

Социальная инженерия: почему люди сами отдают мошенникам деньги.

Великий комбинатор Остап Бендер чтит уголовный кодекс. Банальному грабежу он предпочитал психологические уловки, чтобы жертвы его обаяния добровольно отдавали ключи от квартир, где деньги лежат. Позже для таких махинаций придумали специальное название — социальная инженерия. Рассказываем, какие схемы социальные инженеры используют сегодня и как от них защититься.



Кто такие социальные инженеры?

В широком смысле — это специалисты, которые умеют манипулировать другими. Но обычно мы слышим о тех социальных инженерах, которые с помощью психологических приемов выманивают деньги или данные для доступа к чужому счету.

По статистике в большинстве случаев люди теряют свои сбережения не потому, что их счета взламывают хакеры. Владельцы банковских карт чаще всего сами сообщают мошенникам их полные реквизиты, включая номер, срок действия, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций.

Если вы сами передали мошеннику секретные данные, банк не обязан компенсировать похищенное.

Даже самые умные и осторожные люди иногда попадаются на крючок к махинаторам. Разбираем самые распространенные психологические уловки, которые используют мошенники.



Вызвать доверие

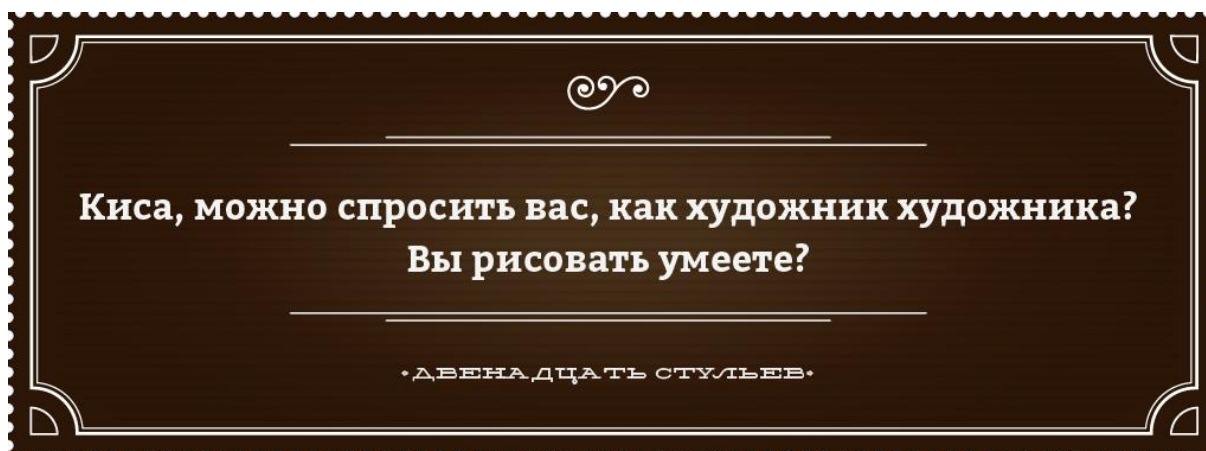
Мошенники часто представляются теми, от кого люди не ждут подвоха: сотрудниками банков, налоговой службы, юридических контор и других официальных организаций.

Социальный инженер может прикинуться вашим приятелем или родственником, например, взломав или сделав дубликат их аккаунтов в соцсетях.

Обычно, прежде чем выйти на контакт, социальные инженеры стараются узнать о потенциальной жертве как можно больше. Они выясняют данные человека, чаще всего — с помощью фишинговых сайтов. Или покупают готовые информационные базы с персональными данными, которые утекли в сеть.

Нередко люди и сами публикуют в соцсетях номера телефонов, электронные адреса и даже выкладывают фотографии своих банковских карт.

Этой информации недостаточно, чтобы сразу украсть деньги. Но вполне хватит для того, чтобы начать разговор и усыпить бдительность. Когда махинаторы обращаются к людям по имени и отчеству, сами называют номер карты или другие конфиденциальные данные, кажется, что они действительно представляют знакомую организацию или человека.



Подделать телефонные номера, документы и сайты

Часто трудно сразу догадаться, что имеешь дело с мошенниками. Они умеют виртуозно маскироваться:

- Подменяют номер, с которого звонят или присылают сообщение. С помощью специального программного обеспечения им удается скрыть настоящий номер, а у вас на экране во время их звонка отображается, например, знакомый телефон банка.

