История первая: «Поддержите разработку вакцины от коронавируса»

Валентина, Санкт-Петербург:

«Вчера получила письмо от Всемирной организации здравоохранения. В теме было написано «Разработка вакцины от коронавируса». Я заинтересовалась, открыла письмо. В нем говорилось, что ученые всего мира активно работают над вакциной и лекарством от коронавируса, а ВОЗ курирует эту работу. Но разработка очень дорогая, поэтому всем неравнодушным людям предлагается поддержать исследования. Было написано, что пожертвовать можно любую сумму, даже совсем небольшую. И дальше ссылка на сайт, где это можно сделать. Я решила не оставаться в стороне и перевести 300 рублей. Перешла по ссылке, ввела данные карты, сумму и нажала «оплатить». Списали 300 рублей. А потом еще несколько раз подряд разные суммы, пока все деньги на карте не кончились. Получается, это были аферисты, а никакая не Всемирная организация здравоохранения?»

Комментарий эксперта

Довольно часто мошенники активизируются во время стихийных бедствий, техногенных катастроф и эпидемий. Они призывают людей делать пожертвования якобы для помощи пострадавшим. Часто обманщики маскируются под официальные организации.

Легенды могут быть самыми разными. В случае с коронавирусом махинаторы также предлагают купить медицинские маски, супердезинфицирующее средство, лекарства, вакцину и даже амулеты, которые защищают от любых болезней.

В некоторых случаях мошенники даже не призывают переводить деньги или что-то покупать. Они просто направляют письмо или сообщение, в которых дают ссылку на самые актуальные рекомендации, как защититься от коронавируса, от имени авторитетных организаций.

В действительности обманщики используют ситуацию в своих интересах — украсть деньги с карты либо получить доступ к персональным данным, сообщениям и банковским приложениям человека, который попался на их крючок.

Махинаторы создают специальные фишинговые сайты, которые собирают личные данные и платежные реквизиты пользователей. Такая информация позволяет им обнулить чужие счета.

Вместо рекомендаций по борьбе с коронавирусом человека, скорее всего, ждет вредоносная программа. Она проникнет в телефон, планшет или компьютер и получит доступ к конфиденциальным данным — например, к паролю от онлайн-банка.

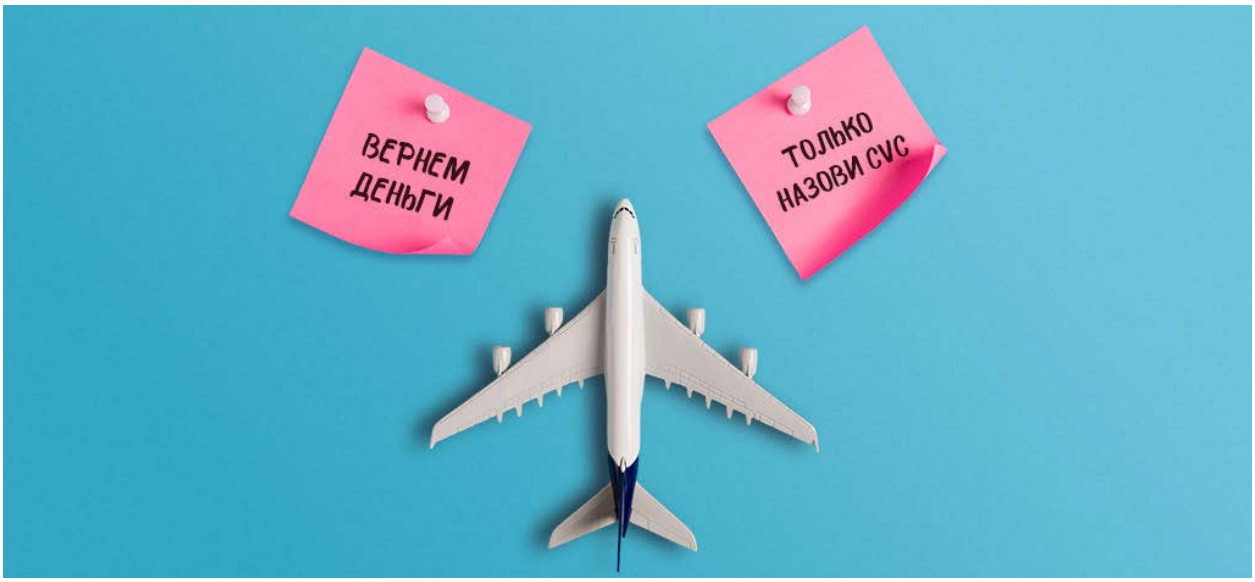
Если вам предлагают внести пожертвование на счет какой-либо известной организации, необходимо зайти на ее официальный сайт и убедиться, что она действительно проводит сбор денег. На сайте должны быть указаны реквизиты организации или ссылки на страницы, где деньги можно перевести безопасным способом.

В случаях, когда организация или интернет-магазин вам неизвестны, стоит сначала поискать информацию и отзывы о них в интернете.

