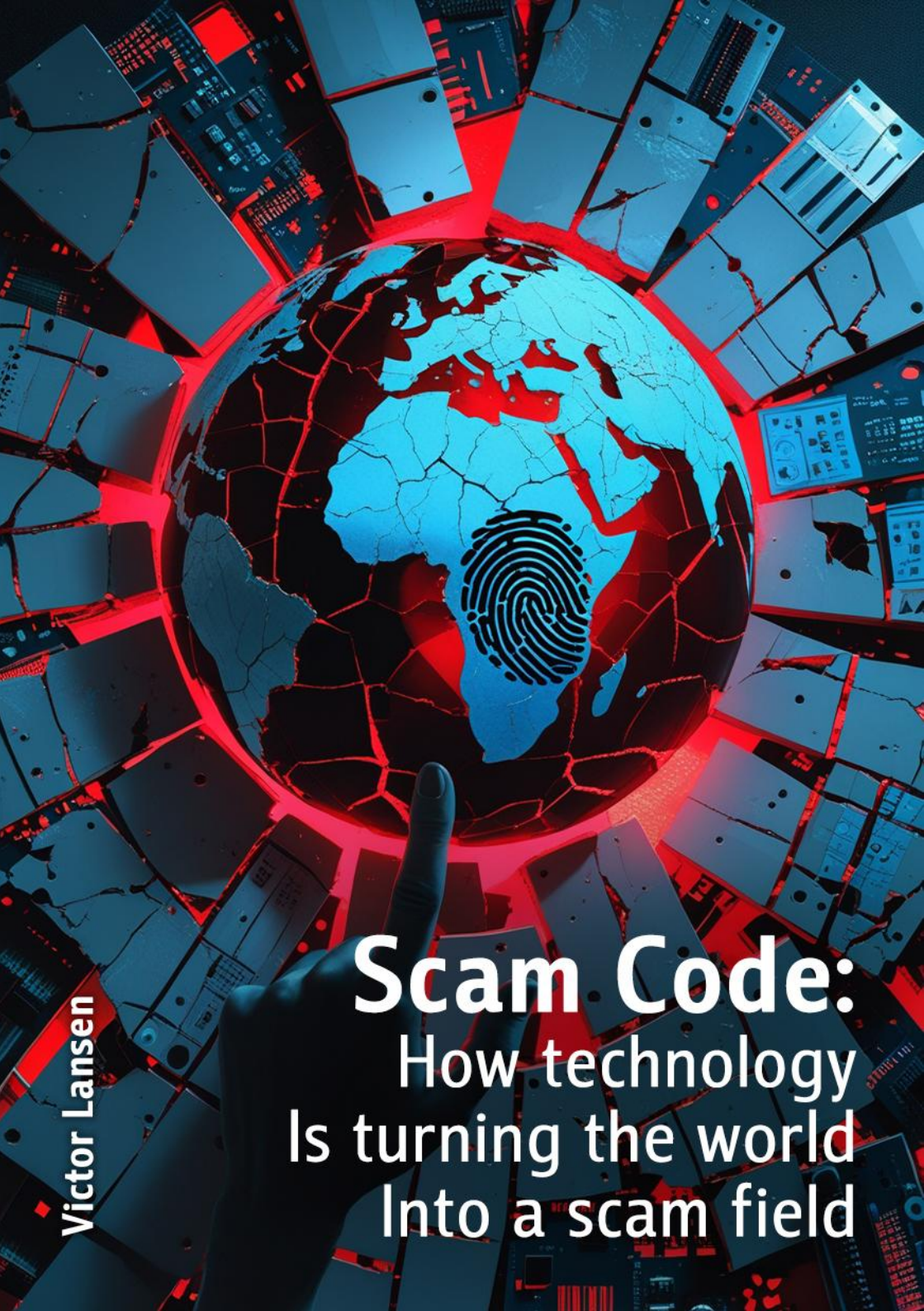

Scam Code:
How technology Is turning the world Into a scam field

Victor Lansen

Виктор Лансен

Scam Code:

Как технологии превращают мир в поле для афер

Victor Lansen
Scam Code: How technology is turning the world into a scam field

Disclaimer

Эта книга создана искусственным интеллектом. Её содержание основано на анализе открытых источников, но может содержать неточности. Рекомендуется перепроверять ключевые факты по авторитетным научным или профессиональным материалам.

NeuraBooks – некоммерческий проект, использующий нейросети (ChatGPT, DeepSeek, Gemini и другие модели) для генерации образовательного контента. Авторы, указанные в книге, а также возможные участники, поделившиеся своим мнением, являются вымышленными персонажами. Некоторые ситуации могут быть нереальными, но важными для освещения той или иной проблемы.

Используйте эту книгу как отправную точку для изучения темы, а не как единственный источник истины.

Более подробная информация доступна на нашем сайте neurabooks.ru

Введение: Игра, в которой вы уже участвуете

В тот день я потерял 5,000 евро за 17 минут.

Нет, меня не ограбили в тёмном переулке. Я сидел в светлом офисе, с чашкой кофе, перед монитором с графиками «перспективной криптовалюты». Я – эксперт по кибербезопасности, человек, который консультирует банки о защите от мошенников, – добровольно перевёл деньги на биржу, которой на следующий день уже не существовало.

Мне было стыдно. Я был зол. И я был... благодарен.

Благодарен, потому что эта ошибка стоимостью в 5,000 евро спасла мне карьеру. Она напомнила то, что я должен был помнить всегда: *никто не застрахован от обмана*.

Возможно, вы читаете эту книгу, потому что вас уже обманули. Или вы боитесь, что вас могут обмануть. Может быть, вы просто любопытны – как устроен мир современного мошенничества? В любом случае, вы приняли правильное решение. Потому что первый шаг к безопасности – это признание факта: мы все уязвимы.

Когда я рассказываю на конференциях о кибермошенничестве, после выступления ко мне часто подходят люди с одной и той же фразой: *«Меня-то не обманут, я слишком умный для этого»*.

Эти же люди через полгода звонят мне с просьбой помочь вернуть деньги, украденные с их счетов.

Дело не в интеллекте. Профессора Гарварда и инженеры Google становятся жертвами мошенников с той же частотой, что и пенсионеры из маленьких городков. Разница лишь в типе приманки, на которую они клюют.

За последние 20 лет технологии изменили нашу жизнь до неузнаваемости. Мы совершаем покупки, не выходя из дома. Находим любовь через приложения. Инвестируем в компании, которые никогда не видели. Доверяем цифрам на экране больше, чем наличным в кармане.

И с каждым новым удобством, каждой новой технологией открывается новая брешь для тех, кто хочет завладеть вашими деньгами.

В 2022 году мировые потери от кибермошенничества превысили 600 миллиардов долларов. Эта сумма больше, чем ВВП Швеции – страны, где я живу. И каждый год эта цифра растёт на 15–20%.

Но дело не только в деньгах.

Когда вы становитесь жертвой мошенников, вы теряете нечто более ценное – веру в людей. Доверие к технологиям. Чувство безопасности в современном мире. Некоторые жертвы никогда больше не совершают онлайн-платежи. Другие перестают отвечать на звонки с незнакомых номеров. Третьи уходят из соцсетей.

Мошенники крадут не только деньги – они крадут будущее. Наше цифровое будущее.

В этой книге я не буду вас запугивать. Я не собираюсь призывать вернуться к наличным расчётам и бумажным письмам. Мир движется вперёд, и мы должны двигаться вместе с ним.

Вместо этого я хочу показать вам невидимые нити, за которые дёргают современные мошенники. Расследовать вместе с вами самые изощрённые схемы обмана. И научить вас видеть тревожные сигналы там, где большинство видит только возможности.

Мы проследим эволюцию мошенничества – от древних фальшивомонетчиков до NFT-скамов[1] и deepfake[2]-видео. Поговорим о психологии обмана и о том, почему даже самые умные люди попадаются на примитивные уловки. И, конечно, я дам вам конкретные инструменты защиты – технические и психологические.

«Если предложение кажется слишком хорошим, чтобы быть правдой – скорее всего, это ложь». Вы наверняка слышали эту фразу. Проблема в том, что современные мошенники уже не предлагают вам «слишком хорошие» сделки.

Они предлагают *правдоподобные*.

«Инвестируйте и получите 7% годовых» звучит разумнее, чем *«станьте миллионером за месяц»*. *«Ваша посылка*

---

[1] ***Скам*** *(от англ. scam – «мошенничество») – это обманная схема, при которой организаторы обещают высокую прибыль или ценный продукт, но исчезают с деньгами участников, не выполняя обязательств.*

[2] ***Deepfake*** *(от англ. deep learning + fake – «глубокое обучение» + «подделка») – это технология искусственного интеллекта, создающая поддельные фото, видео или аудио, где человек говорит или делает то, чего не было в реальности, с помощью нейросетей.*

задержана, оплатите пошлину в 15 евро» выглядит более реалистично, чем *«вы выиграли миллион в лотерею»*.

Современное мошенничество не кричит. Оно шепчет. И звучит так же, как правда.

Перед вами не просто книга. Это – детективное расследование. Руководство к выживанию. И, надеюсь, прививка от наивности, которой так не хватает в нашем перенасыщенном информацией мире.

Готовы увидеть невидимое?

Тогда переворачивайте страницу. Погружение в мир профессионального обмана начинается.

И помните: самый опасный мошенник – тот, о существовании которого вы даже не подозреваете.

Виктор Лансен

Стокгольм, 2024

Часть 1

История мошенничества: от древности до XX века

Глава 1. Искусство обмана: первые мошенники в истории человечества

Когда мошенничество было искусством

Представьте: Древний Рим, шумный рынок, торговец с широкой улыбкой предлагает вам монету с профилем императора. Блестящая, тяжелая, она выглядит точно настоящая. Вы отдаёте свои сбережения, а через неделю узнаёте, что внутри – обычный свинец, покрытый тонким слоем золота.

Поздравляю: вы только что стали жертвой одной из древнейших афер в истории человечества.

Когда мы говорим о мошенничестве, многие представляют хакеров в тёмных комнатах, компьютерные коды и крипто-схемы. Но правда в том, что мошенничество старше, чем письменность. Оно возникло в тот момент, когда один человек понял, что может получить выгоду, обманув другого.

Я начал исследовать историю мошенничества после того, как меня самого обманули. Мне хотелось понять: было ли то, что случилось со мной, чем-то принципиально новым? Или я просто стал жертвой древнего как мир трюка, просто в новой упаковке?

То, что я обнаружил, поразило меня: **почти все современные схемы мошенничества имеют прототипы в далёком прошлом**. И знание этих прототипов может стать нашим щитом сегодня.

Фальшивомонетчики: первые финансовые хакеры

Самое раннее зафиксированное мошенничество в истории связано с подделкой денег. Археологи находят фальшивые монеты, датируемые 500–600 годами до нашей эры. Представьте себе древнегреческого или персидского «хакера», который вместо взлома банковского приложения создавал поддельные драхмы или дарики.

Технология была простой, но эффективной: брали дешёвый металл (обычно свинец или медь), покрывали его тонким слоем драгоценного металла и штамповали изображение, имитирующее настоящие монеты. Такие подделки идеально работали при слабом свете рыночных прилавков.