- Подделывают документы: с помощью фотошопа преступники создают фейковые налоговые уведомления, квитанции о штрафах, счета за квартиры и присылают их на домашний адрес, по СМС или электронной почте. Если человек оплатит такое уведомление, все деньги уйдут к мошенникам:

«Вчера получил письмо, якобы из налоговой инспекции, с требованием оплатить налоговые сборы. Письмо очень похоже на оригинальное, содержит QR-код для ввода данных со смартфона. Первое, что бросилось в глаза, это непривычно высокая сумма налогового сбора...»

Будьте бдительны, не наступайте на чужие грабли!

- Копируют сайты банков, микрофинансовых организаций, страховых компаний, популярных онлайн-магазинов, а также порталы объявлений и платежные страницы. Мошенники рассчитывают, что пользователь либо сразу переведет деньги на их счет, либо оставит конфиденциальные данные своей банковской карты.



Запугать потерей денег

Вызвать страх — уже поддела для обманщика. Испуганный человек гораздо лучше поддается внушению. Например, мошенник звонит «из службы безопасности банка» и сообщает, что по карте «прямо сейчас» проводится подозрительная операция.

Растерянному «клиенту» предлагают срочно назвать трехзначный код с обратной стороны карты, чтобы отменить транзакцию. Или перевести деньги на некий «безопасный счет».

Если человек поддастся панике и выполнит инструкции «экспертов», то, не ведая того, он сам отправит все сбережения мошенникам.



Заманить выигрышем

Мошенники активно эксплуатируют стремление людей к легкому обогащению. Они создают специальные сайты с аттракционами невиданной щедрости. Например, предлагают пройти опрос с заманчивым денежным вознаграждением или поучаствовать в «беспроигрышных» конкурсах, получить социальные выплаты или вернуть налоги.

Эти сайты махинаторы рекламируют в социальных сетях, рассылают в мессенджерах, по электронной почте и СМС. Нередко подобная реклама сопровождается фотографиями и склеенными нарезками из видео с медийными персонами, которые призывают людей участвовать в этой афере. Перейдя по ссылке на сайт конкурса или лотереи, человек видит множество восторженных отзывов от тех, кто якобы уже получил свои деньги.

«Участвовала в конкурсе в соцсети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала вещь, написала организаторам, после чего мне предложили оплатить доставку в размере 450 Р...»

Будьте бдительны, не наступайте на чужие грабли!

Однако в реальности вместо денежных призов людей ждут лишь убытки. Организаторы схемы под разными предлогами просят их ввести данные карты, чтобы оплатить символический налог, услуги «юристов» или комиссию за участие. Основная опасность кроется не в потере незначительной суммы. После того как человек оставляет конфиденциальную информацию на фишинговой странице, мошенники получают доступ к деньгам на его счете.



Восстановить справедливость

Как правило, махинаторы ведут базы данных людей, которые уже однажды поддались на их обман и могут снова клюнуть на их уловки. Тем, кто потерял деньги на финансовых пирамидах, псевдолотереях и прочих лохотронах, мошенники предлагают «компенсации».

Цель все та же — под предлогом оплаты «услуг юриста» или «комиссии за перевод денег» человека убеждают указать полные реквизиты карты, чтобы он снова получил шанс потерять свои деньги.



Использовать громкие информационные поводы

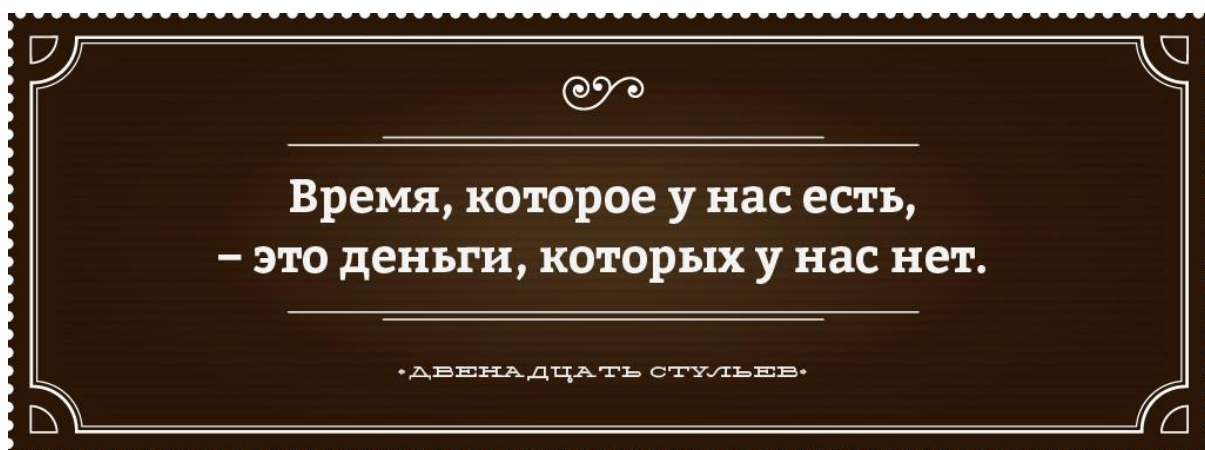
Мошенники активизируются на фоне различных катастроф, стихийных бедствий и эпидемий. Например, во время пандемии коронавируса обманщики собирают деньги «на разработку вакцины» под видом Всемирной организации здравоохранения.

