

Все самые распространенные виды мошенничества объединяются одним общим знаменателем – они осуществляются с учетом психологии потенциальных жертв аферистов. Аферы продумываются до мельчайших деталей и способны обмануть бдительность даже самых осторожных и внимательных людей. Именно поэтому необходимо помнить о том, что персональные данные, такие, как пароль, логин, номер банковского счета, кодовое слово, CVV2-код на банковской карте нельзя передавать в третьи руки.

1. Сообщение от друзей

Схема обмана: От знакомого, обычно которого вы долго не видели, приходит сообщение через мессенджер или в соцсети, о том что он попал в беду или просто просит кинуть на его телефон или карту небольшую сумму. Конечно же он обещает вернуть эти деньги в ближайшее время.

На самом деле с вашим другом ничего не случилось, его профиль взломали и рассылку делают мошенники. Если проигнорировать просьбу, то чаще всего ваш друг сам замечает неладное и делает рассылку с сообщением об обмане. Если вы сомневаетесь в ситуации, перезвоните, поинтересуйтесь всё ли в порядке у вашего знакомого и расскажите о случившемся.

2. Нежданный выигрыш

Схема обмана: Вам на телефон звонят или присылают СМС-сообщение с информацией о том, что вы выиграли приз или крупную сумму. Причем вы знаете, что ни в каком розыгрыше вы не участвовали. Для получения подарка мошенники обычно просят заплатить пошлину, налог или внести иной платеж. Причем сумма может быть как в несколько сотен, так и в несколько тысяч рублей – все зависит от схемы аферы.

На самом деле, если вы верите в манну небесную и платите деньги – вы не получаете никакого приза, а еще и лишаетесь какой-то суммы денег. Чтобы не попасться на хитрую уловку – игнорируйте уж слишком заманчивые предложения. Просто положите трубку либо попробуйте обхитрить мошенника, предложив ему взять необходимую сумму для оплаты налога с вашего выигрыша.

3. Оплатите штраф

Схема обмана: Вам приходит СМС или письмо на электронную почту о наличии задолженности за нарушения правил дорожного движения. При этом мошенники указывают регистрационный знак вашего автомобиля, однако нет ни информации о номере постановления, а также даты его вынесения, ни фото нарушения. Оплатить предлагают сразу же, достаточно перейти по указанной ссылке и перевести деньги по реквизитам, которые заполняются автоматически.

На деле никакого штрафа нет. Оплатив фальшивый штраф – вы просто переводите деньги мошенникам. А при худшем сценарии – данные вашей карты попадают в руки злоумышленников, и тогда уже можно лишиться всех денег с карты. Поэтому оплачивайте штрафы только через официальные сервисы: портал госуслуги, мобильный банк, либо ждите уведомления по почте с фото вашего автомобиля. А еще лучше старайтесь не нарушать ПДД.

4. Скинь реквизиты! - готов выслать вам деньги за товар!

Схема обмана: Вы выставляете какую-то вещь на Авито или Юлу. Звонит потенциальный покупатель и сообщает, что готов купить вашу вещь. И тут начитаются различные предлоги: не могу приехать сейчас, живу в другом городе или просто в отдаленном муниципалитете и пр. Но мошенник готов внести аванс на вашу карту, чтобы вы не продали вещь никому другому. А для этого просит номер вашей карты и код подтверждения из СМС.

После того как код получен – продавец сам лишается суммы якобы аванса, который рассчитывал получить. Причем вернуть деньги не получится – так как банк видит, что вы сами передали секретные данные мошеннику. Поэтому продавая товар помните, что для перевода денег на вашу карту нужен только её номер. Ни код из СМС, ни код с обратной стороны карты – никому сообщать нельзя!

5. Пирамиды: заманчивые предложения в духе МММ

Схема обмана: Яркая и назойливая реклама предлагает 200-500% готовых и выше? За такими предложениями чаще всего скрываются мошенники. Видя такие предложения вспомните 90-ые и печальный опыт вкладчиков МММ.