В Древнем Риме фальшивомонетничество процветало настолько, что император Константин приравнял его к государственной измене и карал смертной казнью. Но даже угроза сожжения заживо не останавливала мошенников. Почему? Потому что прибыль стоила риска.

Это первый урок, который нам даёт история мошенничества: там, где есть возможность большой и быстрой прибыли при низких начальных затратах, всегда найдутся желающие обмануть систему.

Современные мошенники, создающие фишинговые[3] сайты банков, следуют той же логике. Затраты минимальны

[3] ***Фишинг*** *(от англ. phishing – «ловля паролей») – это вид кибермошенничества, при котором злоумышленники маскируются под легитимные компании или знакомых, чтобы выманить у жертвы конфиденциальные данные (логины, пароли, банковские реквизиты) через поддельные письма, сайты или сообщения.*

(домен, хостинг, базовое программирование), а потенциальная прибыль огромна. Только вместо свинца с позолотой они используют HTML-код и логотипы известных брендов.

«Эликсиры жизни»: первый медицинский маркетинг

Если вы когда-нибудь получали спам о «чудодейственных» таблетках для похудения или препаратах, «которые официальная медицина скрывает», знайте: вы столкнулись с прямым наследником средневековых алхимиков.

В середине XIV века, когда Европу опустошала Чёрная смерть, улицы заполнились торговцами «чудодейственными эликсирами», якобы защищающими от чумы. Состав этих снадобий был абсурдным: от порошка из измельченных египетских мумий до настоя из лягушачьей кожи.

Одним из самых известных мошенников того времени был Леонардо Фиораванти, итальянский алхимик XVI века. Он путешествовал по Европе, продавая «универсальное лекарство», которое, по его утверждению, могло вылечить всё – от бородавок до чумы. Позже выяснилось, что его «чудо-средство» содержало в основном спирт и травы с незначительным медицинским эффектом.

Второй урок: в моменты страха и неопределенности люди особенно уязвимы перед мошенниками.

Вспомните начало пандемии COVID-19, когда в интернете мгновенно появились «защитные амулеты», «антивирусные эссенции» и прочие бесполезные продукты по завышенным ценам. Механизм тот же: эксплуатация страха ради прибыли.

Брачные аферисты: любовь как инструмент обмана

Возможно, вы слышали о современных романтических мошенниках, которые выманивают деньги через сайты знакомств. Представьте моё удивление, когда я обнаружил, что первые задокументированные случаи «брачного мошенничества» относятся к XVII веку.

В 1670-х годах в Англии некий Джон Колл прославился тем, что поочередно женился на богатых вдовах, выманивал их состояние и исчезал. По разным данным, его жертвами стали от 7 до 12 женщин. Его метод был прост: он представлялся богатым джентльменом, влюблял в себя состоятельную даму, а после свадьбы убеждал её продать имущество и «инвестировать» в несуществующий бизнес.

Сегодня схема практически не изменилась. Мошенники из приложений для знакомств используют те же приёмы: создание ложной личности, быстрое эмоциональное сближение, а затем «неожиданные проблемы», требующие финансовой помощи.

Третий урок: когда эмоции берут верх над разумом, мы становимся уязвимыми для обмана.

Финансовые пирамиды: старше, чем вы думаете

Многие считают, что первые финансовые пирамиды появились в XX веке. На самом деле, первая зафиксированная в истории финансовая пирамида была создана в 1719–1720 годах и называлась «Компания Южных морей».

Компания получила от британского правительства монополию на торговлю с Южной Америкой и начала продавать акции, обещая невероятные прибыли от эксплуатации якобы неисчерпаемых ресурсов Нового Света. Акции стремительно росли в цене – с £100 до £1,000 за несколько месяцев. Люди брали кредиты, продавали имущество, лишь бы купить заветные бумаги.

Был только один нюанс: реальной торговли практически не было. Испания контролировала большую часть Южной Америки и не пускала британские корабли к своим колониям. Но компания скрывала этот факт и продолжала раздувать стоимость акций с помощью фальшивых новостей и подкупа влиятельных лиц.

К сентябрю 1720 года пузырь лопнул. Цена акций рухнула до изначальной, тысячи инвесторов разорились, а некоторые даже покончили с собой.

Знакомо звучит? Вспомните криптовалютный бум 2017 года, когда ICO (Initial Coin Offering) обещали революцию в мире финансов и тысячекратную прибыль инвесторам. Большинство этих проектов оказались пустышками, а некоторые – откровенными пирамидами.

Четвёртый урок: гарантированная высокая доходность при минимальном риске – первый признак мошенничества, вне зависимости от эпохи.

Карточные шулеры и «напёрсточники»: психология обмана

История игорного мошенничества особенно интересна, потому что она раскрывает фундаментальные принципы психологической манипуляции, которые используются мошенниками и сегодня.

В XVIII–XIX веках профессиональные карточные шулеры путешествовали по Европе и Америке, обчищая карманы доверчивых игроков. Они использовали меченые карты, подставных игроков и виртуозно владели техникой «ловкости рук».

Но самое интересное не техническая сторона, а психологические приёмы. Классическая схема работала так:

1. Шулер позволял жертве выиграть несколько небольших партий;
2. Создавал иллюзию, что жертва особенно удачлива или талантлива;
3. Поощрял увеличивать ставки;
4. В решающий момент, когда на кону стояла серьёзная сумма, забирал всё.

Эта схема – прообраз многих современных мошенничеств в сфере инвестиций. Мошеннические брокерские платформы часто используют «демо-счета» или позволяют новичкам сделать несколько успешных сделок с минимальными суммами. Когда жертва, уверенная в своем везении, вносит крупную сумму – деньги исчезают.

Ещё один показательный пример – игра в напёрстки, появившаяся в средневековой Европе и достигшая пика популярности в XIX веке. Суть проста: нужно угадать, под каким из трёх

стаканов находится шарик после того, как мошенник быстро перемещает их.

Хитрость в том, что в большинстве случаев шарика нет ни под одним из стаканов – ловкость рук позволяет мошеннику незаметно извлечь его. Но что ещё важнее – «напёрсточник» никогда не работает один. Вокруг всегда есть «подсадные утки» – сообщники, которые делают вид, что легко выигрывают, подогревая азарт настоящих жертв.

Этот принцип «социального доказательства» широко используется в современных схемах. Фальшивые отзывы о «чудо-таблетках», боты в комментариях к инвестиционным проектам, фиктивные профили «успешных трейдеров» – всё это современные «подсадные утки», создающие иллюзию, что схема работает.

Пятый урок: если вы видите, что другие легко зарабатывают на чём-то, будьте вдвойне осторожны – возможно, это «подсадные утки».

Мошенники и технологии: гонка вооружений

История мошенничества – это история адаптации. С появлением каждой новой технологии мошенники быстро находили способ использовать её в своих целях.

Когда в середине XIX века появился телеграф, мошенники изобрели «телеграфные аферы» – отправляли ложные сообщения о колебаниях цен на бирже, чтобы манипулировать рынком.

С распространением почтовой системы возникли «письма счастья» и прототип современных «нигерийских писем» – просьбы о помощи в получении наследства.

Появление телефона породило телефонных мошенников, выдающих себя за банковских сотрудников или родственников в беде.

Интернет вывел мошенничество на новый уровень, сделав его глобальным, анонимным и масштабируемым. Но базовые принципы остались теми же.

Шестой урок: мошенничество эволюционирует вместе с технологиями, но его сущность остается неизменной.

Чему нас учит история мошенничества?

Изучая историю обмана, я пришел к важному выводу: несмотря на всю технологическую сложность современных схем, они эксплуатируют те же человеческие слабости, что и тысячи лет назад:

- **Жадность** – желание получить что-то ценное задешево или «быстро разбогатеть»;
- **Страх** – боязнь упустить возможность или столкнуться с опасностью;
- **Доверие** – склонность верить авторитетам или «официальным» источникам;
- **Спешка** – необходимость принять решение «здесь и сейчас», не имея времени на проверку.

Современные мошенники добавили к этому списку ещё одну слабость:

- **Технологический разрыв** – недостаточное понимание работы новых технологий.

Когда пожилая женщина отдаёт деньги телефонному мошеннику, потому что тот «звонит из банка», она становится жертвой того же принципа, что и средневековый крестьянин, покупающий «чудодейственный эликсир» у шарлатана, утверждающего, что он придворный врач короля.

Что делать: уроки из прошлого для защиты в настоящем

1. **Помните о вечных приманках**

Необычайно высокая прибыль, гарантированный результат, эксклюзивный доступ, ограниченное предложение – всё это красные флаги, не зависящие от эпохи и технологии.

2. **Не принимайте решения в спешке**

Мошенники всех времен создают искусственное чувство срочности. *«Только сегодня»*, *«последняя возможность»*, *«счёт заблокируют через час»*. Сделайте паузу. Проверьте информацию по официальным каналам.

3. **Ищите социальное подтверждение из независимых источников**

Если кто-то утверждает, что его продукт или услуга популярны, ищите подтверждение этому не на его сайте, а на независимых платформах и у людей, которым вы доверяете.

4. **Изучайте технологии, которыми пользуетесь**

Современные мошенники часто эксплуатируют технологический разрыв. Базовое понимание принципов работы платёжных систем, криптовалют или онлайн-банкинга – ваш щит от обмана.

5. **Применяйте «правило бабушки»**

Перед тем как согласиться на предложение или совершить платёж, спросите себя: *«Как бы я объяснил это решение своей бабушке?»*. Если объяснение получается запутанным или стыдным, возможно, вы имеете дело с мошенничеством.

В следующей главе мы погрузимся в золотой век мошенничества – XIX и XX века, когда появились первые масштабные финансовые пирамиды, страховые аферы и «бизнес-возможности», ставшие прообразами многих современных схем обмана. Мы увидим, как индустриализация и массовые коммуникации трансформировали мошенничество из «ремесла» в «индустрию».

А пока запомните главное: то, что кажется новой, невиданной ранее схемой обмана, часто оказывается старым трюком в новой обёртке. И зная прошлое, мы лучше защищены в настоящем.

Глава 2. Золотой век обмана: как мошенники индустриализировали свое ремесло

Когда аферы стали масштабными

На рубеже XIX–XX веков мир стремительно менялся. Индустриализация, массовая пресса, телеграф, телефон, железные дороги – все это не только упрощало жизнь честных граждан, но и открывало невиданные перспективы для мошенников.

Если древние аферисты редко могли обмануть больше нескольких десятков человек, то их наследники в индустриальную эпоху научились обманывать тысячи и даже миллионы. Они создали настоящие империи обмана, превратили мошенничество из кустарного промысла в хорошо отлаженную индустрию.

Когда я рассказываю студентам на своих лекциях о схемах XIX–XX веков, они часто удивляются: *«Как люди могли быть такими наивными?»* Но если посмотреть внимательнее, становится очевидно: современные жертвы киберпреступников попадаются по тем же причинам, что и их прадедушки.

Более того, многие сегодняшние криптовалютные пирамиды или инвестиционные аферы – это почти точные копии схем столетней давности, просто замаскированные под технологический прогресс. Как говорится, хочешь предсказать будущее мошенничества – изучи его прошлое.