Социальные инженеры следят за новостями и настроениями и быстро адаптируются к текущей ситуации. В период самоизоляции они рассылают всем подряд СМС о «штрафе» за нарушение карантина со ссылкой на несуществующие законы.

От имени авиакомпаний предлагают «компенсации» за отмененные рейсы в обмен на секретные данные банковской карты.

Самые отчаянные наряжаются в защитные костюмы и идут по квартирам. Они сообщают людям о том, что у их соседей «положительный анализ на коронавирус».

Поэтому им тоже стоит пройти тест — за умеренную плату. Результатов мазка можно ждать бесконечно долго, мошенников интересует только оплата их визита.



Не дать время на размышления

Мошенники специально торопят и давят, чтобы лишить человека возможности принять взвешенное решение в спокойной обстановке. Они требуют немедленно перевести деньги, срочно оплатить какую-либо услугу, «как можно скорее» назвать секретный номер, пароль или код.

«Звонит незнакомый мужчина и говорит, что по ошибке прислал мне 30 000 рублей. Просит отправить их ему по номеру карты, который мол сейчас продиктует. Я так прикинул, что это развод и положил трубку. Проверяю мобильный банк, а деньги реально пришли. Тут тот мужчина звонит еще раз и начинает орать в трубку...»

Будьте бдительны, не наступайте на чужие грабли!

Если вы чувствуете явный прессинг, когда пытаетесь принять какое-либо финансовое решение, это верный признак, что вы имеете дело с махинаторами. При малейших подозрениях кладите трубку и сами звоните в банк по телефону горячей линии — он есть на сайте организации и на обратной стороне банковской карты.



Как обезопасить себя от социальных инженеров?

Аферисты постоянно придумывают новые схемы обмана. Единственный способ избежать денежных потерь при встрече с мошенниками — критически воспринимать любые предложения, перепроверять информацию и никогда не торопиться при принятии финансовых решений.

Следуйте базовым правилам финансовой безопасности:

- Никому ни при каких обстоятельствах не сообщайте полные реквизиты банковской карты, включая трехзначный код с обратной стороны; а также ПИН-коды и пароли из СМС от банка.
- Не переходите по сомнительным ссылкам из сообщений и не переводите незнакомцам деньги по первому требованию.
- Не храните много денег на карте, которой расплачиваетесь в интернете: кладите только ту сумму, которую собираетесь потратить в данный момент. В этом случае, даже если мошенники попытаются украсть деньги, им не удастся вывести слишком много.
- Получив внезапный звонок из какой-либо финансовой организации со срочным вопросом или предложением, положите трубку и позвоните туда сами, найдя номер на ее официальном сайте. Набирайте этот номер вручную. Если с вами связались из компании, клиентом которой вы не являетесь, сначала проверьте ее по справочнику финансовых организаций.
- Не соглашайтесь сразу ни на какие «заманчивые предложения» — будь то «выгодный кредит» или внезапная компенсация. Дайте себе время на размышление, посоветуйтесь со знакомыми, пробейте в интернете информацию о компании и «уникальной акции», которую она вам рекламирует.
- Не публикуйте в открытом доступе свои персональные данные: номер телефона, домашний адрес, данные паспорта. Мошенники охотно задействуют эту информацию в своих аферах.

Как быстро распознать мошенника

У Ивана Сергеевича зазвонил телефон, номер был незнаком. Солидный мужской голос на фоне шума офиса звучал встревоженно: «Добрый день. Иван Сергеевич? Это служба безопасности банка «Лапша-Финанс». Мы зафиксировали, что киберпреступники пытаются получить доступ к вашему личному кабинету. Надо срочно перевести все деньги на безопасный счет, иначе их украдут!» Иван Сергеевич немедленно положил трубку. Рассказываем, по каким признакам он вычислил обманщиков.