Чтобы не попасться на уловки преступников, необходимо соблюдать и другие правила кибербезопасности:

- Не переходите по ссылкам из писем незнакомых отправителей.
- Проверяйте адресную строку сайта — часто фишинговые сайты отличаются от официальных всего одной-двумя буквами.
- Используйте отдельную карту для онлайн-платежей и кладите на нее нужную сумму непосредственно перед покупкой.
- Установите на все свои устройства антивирус и регулярно обновляйте его. Хороший антивирусный пакет включает защиту от спама и фишинговых писем. Он сам распознает подозрительных адресатов.
- Если преступники уже получили данные вашей карты, заблокируйте ее и попросите банк выпустить новую.

История вторая: «Отменился рейс из-за коронавируса? Мы вернем деньги»



Георгий, Санкт-Петербург

«Поступил звонок с номера, который начинается с 800. Девушка представилась сотрудницей известной авиакомпании. Сказала, что мне вернут деньги за рейс в Черногорию, который отменили из-за эпидемии коронавируса. А я как раз узнал, что мой рейс отменили и хотел заняться вопросом возврата денег. Она назвала номер рейса, номер моей брони и цену билетов. Я говорю: да, все верно. Очень обрадовался, что все деньги вернут и что сами позвонили.

Девушка спросила, куда мне перевести деньги, я сказал, что на карту. Тогда она попросила сначала номер карты, я ей продиктовал, а потом еще срок действия и три цифры с обратной стороны. Тут уже я напрягся, что у меня просят данные, которые нельзя никому сообщать. Но девушка настаивала, что для перевода нужен именно трехзначный код. Я сказал, что она мошенница и бросил трубку. Буду теперь сам звонить в авиакомпанию и выяснять, когда вернут деньги за билеты. Не понял только, откуда у мошенников такие подробные данные о моих полетах?»

Комментарий эксперта

Мошенники всегда используют шумиху вокруг различных стихийных бедствий, эпидемий и глобальных потрясений, чтобы подзаработать. В стрессовых ситуациях у людей снижается бдительность, и злоумышленники этим пользуются.

Георгию удалось вовремя распознать обман. Если бы он сообщил «девушке из авиакомпании» полные данные своей банковской карты, включая секретные коды, то вместо возврата денег за полет лишился бы остатка на своем счете.

Для убедительности мошенники могут назвать ФИО, реквизиты паспорта, а в данном случае – даже номер рейса и стоимость билетов. Махинаторы добывают эту информацию сами из открытых источников (например, из соцсетей) или покупают у хакеров, которые продают базы данных на черном рынке.

Кибермошенники могли взломать электронную почту Георгия, на которую ему приходили письма с информацией о полете, либо подобрать доступ к его личному кабинету на сайте авиакомпании и взять данные оттуда.

Для возврата денег за отмененные рейсы необходимо обращаться напрямую в авиакомпанию. Вы можете написать сообщение через форму обратной связи на официальном сайте перевозчика либо позвонить по номеру горячей линии – он также указан на сайте.

Будьте бдительны: злоумышленники придумывают самые разные схемы, связанные с коронавирусом. Например, призывают собирать деньги на разработку вакцины, предлагают купить лекарства и медицинские маски по низкой цене, выдают себя за интернет-магазины и сервисы доставки еды.

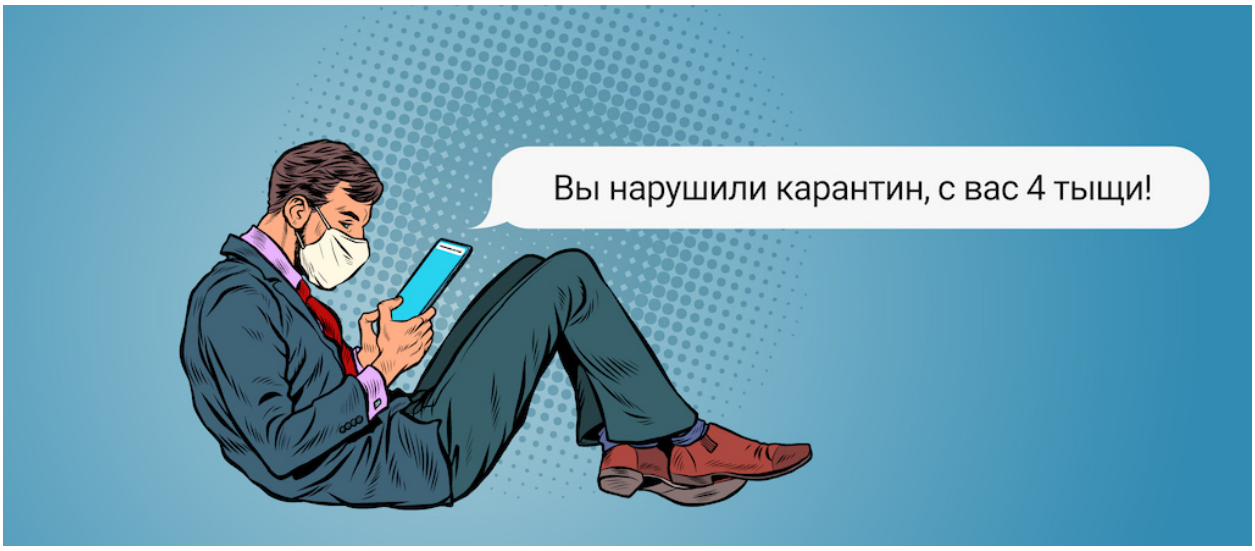
Также в последнее время в соцсетях предлагают пройти тест, который якобы поможет понять, есть ли у вас коронавирус. Результат таких опросов всегда один: «Вы в зоне особого риска!». Затем вам рекомендуют заказать противовирусные лекарства с доставкой – и все для того, чтобы узнать ваши персональные данные и реквизиты банковской карты.