Виктор Люстиг: человек, продавший Эйфелеву башню

Один из моих любимых исторических мошенников – Виктор Люстиг, человек, который дважды продал Эйфелеву башню, не будучи её владельцем.

В 1925 году Люстиг, выдавая себя за государственного чиновника, собрал группу парижских торговцев металлоломом и сообщил им «конфиденциальную информацию»: правительство якобы решило демонтировать Эйфелеву башню из-за дороговизны её содержания. Он предложил продать башню на металлолом, устроив закрытый аукцион среди присутствующих.

Одному из дилеров, Андре Пуассону, Люстиг намекнул, что для получения контракта потребуется «вознаграждение» – взятка. Пуассон, боясь упустить выгодную сделку, заплатил и за башню, и взятку. Когда он понял, что его обманули, было уже поздно – Люстиг скрылся с деньгами.

Самое удивительное, что через несколько месяцев Люстиг вернулся в Париж и провернул тот же трюк с другой группой торговцев. На этот раз жертва сразу обратилась в полицию, но мошенник успел скрыться.

Чему нас учит эта история? Большинство масштабных афер строится на эксплуатации двух человеческих слабостей: жадности и страха упустить выгоду. Пуассон настолько боялся, что кто-то другой получит «выгодную сделку», что отключил критическое мышление.

В наши дни механизм тот же. Когда вы видите рекламу *«уникальной инвестиционной возможности»* или токена, который *«точно вырастет в 100 раз»*, спросите себя: не боюсь ли я

упустить выгоду настолько, что готов принять решение без должной проверки?

Чарльз Понци и его «схема»

Имя Чарльза Понци стало нарицательным – «схема Понци» теперь синоним финансовой пирамиды. Но что именно сделал этот итальянский иммигрант в Америке начала XX века?

В 1919 году Понци основал компанию «Securities Exchange Company» и предложил инвесторам 50% прибыли за 45 дней или 100% за 90 дней. Он утверждал, что разработал гениальную схему арбитража с международными почтовыми купонами.

Идея звучала убедительно: купить купоны в странах с ослабленной валютой и обменять их в США по гораздо более высокой стоимости. Звучит как современные схемы арбитража с криптовалютами, не правда ли?

На самом деле, Понци просто платил ранним инвесторам деньгами новых вкладчиков. За восемь месяцев он собрал около 15 миллионов долларов (эквивалент примерно 200 миллионов долларов в сегодняшних деньгах) от более чем 40,000 инвесторов.

Схема рухнула после расследования газеты Boston Post. Обнаружив несоответствия в бизнес-модели Понци, журналисты опубликовали разгромную статью. Вкладчики бросились забирать свои деньги, и пирамида рухнула.

Важный урок: То, что схему Понци разоблачили журналисты, а не финансовые регуляторы, напоминает нам о важности независимых расследований и скептицизма. В наши дни любой

может быть «журналистом» – проверяйте информацию из нескольких источников, особенно если речь идет о ваших деньгах.

«Дети» Понци: великие пирамиды XX века

Схема Понци вдохновила множество подражателей. Вот три наиболее впечатляющих:

1. Лу Пирлман и Trans Continental Airlines

В 1980-х годах Пирлман создал вымышленную авиакомпанию и привлек более 300 миллионов долларов от банков и инвесторов. Деньги он использовал для создания музыкальной империи, запустив такие бойз-бэнды как Backstreet Boys и NSYNC.

Но авиакомпания существовала только на бумаге – фальшивые финансовые отчёты, поддельные офисы, несуществующие самолеты. Когда обман раскрылся в 2007 году, Пирлман получил 25 лет тюрьмы.

2. Бернард Мэдофф и самая крупная пирамида в истории

Мэдофф создал инвестиционный фонд, который якобы стабильно приносил 10–12% годовых независимо от рыночных условий. За почти 20 лет он привлёк около 65 миллиардов долларов от тысяч инвесторов, включая благотворительные фонды и знаменитостей.

Его схема рухнула во время финансового кризиса 2008 года, когда инвесторы попытались вывести средства, а новых

вкладчиков не было. Мэдофф признался в мошенничестве и был приговорён к 150 годам тюрьмы.

3. Сергей Мавроди и МММ

Для моей семьи, как и для многих русских, переехавших в Европу, эта история особенно близка. В 1990-х Мавроди создал в России финансовую пирамиду МММ, обещавшую доходность до 1000% годовых. Его рекламная кампания была гениальной – обычные люди в телевизионных роликах рассказывали, как разбогатели с МММ.

По разным оценкам, жертвами стали от 10 до 40 миллионов человек, потерявших в совокупности около 10 миллиардов долларов. После краха МММ Мавроди несколько раз пытался возродить свою схему в России и других странах, включая Индию и ЮАР.

Общий урок этих историй: независимо от эпохи, страны или масштаба, финансовые пирамиды имеют одинаковые признаки – обещание аномально высокой доходности при отсутствии прозрачной бизнес-модели. И все они неизбежно рушатся, когда приток новых средств становится меньше, чем выплаты старым инвесторам.

Букмекерские аферы: математическое мошенничество

В начале XX века появился новый тип мошенничества, который особенно интересует меня как человека с математическим бэкграундом – «беспроигрышные» букмекерские схемы.

Джозеф Вейл, известный как «Жёлтый Малыш», изобрёл схему, получившую название «проволочная афера». Он нанимал сообщников на ипподромах по всей Америке, которые с помощью скрытых телеграфных линий («проволок») передавали результаты скачек прежде, чем они становились известны в букмекерских конторах в других городах.

Пока информация о победителе гонки доходила до букмекеров официальными каналами, сообщники Вейла успевали сделать «беспроигрышные» ставки.

Со временем аферу усовершенствовали – мошенники открывали фальшивые букмекерские конторы, где принимали ставки на уже завершившиеся скачки, результат которых знали только они. Жертвам казалось, что они получили инсайдерскую информацию, и они уверенно ставили – и, конечно, проигрывали.

Современный аналог: Форекс-трейдеры и криптовалютные «гуру», предлагающие *«проверенные сигналы»* и *«беспроигрышные стратегии»*. Когда вам кажется, что вы получили информационное преимущество, спросите себя: почему этот человек делится ею со мной, а не использует сам?

«Испанский узник»: прадедушка «нигерийских писем»

Одна из самых длительных мошеннических схем в истории – так называемый «испанский узник». Первые упоминания о ней датируются началом XIX века, но она жива до сих пор в виде «нигерийских писем» или «писем счастья».

Изначальная схема была такой: жертва получала письмо якобы от испанского аристократа, заключенного в тюрьму по ложному обвинению. Аристократ сообщал, что имеет доступ к огромному состоянию, но не может получить его из-за заключения. Он предлагал адресату помочь с освобождением (внести залог или подкупить стражу) в обмен на щедрое вознаграждение из своего состояния.

С распространением почтовых служб в XIX веке эта афера стала массовой. Мошенники рассылали тысячи писем, и даже если отвечал всего один процент получателей, схема оказывалась прибыльной.

Современная версия: каждый из нас получал электронные письма от *«нигерийских принцев»* или *«попавших в беду миллионеров»*. Технология изменилась, но суть осталась той же – заставить жертву поверить, что небольшие начальные инвестиции принесут огромную прибыль.

Фальшивая лотерея: когда выигрыш оборачивается потерями

В Англии викторианской эпохи процветала схема «испанской лотереи». Жертва получала письмо о якобы выигранном призе в испанской лотерее. Но чтобы получить выигрыш, требовалось заплатить «налог», «комиссию» или «сбор за перевод».

Разумеется, никакой лотереи не существовало, и после отправки денег связь с «организаторами» обрывалась. Схема была настолько распространена, что в 1890-х годах британское правительство выпустило специальные предупреждения для граждан.

В 1923 году в США появился более сложный вариант этой схемы. Оскар Харцелл утверждал, что является наследником состояния сэра Фрэнсиса Дрейка, знаменитого мореплавателя XVI века. Он убедил более 70,000 американцев инвестировать в судебные разбирательства по получению наследства в обмен на долю в будущих выплатах.

Несмотря на то, что Дрейк умер за 300 лет до этого и не оставил прямых наследников, схема работала почти 10 лет и собрала миллионы долларов, прежде чем власти арестовали Харцелла.

Актуальный пример: SMS о выигрыше в конкурсе, в котором вы не участвовали, или электронные письма о призах в лотереях неизвестных стран. Если вас просят заплатить что-то, чтобы получить «выигрыш» – это почти наверняка мошенничество.

Иллюзия эксклюзивности: продажа несуществующего

В начале XX века в США процветала продажа несуществующей недвижимости. Чарльз Фишер и его сообщники продавали участки земли во Флориде, которые на самом деле были болотами или вообще не существовали. Они создавали красивые буклеты с фотографиями тропического рая и привлекали клиентов со всей страны.

Схема была особенно успешной, потому что предполагаемые участки находились далеко от мест проживания покупателей, и проверить реальность предложения было сложно. К тому

моменту, когда обман раскрывался, мошенники уже исчезали с деньгами.

В то же время в Европе процветала схема «эксклюзивных инвестиционных клубов». Мошенники создавали впечатление закрытых элитных сообществ, куда можно попасть только «по рекомендации» и после внесения существенного взноса. Внутри якобы делились инсайдерской информацией о биржевых торгах или бизнес-возможностях.

Современный вариант: Закрытые криптовалютные группы в Telegram, где «эксперты» делятся «секретными сигналами», или платные курсы с обещанием раскрыть «тайны быстрого обогащения». Иллюзия эксклюзивности заставляет людей отключать критическое мышление – *«если информация доступна не всем, значит, она ценная»*.

Уроки золотого века мошенничества

Изучая классические схемы мошенничества XIX–XX веков, я выделил пять ключевых принципов, которые остаются актуальными и сегодня:

1. **Масштабирование через технологии**

Мошенники всегда используют новейшие технологии для расширения своего охвата. Почта, телеграф, радио, интернет – каждая новая технология связи становится инструментом обмана.

2. **Эксплуатация информационной асимметрии**

Многие схемы работают именно потому, что жертва не может проверить информацию. «Испанский узник» был далеко,

букмекерские результаты невозможно было моментально проверить, земля во Флориде была недоступна для осмотра.

3. **Социальное подтверждение и ложное большинство**

Массовые пирамиды вроде МММ работают за счёт создания иллюзии: *«все вокруг зарабатывают, только вы ещё нет»*. Чем больше людей вовлечено, тем меньше скептицизма у новых жертв.

4. **Использование доверия к авторитетам**

Мошенники часто выдают себя за представителей государства, известных компаний или создают поддельные документы с официальными печатями. Люстиг представлялся правительственным чиновником, Мэдофф – уважаемым финансистом.

5. **Эксплуатация надежды и отчаяния**

Великая депрессия, послевоенные годы, экономические кризисы – периоды, когда люди особенно уязвимы для мошенников, обещающих быстрое решение финансовых проблем.

Что делать: защита от классических схем в современном мире

1. **Изучайте историю мошенничества**

Знание классических схем помогает распознавать их современные версии. Если предложение напоминает вам исторические аферы – будьте особенно осторожны.

2. **Проверяйте информацию из независимых источников**

То, что схему Понци разоблачили журналисты, а не инвесторы, напоминает нам о важности независимых расследований. Не доверяйте только информации от заинтересованной стороны.

