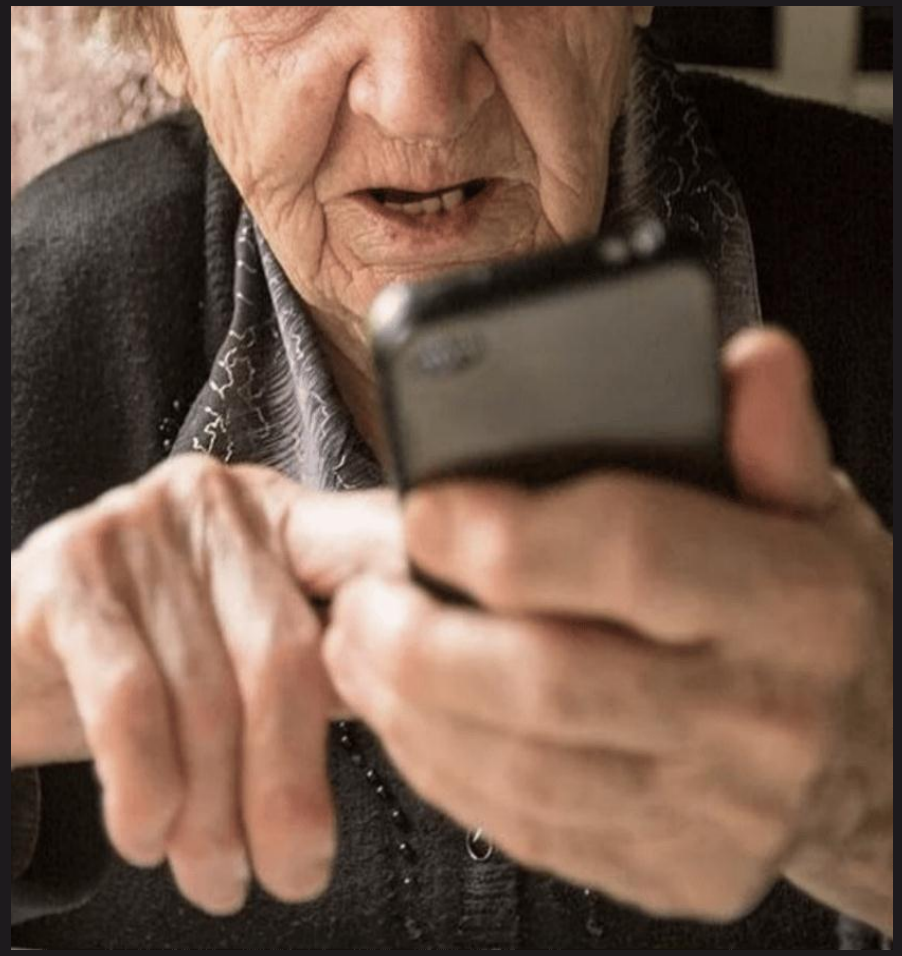
ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Профессор Департамента информационной безопасности
д.т.н., доцент