Не дайте злоумышленникам себя обмануть и следуйте правилам финансовой безопасности:

1. Никому не сообщайте полные реквизиты банковской карты, особенно секретные коды, пароли из СМС и ПИН-коды.
2. Не используйте одинаковые пароли для входа в свои аккаунты на различных сайтах. Создавайте как можно более сложные пароли из комбинаций букв, цифр и символов.
3. Не переходите по ссылкам из писем незнакомых отправителей.
4. Не публикуйте в соцсетях конфиденциальную информацию о своих перелетах: например, посадочный талон, на котором виден код брони. Мошеннику будет достаточно этого кода и вашей фамилии для доступа к управлению вашим бронированием на сайте авиакомпании.

В любой ситуации старайтесь сохранять спокойствие и критично оценивайте сообщения от незнакомцев.

История третья: «Вы нарушили карантин, скиньте деньги на телефон»



Егор, Краснодар

«Я сижу дома на самоизоляции из-за пандемии. Вчера вечером получил прекрасное смс: якобы согласно моей геолокации, я нарушил режим карантина и должен оплатить штраф 4000 рублей. В смс мое ФИО и ссылки на всякие статьи из законов, постановление ФСИН и все такое. И если я не заплачу этот штраф за 24 часа, мне грозит уголовка. Фишка в том, что я уже неделю вообще никуда не выходил, работаю из дома, еду заказываю через интернет.

Самое смешное, что эти штрафные 4000 р. надо закинуть на какой-то номер мобильника. Да и причем тут ФСИН, думаю.

В общем, на всякий случай загуглил эту тему, естественно никакого такого постановления ФСИН № 168-322 от 10 апреля не существует.

Забавно, но ведь скорее всего, были люди, которые перекинули деньги мошенникам. Будьте бдительны!»

Комментарий эксперта

Мошенники понимают, что в период коронавируса ситуация нервозная, и используют любой информационный повод, чтобы запугать людей и украсть их деньги.

На этот раз махинаторы решили сыграть на эмоциях тех, кто нарушил режим самоизоляции. Обманщики разослали СМС-сообщения с требованием оплатить штраф, ссылаясь на выдуманные постановления.

К людям обращались по имени и отчеству якобы от имени государственной службы. На самом деле базы данных для подобных рассылок преступники покупают на черном рынке либо сами собирают информацию из открытых источников — например, социальных сетей.

Чтобы не дать мошенникам вас обокрасть, ни в коем случае не пересылайте незнакомцам деньги и не сообщайте полные реквизиты своей банковской карты (особенно трехзначный код с ее обратной стороны).

Будьте бдительны сами и обязательно предупредите близких, чтобы они всегда перепроверяли информацию, как поступил Егор.

Составлять протоколы о правонарушении и назначать штрафы могут только сотрудники органов исполнительной власти, например полиции. При оплате штрафа следует всегда внимательно проверять реквизиты получателя. Им не может быть частное лицо.

Если вы столкнулись с мошенничеством, звоните в полицию по номеру «02» со стационарного телефона или «102» с мобильного.

Это далеко не первая и наверняка не последняя схема обмана на фоне пандемии. Мошенники вымогают деньги и данные банковских карт и другими способами:

- Звонят людям от имени городских поликлиник и сообщают о плохих результатах анализов, а затем продают напуганным пациентам дорогие «лекарства». Позже люди обнаруживают, что купили обычные пищевые добавки.
- Сообщают, что человек якобы контактировал с зараженным и к нему выехали специалисты для проведения платного анализа на коронавирус. Просят заранее перевести 5 000 рублей за процедуру и, получив деньги, исчезают.
- Собирают деньги на разработку вакцины под видом Всемирной организации здравоохранения.
- Предлагают«компенсации» за отмененные рейсы от имени авиакомпаний в обмен на секретные данные банковской карты.

- Копируют популярные сайты: создают фишинговые страницы в интернете, маскируясь под сайты служб доставки, онлайн-магазинов, а также сервисов для видеоконференций.

История четвертая: «Возместим все, что у вас украли мошенники»

Лина, Красноярск

«Хочу поделиться своей историей. Надеюсь, она кого-то чему-то научит. Неделю назад я участвовала в онлайн-опросе, за который мне обещали 15 000 рублей. Оказалось, что это мошенники, с меня взяли комиссию 100 рублей, а потом сняли с карты все что там было — еще четыре тысячи с лишним. Я очень расстроилась и разозлилась, но сама была виновата. Написала на сайт онлайн-опроса гневные отзывы, напостила в соцсетях много информации об их схеме — предупредила всех, что это полный развод.