3. **Помните об информационной асимметрии**

Всегда спрашивайте себя: *«Могу ли я проверить эту информацию?»*. Если нет – риск мошенничества значительно возрастает.

4. **Избегайте давления срочности**

«Только сегодня», *«последняя возможность»*, *«осталось всего 5 мест»* – классические приёмы, заставляющие принимать решения в спешке. Берите время на размышление и проверку.

5. **Применяйте правило «слишком хорошо, чтобы быть правдой»**

Если предложение кажется исключительно выгодным – скорее всего, в нём есть подвох. Особенно если оно сочетается с ограниченной возможностью проверки.

В следующей главе мы перенесёмся в настоящее время и рассмотрим современные финансовые мошенничества – от инвестиционных пирамид до крипто-афер. Мы увидим, как классические схемы адаптировались к цифровой эпохе, и научимся распознавать их под новыми масками.

А пока запомните: схемы мошенничества меняются, но психология мошенников и их жертв остаётся неизменной.

Именно поэтому история – наш лучший учитель в вопросах защиты от обмана.

Часть 2

Современные схемы мошенничества

Глава 3. Цифровые пирамиды: когда финансовое мошенничество надевает костюм инноваций

Помню, как в 2017 году один клиент позвонил мне в панике: *«Виктор, я вложил все свои сбережения в криптофонд с гарантированной доходностью 25% в месяц. Они перестали отвечать на звонки»*. Я молчал несколько секунд. Прозвучит жестоко, но его деньги исчезли в тот момент, когда он поверил в *«гарантированные 25% в месяц»*. Это всё равно что поверить, что гравитация иногда берёт выходной.

Финансовое мошенничество – старейшая форма обмана, принявшая цифровой облик. Жадность остаётся неизменной константой, только методы привлечения жертв совершенствуются с каждым технологическим витком. Сегодня мошенники не стоят с мешком фальшивых монет на рыночной площади – они создают безупречные на вид сайты с графиками, отзывами и круглосуточной поддержкой. Деньги утекают не в мешок, а в криптокошельки на другом конце мира.

Пирамиды 2.0: От МММ до крипто-хайпов

В 1994 году Сергей Мавроди создал, возможно, самую известную финансовую пирамиду на постсоветском пространстве – МММ. Миллионы людей поверили в обещание доходности в 1000% годовых. Все знают, чем это закончилось.

Сегодня финансовые пирамиды вернулись в новом облике. Они называют себя «инвестиционными платформами», «трейдинговыми ботами» или «криптофондами».

«Инвестируйте всего $100 и получайте $10 каждый день, просто рекомендуя наш проект друзьям!»

Узнаёте знакомый почерк? Но теперь такие предложения приходят не в газете, а через таргетированную рекламу в социальных сетях, где искусственный интеллект точно определил, что вы – идеальная цель: человек, мечтающий о финансовой независимости, но не слишком хорошо разбирающийся в инвестициях.

Анатомия современной пирамиды

Современные пирамиды имеют характерные признаки:

1. **Обещание нереальной доходности**. Любая гарантия доходности выше 20% годовых должна вызывать подозрения. А если вам обещают 100% годовых или 10% ежемесячно – перед вами, скорее всего, пирамида.

2. **Непрозрачная бизнес-модель**. Когда на вопрос *«Как вы зарабатываете деньги?»* следует ответ, наполненный жаргоном и размытыми формулировками: *«Мы используем передовые алгоритмы и блокчейн[4]-технологии для арбитража на межбиржевых спредах с применением алгоритмов машинного обучения»* – скорее всего, это лапша на уши.

[4] ***Блокчейн*** *(англ. blockchain – «цепочка блоков») – это децентрализованная цифровая база данных, в которой информация хранится в виде последовательности связанных блоков.*

3. **Агрессивная реферальная программа**. Если проект больше сосредоточен на привлечении новых участников, чем на своём основном продукте – это классический признак пирамиды.

4. **Ограниченное время входа**. *«Только сегодня»*, *«Последние 50 мест»*, *«Закрытие регистрации через 24 часа»* – всё это приёмы создания искусственного дефицита, чтобы заставить вас принять решение под давлением.

Кейс из практики: Crypto World Evolution

В 2019 году я консультировал группу инвесторов, пострадавших от схемы под названием Crypto World Evolution (CWE). Компания обещала 8% еженедельного дохода благодаря «революционному торговому боту». Платформа действительно показывала впечатляющие результаты в течение первых месяцев, выплаты поступали вовремя.

Инвесторы, получив первые выплаты, начали приглашать друзей и родственников. Классический приём – сначала дать жертве «поверить» и превратить её в неосознанного соучастника.

Через восемь месяцев сайт исчез, а с ним и $200 миллионов инвесторских денег. Расследование показало, что никакого торгового бота не существовало. Ранние выплаты производились за счёт денег новых участников – классическая схема Понци.

Что делать?

- Помните правило: если предложение звучит слишком хорошо, чтобы быть правдой – скорее всего, так и есть.
- Всегда ищите бизнес-модель. Если компания не может внятно объяснить, как именно она генерирует прибыль – бегите.
- Проверяйте юридическую информацию: лицензии, регистрационные данные, физический адрес.
- Не поддавайтесь на тактики психологического давления и ограниченного времени.

Фейковые[5] инвестиции: от форекс-кухонь до лжеброкеров

В 2016 году я впервые столкнулся с «форекс-кухней» – так в профессиональном жаргоне называют подставные брокерские компании, которые имитируют торговлю, но никогда не выводят сделки на реальный рынок. Тогда мой друг-программист потерял $15,000 на платформе с красивым названием и поддельной лицензией.

Сегодня фейковые брокеры эволюционировали. Они создают полноценные торговые платформы с котировками в реальном времени, аналитическими инструментами и даже мобильными приложениями. Если в начале 2000-х такая инфраструктура стоила миллионы, сегодня готовую «брокерскую

[5] ***Фейк*** *(от англ. fake – «подделка») – это ложная информация, поддельный объект или событие, созданное для введения в заблуждение с целью манипуляции, обмана или развлечения.*

платформу под ключ» можно купить на чёрном рынке за $5,000–10,000.

Как работает схема лжеброкера

1. **Привлечение клиентов** через агрессивную рекламу с обещаниями лёгкого заработка. *«Начните зарабатывать от $1,000 в день на колебаниях курса валют!»*

2. **Персональный менеджер** – ключевая фигура в схеме. Он звонит вам, создаёт впечатление заботы, даёт «эксклюзивные рекомендации» и постоянно подталкивает к увеличению депозита.

3. **Манипуляция платформой**. В отличие от реальных брокеров, здесь вы торгуете в «песочнице» – симуляторе, где результаты сделок могут произвольно корректироваться в пользу «брокера».

4. **Затруднение вывода средств**. Когда клиент решает вывести деньги, начинаются проблемы: технические сбои, требования дополнительной верификации, комиссии и скрытые условия.

Помню случай с преподавателем из Гётеборга, который открыл счёт у брокера SuperFX (название изменено). После нескольких успешных сделок (разумеется, искусственно созданных системой) его убедили увеличить депозит до $50,000. Затем его «персональный аналитик» рекомендовал крупную сделку, которая завершилась потерей 80% капитала. Когда клиент попытался вывести оставшуюся сумму, выяснилось, что по условиям бонусной программы (напечатанным микроскопическим шрифтом) нужно совершить торговый оборот, в 50 раз превышающий сумму депозита, прежде чем деньги можно вывести.

Усложнённые схемы: инвестиционные боты и сигнальные группы

Разновидностью брокерского мошенничества стали «инвестиционные боты» и «сигнальные группы». Схема выглядит так:

1. Вы видите рекламу торгового бота или приватной группы с торговыми сигналами и впечатляющей статистикой: *«97% прибыльных сделок»*.
2. Для использования бота или доступа к сигналам вас направляют к «надёжному брокеру-партнёру» – на самом деле, мошенническому.
3. Вы депозитируете деньги, и на первом этапе бот или сигналы могут действительно показывать прибыль (на бумаге).
4. Когда депозит достигает значительной суммы, следует разорительная сделка или серия сделок.

Как не стать жертвой?

- Проверяйте лицензию брокера через официальные регуляторы (FCA, CySEC, FINMA и т.д.), а не просто наличие логотипов на сайте.
- Никогда не переводите деньги по настоянию «персонального менеджера».
- Начинайте с минимальной суммы и сразу пробуйте вывести небольшую часть – это проверка работоспособности вывода.
- Помните, что реальный трейдинг – это сложно, и стабильная высокая доходность невозможна.

Микрофинансовые ловушки: когда 1% в день не кажется большим числом

«Всего 1% в день» – звучит невинно, правда? Но элементарная математика показывает, что это более 365% годовых. Микрофинансовые организации (МФО) и онлайн-кредиторы давно освоили цифровое пространство, предлагая *«быстрые деньги до зарплаты»* под грабительские проценты.

В 2018 году мне пришлось работать с госпиталем в пригороде Стокгольма, где заметили странную тенденцию – молодые медсёстры массово брали отгулы по болезни. Расследование показало шокирующую картину: сотрудники попадали в долговую спираль из-за онлайн-займов, полученных буквально в два клика через мобильные приложения.

Цифровые капканы микрокредитования

Современные микрокредитные организации используют алгоритмы и «большие данные» для оптимизации своего бизнеса:

1. **Таргетированная реклама**[6] на финансово уязвимые группы. Системы анализируют поисковые запросы, историю покупок, даже скорость печати при заполнении форм, выявляя людей в отчаянном финансовом положении.

2. **Геймификация процесса займа**. Приложения превращают получение кредита в подобие игры: красочные

[6] ***Таргетированная реклама*** *– это персонализированная рекламная кампания, которая показывает контент конкретной аудитории, отобранной по заданным параметрам (демография, интересы, поведение в сети), чтобы повысить конверсию и минимизировать бесполезные показы.*

интерфейсы, прогресс-бары, бонусы за «своевременное погашение» и предложения «повысить кредитный лимит».

3. **Скрытые условия и автоматические продления**. Договоры составлены так, что заёмщик автоматически соглашается на продление кредита, если не может погасить его в срок, что запускает лавинообразный рост долга.

4. **Агрессивные методы взыскания**. От спам-звонков до использования данных геолокации для отслеживания должников и психологического давления.

Кейс «Быстроденьги-онлайн»

Показателен случай с платформой «Быстроденьги-онлайн» (название изменено), которая предлагала первый заём под 0% на 7 дней. Что упускали заёмщики:

- Небольшую «комиссию за обслуживание счёта» в размере 1% от суммы займа ежедневно (365% годовых);
- Автоматическую подписку на «страховку займа» (ещё 30% от суммы);
- Автоматическое продление займа по окончании срока, если полная сумма не возвращена.

В результате, человек, взявший €500 *«под 0%»*, через месяц оказывался должен уже около €1,000, а через три месяца сумма могла превышать €5,000.

Когда я рассказываю эту историю на конференциях, многие не верят, думают, что я преувеличиваю. Но математика безжалостна: из-за сложного процента и комиссий, долг может расти экспоненциально. А цифровые технологии делают весь

процесс невидимым и бесшумным – пока не становится слишком поздно.

