высокой оплатой. И ради этого устраивают видеособеседования с потенциальным «работодателем». Каждый день появляются всё новые методики, но средства борьбы с преступниками тоже не стоят на месте.

Виды мошенничества по телефону

По-прежнему в ходу безотказные способы «сравнительно честного» отъёма денег у населения.

«Телефонные мошенники похищают со счетов россиян 3,5-5 миллиардов рублей ежемесячно. Средний чек по успешной мошеннической операции находится на уровне 8 тысяч рублей»

Мошенничество с банковскими картами и счетами

Платежная карточка, безусловно, удобная и полезная вещь. Но крайне соблазнительная для криминальных воздействий. Весьма распространена схема воровства «на доверии». Так, телефон из объявления в интернете или СМИ о продаже любого имущества немедленно попадает в поле зрения мошенников. И владельцу звонит некий «потенциальный покупатель», готовый платить, не торгуясь, но только на карту.

Для этого он просит сообщить её номер, срок действия, CVV-код с обратной стороны карты. И SMS-код из сообщения банка о проведённой операции. Даже если не удаётся получить весь набор информации, недостающие данные восполняются квалифицированными хакерами. И карточный счёт не пополняется, а опустошается путём перевода наличности на некий электронный кошелек, который немедленно исчезает из сети после вывода средств с него.

Звонки от «служб безопасности» банков

Не менее распространены звонки из «службы безопасности банка-эмитента платежной карты» о совершённой подозрительной операции или сбое в программном обеспечении, который привел к потере средств. Для восстановления счёта и возврата денег якобы необходимы вышеперечисленные данные. Для защиты от подобных инцидентов рекомендуют установить определенные программы, замаскированные под известные сервисы. Но на самом деле эти утилиты отправляют мошенникам коды доступа к счетам, полностью развязывая преступникам руки.

Звонки от «сотрудников» правоохранительных органов и государственных служб

Особенно циничны звонки из правоохранительных органов, якобы расследующих случаи мошенничества по телефону. Цель та же самая — усыпить бдительность и выманить нужную информацию. На фоне пандемии активизировались мошенники, которые представляются работниками Роспотребнадзора или Пенсионного фонда с сообщениями о новых социальных выплатах. Но для их получения необходимы все те же данные платежных карт.

Звонки с подмененных номеров

Большинство банков имеют специальные номера, которые используются только для сообщений клиентам. Сбербанк, например, рассылает свои уведомления только с номеров 900 или 9000. Но существуют специальные программы-обманки, которые маскируют настоящий номер звонящего, и абонент видит знакомый ему идентификатор.

Махинации со счетами мобильных телефонов

Самый распространённый вариант такого мошенничества — сообщение или звонок об ошибочном переводе денег на счёт мобильного телефона и просьба вернуть их владельцу. Могут быть даже угрозы обращения в полицию или оператору с требованием блокировки телефона.

Сообщения о попавшем в беду родственнике и просьбы о помощи

Панический звонок о попавшем в беду родственнике обычно случается среди ночи, полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счёт мобильника.

Сообщения о выигрыше в лотерею

Отличная новость сопровождается требованием перевода на покрытие технических издержек самой лотереи. Здесь расчёт на незнание законодательства РФ, согласно которому все расходы организаторов ложатся на них самих.

Сообщения-«грабители»

Жертве приходит SMS с просьбой перезвонить по мобильному номеру, где ему сообщают якобы должны сообщить важную новость (о выигрыше в лотерею, проблемах с банковской картой, получении наследства). На звонок долго нет ответа, а после отключения обнаруживается, что со счёта списана большая сумма. Мошенники используют возможность зарегистрировать сервис с платным звонком. Обычно подобные сервисы развлекательные и обязательно сообщают о платности в рекламе. Но мошенники этого не делают и за любой звонок по этому телефону взимают немалую плату.

Махинации с короткими номерами

В этом случае мошенники тоже используют мобильный сервис. При заказе некой услуги абонент получает сообщение, что для её подключения нужно отправить сообщение на короткий номер такой-то. После отправки со счёта списываются деньги. Механизм тот же, короткий номер тоже можно зарегистрировать как платный и не сообщать об этом абоненту.

Телефонные вирусы

Жертве приходит сообщение о том, что ей пришло сообщение в некий мессенджер, и его можно получить, пройдя по ссылке. После чего в смартфон внедряется вирус, получающий полный контроль над гаджетом.