Аферисты постоянно придумывают новые способы выманить у людей деньги или конфиденциальные данные для доступа к счетам. Но какой бы ни была легенда, есть пять примет, по которым можно сразу же вычислить мошенников.

Признак 1. На вас выходят сами

Вам звонит незнакомец, присылает СМС-сообщение, электронное письмо или ссылку в мессенджере. Кем бы он ни представился — сотрудником банка, полиции, магазина, вашим троюродным братом-миллионером из Зимбабве — насторожитесь. Раз он стал инициатором контакта, ему что-то от вас нужно.

Быстро проверить, тот ли он, за кого себя выдает, не получится. Номер, который высвечивается при входящем вызове, можно подменить, аккаунты или сайты известных людей или организаций — подделать. Так что стоит быть бдительным и никому не верить на слово.

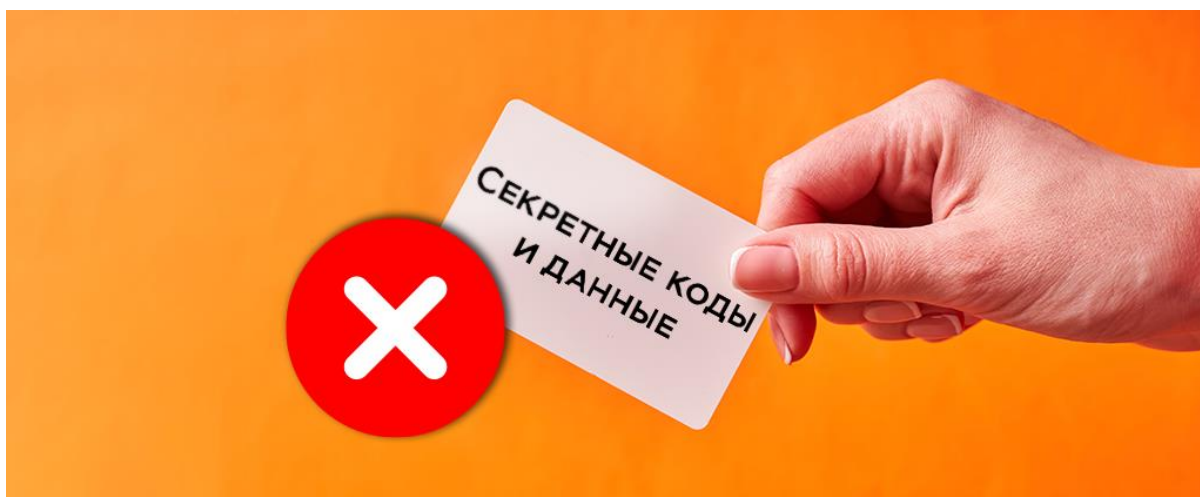
Признак 2. С вами говорят о деньгах

Основная задача мошенников — получить доступ к чужим деньгам. Схемы обмана почти всегда связаны с финансами: вам предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно» инвестировать свои сбережения (на самом деле — в финансовую пирамиду).

«На днях бабушке позвонили якобы из службы безопасности ее банка. Сказали, что с ее карточки кто-то только что попытался украсть деньги. Они операцию заблокировали, но деньги надо срочно перевести на некий безопасный счет...»

Будьте бдительны, не наступайте на чужие грабли!

Легенды могут быть какими угодно, но речь всегда про деньги — которые вы можете потерять или получить.



Признак 3. Вас просят сообщить данные

Если ворам нужны ключи от квартиры, то социальным инженерам— «ключ» к деньгам на ваших счетах. Это могут быть конфиденциальные данные вашей карты, включая срок действия и три цифры с ее обратной стороны. Либо логины и пароли к личному кабинету на сайте банка или мобильному приложению. И почти всегда — коды из банковских уведомлений.

Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли.

Когда банк замечает сомнительный платеж или перевод с вашего счета, с вами связываются, чтобы подтвердить или отклонить операцию, и только. Конфиденциальные данные для этого не требуются. Если о них спрашивают — будьте уверены, звонят не из банка и вас точно пытаются обмануть.