С. И. Козьминых

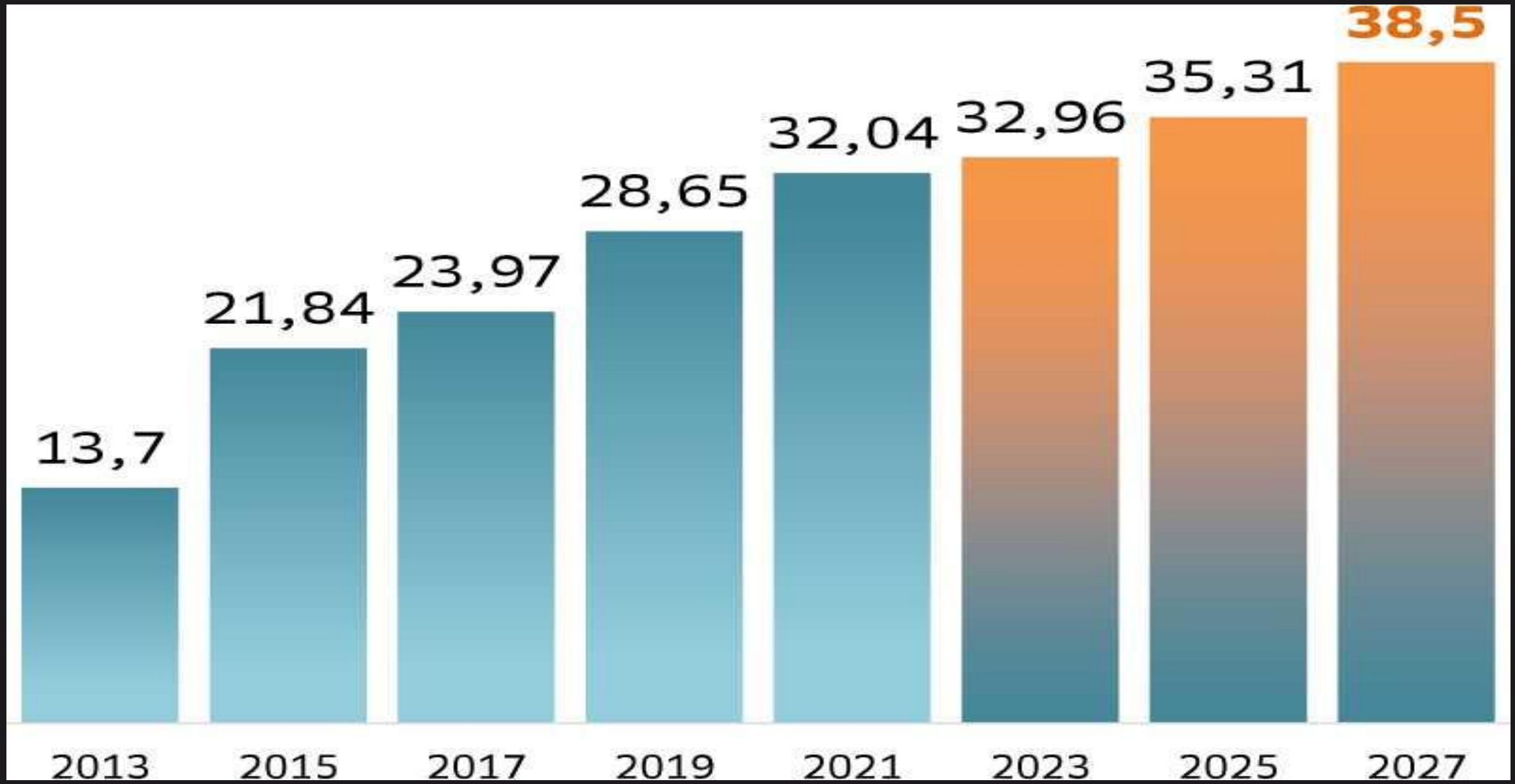
«Телефонное мошенничество в Российской Федерации»



С тех пор, как в нашей стране стала массово внедряться мобильной связь, появились телефонные мошенники. Сначала звонили «операторы связи» и грозили отключить телефон, если абонент не направит СМС сообщение, которое присылал мошенник. При этом все деньги с телефона переводились на телефон мошенника. Но как правило на счете телефона не хранили большие суммы, поэтому мошенники стали придумывать новые схемы отъема денег.

