

Типичные уловки и ошибки мышления, которыми пользуются мошенники

Жертвами обмана мошенников может стать любой человек вне зависимости от его образования и уровня интеллекта. Причиной является то, что мошенники используют **уловки, нацеленные на заложенные природой человека ошибки мышления, а также воздействуют на его эмоции**. Даже самый сознательный человек в момент стресса, спешки или в незнакомой сфере может отключить критическое мышление и попасть в ловушку.

Оглавление

Давление временем	2
Эффект дефицита (ограниченности предложения).....	2
Эффект авторитета	2
Принцип взаимности.....	3
Соглашение с мнением большинства	3
Эффект «соглашения после малого».....	4
Первое впечатление переносится на весь образ человека	4
Предвзятость подтверждения	5
Предвзятость из-за личной симпатии	5
Эвристика доступности.....	6
Неприязнь к потерям	6
Излишний оптимизм	6
Любопытство.....	7
Форма подачи информации влияет на выбор.....	7
Склонность к статус-кво.....	7
Иллюзия контроля	8

Давление временем

Когда мошенник настаивает на действиях, не терпящих отлагательств, мозг человека переключается на «быстрые решения» и снижает критичность. Поэтому мы хуже проверяем факты и чаще соглашаемся «лишь бы успеть».

Как это используют мошенники (примеры):

«Срочно подтвердите — иначе блокировка», «нужно решение до конца часа».

Звонок якобы родственника или знакомого с просьбой срочно помочь.

Звонок из «коммунальной службы»: «отключим свет через 30 минут — оплатите немедленно».

Мошенническое письмо «аккаунт заблокируют через 10 минут» с фишинговой формой входа.

«Пока мы говорим, злоумышленник уже в вашем аккаунте — действуйте мгновенно.»

Эффект дефицита (ограниченности предложения)

Если человеку говорят, что предложение «очень редкое» или «ограничено во времени», он придаёт ему большую ценность и спешит воспользоваться. Мошенники используют приёмы «горячих предложений», «специальных условий», что отключает критическое мышление.

Как это используют мошенники (примеры):

«Акция действует только сегодня до 23:00, потом условия сгорят».

«Я как специалист могу применить для вас служебный промокод, но только если вы дадите согласие прямо сейчас».

«Это персональное предложение, сгенерированное системой только для вашего аккаунта. Оно не доступно при обычном заказе».

Фразы «это последний экземпляр», «последние места», «специальные условия», «только для вас», «вам повезло», «закрытый доступ».

Эффект авторитета

Люди склонны доверять и подчиняться авторитетам или официальным лицам. Мошенники пользуются этим, выдавая себя за сотрудников банков, полиции, спецслужб, руководителей компаний и т.п.

Как это используют мошенники (примеры):

«Я из МВД/следственного отдела, разговор записывается — отвечайте четко».

«Техподдержка Госуслуг: подтверждаем вашу личность, назовите код из СМС».

«Ваш компьютер заражен и рассылает вирусы. Сейчас я помогу вам устранить угрозу».

Мошенники могут подкреплять обман используя профессиональную лексику, поддельные бланки или визуальные символы власти, чтобы усилить доверие.

Принцип взаимности

Мы чувствуем обязательство ответить тем же за полученное благо. Мошенники дают «что-то бесплатное», чтобы вызвать чувство долга. Это может быть бесплатный бонус, бесплатная консультация, розыгрыш «подарка» – после чего жертва «не может отказать».

Как это используют мошенники (примеры):

«Мы уже заблокировали подозрительный перевод — помогите: назовите код».

«Я оформлю возврат без очереди, а вы просто подтвердите личность».

«Мы бесплатно продлили вам подписку, осталось подтвердить СМС».

«Вам положена компенсация/выплата»: сначала «помогают оформить», потом просят оплатить «комиссию».

«Приз/подарок от бренда — нужно оплатить только доставку».

Соглашение с мнением большинства

Люди склонны повторять действия других, особенно если они успешны или многочисленны. Мошенники сообщают жертве, что «многие уже выиграли/получили выгоду» от схемы, показывают фальшивые отзывы и «лайки», создают видимость массового спроса.

Как это используют мошенники (примеры):

Техника «Все уже согласились»: мошенник, выдавая себя за IT-специалиста, заявляет «Мне срочно нужно установить обновление безопасности на все компьютеры. Я уже договорился с вашим начальником Ивановым, и все отделы, кроме вашего, уже выполнили установку. Давайте ваши данные для входа, чтобы не задерживать процесс».