И вот вчера мне на мейл приходит письмо от Центра финансовой защиты. Пишут, что они возвращают деньги людям, которых мошенники обманули и обокрали в интернете. Я думаю, ураа, ну наконец-то. Перешла по ссылке на их сайт, вбила последние цифры с номера карты и нажала «проверить свою компенсацию». Высветилось, что мне дадут аж 50 000 рублей! Я подумала, что очень много, но там были отзывы людей, которые чуть ли не по 150 000 получили.

Потом открылся чат с юристом, Александр его звали. Надо было ответить на вопросы онлайн. Мы поговорили в чате, я рассказала, как меня обманули, сообщила ФИО и свой номер телефона. Он мне на это пишет, что для

оформления документов надо оплатить его услуги — 500 рублей, и скинул ссылку. Я перешла и оплатила.

Короче, это тоже оказался лохотрон!!! У меня с карты сняли сразу 3000 рублей и потом пытались снять еще какую-то сумму, но ее на карте не было уже! Я не понимаю, как так можно обманывать людей! Я звонила в банк, они сказали мне срочно заблокировать карту и писать заявление в полицию. Ребята, это ужас, два раза на одни грабли. Просто не знаю, что сказать. Не верьте никому в интернете!»

Комментарий эксперта

Схема двойного обмана довольно популярна. Мошенники предлагают компенсацию ущерба людям, которые уже пострадали от интернет-преступников. Но ничего не возвращают, а выманивают данные банковских карт и снова крадут с них деньги. Мошенники понимают, что если человек однажды поверил в небылицы махинаторов, то может сделать это снова.

Чаще всего они действуют от имени несуществующих организаций: «Центра финансовой защиты», «Единого центра возвратов» и других фейковых контор. Псевдоюристы мониторят жалобы в интернете или используют базы контактов, которые вели для других онлайн-лохотронов. А затем рассылают пострадавшим письма по электронной почте, через социальные сети и мессенджеры. В дополнение к этому запускают интернет-рекламу с поддельными скриншотами теленовостей и интервью с людьми, которые уже якобы получили возмещение.

Повод для «выплат» бывает каким угодно: от возврата потерь из-за участия в фейковых лотереях и опросах до налоговых вычетов, социальных субсидий и компенсации медицинских расходов.

Ссылки в сообщениях мошенников ведут на фишинговые сайты. Там людей убеждают в том, что им положены крупные суммы. Нужно лишь оплатить юридические услуги. Но когда пользователь вводит данные карты, преступники получают доступ к его счету и крадут все деньги.

Чтобы не дать мошенникам себя обмануть, следуйте правилам кибергигиены:

- Никому не сообщайте полные реквизиты банковской карты, особенно секретные коды, пароли из СМС и ПИН-коды.
- Не переходите по ссылкам из писем незнакомых отправителей.
- Не спешите переводить деньги неизвестным получателям по первому требованию.
- Не публикуйте в открытом доступе в соцсетях свои персональные данные: номер мобильного телефона, адрес, данные паспорта. Вся эта информация может быть использована против вас. Мошенники могут

оформить на ваш паспорт займы или кредиты, а также закидывать вас по телефону и почте «заманчивыми» предложениями.

История пятая: «В вашей кредитной истории произошли критические изменения»

Мария, Подольск

«Мне позвонили с незнакомого городского номера. Строгий автоматический голос сказал: «В вашей кредитной истории произошли критические изменения». И продиктовали адрес сайта, где можно узнать подробности. Название содержало сокращенное название бюро кредитных историй – БКИ. Я испугалась, что кто-то взял кредит на мое имя, и пошла на сайт проверять.

На сайте было указано, что они партнеры БКИ, и у них можно получить отчет по своей кредитной истории. Вбила там свои фамилию-имя-отчество, дату рождения. Нажала кнопку «получить отчет». На экране появился файл, но, чтобы его скачать, надо «оплатить стоимость отчета» – 299 рублей. Стоп, думаю. Вроде кредитную историю сколько-то раз должны давать бесплатно? А я в первый раз ее запросила. Решила, что здесь что-то нечисто, и ушла с этого сайта. Я правильно сделала? И как мне теперь убедиться, что с моей кредитной историей все в порядке?»

Комментарий эксперта

Организация, с которой столкнулась Мария, выдавала себя за посредника между заемщиком и бюро кредитных историй (БКИ). На сайтах таких компаний предлагают не только получить отчет, но и оформить платную подписку – например, они обещают отслеживать «критические изменения в кредитной истории» и «мониторить кредитный рейтинг».

По закону кредитный отчет из БКИ можете получить только вы или организация, которой вы сами дали на это согласие. Например, банк или МФО, в которых вы хотите взять кредит или заем.

Право на доступ к кредитной истории есть у наследников, законных представителей или тех, на кого оформлена нотариальная доверенность. Никакие посредники не имеют доступа к кредитным историям. И БКИ сами никогда не звонят заемщикам.

Если поверить посредникам, вы потеряете деньги за «отчет» или «мониторинг критических изменений». Кроме того, мошенники узнают ваши персональные данные и реквизиты карты, которой вы оплатите их услуги. Эта информация позволит им украсть деньги с вашего карточного счета.

