Позвони мне, позвони: как действуют телефонные мошенники

Ещё пару десятилетий назад мы с удивлением смотрели фантастические фильмы о злобных компьютерных хакерах, взламывающих счета американских банков, и не предполагали, что технический прогресс дойдёт до такого уровня, что это станет реальной проблемой. Обычные кнопочные телефоны сменились передовыми планшетами и смартфонами, а опытные телефонные мошенники иногда зарабатывают на обмане столько, сколько не снилось ни одному хакеру.

В России не первый год говорят о проблеме телефонного мошенничества и о том, что ситуацию необходимо решать на государственном уровне. Только за прошлый год почти 150 миллиардов рублей выманили онлайн-мошенники со счетов россиян. Цифра сравнима с годовым бюджетом целого Ставропольского края. Поймать злоумышленников нелегко: они работают с подставными номерами. По данным МВД, в 2020 году зарегистрировано 510 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 73% больше, чем годом ранее. Суды назначают до 5 лет лишения свободы за подобные деяния. Но, как показывает практика, этого недостаточно. Стоит отметить, что современные аферисты используют самые разные методики выманивания денег у граждан, от сообщений о выигрышах до просьб о помощи «попавшим в беду родственникам». Так, за последний год мошенники-«звонари» предлагали россиянам ложные банковские услуги (38%), банковские карты (27%), кредитование (8%), предложения перечислить денег (5%), а также информировали о призах и медицинских услугах (по 3%). Но какой бы ни была сказочная история, мошенники всегда стремятся создать для своей жертвы стрессовую ситуацию, либо надавить на жалость, либо даже запугать, что подталкивает людей к немедленному принятию необдуманных решений.

Кто попадается?

Кто же чаще всего по статистике становится жертвой телефонных вымогателей? Это, как ни странно, финансово благополучные люди, которые легко расстаются с деньгами и доверяют высоким технологиям. Школьники и студенты, домохозяйки и пенсионеры. Несмотря на то, что частная жизнь и права граждан должны оберегаться государством, их личные данные по-прежнему попадают к преступникам из-за утечек баз данных, недобросовестных операторов, халатности или злого умысла сотрудников, имеющих к ним доступ. Базы телефонов, паспортные данных и другие сведений россиян утекают от сотрудников банков, операторов, коллекторских агентств. Мы с периодичностью раз в месяц, а то и чаще читаем в СМИ, как был взломан тот или иной сервер банка или мобильного оператора, а сведения попали в общий доступ. Найти жертву, ее номер и личные данные сейчас не проблема. На черном рынке их продажа поставлена на поток.

Как отмечается в исследованиях «Лаборатории Касперского», почти каждый десятый россиянин (около 9%) терял значительную для себя сумму денег из-за телефонного мошенничества, а каждый третий (33%) признался, что он или его близкие сталкивались с таким мошенничеством. При этом лишь 4% граждан обращались в правоохранительные органы с целью привлечь к ответственности грабителей.