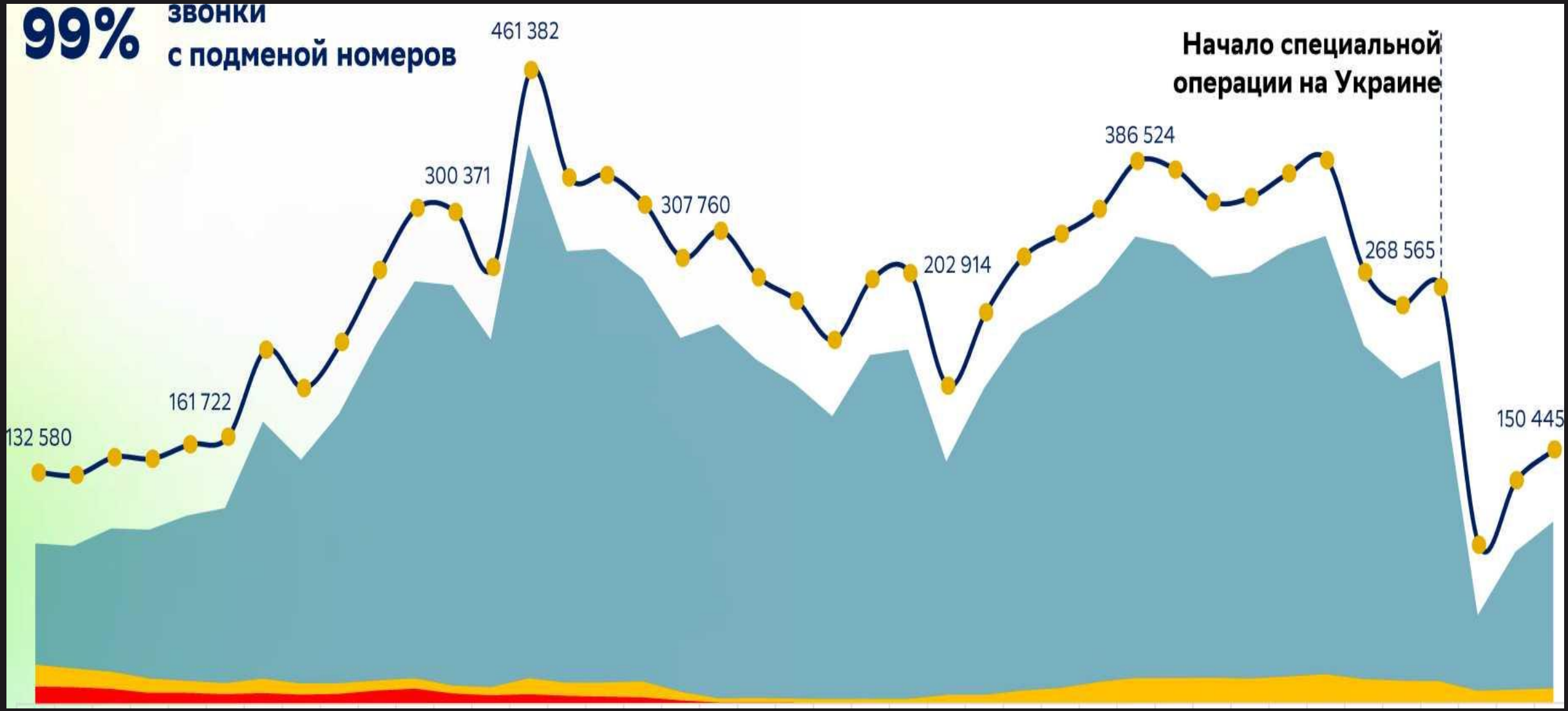
Тренды кибермошенничества с каждым годом меняются. Ранее преобладало вирусное заражение через установку вирусного программного обеспечения и СМС-банкинг. Скимминг - мошенничество посредством банкоматов – ушел в историю. А вот фишинг - техника, используемая для кражи личных данных (логина, пароля, цифр на банковской карте) - остается рабочей схемой мошенников. Социальная инженерия сейчас является основной в кибермошенничестве, так как на человека воздействовать проще, чем технически разрабатывать вирусы и приложения. Прогноз мировых потерь от кибермошенничества к 2027 году может составить 38 млрд.$