Аппаратные средства для защиты от мошенничества по телефону

Может сложиться впечатление, что от телефонных мошенников нет спасения. Но службы безопасности банков активно им противодействуют. Сбербанк, например, разработал и внедрил систему кибербезопасности с использованием искусственного интеллекта. Все звонки, касающиеся переводов или снятия средств со счетов, контролируются и таким образом выявляются признаки преступной деятельности. В базе данных банка множество мошеннических колл-центров и 130 преступных схем. На экране онлайн-банкинга появляется красный транспарант в случае подозрения о мошеннической операции.

Как проверить номер, с которого поступают звонки

В интернете существует достаточно много сервисов для того, чтобы определить если не владельца конкретного телефонного номера, то по крайней мере город или страну, откуда пришел звонок. До 40% таких сообщений производятся из-за границы, еще 40% — из мест заключения. В любом случае поможет звонок в проверенную службу безопасности или колл-центр банка, а не по указанному грабителем номеру.

Как вычислить телефонного мошенника?

Чаще всего мошенники представляются сотрудниками службы безопасности банков или правоохранительных органов. Звонящий сообщает о попытке взлома или

блокировки банковской карты, подозрительных действиях в интернет-банке, пропущенном платеже по кредиту или угрозе штрафа по надуманному обвинению. На самом деле сотрудники служб безопасности банков никогда не звонят клиентам, а о подозрительной деятельности или других проблемах сообщают другими способами.

Как вести себя во время разговора с незнакомым человеком?

Получив звонок от незнакомого человека, обратите внимание на то, что и как он хочет вам сообщить. Мошенники стремятся теми или иными способами надавить на жертв — торопить, запутывать, угрожать возможными последствиями. В такой ситуации важно сохранять спокойствие. Даже если вам угрожают потерей всех денег на счетах, не спешите выполнять требования звонящего.

Также мошенник может несколько раз подряд задавать жертве вопросы, на которые можно ответить только словом «да». Столкнувшись с такими вопросами, старайтесь давать другие ответы, переспрашивать или переводить тему.

Если вам звонят из банка — попробуйте задать уточняющие вопросы, например, о состоянии счета или последних операциях по карте. Скорее всего, злоумышленник ничего не сможет ответить. Если вам предлагают какую-либо выплату — уточните основание, на котором она производится.

Какую информацию нельзя сообщать собеседнику по телефону?

Мошенники стремятся получить секретные данные карты — трёхзначный код CVC/CVV с обратной стороны, коды подтверждения из SMS, логины и пароли от интернет-банков. Настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства. Для отправки платежа нужен только номер карты — другие данные для этого не нужны.

Если вы столкнулись с телефонным мошенничеством — как можно скорее обратитесь в полицию, даже если вы не отправляли деньги или данные карты. В заявлении подробно опишите обстоятельства происшествия — время звонка номер телефона, ФИО и «должность» звонящего, содержание и итог разговора, если вы переводили деньги — отправленную сумму. В качестве основания укажите статью 159 УК РФ (если мошенник смог получить от вас деньги) и часть 3 статьи 30 УК РФ (если этого сделать не удалось). Если у вас есть запись звонка (его можно записать с помощью специального приложения) — приложите ее к заявлению.

Заявление будет рассматриваться в течение 10-30 дней. По итогам будет принято решение о возбуждении уголовного дела. Если вы получили отказ, то можно обжаловать его в прокуратуре — для этого потребуются копия заявления и постановление об отказе.

Как обезопасить пожилых людей от телефонных мошенников?

Очень часто от мошеннических звонков страдают пожилые люди.

Злоумышленники пользуются их доверчивостью и незнанием нюансов работы банков или других организаций. Чтобы обезопасить близких от подозрительных звонков, напоминайте им об основных правилах безопасности:

Никому не сообщайте код с обратной стороны карты, коды из SMS, данные для входа в интернет-банк;

Для перевода денег используйте только официальные сервисы банков, платежных систем и торговых площадок;

Не перезванивайте по незнакомым номерам, даже если вам поступил звонок, который был сразу же сброшен;

Звоните в банки и государственные структуры только по их официальным номерам;

Не переходите по подозрительным ссылкам, которые отправляют звонящие;

Если вам позвонили якобы из банка и сообщили о блокировке или других проблемах с картой — сбросьте звонок и перезвоните в банк сами;

Если вам предлагают получить какую-либо выплату — не соглашайтесь на нее сразу, а поищите информацию о ней в других источниках;

Если вы потеряли карту или сообщили подозрительному человеку ее номер — сразу же заблокируйте ее и запросите перевыпуск.

В общем — будьте бдительны и не станете жертвами телефонных мошенников.

Разъяснение, провел Зам.Льговского межрайпрокурора советник юстиции А.В. Иванов.