Что делать?

- Рассчитывайте полную стоимость кредита до копейки, включая все комиссии и страховки.
- Внимательно читайте договор, особенно мелким шрифтом, ищите пункты об автоматическом продлении.
- Помните, что «быстрые деньги» никогда не бывают дешёвыми.
- Используйте микрозаймы только в крайних случаях и с чётким планом погашения.

Инвестиционные скамы в социальных сетях

«Вы видели сколько зарабатывает Илон Маск? А хотите так же?» – такое сообщение получил мой коллега от своего давнего друга в Facebook. Только это был не его друг, а взломанный аккаунт, используемый для распространения инвестиционной схемы.

Социальные сети стали золотым дном для финансовых мошенников. Они предлагают «эксклюзивные инвестиционные возможности», используя доверие пользователей к знакомым лицам и авторитетам.

Варианты мошенничества в социальных сетях

1. **Взломанные аккаунты друзей**, рассказывающих о *«проверенной инвестиционной платформе»*.

2. **Поддельные аккаунты знаменитостей**, якобы делящихся секретами своего финансового успеха.

3. **Фейковые новостные статьи** о революционных финансовых продуктах, «одобренных» известными бизнесменами или политиками.

4. **Закрытые инвестиционные группы**, где «эксклюзивный доступ» создаёт иллюзию избранности и уникальной возможности.

Особенно изобретательна схема с «инвестиционными группами». Мошенники создают впечатление элитарного сообщества успешных инвесторов. Новичку обещают доступ *к «инсайдерской информации»* или *«закрытым IPO»*. Группа может существовать месяцами, создавая видимость успешных инвестиций, прежде чем провернуть финальную аферу.

Я столкнулся с таким случаем, когда расследовал группу «Stockholm Investment Club». Более 200 человек поверили, что вступают в элитарное инвестиционное сообщество. Несколько месяцев они получали «аналитику» и рекомендации по акциям, которые действительно росли (мошенники просто выбирали уже растущие акции). Затем пришла «сделка века» – инвестиции в предварительный раунд финансирования некоего стартапа. Когда деньги были собраны, группа исчезла вместе с организаторами.

Как не стать жертвой?

- Не доверяйте сообщениям даже от знакомых, если они неожиданно начинают рекламировать инвестиционные возможности.
- Проверяйте информацию через официальные источники, не переходите по подозрительным ссылкам.
- Помните: реальные элитные инвестиционные возможности не рекламируются в социальных сетях.
- Никогда не отправляйте деньги на личные счета «менеджеров» или «консультантов».

Заключение

Финансовое мошенничество не изобрели в цифровую эпоху – его просто оцифровали и масштабировали. Технологии сделали этот процесс безликим, автоматизированным и практически промышленным.

Парадоксально, но базовые принципы защиты остаются прежними, несмотря на всю технологическую эволюцию:

1. Если предложение звучит слишком хорошо – это, скорее всего, обман.
2. Никогда не принимайте финансовые решения под давлением.
3. Проверяйте, перепроверяйте и снова проверяйте.
4. Помните, что технологии – это всего лишь инструмент, а за ним всегда стоят люди с их мотивами.

Я часто говорю своим клиентам: *«Лучшая защита от мошенников – это здоровый финансовый скептицизм»*. Звучит не

так романтично, как истории о мгновенном обогащении, но зато ваши деньги останутся там, где им и положено быть – у вас.

В следующей главе мы рассмотрим, как мошенники проникли в наши телефоны и почтовые ящики, и как отличить звонок из настоящего банка от звонка аферист а, сидящего в тысячах километров от вас в подпольном колл-центре.

Глава 4. Когда звонит «банк»: театр мошенничества в телефоне и браузере

В 2021 году я проводил эксперимент: две недели отвечал на все подозрительные звонки с неизвестных номеров. Жена думала, что я сошёл с ума, коллеги крутили пальцем у виска. Но результаты стоили потраченного времени: 12 из 23 звонков оказались мошенническими. Пять *«сотрудников службы безопасности банка»*, три *«технических специалиста Microsoft»*, четыре *«представителя налоговой службы»* и даже один *«внезапно обнаружившийся дальний родственник из России, попавший в беду»*.

Мир телефонного и интернет-мошенничества – это современный театр абсурда, где аферисты разыгрывают сценарии, написанные психологами и маркетологами. Они не просто воруют деньги – они крадут доверие, манипулируют эмоциями и эксплуатируют базовые человеческие инстинкты.

Давайте заглянем за кулисы этого театра и разберёмся, как не стать частью представления, в котором единственный, кто аплодирует в конце – это мошенник, считающий ваши деньги.

«Ваша карта заблокирована»: анатомия банковского фишинга

Мало кто остаётся равнодушным к сообщению о проблемах с банковской картой. Именно на этом строится одна из самых распространённых мошеннических схем.

Помню случай с профессором математики из Уппсальского университета. Человек, способный решать дифференциальные уравнения в уме, попался на примитивную схему «звонка из банка». Почему? Потому что мошенники не апеллируют к интеллекту – они бьют по эмоциям.

Как работает сценарий «банковского звонка»

1. **Первый контакт**: SMS или автоматический звонок о «подозрительной транзакции» или «блокировке карты».
2. **Создание срочности**: *«Необходимо действовать немедленно, иначе все средства будут заморожены на 48 часов»*.
3. **Переключение на «специалиста»**: звонок якобы из службы безопасности банка, где мошенник представляется полным именем и указывает фальшивый ID-номер сотрудника.
4. **Подтверждение личности жертвы**: мошенник называет ваши настоящие данные (имя, иногда дату рождения или последние цифры номера карты), полученные из утечек или социальных сетей, создавая иллюзию, что это действительно банк.
5. **Легенда о мошенниках**: парадоксально, но чаще всего используется история *«мы обнаружили попытку мошенничества с вашим счётом»*.

6. **Манипуляция страхом**: *«Прямо сейчас мошенники пытаются снять ваши деньги»* или *«Ваши данные в опасности»*.

7. **Призыв к действию**: *«Для защиты нужно перевести деньги на безопасный счёт»* или *«назвать код из SMS для блокировки подозрительной операции»*.

В случае с профессором-математиком мошенники использовали усовершенствованную схему. Они позвонили ему, представившись службой безопасности банка Swedbank, и сообщили о подозрительной транзакции. Когда профессор усомнился, они предложили ему «проверить подлинность» их звонка – перезвонить в банк по официальному номеру на обороте карты.

Но здесь сработала техническая уловка: мошенники не разорвали соединение. В шведской телефонной системе, как и во многих других, соединение может оставаться активным, если только звонящий не завершит вызов. Когда профессор «набрал» номер банка, он всё ещё разговаривал с мошенниками, которые изобразили ответ банковского автоответчика и перевели звонок «специалисту».

Эта дополнительная верификация окончательно убедила жертву, и профессор выполнил все инструкции «специалиста», включая установку приложения для «защиты» (на самом деле, программы удалённого доступа), что позволило мошенникам опустошить его счёт.

Что делать?

- Банк никогда не просит перевести деньги на «безопасный счёт» или сообщить коды из SMS.

- Если вам звонят из «банка», положите трубку и перезвоните сами по официальному номеру, указанному на карте или официальном сайте. **Важно:** выждите 30 секунд или используйте другой телефон.
- Используйте специальное приложение банка для проверки транзакций, а не верьте информации от звонящего.
- Не устанавливайте программы удалённого доступа (AnyDesk, TeamViewer и т.п.) по чьей-либо просьбе.

«Ваш родственник в беде»: социальная инженерия на стероидах

«Мама, привет, у меня проблемы! Я попал в аварию, срочно нужны деньги для адвоката. Мой телефон разбился, пишу с чужого».

Это сообщение получила моя мать в WhatsApp в 2022 году. К счастью, она не поверила, что я разбил свой телефон и тут же попросил денег, не позвонив. Но тысячи родителей по всему миру ежедневно переводят деньги мошенникам, думая, что помогают своим детям.

Эволюция схемы «родственник в беде»

Эта схема существует десятилетиями, но цифровые технологии вывели её на новый уровень:

1. **Социальные сети как источник данных**. Мошенники изучают профили потенциальных жертв, узнавая имена родственников, их местонахождение, особенности коммуникации.

2. **Мессенджеры вместо звонков**. Раньше мошенники звонили и имитировали голос родственника в панике. Сейчас чаще используются текстовые сообщения, где подделать идентичность проще.

3. **Искусственный интеллект на службе обмана**. В 2023 году появились первые случаи использования ИИ для имитации голоса родственников. Мошенники используют образцы голоса из социальных сетей и создают убедительные фейки.

4. **Сложные легенды**. Если раньше использовались примитивные истории (*«арестовали, нужны деньги на залог»*), то сейчас легенды стали изощрённее: *«Я в больнице, страховка не покрывает лечение»*, *«У меня украли документы и телефон в другом городе»*.

5. **Психологический прессинг**. *«Только никому не говори»*, *«Решить нужно в течение часа»*, *«Это вопрос жизни и смерти»* – всё это тактики, не дающие жертве время на размышление.

Кейс: голосовой deepfake

В феврале 2023 года я консультировал семью из Мальмё, ставшую жертвой новейшей вариации этой схемы. 63-летней женщине позвонил «сын», голос которого был неотличим от настоящего. Он рыдал и говорил, что попал в автокатастрофу, где пострадал ребёнок, и ему грозит уголовное дело, если он срочно не выплатит компенсацию семье пострадавших.

Технология deepfake была настолько совершенна, что мать не усомнилась в подлинности голоса. А фоновый шум и прерывающаяся связь маскировали небольшие несоответствия.

В результате женщина перевела мошенникам €8,000, думая, что спасает сына от тюрьмы.

Расследование показало, что мошенники, вероятно, использовали образцы голоса из видео, которые сын публиковал на Facebook. Десяти 30-секундных роликов достаточно, чтобы современные алгоритмы создали убедительную голосовую модель.

Как не стать жертвой?

- Установите кодовое слово для экстренных ситуаций, известное только близким родственникам.
- Всегда перезванивайте на знакомый номер родственника, о котором идёт речь.
- Задавайте вопросы, ответы на которые знаете только вы и ваш родственник.
- Не поддавайтесь на срочность и просьбы сохранить всё в тайне.
- Помните, что технологии голосового deepfake становятся доступнее, не полагайтесь только на распознавание голоса.

Фейковые магазины: когда цена слишком хороша, чтобы быть реальной

В 2020 году, во время первой волны COVID-19, я наблюдал настоящий бум фейковых интернет-магазинов. Маски, дезинфицирующие средства, лекарства – всё это продавалось на сайтах-однодневках по «специальным ценам». Кризис создал

идеальные условия для такого мошенничества: дефицит товаров, всеобщая паника и переход покупателей в онлайн.

Но фейковые магазины существовали задолго до пандемии и никуда не исчезли после. Они эволюционировали от примитивных страниц с грамматическими ошибками до безупречных копий известных брендов.

Разновидности фейковых магазинов

1. **Полные подделки брендовых сайтов**. Доменное имя отличается на один символ, дизайн идентичен оригиналу, но цены подозрительно низкие.

2. **«Распродажные» аутлеты**. Сайты, якобы продающие товары известных брендов со скидками 70–90% из-за «закрытия склада» или «конца сезона».