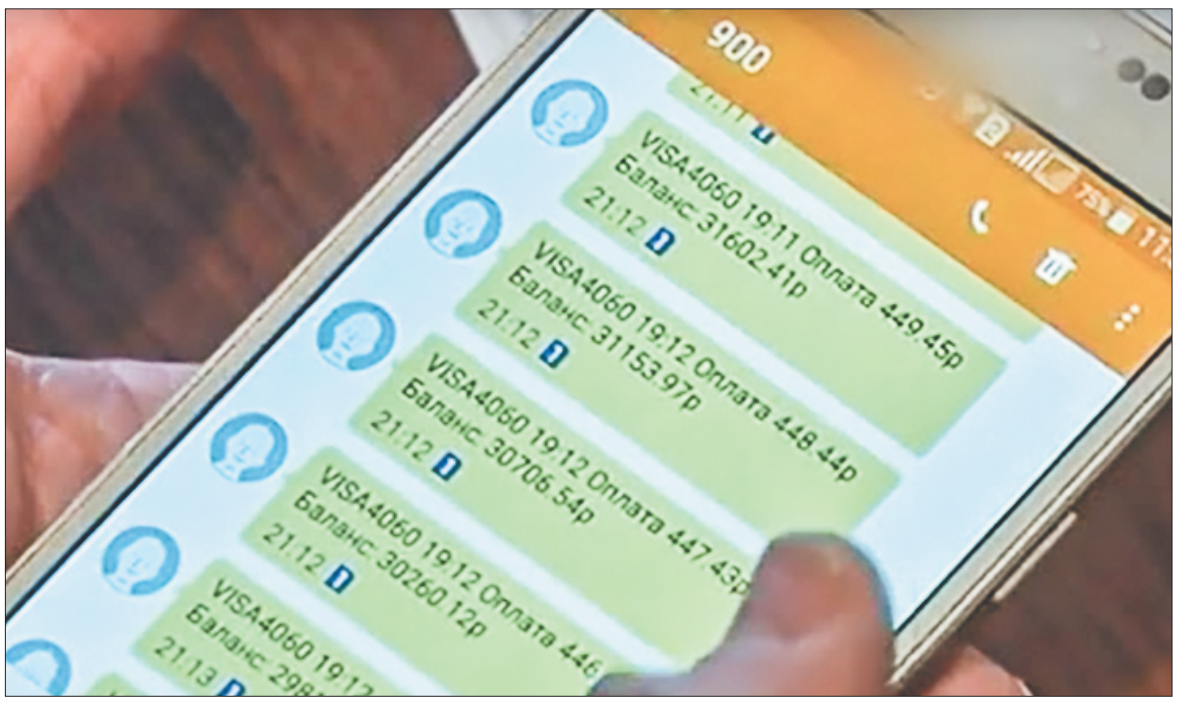
В интернете можно найти множество достоверных фактов и историй обманутых граждан. Вот, например, в роли жертвы – пожилая пара инженеров. Об этом случае написала на своей странице в Facebook родственница пострадавших Ирина Цвей.

По словам Ирины, с пенсионерами связался по телефону мошенник, который сказал, что фирма, где пожилые люди когда-то покупали БАДы, разорилась, и якобы теперь им полагается компенсация в 350 тыс. руб. Но для того, чтобы ее получить, старики должны заплатить за ячейку, хранение, страховку, перевоз денег. И добавил, что если они немедленно не переведут деньги на указанную карту, у них «отнимут пенсию».

После этого разговора мужчина звонил пенсионерам каждый день, и каждый день они переводили определенную сумму. За месяц они перечислили все свои деньги, накопленные за 52 года работы. О мошенничестве стало известно, когда пожилые люди обратились за помощью к родственникам – им не хватало на очередной ежедневный платеж.

Вот недавний пример из СМИ. Жертвой телефонных мошенников в Удмуртии стал 30-летний житель Алнашского района. Как сообщили в пресс-службе МВД по Удмуртии, мужчина поверил в популярную легенду злодеев и лишился почти 1 млн руб.

По версии следствия, потерпевшему позвонил незнакомец, который представился сотрудником Центробанка и попросил подтвердить заявку на оформление кредита в размере 500 тыс. руб. Удивленный мужчина ответил, что не подавал подобной заявки, после чего получил предложение оформить «зеркальный кредит» на полмиллиона, чтобы предотвратить незаконную операцию. Он послушался звонившего, выполнил его указания и перевел полученные деньги на указанный счет. В течение ближайших дней мужчине еще несколько раз звонили незнакомцы, которые, представляясь сотрудниками банков и правоохранительных органов, под схожими предлогами убеждали его оформлять новые кредиты и переводить деньги на якобы безопасные счета.



«При этом злоумышленники контролировали все действия потерпевшего, а также его местонахождение. В общей сложности мужчина перевел на различные счета 988 000 рублей», – говорится в сообщении.

Кто они?

Так кто они, мошенники-аферисты, которые звонят под видом сотрудников банков и правоохранительных органов и даже лжемедиков и соцработников?

Если говорить об уже известных и изученных органами схемах, то в московском управлении МВД выяснили, что 50–60% звонков идут с территории Украины, то есть «черные» колл-центры находятся в этой стране, которая разорвала с Россией соглашение об обмене правовой информацией. Наши оперативники устанавливают местоположение преступников, но привлечь их к уголовной ответственности не могут. Как отмечают СМИ, проводившие свое расследование, подобные колл-центры – это целая индустрия на Украине. На территории страны, по предварительным данным, более 30 таких центров. В одном работает в среднем 20 человек в смену. Оттуда лжесотрудники банков и иные работники «добрых услуг» делают около 100 тысяч звонков в сутки. Денежный оборот одного такого колл-центра составляет примерно 65 млн рублей в месяц.