Прогноз мировых потерь от кибермошенничества в млрд.$



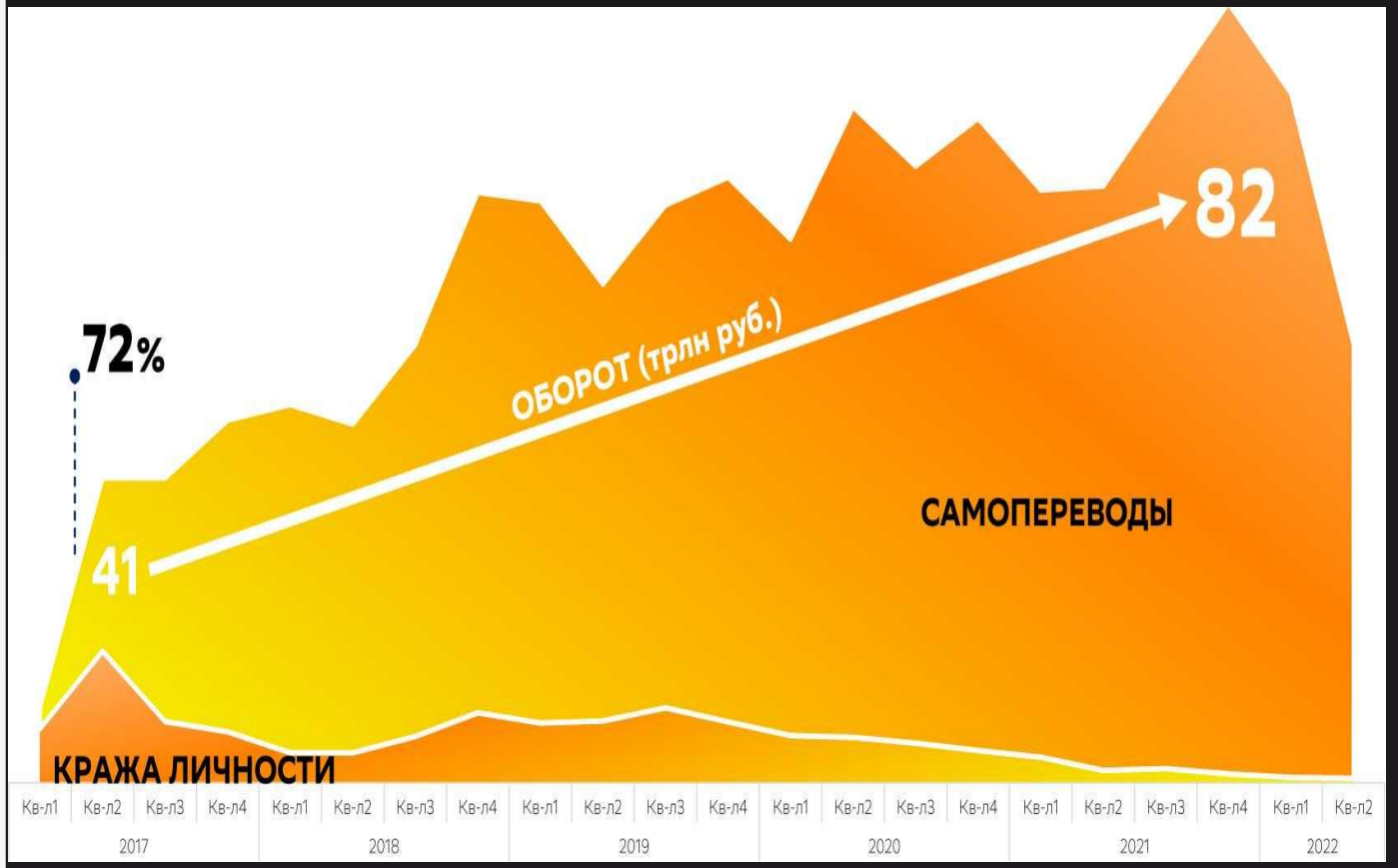
Социальная инженерия - метод, который используют мошенники, чтобы заставить сообщить данные, необходимые для хищения. Для этого организованы специальные контактные центры и офисы с IP-телефонией. Как правило, звонят «сотрудник» службы безопасности банка, представитель государственных органов, предупреждают об оформлении кредита, изменении номера телефона, попытке кражи средств со счета, сообщают о расследовании дела в отношении клиентского менеджера банка. По данным СБЕРа социальная инженерия применяется в 94 % случаев кибермошенничества. Ежемесячно в России совершается несколько сот тысяч мошеннических телефонных звонков.

Телефонное мошенничество в РФ в период с 2019 по 2022 год.