Свою кредитную историю действительно стоит проверять время от времени. Два раза в год БКИ выдают ее бесплатно. Запросить отчет можно в офисе БКИ или дистанционно – с помощью Портала госуслуг.

История шестая: «Суперпредложение – круиз за полцены»

Александра, Ярославль

«У меня была мечта — поехать всей семьей в морской круиз. Но для меня это слишком дорогое удовольствие, и мечта так и оставалась мечтой. Вдруг соседка рассказала, что ее знакомая нашла суперпредложение — круиз за полцены. Правда, есть два условия. Во-первых, деньги нужно вносить частями и заранее — по 100 долларов в месяц. Во-вторых, надо уговорить еще пять человек купить такую же путевку.

Я поехала в офис компании — там было очень красиво, мне показали фотографии лайнера, морских пейзажей, городов, в которые заходит корабль. Сотрудница сказала, что это акция к дню рождения компании, больше таких выгодных предложений не будет.

Кроме того, можно не только сэкономить, но и заработать. Если я приведу больше пяти человек, то за каждого дополнительного получу еще 50 долларов. Они пойдут в счет оплаты моего круиза.

Я поверила. Несколько месяцев делала взносы, уговорила пятерых подружек отправиться в круиз вместе — другие отказались. Заветная дата поездки была все ближе. Написала компании в чат и спросила, когда они будут оформлять визы, но мне никто не ответил. Стала звонить — тоже тишина. Я забеспокоилась и поехала в офис. А на его окнах вывеска — «Сдается в аренду». Я полезла в интернет и нашла группу в соцсетях, где были такие же пострадавшие, как я. Единственное, о чем мы там договорились, — вместе написать заявление в полицию.

Денег ужасно жалко, но еще обиднее, что из-за этого «круиза» я рассорилась с подругами, которых втянула в аферу».

Комментарий эксперта

Александра столкнулась с мошеннической схемой, похожей на финансовую пирамиду: вкладчики должны внести деньги и привести друзей. Но различие в том, что они делали это не ради получения прибыли, как в случае с пирамидами, а ради выгодной поездки в круиз.

На самом деле путешествие было лишь рекламной уловкой. Мошенники преследовали только одну цель — убедить как можно больше людей принести им свои деньги. Злоумышленники зарегистрировали компанию-однодневку и сняли временный офис. Как только они собрали нужную сумму — исчезли. Возможно, сами отправились в круиз.

Мошенники могут притворяться какой угодно компанией. Чтобы распознать обман, важно следовать основным правилам финансовой безопасности:

- Не стоит слепо доверять рекламе. Под громкими и заманчивыми акциями нередко скрываются сомнительные предложения, которые на деле не приносят выгоды.
- Проверяйте сведения о компании. Найдите данные о ней на сайте Федеральной налоговой службы (ФНС) — там есть информация обо всех компаниях, зарегистрированных в России. Для этого надо зайти в раздел «Риски бизнеса: проверь себя и контрагента». Обратите внимание на основной вид деятельности компании, дату ее создания, сверьте информацию на сайте ФНС и на сайте самой организации.
- Найдите компанию в официальных реестрах. Например, финансовая организация обязательно должна быть в реестре Банка России. Туроператор — в реестре Ростуризма.
- Изучите отзывы о компании в интернете, почитайте новости — не фигурирует ли она в скандалах.
- Внимательно читайте договор. Прежде чем отдавать деньги, убедитесь, что вам понятен каждый пункт документа. Изучите, какие обязательства берет на себя компания и что будет, если она их не выполнит.

Если вы все же попались на удочку аферистов и потеряли деньги, пишите заявление в полицию.

История седьмая: «Вноси 2400 рублей и зови друзей – заработаешь в восемь раз больше!»

Игорь, Ставрополь

«Знакомый написал в мессенджере, что нашел супербыстрый способ заработать. Ты вкладываешь 2400, а получаешь 19 200. И выглядит все очень просто. Это онлайн-игра, в которой надо как можно скорее добраться до верхнего уровня. Тогда и получаешь выигрыш.

По сути делать почти ничего не надо. Перед тобой такая таблица в форме пирамидки. Если внесешь стартовый взнос, ты — участник, и твое имя появляется в табличке. Дальше зовешь пару своих друзей. И как только они вступают в игру, ты поднимаешься вверх по пирамидке. Потом они приведут еще по двое, и ты — еще на один уровень выше.

Все очень просто, но реально просыпается азарт. Все время следишь, кто еще присоединился и на какой уровень ты продвинулся. Ну, и зовешь как можно больше знакомых, чтобы все ускорить.

Когда под тобой набирается 14 участников, ты оказываешься на вершине, получаешь 19 200 рублей и выбываешь из игры. На твое место становится следующий по очереди и потом тоже забирает 19 200 рублей. А ты можешь вступить в игру заново.

Приятель сказал, что его знакомые уже так поднялись и получили свои деньги. Прислал скрины переписок и самой игры тоже. То есть все надежно, не кидалово. И я поверил, вообще даже не стал дальше спрашивать — у меня друзей-то полно, нужное число по любому наберется.