Признак 4. Вас выводят из равновесия

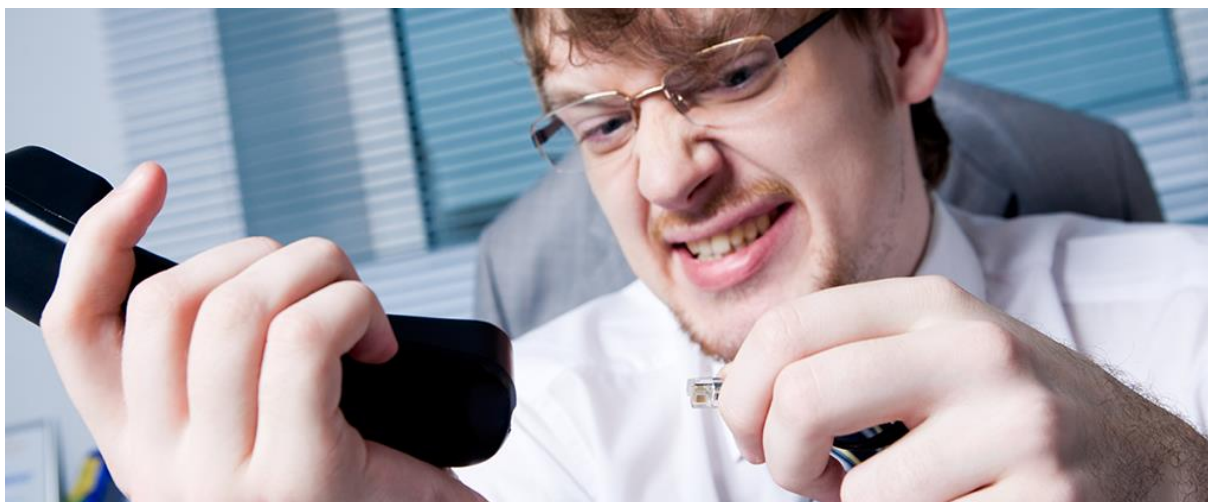
Мошенники стремятся вызвать у вас сильные эмоции — напугать или обрадовать. Так они сбивают с толку и притупляют бдительность потенциальной жертвы. Например, сообщают: «Ваш онлайн-банк взломали!», чтобы вы от растерянности и волнения выполнили любые просьбы и выдали любую информацию, лишь бы спасти деньги.

Либо, наоборот, огорошивают новостью о внезапном выигрыше в лотерею или обещают быстрое обогащение. Взамен вы должны будете «лишь оплатить небольшой взнос», а для этого — ввести данные банковской карты на сайте. Мошенники создают фишинговые страницы, с помощью которых воруют данные карт и получают доступ к банковским счетам доверчивых пользователей.

«Участвовала в конкурсе в соцсети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала кроссовки, написала организаторам, после чего мне предложили оплатить доставку в размере 450 Р...»

Будьте бдительны, не наступайте на чужие грабли!

Всегда сохраняйте здоровый скептицизм и не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.



Признак 5. На вас давят

Мошенники всегда торопят, чтобы не дать вам времени обдумать ситуацию. Вас принуждают к чему-то, ставят условия: «сейчас или будет поздно». Ситуация, в которой вам не дают права выбора и заставляют немедленно действовать, подозрительна.

Если чувствуете психологический дискомфорт, лучше сразу же прекращайте общение. Ведь чем дольше вы разговариваете с мошенником, тем сильнее он будет на вас давить. На все ваши расспросы у обманщиков есть заготовленные ответы, которые только нагнетают обстановку.

«Попал в ужасную ситуацию. Позвонили из моего банка, назвали мое ФИО и попросили подтвердить, что я сейчас оформляю кредит на 550 тысяч рублей. Я очень удивился, потому что ничего не оформлял в тот момент. Сотрудник банка сказал, что если это не я, значит мошенники пытаются взять кредит от моего имени, поэтому надо срочно принять меры».

Будьте бдительны, не наступайте на чужие грабли!

Никогда не принимайте поспешных решений, особенно если они касаются ваших финансов. Всегда берите паузу, чтобы разобраться в том, что происходит. Возьмите за правило проверять любую информацию в первоисточнике.

Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить реальное положение дел.

Прислали странное уведомление от имени Федеральной налоговой службы (ФНС)? Заведите личный кабинет на сайте ФНС — в нем можно проверить суммы налогов и сразу же оплатить их.

Получили «письмо счастья» о государственной выплате? Поищите новости об этом в деловых СМИ. А еще лучше — найдите сам закон, указ или постановление, которые вводят выплаты. Обратите внимание на условия, кому они положены.

Не всегда при общении с аферистом вы заметите все пять признаков мошенничества. Но в любой ситуации стоит проявить бдительность.