Еще одна часть «звонарей», как ни странно, работает из мест отбывания наказаний. Так заключенные иногда коротают свободное время. Несмотря на то, что пронос телефонов на территорию следственных изоляторов, колоний и тюрем в России строго запрещён, истории создания тюремных колл-центров – не редкость.

Как отмечал в 2016 году заместитель главы ведомства ФСИН Анатолий Рудый, за 2015 год ведомством было зарегистрировано аж 1238 случаев телефонного мошенничества, зафиксированных в местах не столь отдаленных.

Как это работает?

Как это работает в тюрьмах и с какими вопросами вам могут звонить заключенные? Самое популярное – это рассылка сообщений с провокационными текстами, о которых все уже наслышаны: «Мама, попал (а) в больницу, срочно нужны деньги, переведи по этому номеру». Кроме этого, мошенник может звонить жертве, представляться сотрудником банка, пугать её несуществующими подозрительными операциями, а потом предлагать перевести деньги на заранее подготовленный якобы резервный и безопасный счёт. Ещё заключённые делают СМС-рассылку. Текст стилизуется под формат банковских уведомлений. Зачастую это сообщение о неожиданном списании денег. От уведомления кредитной организации такое смс отличается только одним – просьбой перезвонить по озвученному номеру для отмены операции. Ещё в одном случае мошенник ищет представителей самой уязвимой категории граждан – пожилых людей. Он также представляется сотрудником банка и под разными предлогами убеждает жертву вместе с ним пройти регистрацию в онлайн-банке. Разумеется, когда человек делает всё под диктовку, мошенник автоматически получает доступ к личному кабинету жертвы.

Если с украинскими мошенниками борьба пока продолжается на международном уровне, то ситуацию отечественных тюремных колл-центров всё-таки взяли на особый контроль. Еще в ноябре прошлого года из тюрем фиксировалось около 2200 звонков в день. В марте 2021 года президент Владимир Путин подписал закон, позволяющий руководству региональных управлений Федеральной службы исполнения наказаний (ФСИН) блокировать номера мобильной связи в местах лишения свободы, и количество звонков из тюрем сократилось в разы.

Как уберечь себя и близких от телефонных мошенников, что для этого нужно делать? Согласно опросу, каждый пятый россиянин (21%) никак не защищает свой телефон от подозрительных звонков. Половина респондентов (51%) ответили, что не берут трубку, если видят на экране неизвестный номер. Еще 17% россиян используют специализированное ПО для защиты от спама и мошенничества, а 37% – встроенные возможности телефона, например, черные списки.

Что делать?

Ну а если же подозрительный звонок все-таки поступил к вам, то существуют уже отработанные правила, которые необходимо запомнить:

Никому не говорить реквизиты банковской карты, не говорить и не показывать трехзначный CVV-код на обратной стороне карты.

Прислушаться к наставлению из банковских SMS: «Никому не сообщайте код».

Не хранить на телефонах и на устройствах, не защищенных антивирусами, фотографии паспортов, карт и других личных документов. По возможности не пересылать их по Интернету: так их воруют хакеры.

Не стоит вводить данные карты на подозрительных сайтах.

Даже если звонят с «настоящего» номера банка – проверить его. Подстраховаться можно так: перезвонить, но не выбрав номер из последних вызовов, а набрав его вручную.

Не используйте простые и короткие пароли. Усложняйте их числами, символами и заглавными буквами.

Подключите двухфакторную аутентификацию. Это система, при которой, помимо стандартных логина и пароля, требуется вводить код из СМС.

Не открывайте вложения из писем от неизвестных отправителей и не переходите по ссылкам из таких писем.

Также не стоит переходить по ссылкам через рекламные баннеры в интернете, которые предлагают поучаствовать в лотерее, пройти опрос за вознаграждение или получить его.

Мария Климанова,
по материалам СМИ