3. **Дропшиппинг[7]-мошенничество**. Технически не все дропшипперы – мошенники, но многие используют схемы обмана: показывают фото брендовых товаров, а отправляют дешёвые копии из Китая с задержкой в месяцы.

4. **Магазины несуществующих товаров**. Продажа товаров, которых не существует или которые невозможно доставить – например, эксклюзивные лекарства или дефицитная электроника.

[7] ***Дропшиппинг*** *(от англ. dropshipping) – это модель онлайн-торговли, при которой продавец принимает заказы, но не хранит товары, а поставщик напрямую отправляет их покупателю, позволяя работать без складов и зарабатывать на разнице цен.*

Кейс: Охота за PlayStation 5

В конце 2020 года, когда новая PlayStation 5 была в дефиците, появились десятки сайтов, предлагающих консоль *«без очереди»* и *«по цене производителя»*. Один из моих клиентов, отчаявшийся отец, желавший порадовать сына на Рождество, заказал приставку на сайте *SonyExpress-Store.com* (домен изменён).

Сайт выглядел профессионально, имел SSL-сертификат и даже отзывы *«счастливых покупателей»*. После оплаты €499 клиент получил письмо о «начале обработки заказа». Затем последовало сообщение о «таможенной задержке» и необходимости доплаты €150 за «экспресс-оформление». После второго платежа сайт просто исчез, а банк отказал в возврате средств, так как клиент сам авторизовал транзакции.

Анализ показал, что сайт существовал всего 12 дней и был создан на базе шаблона, купленного на чёрном рынке. Через этот один сайт мошенники собрали более €50,000, прежде чем исчезнуть.

Типичные признаки фейковых магазинов

1. **Подозрительно низкие цены** – скидки более 50% от рыночной стоимости на популярные товары.
2. **Отсутствие физического адреса** или указание только абонентского ящика.
3. **Ограниченные способы оплаты** – часто только предоплата картой или криптовалютой.

4. **Недавно зарегистрированный домен** – проверить можно через сервисы WHOIS[8].

5. **Отсутствие телефона** для связи или указан только E-mail с бесплатного сервиса.

6. **Подозрительно однотипные положительные отзывы**, созданные в короткий промежуток времени.

7. **Ошибки в тексте** или контент, явно переведённый автоматическим переводчиком.

Что делать?

- Проверяйте домен магазина через сервисы WHOIS – когда он был создан, кем зарегистрирован.
- Ищите отзывы о магазине на независимых площадках, а не только на самом сайте.
- Используйте оплату с защитой покупателя (PayPal, некоторые кредитные карты и карты с 3DSecure) или наложенный платёж.
- Помните: если цена кажется подозрительно низкой – скорее всего, это мошенничество.

QR-коды и короткие URL: невидимые порталы к мошенникам

В начале 2023 года в центре Стокгольма появились странные объявления: QR-коды на столбах и стенах зданий с надписью «Сканируй и выиграй iPhone 14». Любопытные прохожие,

[8] ***Whois*** *(от англ. «who is?» – «кто это?») – это интернет-протокол и публичная база данных, содержащая регистрационную информацию о доменных именах, IP-адресах и их владельцах.*

отсканировав код, попадали на фишинговый сайт, имитирующий розыгрыш от Apple, где для «получения приза» нужно было ввести данные карты для «подтверждения личности и оплаты доставки».

Это новое поколение мошенничества – использование QR-кодов и сокращённых URL как «порталов» к фишинговым сайтам. Почему эта тактика так эффективна? Потому что QR-код непрозрачен для человеческого глаза – вы не можете «прочитать» его без сканирования, а значит, не можете оценить риск заранее.

QR-мошенничество в повседневной жизни

1. **Подмена QR-кодов в ресторанах**. Мошенники наклеивают свои QR-коды поверх настоящих меню. Посетитель, сканируя код, попадает на фишинговый сайт, имитирующий систему заказа, где вводит данные карты.
2. **Фальшивые парковочные QR-коды**. Наклейки с QR-кодами на парковочных автоматах, якобы для оплаты парковки, ведущие на фишинговые сайты.
3. **«Благотворительные» QR-коды**. Коды для «пожертвований» на поддельных благотворительных плакатах.
4. **QR-билеты и регистрация на мероприятия**. Поддельные QR-коды для «регистрации» на конференциях и мероприятиях.

URL-сокращатели как инструмент обмана

Параллельно с QR-кодами мошенники активно используют сервисы сокращения URL (bit.ly, t.co, goo.gl и т.п.).

Маскировка настоящего адреса позволяет обойти психологическую защиту пользователя: вместо подозрительного *fake-bank-login.com* жертва видит нейтральную ссылку вида *bit.ly/2xYz*.

В корпоративной среде это стало серьёзной проблемой. В 2022 году я консультировал компанию, где ключевой сотрудник попался на фишинговое письмо с сокращённой ссылкой якобы на документ от партнёра. Ссылка вела на фейковую страницу корпоративного входа, где мошенники собрали учётные данные и получили доступ к внутренней системе компании.

Эволюция QR и URL мошенничества

Современные схемы становятся всё изощрённее:

1. **Динамические QR-коды**, меняющие целевой URL после определённого количества сканирований – первые несколько человек попадают на легитимный сайт, создавая ложное чувство безопасности.
2. **Геотаргетированные[9] ссылки**, которые ведут на разные страницы в зависимости от местоположения пользователя или времени суток.
3. **Поддельные URL с использованием юникод-символов**, визуально неотличимых от оригинальных доменов (например, использование кириллической «о» вместо латинской в адресе *microsoft.com*).

[9] ***Геотаргетинг*** *(англ. geotargeting) – это технология показа контента или рекламы пользователям в зависимости от их географического местоположения (страна, город, район).*

Как защититься?

- Используйте приложения для сканирования QR-кодов, показывающие URL перед переходом.
- При сканировании QR-кода в общественном месте, проверяйте, не наклеен ли он поверх оригинального.
- С осторожностью относитесь к сокращённым ссылкам – используйте сервисы предпросмотра (например, unshorten.it).
- В корпоративной среде внедряйте политику проверки всех внешних ссылок перед переходом.

Эмоциональное мошенничество: Love-скам и псевдо-благотворительность

«Я потерял почти €30,000 и два года жизни», – с этих слов начал свою историю 58-летний инженер из Гётеборга на моём семинаре по кибербезопасности. История классическая: познакомился на сайте знакомств с «русской женщиной», общались месяцами, затем начались просьбы о финансовой помощи – сначала маленькие суммы, потом всё большие.

Эмоциональное мошенничество – особая категория, где главным инструментом аферист становятся не технологии, а человеческие чувства: любовь, сострадание, желание помочь.

Романтическое мошенничество (Love-скам)

1. **«Русская невеста» и её современные вариации**. Мошенники создают фейковые профили привлекательных людей (чаще женщин) и завязывают романтические отношения

онлайн. После формирования эмоциональной связи начинаются просьбы о помощи.

2. **Мультиплицированные профили**. Один мошенник может одновременно вести переписку с десятками потенциальных жертв, используя шаблонные сообщения и фотографии из стоковых банков или украденные из социальных сетей.

3. **Долгосрочные стратегии**. В отличие от других видов мошенничества, романтические аферисты могут «выращивать» жертву месяцами, прежде чем приступить к вымогательству денег.

4. **Сложные легенды**. *«Я работаю на нефтяной платформе»*, *«Я военный в зарубежной командировке»*, *«Я врач в гуманитарной миссии»* – всё это объяснения, почему встреча в реальности невозможна.

Псевдо-благотворительность и эмоциональные триггеры

Ещё одна форма эмоционального мошенничества — фальшивые благотворительные кампании. После каждого громкого стихийного бедствия или катастрофы в сети появляются десятки фейковых сборов «для помощи пострадавшим».

Во время лесных пожаров в Швеции в 2018 году я обнаружил более 30 фейковых благотворительных кампаний в социальных сетях. Они использовали драматичные фото (часто из других пожаров или даже из фильмов), эмоциональные истории и призывы к немедленному действию.

Особенно циничны кампании с использованием детей — фейковые сборы на лечение несуществующих больных детей стали настоящей эпидемией в социальных сетях. Мошенники

крадут фотографии реальных детей из больниц или из зарубежных благотворительных кампаний и создают душераздирающие истории, играя на самых глубоких человеческих эмоциях.

Как защититься от эмоционального мошенничества?

- В романтических отношениях настаивайте на видеозвонке на ранних этапах общения.
- Проверяйте фотографии через обратный поиск изображений (Google Images, TinEye).
- Жертвуйте только проверенным благотворительным организациям, имеющим официальную регистрацию.
- Помните: настоящая благотворительность никогда не использует эмоциональное давление и срочность.

Заключение: Психологическая самооборона в цифровую эпоху

Многие думают, что жертвами мошенников становятся только технически неграмотные или пожилые люди. Моя практика показывает обратное: профессора университетов, IT-специалисты, даже сотрудники служб безопасности – все могут стать жертвами в момент эмоциональной уязвимости.

Телефонное и интернет-мошенничество – это не столько технологическое, сколько психологическое явление. Мошенники изучают человеческую психологию десятилетиями и знают, какие кнопки нажать, чтобы отключить критическое мышление.

Вот три главных психологических триггера, которые используют мошенники:

1. **Срочность**. *«Решить нужно прямо сейчас»*, *«Предложение действует только сегодня»*, *«Счёт будет заблокирован через час»*. Создание искусственной срочности не даёт жертве времени подумать и проконсультироваться.

2. **Страх и угроза**. *«Ваш аккаунт взломан»*, *«Ваши данные в опасности»*, *«Ваш родственник в беде»*. Страх запускает примитивные реакции мозга, блокируя рациональное мышление.

3. **Жадность и выгода**. *«Эксклюзивное предложение»*, *«Вы выиграли»*, *«Инвестиция с гарантированной прибылью»*. Перспектива лёгкой выгоды активирует центры удовольствия в мозге.

Лучшая защита – это осознание собственных слабостей. Мы все уязвимы перед этими триггерами. Поэтому важно выработать внутренний протокол безопасности:

1. **Правило паузы**: при любом неожиданном контакте, связанном с деньгами или личными данными, сделайте паузу минимум на час. Мошенники рассчитывают на немедленную реакцию.

2. **Правило подтверждения**: всегда проверяйте информацию через официальные каналы. Позвоните в банк по номеру на карте, свяжитесь с родственником по известному вам номеру.

3. **Правило скептицизма**: если предложение кажется слишком хорошим – оно, скорее всего, обман. Если угроза кажется слишком страшной – возможно, это манипуляция.

В следующей главе мы углубимся в мир кибермошенничества и рассмотрим, как технологии создают новые векторы атак

– от фишинговых сайтов до программ-вымогателей и фейковых криптовалютных проектов.

Запомните: самое мощное оружие против мошенников – это не антивирус и не блокировщик рекламы, а ваше критическое мышление и осознанность. Вы можете потерять деньги за секунды, но вернуть их будет практически невозможно. Учитесь распознавать мошенников до того, как станет слишком поздно.