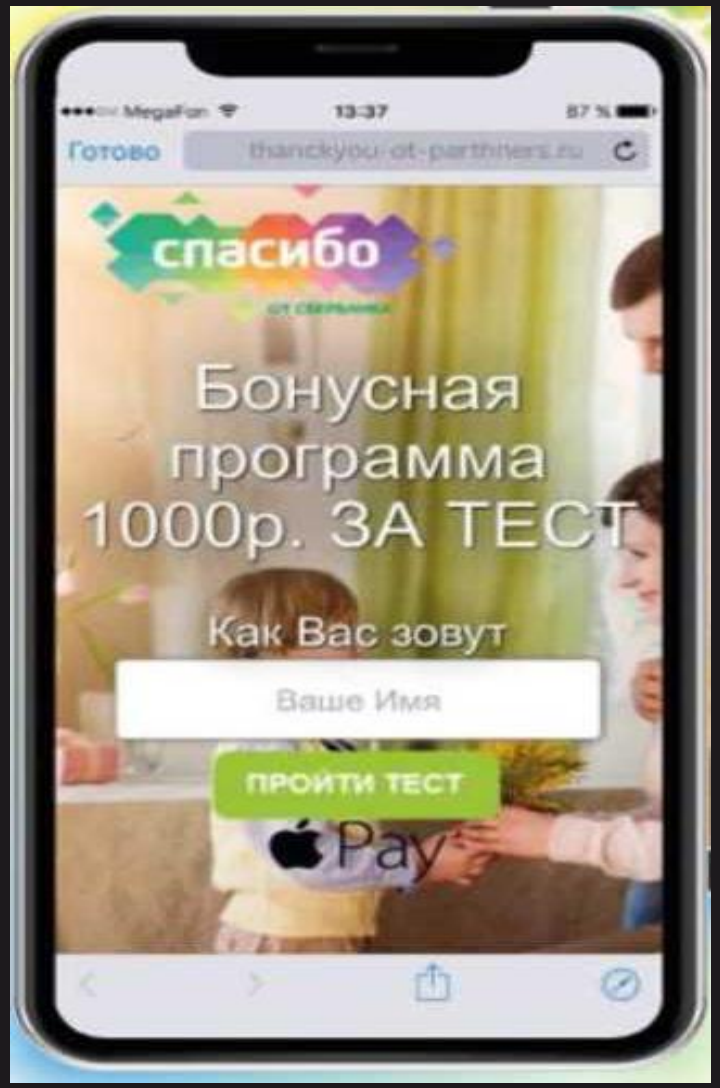


Итог основных результатов действий мошенников при контакте с жертвой социальной инженерии — «самоперевод» (когда клиент самостоятельно переводит деньги под давлением мошенника) и кража личности (злоумышленник получает необходимые данные для перевода на своем устройстве из аккаунта жертвы).

В 99 процентов случаях происходит подмена номера телефона с которого звонят мошенники и поэтому определить от куда они звонят достаточно сложно. Подобные преступления раскрываются очень редко это стимулирует увеличение данного рода схем.