Перечислил 2400 по номеру кошелька, который он скинул, сагитировал двоих друзей. А некоторые, оказалось, уже в игре — их уже позвали другие знакомые.

В итоге прошло уже больше месяца, я так ничего и не получил. Приятель тоже еще не заработал. Там уже очень много участников и все ждут. Прочитал в интернете, пишут, что это лохотрон. По ходу я так и не дождусь своих денег».

Комментарий эксперта

Эта игра очень похожа на финансовую пирамиду. Она заманивает своей простотой, ведь для того чтобы получить деньги, почти ничего не надо делать, только сделать взнос. Вот только шансы на обещанный доход невелики.

Первые участники (это сами организаторы пирамиды и их друзья) действительно быстро получают обещанный выигрыш и хвастаются удачей в соцсетях. Но для того чтобы свой выигрыш смогли забрать новые

участники, их число должно постоянно удваиваться. Сначала будет один победитель на 14 человек. Чтобы каждый участник второго уровня получил деньги, в пирамиду должно вступить уже 28 человек. У всех игроков третьего уровня шансы появляются, только когда вовлечено 56 человек, и так далее.

Пирамида существует за счет прихода новых игроков, но этот поток рано или поздно иссякает. Не остается знакомых, которые хотели бы вступить в игру. Люди либо предусмотрительно отказываются, либо уже стоят на нижних уровнях в игре и ждут продвижения вверх.

Пирамида может лопнуть в любой момент, и когда именно это случится, предсказать невозможно. Каждый участник надеется, что окажется в числе первых и успеет проскочить на вершину пирамиды, но в реальности сделать это практически невозможно.

Как правило, участники вовлекают в такие схемы своих родственников, друзей и знакомых. И затем теряют не только деньги, но и доверие близких.

Распознать признаки финансовой пирамиды бывает довольно сложно. Мошенники могут маскироваться под инвестиционные фонды, онлайн-проекты, финансовые организации.

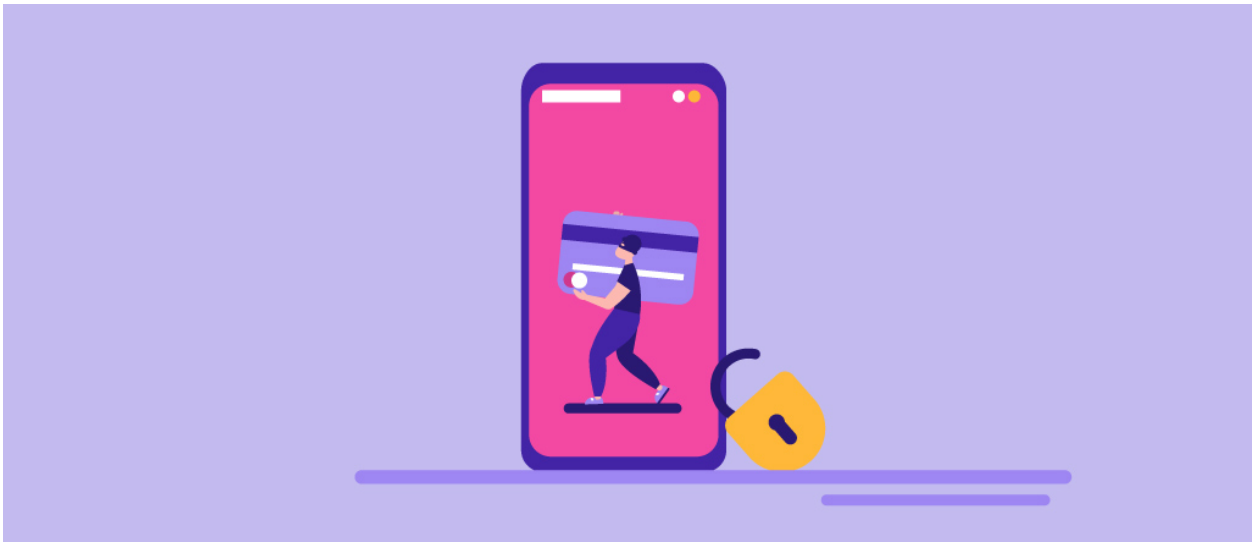
Участие в пирамидах опасно не только потерей вложений, в некоторых случаях есть риск попасть под суд. Тем, кто вовлекает других в финансовые пирамиды и распространяет рекламу в социальных сетях, грозит штраф от 5000 до 50 000 рублей. За организацию финансовой пирамиды и вовсе предусмотрена уголовная ответственность.

Чтобы желание быстро заработать не привело к плачевным последствиям, важно вовремя распознать финансовую пирамиду. У них всегда есть несколько общих признаков:

- Обещают золотые горы: доходность якобы в несколько раз превышает вложения.
- Чтобы получить деньги, обязательно надо привести еще несколько человек.
- Организаторы «проекта» не раскрывают информацию о себе. Непонятно, кто именно его создал, в какой юридической форме существует организация и где она зарегистрирована, какие у нее финансовые показатели.
- Идет агрессивная реклама в интернете.

Если вы уже поддались на уловки мошенников и вложили деньги в пирамиду, обращайтесь в полицию или Роспотребнадзор.