Глава 5. Цифровые ловушки: кибермошенничество новой эры

Когда-то в детстве мой отец показал мне старую книгу о легендарных карточных шулерах. *«Запомни»*, – сказал он, – *«эти парни могли обчистить человека просто потому, что знали, куда тот будет смотреть»*. Сегодня самые опасные шулеры сидят по ту сторону экрана, и они точно знают, куда мы все смотрим.

В предыдущих главах мы рассмотрели эволюцию мошенничества от древних времен до современности, а также разобрали различные типы финансовых афер и телефонное мошенничество. Теперь давайте погрузимся в цифровой мир, где границы между реальностью и обманом становятся все более размытыми.

Фишинг: цифровая маскировка

Фишинг – это не просто термин из компьютерной безопасности. Это целое искусство маскировки и обмана. Представьте, что вы получаете электронное письмо от своего банка с просьбой «обновить данные безопасности». Всё выглядит убедительно: логотип банка, правильные шрифты, даже подпись вашего «менеджера». Вы нажимаете на ссылку, вводите свои данные... и через несколько часов обнаруживаете, что с вашего счёта исчезли все деньги.

Именно так работает классический фишинг. Но мошенники не стоят на месте. Сегодня фишинг принимает все более изощренные формы.

Спирфишинг: персонализированная охота

Если классический фишинг – это сеть, закинутая наугад, то спирфишинг – это охота с гарпуном на конкретную жертву. Мошенники собирают информацию о вас из открытых источников: социальных сетей, профессиональных платформ, форумов. Затем они создают сообщение, которое кажется настолько личным, что практически невозможно заподозрить обман.

Один из моих клиентов, директор крупной строительной компании, получил письмо от «коллеги», с которым недавно встречался на конференции в Барселоне. В письме упоминались детали их разговора и предлагался доступ к *«презентации с закрытыми данными»*, которую они обсуждали. Директор перешёл по ссылке, ввёл корпоративные данные для доступа... и через два дня компания подверглась ransomware-атаке[10] с требованием выкупа в 200,000 евро.

Клоны популярных сайтов

Современные фишинговые сайты – это уже не топорные подделки с очевидными ошибками и кривой верстkой. Это практически идеальные копии оригинальных ресурсов. Я сам консультировал банк, клиенты которого пострадали от

[10] ***Ransomware-атака*** *(от англ. ransom – «выкуп» + malware – «вредоносное ПО») – это кибератака, при которой злоумышленники шифруют файлы или блокируют доступ к системе жертвы, требуя выкуп за их разблокировку.*

фишинговой атаки, и даже опытный сотрудник службы безопасности не сразу заметил разницу между настоящим сайтом и его поддельной копией.

Единственным отличием был URL-адрес: вместо «swedbank.se» было «swedbank-secure.se». Маленькая деталь, которую легко пропустить, особенно на мобильном устройстве, где адресная строка часто скрыта.

Вредоносное ПО: невидимые враги

Если фишинг – это маскировка, то вредоносное программное обеспечение – это невидимый враг, который проникает в ваш компьютер и действует незаметно, пока не становится слишком поздно.

Ransomware: цифровой шантаж

Программы-вымогатели (ransomware) шифруют ваши файлы и требуют выкуп за их восстановление. Ещё в 2017 году атака WannaCry поразила более 200,000 компьютеров в 150 странах. Но с тех пор эта угроза только выросла.

Современные ransomware-атаки часто нацелены на конкретные организации, и суммы выкупа могут достигать миллионов долларов. Хуже того, даже после оплаты выкупа нет гарантии, что вы получите свои данные обратно. Согласно исследованию Cybereason, 80% компаний, заплативших выкуп, подверглись повторной атаке.

В 2022 году я консультировал архитектурное бюро, которое потеряло все проекты за последние 5 лет из-за ransomware-

атаки. Резервные копии? Они были, но хранились на подключённом сервере, который тоже был зашифрован. Полгода работы пришлось начинать с нуля.

Банковские трояны: тихие воры

В отличие от шумных вымогателей, банковские трояны действуют тихо и незаметно. Они не шифруют ваши файлы и не требуют выкупа. Вместо этого они ждут, когда вы войдёте в свой онлайн-банкинг, и перехватывают ваши данные или даже изменяют реквизиты платежей.

Одним из самых известных банковских троянов последних лет стал Emotet, который начинал как банковский вредонос, но со временем эволюционировал в многоцелевую платформу для распространения других типов вредоносного ПО.

Что делать? Используйте двухфакторную аутентификацию везде, где это возможно, особенно для финансовых сервисов. Даже если мошенники получат ваш пароль, им всё равно потребуется физический доступ к вашему телефону для подтверждения операций.

Кейлоггеры и шпионское ПО: цифровое подсматривание

Представьте, что за вашим плечом постоянно стоит человек и записывает всё, что вы печатаете на клавиатуре: пароли, личные сообщения, поисковые запросы. Именно так работают кейлоггеры – программы, которые регистрируют нажатия клавиш.

Шпионское ПО идёт ещё дальше: оно может захватывать скриншоты, записывать звук с микрофона, активировать камеру без вашего ведома. Изначально такие программы разрабатывались для легитимных целей – например, для родительского контроля или мониторинга сотрудников. Но в руках мошенников они становятся опасным оружием.

В 2021 году я расследовал случай, когда на компьютеры сотрудников крупной энергетической компании было установлено шпионское ПО через заражённое рекламное письмо от якобы партнёра. Злоумышленники получили доступ не только к корпоративным секретам, но и к личной переписке сотрудников, что создало почву для дальнейшего шантажа.

Фейковые криптовалютные проекты: золотая лихорадка XXI века

Криптовалюты и блокчейн-технологии открыли новые возможности не только для инноваций, но и для обмана. В этой сфере мошенники эксплуатируют две основные человеческие слабости: жадность и страх упустить возможность (FOMO – Fear Of Missing Out).

Скам-ICO: пустышки с красивыми обещаниями

Initial Coin Offering (ICO) – это способ привлечения инвестиций для криптопроектов, аналог IPO в традиционном бизнесе. Проблема в том, что барьер входа для создания ICO очень

низок: достаточно написать белую книгу (whitepaper)[11], создать красивый сайт и запустить маркетинговую кампанию.

Я сам однажды чуть не инвестировал в проект, который обещал *«революцию в сфере децентрализованных финансов»*. Сайт выглядел профессионально, у проекта были якобы известные консультанты из мира блокчейна, а токен обещал рост в 100 раз в течение года. К счастью, я решил проверить whitepaper проекта и обнаружил, что большая часть технических деталей была просто скопирована из документации Ethereum, а «инновационная технология» описывалась размытыми маркетинговыми терминами без конкретики.

По данным Satis Group, около 80% всех ICO, проведённых в 2017–2018 годах, были скамом. Это тысячи проектов, которые собрали миллиарды долларов и исчезли, не оставив инвесторам ничего, кроме бесполезных токенов.

Поддельные биржи и криптокошельки

Помимо фейковых проектов, существуют поддельные криптовалютные биржи и кошельки. Они могут предлагать привлекательные условия: низкие комиссии, бонусы за регистрацию, высокий процент на стейкинг[12]. Но как только вы

---

[11] ***Whitepaper (белая книга) в криптобиржах*** *– это официальный документ, который детально описывает технологию, экономическую модель и правила работы криптоплатформы. Он служит техническим и маркетинговым обоснованием проекта, привлекая инвесторов и пользователей.*

[12] ***Стейкинг*** *(от англ. staking – «удержание, ставка») – это процесс блокировки криптовалюты на специальном кошельке или в смарт-контракте для поддержания работы блокчейна с целью получения вознаграждения в виде новых токенов.*

переводите туда свои криптоактивы, они исчезают вместе с самой биржей.

Я видел биржу, которая работала почти год, постепенно наращивая аудиторию и репутацию. Она даже позволяла пользователям выводить небольшие суммы, чтобы завоевать доверие. А потом в один день исчезла вместе с депозитами на сумму более 25 миллионов долларов.

Pump and Dump: манипуляции курсом

Схема «Pump and Dump» (*«накачать и сбросить»*) существует на финансовых рынках десятилетиями, но в мире криптовалют она достигла новых масштабов. Группа манипуляторов искусственно раздувает цену малоизвестной криптовалюты через социальные сети и Telegram-каналы. Когда доверчивые инвесторы начинают покупать токен, манипуляторы продают свои запасы по завышенной цене, и курс обваливается.

Я наблюдал, как токен с рыночной капитализацией в несколько сотен тысяч долларов за день вырос в десять раз после упоминания в популярном Telegram-канале. Через неделю его цена вернулась к исходной, а многие инвесторы потеряли значительные суммы.

Как не стать жертвой: Изучайте проекты, в которые собираетесь инвестировать. Читайте не только маркетинговые материалы, но и технические документы. Проверяйте команду разработчиков: есть ли у них опыт в области блокчейна? Можно ли найти их профили в социальных сетях? Участвовали ли они в других успешных проектах? И самое главное: если предложение

звучит слишком хорошо, чтобы быть правдой, скорее всего, это обман.

Психология кибермошенничества: почему мы так уязвимы?

Все описанные выше схемы работают благодаря тому, что мошенники отлично понимают человеческую психологию. Они знают, какие кнопки нажать, чтобы мы действовали импульсивно, не задумываясь.

Ургентность[13] и FOMO

Мошенники всегда создают ощущение срочности. Это классический приём, который заставляет нас принимать решения быстро, не давая времени на проверку информации.

В случае с криптовалютами FOMO (страх упустить возможность) работает особенно сильно. Когда мы видим, как другие зарабатывают огромные деньги на росте Bitcoin или другой криптовалюты, мы боимся опоздать на «последний поезд». Именно в такие моменты мы наиболее уязвимы для мошенников.

[13] ***Ургентность*** *(от англ. urgency – «срочность») – это психологический приём в маркетинге и продажах, создающий у человека ощущение дефицита времени или возможности, чтобы подтолкнуть к быстрому принятию решения (часто импульсивному).*

Авторитет и доверие

Другой мощный психологический рычаг – это апелляция к авторитету. Фишинговые письма часто приходят от имени банков, государственных органов или крупных компаний. Фейковые криптопроекты привлекают известных «советников» или «инвесторов» (часто без их ведома).

Я видел ICO, на сайте которого был размещён логотип венчурного фонда, который якобы инвестировал в проект. Когда я связался с этим фондом, они были шокированы: они никогда не слышали о данном проекте и не давали разрешения на использование своего логотипа.

Социальная инженерия: манипуляция на системном уровне

Социальная инженерия – это использование психологических манипуляций для получения конфиденциальной информации или доступа к системам. Мошенники изучают ваши привычки, предпочтения, страхи и используют это против вас.

Они могут представиться сотрудником службы поддержки и попросить данные для *«проверки безопасности»*. Или прислать вам *«срочное предупреждение о взломе вашего аккаунта»*, требующее немедленных действий. Или создать поддельный профиль вашего друга и попросить денег на *«экстренную ситуацию»*.

В эпоху социальных сетей у мошенников есть доступ к огромному количеству информации о нас. Они знают, где мы работаем, с кем дружим, куда ездим в отпуск, что покупаем,

какими сервисами пользуемся. Вся эта информация делает их атаки намного более убедительными.

Что делать?