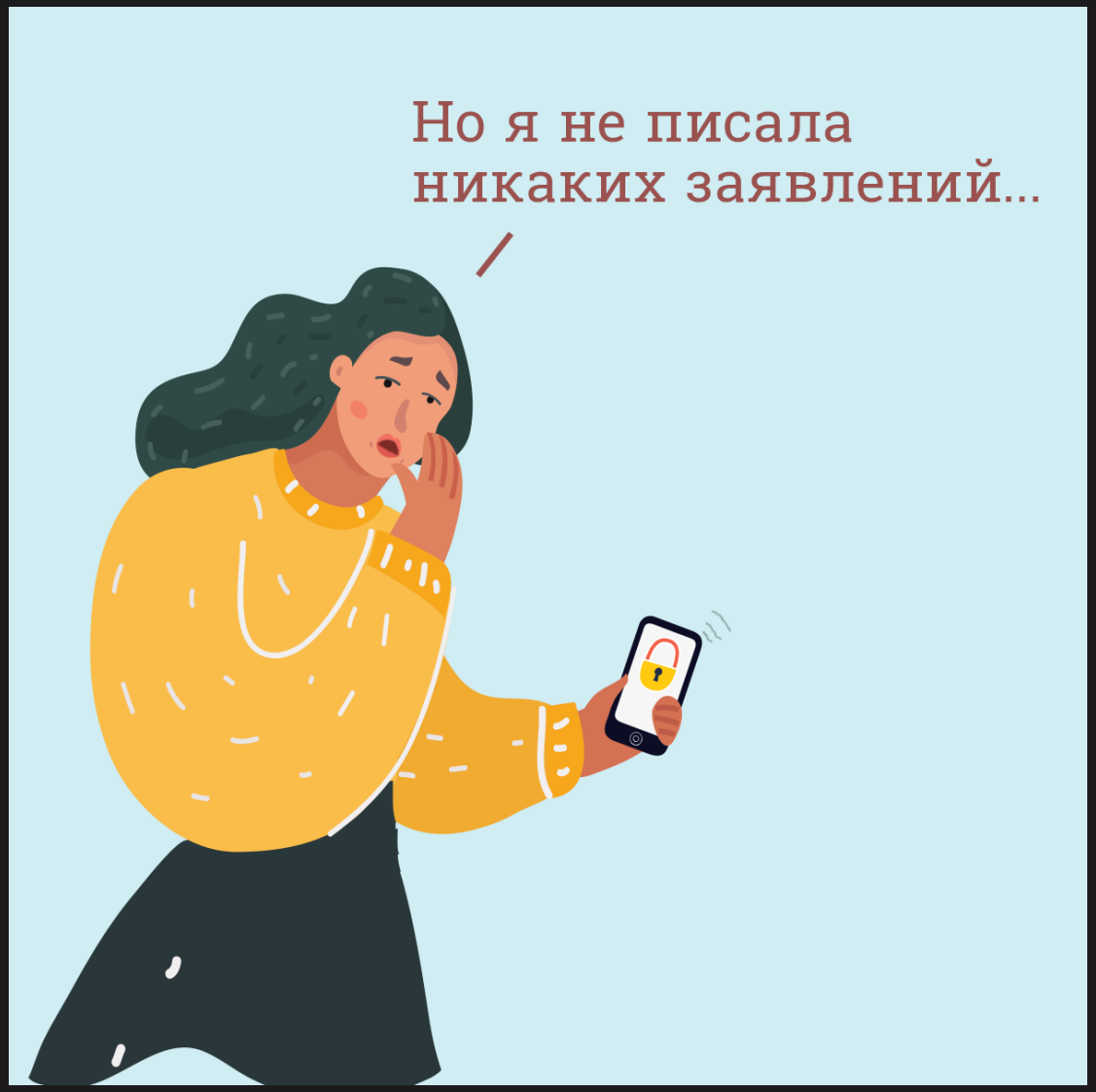
8



Вам на телефон приходит фишинговая рассылка - письмо, в котором написано, что вам полагается приз, если вы правильно выберете коробочку на интерактивной картинке и вам дается три попытки. Первые две попытки как правило не удачные, а третья открывает приз со значительной суммой денег. Вы счастливы и уже думаете куда их потратить. Но для того, чтобы получить приз вы должны ввести номер вашей карты, на которую переведут деньги. Приз вы, конечно, не получите, а вот данные карты позволят мошеннику снять с нее деньги. Как говориться: «Бесплатный сыр бывает только в мышеловке». Надо всегда об этом помнить. Иногда приходят предложения пройти тест, за который вам полагается 1000 руб. В ходе теста вы должны заполнить свои персональные данные, а для получения денег ввести номер карты. Результат будет тот-же.