«Все ваши соседи уже получили перерасчет, вы остались последним».

«Девяносто процентов клиентов подтверждают по телефону — это стандарт».

Жертву добавляют в Telegram-чат или WhatsApp-чат, где «успешные инвесторы» (актеры или боты) активно делятся скриншотами своих доходов, благодарят «советника» и подогревают ажиотаж.

«Все уже прошли проверку — вы последний».

«Все сотрудники прошли обновление — остались только вы».

На фишинговой странице или сайте-одностраничнике появляются всплывающие окна вроде «Елена из Москвы только что купила этот курс», «Еще 3 человека рассматривают этот товар прямо сейчас», «Осталось 2 места по акции».

Поддельные комментарии: «подтверждаю, служба поддержки помогла».

Эффект «соглашения после малого»

Если человек уже согласился на небольшую просьбу, то ему сложнее отказаться от большой. Мошенники используют технику «нога в двери»: сначала просят небольшое одолжение или действие, после чего просьба становится крупнее. Формируется убеждение «я — человек, который помогает/сотрудничает», и жертва продолжает.

Как это используют мошенники (примеры):

Сценарий «подтверждение данных»: жертве приходит письмо или сообщение якобы от банка с просьбой подтвердить один-два параметра (например, дату рождения или последние цифры номера карты) для «проверки безопасности» или «активации нового сервиса».

Звонок или сообщение о том, что человек выиграл приз или ему положена компенсация (например, за переплату по ЖКХ). Для начала просят назвать лишь ФИО и адрес для «проверки в базе».

«Вы начали процедуру возврата, нельзя бросать на середине».

«Вы уже отправили данные, остался финальный шаг — подтвердите операцию».

Первое впечатление переносится на весь образ человека

Когда у человека сложилось положительное первое впечатление о ком-то, он склонен воспринимать его и последующие его действия или черты более благоприятно, чем они могут быть на самом деле.

Как это используют мошенники (примеры):

Мошенники создают сайт-подделку известного интернет-банка (с фирменным дизайном) и присылают его как ссылку.

Мошенник может точно назвать данные жертвы (купленные в даркнете), использовать профессиональную лексику, номер телефона, подделанный под официальный (подменный номер).

Мошенник говорит уверенно, использует технические термины.

Предвзятость подтверждения

Мы склонны замечать и запоминать только ту информацию, которая подтверждает наши ожидания и убеждения, игнорируя противоречащие данные. Мошенники подстраивают историю под ваши ценности/страхи/убеждения.

Как это используют мошенники (примеры):

Мошенник изучает публичную активность жертвы (в соцсетях, на форумах) и предлагает жертве «уникальную возможность», соответствующую её убеждениям.

Мошенники нацеливаются на людей, глубоко вовлеченных в религиозные или духовные практики (например, через группы в соцсетях), и предлагают «особую молитву», «заряженный» предмет или платный обряд для решения проблемы (здоровье, деньги, любовь), ссылаясь на авторитетных для жертвы духовных лидеров или тексты.

Если жертва убеждена, что «миром правят тайные заговоры», а официальные СМИ лгут, то мошенники предлагают ей «секретную информацию» или «запрещенную технологию».

Предвзятость из-за личной симпатии

Мы легче доверяем тем, кто нам нравится: «похож на нас», «вежливый», «общий знакомый». Приятный тон и «общие темы» снижают настороженность.

Если нам кто-то симпатичен (из-за внешности, чувства юмора, общих интересов), мы неосознанно начинаем выше оценивать его профессиональные качества, ум, правоту в споре или надёжность, даже если для этого нет объективных оснований.

Как это используют мошенники (примеры):

Мошенник изучает профиль жертвы в соцсетях, находит общие точки: один город, университет, хобби, сфера работы. В первом же сообщении он упоминает это.

Мошенник вступает в тематическую группу (рыбалка, вязание, IT, криптовалюта), ведет себя как активный и знающий участник, помогает другим, вызывает симпатию и уважение, но через некоторое время он начинает «по-дружески» советовать перейти по ссылке и воспользоваться «выгодным» предложением.

«Я вам искренне сочувствую — давайте помогу, только сделайте как скажу».
«Мы с вами отлично поняли друг друга, доверьтесь мне — я на вашей стороне».

«Я тоже пострадал от такого, поэтому знаю, как быстро все исправить».