Получить столь высокую доходность очень сложно, а если и возможно, то риск потерять все – крайне высок. Когда такое предложение сопровождается привлекательной рекламной кампанией – это сто процентов финансовая пирамида. И вложившись в нее, вы не получите ни дохода, ни вложенных денег. Поэтому вкладывайте только в проверенные финансовые инструменты: банковские вклады, ценные бумаги, недвижимость и пр. И помните, что любые инвестиции несут риск.

6. Бесплатные юридические консультации по пенсионным вопросам

Схема обмана: СМИ кишат рекламой юристов, которые бесплатно готовы решить ваши проблемы с пенсией или даже предлагают помочь получить от ПФР определенную сумму. Чаще всего бесплатная консультация незаметно трансформируется в платную. Вы платите кругленькую сумму за оформление документов (чаще всего не имеющих отношения к реальным законам РФ). А на деле не получаете никаких денег.

Поэтому помните про бесплатный сыр. Не думайте, что кто-то будет тратить огромные деньги на рекламу в СМИ и бесплатно вас обслуживать.

7. Обман с арендой жилья

Схема обмана: Вы ищете квартиру для аренды, находите объявление, с привлекательной ценовой. Подвох – необходимо оплаты комиссию риелтору, причем до оформления договора и вообще до встречи с ним.

Но после перевода денег все контакты с вами прерываются. Поэтому решив арендовать жилье, сначала посмотрите его, подпишите договор (предварительно изучив его) и только после этого переводите вознаграждение.

8. Регистрация ООО или ИП

Схема обмана: Вам предлагают стать учредителем фирмы за небольшое вознаграждение. Казалось бы, в чем может быть подвох? Но далее фирма начинает вести нелегальную деятельность, а по закону несет ответственность ее учредитель. И здесь дело может дойти вплоть до уголовной ответственности.

Не соглашайтесь на подобные предложения от незнакомых людей, вполне возможно несколько тысяч сегодня – могут обернуться огромными проблемами в будущем.

9. Ваша карта заблокирована, перезвоните

Схема обмана: Вы получаете СМС-сообщение от банка, где говорится о блокировке карты. В конце — предложение перезвонить по указанному номеру. И если вы перезваниваете, то вас просят назвать номер карты и код из поступившего СМС.

И, как мы уже знаем, из схемы обмана №4 ваши деньги поступают на счет мошенника. Так что, получив подобное СМС игнорируйте! Банк не рассыпает предложения перезвонить и, конечно, не запрашивает данные карт, не спрашивает ваш ПИН-код или коды из СМС.

10. Заражение вредоносным ПО смартфона

Схема обмана: Мошенники всячески пытаются запустить вредоносную программу в ваш телефон. Один из вариантов рассылка интригующих СМС-сообщений, в том числе через мессенджеры с гиперссылками.

Не доверяйте неизвестным, которые звонят Вам на телефон и сообщают о том, что Ваш родственник попал в беду – не впадайте в панику и не поддавайтесь влиянию неизвестных, а прежде всего, позвоните родным и удостоверьтесь, что с ними все в порядке!

Если Вам пришло СМС-сообщение с неизвестного номера с текстом, что Ваша карта заблокирована:

не вступайте в беседу по телефону с неизвестными, а обратитесь в официальный офис банка и удостоверьтесь в подлинности сообщения, либо свяжитесь с банком по официальному телефону «горячей линии»;

никому не сообщайте своих данных и не осуществляйте никаких операций с Вашими деньгами, а обратитесь в официальный офис банка и Вам дадут всю необходимую информацию о Вашей карте!

Не доверяйте звонящим неизвестным которые под различным предлогом пытаются установить Ваши личные данные, данные ваших карт и счетов – ни в коем случае не передавайте личные данные неизвестным лицам!