История восьмая: «Введите номер СНИЛС и получите 120 000 рублей!»



Тимур, Железногорск

«В инстаграме вылезла реклама о том, что государство начало выплачивать всем деньги по номеру СНИЛС — до 120 000 руб! Якобы ввели такой новый закон. Причем пост выглядит как новость от известного ТВ-канала с фоткой ведущей из студии. И под ним много комментариев от людей, которые уже получили деньги.

По ссылке «Подробнее» открылся сайт какого-то фонда и написано, что сегодня они выплатили людям уже несколько миллионов рублей. Надо ввести номер СНИЛС и тогда узнаешь, сколько денег тебе полагается. Я поверил и ввел свой номер СНИЛС. Дальше появились строки с суммами от разных страховых и внизу написано, что могу получить 115 000 руб.

Я нажал кнопку ПОЛУЧИТЬ ДЕНЬГИ и тут началось самое интересное. Сайт сообщил, что надо заплатить с карты какую-то комиссию 200 рублей за подключение к базе. Я оплатил, и потом с меня просят еще 500 рублей за идентификацию личности и проверку личных данных.

Вот тогда до меня уже дошло, что это какой-то развод на деньги. И вдруг получаю смс от банка, что с карты попытались снять еще 1000 рублей. Хорошо, что на моей карте не было больше денег. На всякий случай карту заблокировал. Люди, не ведитесь!»

Комментарий эксперта

Мошенники активно используют социальные сети, чтобы выманивать персональные данные, платежную информацию и деньги пользователей. Преступники подделывают аккаунты известных СМИ и популярных блогеров, чтобы распространять фейковые рекламные посты от их имени. Это могут быть объявления о социальных выплатах, конкурсах с денежными призами и другие «аттракционы невиданной щедрости».

Чтобы предложение выглядело максимально правдоподобно, злоумышленники нередко сопровождают пост фальшивым видео с участием медийного лица — умело смонтированной нарезкой из роликов с ним.

И все ради того, чтобы пользователь перешел на мошеннический сайт и оплатил «небольшую комиссию». Потеря 200–300 рублей, возможно, не так страшна. Но человека просят ввести секретные данные банковской карты: номер, имя владельца, срок действия и трехзначный CVC/CVV-код с обратной стороны карты. После этого преступники получают доступ к его счету и могут украсть остальные деньги.

Опасность ситуации, в которой оказался Тимур, еще и в том, что преступники могут использовать номер СНИЛС и в других мошеннических схемах. Например, зная данные паспорта и СНИЛС, попытаться оформить займы на его имя.

Чтобы избежать неприятностей, следуйте важным правилам финансовой безопасности:

- Всегда перепроверяйте информацию из социальных сетей. Если государство назначает какие-либо выплаты и компенсации — об этом обязательно напишут ведущие издания. Посмотрите, есть ли что-то по теме в разделах новостей в поисковых системах. В идеале стоит найти ссылку на сам закон или постановление и изучить его.
- Не доверяйте конкурсам, опросам и другим обещаниям внезапного обогащения, в особенности если организаторы требуют что-либо оплатить.
- Не спешите переводить деньги неизвестным получателям по первому требованию и никогда не переходите по ссылкам от незнакомцев.
- Не вводите на сомнительных сайтах конфиденциальные данные, в том числе информацию о карте, ПИН-коды, пароли из СМС, а также данные паспорта и других документов.
- Не храните крупные суммы денег на карте, которую используете для повседневных трат. Лучше завести отдельную карту для покупок в интернете и каждый раз класть на нее ровно столько, сколько нужно заплатить.
- Подключите СМС-оповещения или push-уведомления об операциях по карте. В этом случае вы сразу же узнаете о платеже, который вы не совершали, и сможете заблокировать карту и опротестовать операцию.

- Установите антивирус на всех своих гаджетах — это поможет защитить их от вредоносных программ.

Если вы столкнулись с подозрительным объявлением в социальной сети, пожалуйтесь ее администрации. Чем больше жалоб от пользователей, тем быстрее эту рекламу удалят. И меньше шансов, что кто-то пострадает от действий преступников.

История девятая: «Гарантируем получение кредита людям с плохой кредитной историей»

Михаил, Барнаул

«Мне был очень нужен кредит на ремонт машины, а банки отказывали. Думаю, дело в моей кредитной истории — она не очень хорошая. Не всегда платил вовремя. И тут я вижу рекламу: поможем получить кредит людям с плохой кредитной историей. Позвонил. Да, говорят, мы, финансовые брокеры, помогаем получать деньги тем, кому банки напрямую отказывают.

Я им оставил свои данные. На следующий день позвонили: вам одобрили кредит в таком-то банке. Но сначала надо застраховать свою жизнь — это как бы подтвердит серьезность моих намерений. Приехал курьер, привез договор страховки. Я его подписал и заплатил, сколько потребовали.

Потом пошел в банк. Оказалось, никакого кредита мне не одобряли, никаких брокеров не знают, а страховка липовая. Попал как дурак. В итоге на ремонт еще меньше денег осталось».