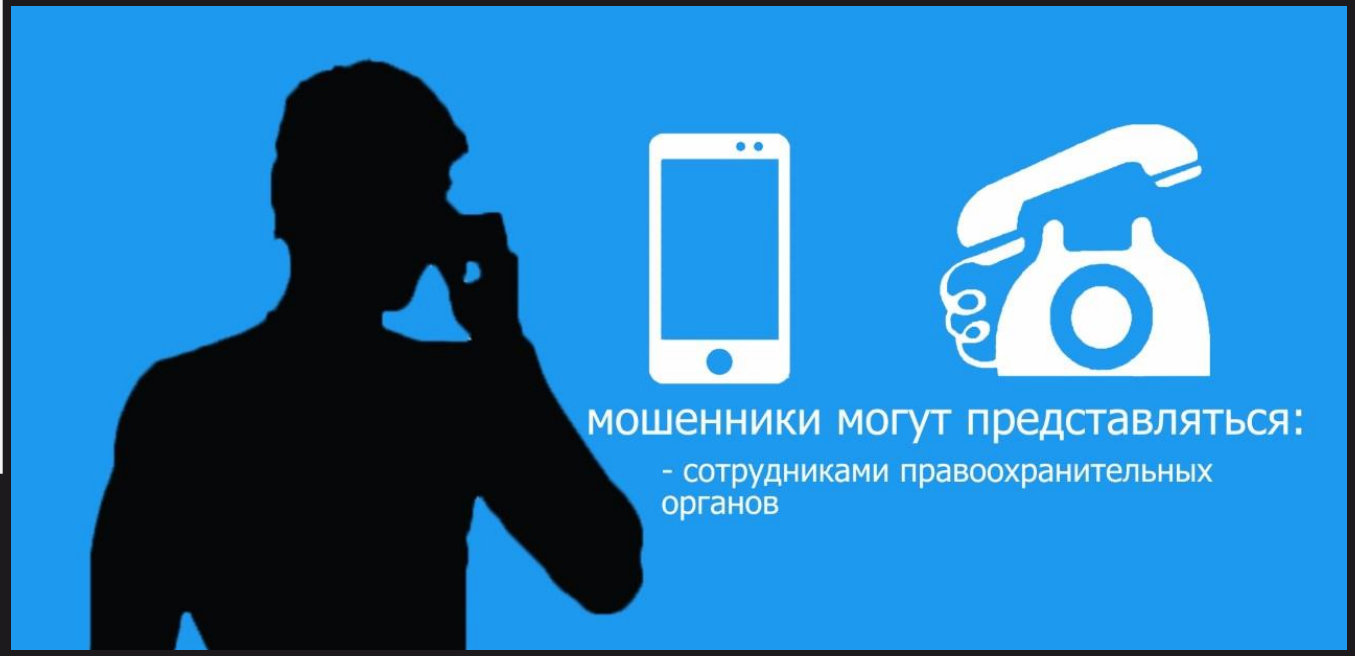
Звонит «оператор банка» или сотрудник службы безопасности. С вашего счета пытаются снять деньги, их надо срочно перевести на другой счет. Клиент начинает нервничать, на него давит мошенник и он переводит деньги на неизвестный ему счет и теряет их окончательно. Известен случай, когда мошенники таким путем завладели 300 млн. рублей. Женщина целую неделю под руководством мошенника снимала деньги со счета и через платежный терминал переводила их на неизвестный ей счет, а муж помогал ей это делать. Мошенников так и не поймали. Это классика социальной инженерии, это как надо было запудрить мозги, чтобы заставить добровольно отдать такие деньги!

Что делать. Помнить, что из банка звонят клиентам только чтобы что бы предложить новые услуги банка. Кстати, об услугах банка можно ознакомиться на его сайте. В остальных случаях никто звонить не будет. Если есть сомнения по поводу несанкционированного доступа к счету, надо срочно позвонить в банк и заблокировать карту или счет. Телефон на оборотной стороне вашей карты. В целях защиты ваших денег можно скрыть данные вашей карты и счета. СБЕР предоставляет такую услугу и это можно сделать из вашего личного кабинета, тогда мошенники вообще не смогут получить доступ к вашим деньгам.



Еще пример. Звонит «оператор банка» или сотрудник службы безопасности и сообщает, что на ваше имя пришел запрос на оформление кредита. В ходе выяснения ситуации мошенник умело выясняет ваши персональные данные, данные вашей карты, номер счета и потом использует эти данные для кражи денег. Конечно, ни один банк по телефону не решает вопросы выдачи кредитов, если вам звонят по этому вопросу, это мошенник.

Другой вариант. Звонит сотрудник службы безопасности и просит вас помочь поймать нечестного сотрудника банка и когда он позвонит сыграть с ним в игру «переведи деньги». Если вы пойдете навстречу этому сотруднику, то тоже попрощаетесь со своими деньгами. Иногда мошенники наглеют на столько, что после того, как вы потеряли деньги опять звонят вам от имени правоохранительных органов и предлагают еще перевести деньги на указанный счет, чтобы поймать преступников и вернуть вам все что вы перевели. Результат уже понятен.