Эвристика доступности

Мы переоцениваем вероятность событий, о которых «вспоминается легко» (новости или недавний опыт, особенно эмоционально заряженные). После громкого инцидента легче поверить в похожую угрозу. Мошенники подстраиваются под информационную повестку и недавние события.

Как это используют мошенники (примеры):

После новостей о взломе крупного сервиса (например, соцсети) жертве приходит письмо якобы от этой компании: «В связи с недавним инцидентом безопасности мы вынуждены сбросить ваши пароли. Для защиты аккаунта немедленно смените пароль по ссылке».

После переезда/ремонта: «служба домофона/управляющая компания» → «оплатите замену ключей по ссылке».

«Сейчас массово взламывают мессенджеры, у вас типичные признаки».

«Мы видим вход из другой страны, как это часто бывает при взломе».

Неприязнь к потерям

Потеря психологически ощущается сильнее, чем равная по размеру выгода. В жизни: «не потерять» мотивирует сильнее, чем «получить» и поэтому человек готов делать лишнее, чтобы «спасти» деньги/аккаунт.

Как это используют мошенники (примеры):

«Ваши деньги в опасности — срочно переведите на “защищенный счёт”».

«Подозрительная покупка на маркетплейсе — подтвердите отмену по ссылке».

Псевдо-банк: «чтобы не потерять доступ, назовите одноразовый код из SMS».

«Кредит на ваше имя уже оформляют — нужно срочно остановить».

Излишний оптимизм

Или «со мной такого не случится». Вероятность негативных событий часто недооценивается, а позитивных переоценивается.

Как это используют мошенники (примеры):

«Я просто посмотрю ссылку» — кликает по фишингу, считая риск минимальным.

«Я быстро разберусь» → устанавливает программу удалённого доступа «для поддержки».

«Со мной не случится» → отправляет предоплату за аренду без просмотра или вкладывается в сомнительные инвестиции.

Любопытство

Человека привлекает неизвестность или интрига – и он готов рискнуть, чтобы раскрыть её. Мошенники специально провоцируют любопытство сверх обычного.

Как это используют мошенники (примеры):

Фишинг-схема «Это вы на фото?»

Сообщение «Вас упомянули в этой статье» и ссылка на файл .apk или сайт. Люди кликают «чтобы узнать, что говорят о них».

Анонс «секретного разоблачительного видео»: присылается ссылка на сайт с «эксклюзивом», но он оказался фейковым и запросил ввод пароля.

СМС-сообщение «Вы в списке счастливицов на миллион – узнайте результат по ссылке».

Форма подачи информации влияет на выбор

Одно и то же может звучать иначе в разных формулировках. Мошенники подают своё предложение в максимально выгодном свете.

Как это используют мошенники (примеры):

«Это не перевод мошеннику, а возврат/компенсация — просто подтвердите платёж».

«Мы не просим деньги, мы проверяем счёт» — на самом деле перевод на счёт злоумышленника.

Не удалённый доступ с целью захвата управления устройством, а «диагностика поломки» или «помощь в обновлении»

«Мы не просим данные — мы лишь подтверждаем, что вы владелец».

«Это не оплата, а верификация карты для возврата средств».

«Вы не теряете деньги — вы их замораживаете до проверки».

Склонность к статус-кво

Люди предпочитают сохранять текущее положение дел. Мошенники пользуются стремлением своих жертв к сохранению привычного, основанном на

психологическом комфорте и страхе перед потерями. Мошенники заставляют поверить, что ничего не делать (или не следовать их инструкциям) — это риск потерять имеющееся.

Как это используют мошенники (примеры):

«Для сохранения текущего тарифа/услуги нужно подтвердить данные».

«Чтобы карта продолжала работать как обычно, пройдите верификацию».

«Чтобы не потерять доступ к государственным услугам, подтвердите учётную запись».

«Для продолжения бесплатного использования обновите лицензионный ключ».

«Ваша подписка будет автоматически продлена по увеличенной ставке, если не отмените».

Иллюзия контроля

Это тенденция людей верить, что они могут контролировать или по крайней мере влиять на результаты событий. Нам кажется, что «я все контролирую», если сам делаю действия — даже если это ловушка.

Как это используют мошенники (примеры):

«Вы сами отмените списание: продиктуйте код, и вы поставите блок».

«Сейчас вы вручную включите защиту — откройте ссылку и нажмите “активировать”».

«Вы лично подтвердите безопасность, введя данные на странице проверки».

«Только вы можете остановить операцию, действуйте сами прямо сейчас».

«Сделайте перевод самостоятельно — тогда деньги будут под вашим контролем».