Комментарий эксперта

Мошенники нередко выдают себя за кредитных и страховых брокеров. Они пользуются тем, что многие люди не понимают, какие у брокеров функции и полномочия.

Страховые брокеры — это легальные посредники между клиентами и страховщиками. Они вправе не только помочь выбрать подходящий страховой полис, но и заключить договор от имени страховой компании. Но прежде чем подписывать такой договор, стоит проверить, есть ли у брокера лицензия. Реестр лицензированных страховых брокеров можно посмотреть на сайте Банка России.

Понятия «кредитный брокер» в законодательстве нет, и ни один посредник не может заключать договоры от имени банков. Кредитными брокерами обычно называют себя финансовые консультанты, которые помогают потенциальным заемщикам выбрать банк, собрать документы и оформить заявку на кредит. За свои советы и помощь консультанты вправе брать деньги. И вам решать — стоит ли оплачивать их услуги.

Честные финансовые консультанты никогда не обещают, что вы точно получите кредит. Ведь решение чаще всего принимает даже не сотрудник банка, а программа, которая автоматически оценивает заемщика на основе документов о его доходе, стаже работы и кредитной истории. Повлиять на эту программу консультант не в состоянии.

Мошенники же «гарантируют», что их «связи в банке» обеспечат вам кредит. И берут деньги не просто за советы и информацию, но и «за гарантии». Также они могут выставить клиенту счет за фиктивную страховку.

Стоит иметь в виду, что страховка не может быть условием и тем более гарантией получения кредита. По закону заемщик обязан покупать полис в единственном случае — когда оформляет ипотеку. Жилье, которое находится в залоге у банка, должно быть застраховано.

Банк вправе предложить заемщику застраховать свою жизнь и здоровье, а также залог по кредиту. И если клиент согласится, может понизить ему процент по кредиту. Но навязывать страховку банк не имеет права.

Если у вас плохая кредитная история, не стоит доверять «помощникам», которые обещают вам кредит. Лучше постараться самостоятельно исправить положение.

История десятая: «Вы оплатили товар, но можете отменить платеж»

Татьяна, Псков

«Получила смс, что с карты списали 14 500 рублей за покупку в интернет-магазине — и название магазина. Я такого не знаю. И в конце — если хотите отменить списание, позвоните по номеру… Я позвонила.

Говорят, вы разве у нас не делали покупку? Но вы — и мое имя-отчество называют — у нас значитесь покупателем, оплачено с вашей карты. И называют ее номер. Я подтверждаю — да, карта моя, но я ничего у вас не покупала. Они: можем отменить покупку и вернуть платеж. Но для этого нужно уточнить дату действия карты и три цифры с обратной стороны. Я им: вроде это секретный код, разве можно его говорить? Тут они: у вас есть 20 минут, чтобы отменить платеж. А потом придется писать заявление, его две недели будут рассматривать. Потом еще до двух недель деньги будут идти обратно.

Ну, сумма-то для меня большая. Месяц ее ждать я не могу. И назвала код. Хорошо, говорят, в течение 10–15 минут деньги вернутся. Положила трубку. А потом посыпались смски: списано 14 500, потом еще 10 тысяч, потом еще 5 тысяч. Не успела даже сделать ничего — все деньги с карты ушли.

Позвонила в банк — а мне говорят: вы же сами секретный код сказали. Значит, вы нарушили правила использования карты. Деньги вернуть не сможем. Могу я у банка потребовать вернуть их назад? Это же точно мошенники были».

Комментарий эксперта

По закону банк обязан вернуть клиенту деньги, если мошенники списали их без ведома владельца карты и он оспорил операцию не позднее следующего дня.

Но если человек сам сообщил мошенникам CVC/CVV-код с обратной стороны карты, считается, что он добровольно дал согласие на перевод денег. В этом случае банк не должен возмещать потери.

Татьяне стоит обратиться в полицию. По номеру телефона, на который она звонила, и номеру счета, на который ушли ее деньги, полиция может напасть на след преступников.

Чтобы не наступать на те же грабли, нужно запомнить несколько основных правил для защиты своих денег:

1. Никому нельзя говорить полные реквизиты своей карты, включая трехзначный код на ее обратной стороне.
2. Данные могут выведать не только по телефону. Например, вашу карту могут сфотографировать, когда вы пытаетесь расплатиться в маленьком магазине или кафе. Карту уносят «на минутку, чтобы поймать сеть», а через некоторое время с нее списывают деньги. Лучше никогда не выпускать карту из поля зрения.
3. Не стоит оставлять полные данные карты на сайте, если вы не уверены на 100% в его надежности. Делать покупки можно только на тех сайтах, которые обеспечивают безопасное соединение. Смотрите на адресную строку в браузере: перед названием сайта должно стоять https://, а в конце строки – значок закрытого замка.
4. Для покупок в интернете лучше завести отдельную дебетовую карту и класть на нее нужную сумму непосредственно перед оплатой.

Оспорить любую подозрительную операцию по карте можно не позднее следующего дня после того, как пришло уведомление о списании денег. Поэтому, с одной стороны, не надо медлить. Но с другой – не надо спешить. Если вас убеждают предпринять какие-то действия немедленно, в течение нескольких минут, это почти наверняка мошенники.