Раньше присылали СМС «мама положи деньги на этот телефон», теперь вам звонит ваш сын, дочь, внук или близкий друг, говорит, что у него сел телефон, поэтому он звонит с чужого и просит срочно на этот телефон или по номеру телефона перевести деньги на счет, так как он якобы попал в какую-нибудь сложную ситуацию: попал в автоаварию, сбил человека, сломал ногу, кончился бензин или что-то подобное. Современные технологии позволяют подделать любой голос. Вспомните наших знаменитых пранкеров Лексуса и Вована. Эти технологии стали широко доступны, и жулики их уже используют их для отъема денег у населения. В этом случае не торопитесь переводить деньги. В ходе разговора задайте пару вопросов, ответы на которые знает только тот, от чего имени звонят. Кличку собаки, любимое место встреч, девичью фамилию матери или еще что-то личное. Попробуйте дозвониться, тому кто звонил. Главное не принимайте скоропалительных решений, и вы выведете жулика на чистую воду.

А вот еще один способ завладеть вашими деньгами. После того как мошенник получили доступ к вашим данным, через знакомого оператора связи оформляет сим карту на ваш номер телефона и таким образом получают доступ к вашему мобильному банку, дальше не требуется много времени, чтобы перевести деньги с вашего счета. Как только активируется другая сим-карта ваш телефон перестает работать, и вы не узнаете о том, что у вас крадут деньги. Как защититься в такой ситуации? Прежде всего не разглашайте свои данные, сразу как у вас отключился телефон, необходимо заблокировать карту, это можно сделать с любого телефона. Можно скрыть данные карты и счета. Можно ограничить переводы с вашей карты, посчитайте сколько вы тратите в день, обратитесь в банк, и он ограничит сумму ежедневных переводов. Помните, что ежемесячно в России совершается несколько сот тысяч мошеннических телефонных звонков.

Как еще мошенники могут получить доступ к вашему телефону. Вам звонит «оператор» мобильной сети и сообщает, что видимо к вашему телефону мошенниками подключена переадресация. Для отключения пере-адресации вам предлагают послать нужную команду, в Билайне на теле-фоне надо послать: *110*031#. В Мегафоне послать команду **21#. При направлении такой команды вы сами подключаете переадресацию на теле-фон мошенника и при этом все СМС будут приходить к нему, и вы не узнаете, когда с вашего счета будут сниматься деньги.

Можно было бы привести еще несколько примеров, но все они сводятся к одному - желанию мошенника залезть в ваш кошелек, получить доступ к карте или счету, заставить вас перевести ваши деньги на чужой счет. Если вас просят перевести деньги на незнакомый счет представьте, что, вы вынули из кармана кошелек с деньгами и отдаете его незнакомцу. У людей часто деньги на карте не ассоциируются с «живыми» купюрами, они легче тратятся. Если хотите сэкономить, снимите деньги, положите в конверт и записывайте расходы. Тратить живые деньги жалко, а с карты не очень.

Последний совет. Не отвечайте на незнакомые звонки и СМС сообщения. У вас есть список ваших абонентов и если звонит кото-то незнакомый, то лучше всего с ним вообще не разговаривать. Установите на теле-фоне программу WhoCalls (кто звонит) ее бесплатно можно скачать на Google Play. Эта программа подскажет вам что идет массовый обзвон или звонят из Свердловской области, где у вас нет знакомых. Назойливые звонки и СМС сообщения заносите в черный список, обозначайте как спам, блокируйте на своем телефоне. Помните враг не дремлет и с ним надо уметь бороться.

Чего ожидать в будущем? Дальше будет еще круче. Недавно по телевидению был показан ролик Мегафона с участием Азамата Мусагалиева и помолодевшего Брюса Уиллиса, вот только один из самых высокооплачиваемых актёров мира на съёмочную площадку так и не приехал - вместо этого разработчики проекта использовали его образ, который был «нарисован» нейросетями для наложения на кадр (Deepfake). Искусственный интеллект с использованием нейросетевых технологий уже используется для производства рекламы. А дальше его могут взять на вооружение злоумышленники. Они уже освоили подмену телефонных номеров, осваивают подмену голоса и скоро освоят подмену изображения. И тогда вам с телефона вашего сына на смартфон поступает видеозвонок, мошенник с лицом сына (смонтированным по фотографиям из соцсетей) и его голосом слезно просит срочно перевести деньги на его телефон, вряд ли вы откажите. Но деньги, которые вы пошлете сыну скорее всего попадут к мошеннику - подумайте заранее, как этому можно будет помешать (например, придумать кодовое слово для общения с родственниками).

СПАСИБО ЗА ВНИМАНИЕ