Киберпреступность развивается с ошеломляющей скоростью. Появляются новые схемы, новые инструменты, новые способы обмана. Но базовые принципы защиты остаются неизменными:

1. **Проверяйте источники.** Всегда внимательно проверяйте адрес отправителя электронной почты, URL-адреса сайтов, особенно когда речь идёт о финансовых операциях.

2. **Используйте двухфакторную аутентификацию** везде, где это возможно, особенно для финансовых сервисов и электронной почты.

3. **Обновляйте ПО.** Регулярно устанавливайте обновления для операционной системы и программ, особенно для браузеров.

4. **Не открывайте вложения и не переходите по ссылкам** в письмах от незнакомых отправителей или в сообщениях, которые вызывают подозрение.

5. **Создавайте надёжные пароли и не используйте один и тот же пароль** для разных сервисов. Лучше всего использовать менеджер паролей.

6. **Регулярно делайте резервные копии** важных данных и храните их отдельно от основного компьютера.

7. **Не доверяйте случайным сообщениям в социальных сетях**, даже если они кажутся отправленными от знакомых людей. Всегда проверяйте информацию по альтернативным каналам связи.

8. **При инвестициях в криптовалюту используйте проверенные биржи** с хорошей репутацией и серьёзно изучайте проекты, в которые собираетесь вкладывать деньги.

9. **Помните о базовом принципе: если что-то звучит слишком хорошо, чтобы быть правдой, скорее всего, это обман.**

Лучший способ не стать жертвой кибермошенников – это сочетание технической грамотности и здорового скептицизма. Не поддавайтесь на манипуляции, не принимайте поспешных решений под давлением, всегда проверяйте информацию из нескольких источников.

Как говорил мой отец о карточных шулерах: *«Они побеждают не потому, что умнее тебя, а потому, что знают правила игры лучше»*. Те же слова применимы и к кибермошенникам. Знайте правила игры, и вы сможете защитить себя и своих близких от цифровых ловушек.

Глава 6. За фасадом репутации: бытовое и корпоративное мошенничество

Помню, как однажды в Стокгольме мой сосед, преуспевающий архитектор, уехал в отпуск, а вернувшись, обнаружил, что его квартира продана. Не ограблена, а именно продана – с оформленными документами и новыми владельцами, въехавшими на законных основаниях. Это звучит как сюжет из кинофильма, но произошло в реальности и в стране с одной из самых надёжных правовых систем мира.

Пока в предыдущих главах мы погружались в дебри высокотехнологичного мошенничества, существует целый пласт афер, которые происходят в привычном, осязаемом мире вещей и договоров. И что самое интересное – они часто используют нашу веру в репутацию, юридические системы и «правильно оформленные бумаги». Добро пожаловать в мир, где обман облачен в костюм с галстуком и прячется за солидным логотипом.

Квартирные аферы: когда документы лгут

Возвращаясь к истории моего соседа: как такое возможно в эпоху цифровых реестров и многоуровневой идентификации? Оказалось, мошенники использовали комбинацию классической подделки документов и современных технологий. Они получили копию паспорта моего соседа (возможно, через фишинг или утечку данных), создали поддельную доверенность и наняли актёра, который выдавал себя за владельца квартиры.

Это не единичный случай. Квартирные аферы – один из самых болезненных видов мошенничества, ведь здесь речь идёт не о нескольких тысячах евро, а о суммах, сопоставимых с ценой недвижимости.

Подмена субъекта: «хозяин» поневоле

Классическая схема мошенничества с недвижимостью основана на подмене настоящего владельца. Мошенники выбирают квартиры, хозяева которых редко бывают на месте: пожилые люди в домах престарелых, граждане, работающие за границей, недвижимость, используемая только для сезонного проживания.

В менее защищенных странах Восточной Европы я видел случаи, когда мошенники просто подделывали подписи в договорах купли-продажи и заверяли их у нотариусов-сообщников. В более развитых странах схема усложняется: используются поддельные цифровые подписи, компрометируются учётные записи в системах электронного документооборота, подкупаются сотрудники регистрационных органов.

Что делать? Если вы владеете недвижимостью, которую редко посещаете, регулярно проверяйте её статус в государственных реестрах. Многие страны сейчас предлагают системы оповещения, которые уведомляют собственника о любых действиях с его недвижимостью. Подключите такую услугу, даже если она платная – это дешевле, чем потерять квартиру.

Двойные продажи и несуществующие объекты

Другая распространенная схема – двойная продажа или продажа несуществующих объектов. В первом случае мошенник продает одну и ту же недвижимость нескольким покупателям, используя временные лазейки в процессе регистрации сделок. Во втором – продаёт квартиры в несуществующих или недостроенных домах.

В 2019 году я консультировал группу инвесторов, купивших апартаменты в строящемся комплексе на побережье Испании. Красивые 3D-визуализации, официальные разрешения на строительство, встречи с «архитекторами проекта» – всё выглядело безупречно. Но через год выяснилось, что участок земли, на котором должен был стоять комплекс, принадлежал совсем другой компании, а полученные деньги (более 4 миллионов евро) были выведены через цепочку офшорных компаний.

Аренда: одноразовая выгода

Мошенничество с арендой недвижимости – это обычно разовая афера, но с множеством пострадавших. Схема проста: мошенник арендует квартиру на короткий срок, фотографирует её и размещает объявление о долгосрочной аренде по привлекательной цене. Потенциальным арендаторам он показывает квартиру как хозяин и собирает с каждого предоплату и залог. После чего исчезает.

У меня есть знакомая пара, которая попалась на эту удочку в Берлине. Они заплатили 3,000 евро (первый месяц + залог) за квартиру, которую «арендодатель» показал им лично. Через

неделю, когда они приехали с вещами, их встретил настоящий хозяин, который понятия не имел о сделке.

Как не стать жертвой?

Всегда проверяйте документы на недвижимость. Запрашивайте выписку из реестра собственников. Если продавец отказывается её предоставить или предлагает «ускорить процесс» без официальной проверки – это повод насторожиться. При аренде старайтесь работать через проверенные агентства, даже если это стоит дороже. И никогда не переводите деньги до подписания официального договора.

Медицинское мошенничество: когда здоровье становится товаром

Здоровье – бесценный актив, и именно поэтому мошенничество в сфере медицины особенно цинично. Оно существует в различных формах: от продажи поддельных лекарств до предложения «чудодейственных» методов лечения неизлечимых болезней.

Фармацевтические подделки: смертельный бизнес

По данным Всемирной организации здравоохранения, около 10% лекарств в мировом обороте – подделки. В некоторых развивающихся странах эта цифра может достигать 30%. И речь идёт не только о дорогих препаратах для лечения рака или

СПИДа, но и о самых обычных антибиотиках, обезболивающих, противовоспалительных средствах.

В лучшем случае поддельные лекарства просто не содержат активного вещества. В худшем – включают опасные компоненты, которые могут нанести непоправимый вред здоровью.

Я столкнулся с этой проблемой лично, когда моей матери после операции требовался дорогостоящий антикоагулянт. Препарат был в дефиците, и знакомый предложил купить его *«по знакомству»* в соседней стране. К счастью, прежде чем согласиться, мы проверили информацию и выяснили, что предлагаемый препарат с высокой вероятностью был подделкой – производитель, указанный на упаковке, никогда не выпускал лекарство в таких дозировках.

«Чудо-методики»: когда надежда затмевает разум

Особой категорией медицинского мошенничества являются «чудо-методики» лечения серьёзных заболеваний. Мошенники прекрасно понимают психологию тяжелобольных людей и их близких: когда официальная медицина разводит руками, любая соломинка кажется спасением.

Я расследовал деятельность клиники в Восточной Европе, которая предлагала *«инновационное лечение последних стадий рака»* методом, якобы разработанным *«секретным советским НИИ»*. Пациентам вводили обычный физраствор с добавлением безвредных, но абсолютно бесполезных компонентов, и брали за это десятки тысяч евро. Самое страшное, что некоторые пациенты отказывались от паллиативной помощи, веря в

чудесное исцеление, и проводили последние месяцы жизни, испытывая невероятные страдания.

БАДы и «натуральная медицина»: между правдой и обманом

Биологически активные добавки и продукты «натуральной медицины» занимают особую нишу. С одной стороны, многие из них действительно могут быть полезны как дополнение к основному лечению. С другой – этот рынок минимально регулируется, что открывает широкое поле для злоупотреблений.

Типичный пример мошенничества – БАД, который позиционируется как *«альтернатива инсулину для диабетиков»* или *«натуральное средство от гипертонии»*. Такие продукты часто сопровождаются *«научными исследованиями»* и отзывами *«излечившихся пациентов»*. Реальность же такова: в лучшем случае человек просто потеряет деньги, в худшем – отказавшись от проверенного лечения в пользу «натурального», рискует здоровьем и жизнью.

Совет

Всегда приобретайте лекарства только в официальных аптеках или через проверенные онлайн-сервисы, имеющие фармацевтическую лицензию. Не верьте в «чудодейственные методики» – в современном мире научные прорывы не скрываются в подпольных клиниках, а публикуются в авторитетных медицинских журналах и быстро становятся достоянием всего медицинского сообщества. И помните: если БАД обещает лечить серьёзные заболевания – это почти наверняка обман.

Корпоративное мошенничество: преступления в галстуках

Если вы думаете, что мошенничество происходит только на тёмных улицах или в сомнительных интернет-магазинах, я вас разочарую. Некоторые из самых масштабных афер совершаются в стерильных офисах корпораций людьми в дорогих костюмах.

Откаты и коррупционные схемы: невидимый налог на бизнес

Откаты – это, пожалуй, древнейшая форма корпоративного мошенничества. Суть проста: сотрудник компании, ответственный за выбор поставщика или подрядчика, получает «благодарность» за выбор конкретной компании, часто не самой выгодной для работодателя.

В 2020 году я консультировал производственную компанию, которая подозревала своего закупщика в нечестной игре. Расследование показало, что он годами закупал сырьё у поставщика, цены которого были на 15–20% выше рыночных. Взамен он получал «консультационные выплаты» на счёт своей жены в размере 3% от каждой сделки. За пять лет такой «работы» компания переплатила более 2 миллионов евро, а закупщик заработал около 300,000 евро «комиссионных».

Поддельные тендеры: имитация конкуренции

Более сложная форма корпоративного мошенничества – поддельные тендеры. Компания объявляет конкурс на

выполнение работ или поставку товаров, но победитель известен заранее. Остальные участники либо являются дружественными компаниями, которые намеренно предлагают невыгодные условия, либо их заявки отклоняются по формальным причинам.

Я сталкивался с тендерами, где все «конкуренты» победителя оказывались компаниями, зарегистрированными за месяц до конкурса на подставных лиц. Они существовали только на бумаге и были созданы специально для имитации конкурентной борьбы.

Бухгалтерские махинации: игра с цифрами

Бухгалтерское мошенничество – это искажение финансовой отчётности компании с целью ввести в заблуждение инвесторов, кредиторов или налоговые органы. Это может быть завышение доходов, занижение расходов, сокрытие убытков или манипуляции с активами и обязательствами.

Самый известный пример такого мошенничества – скандал с компанией Enron, который привёл к её банкротству в 2001 году. Но подобные схемы используются и в наши дни, хотя и в более изощренных формах.

Я работал с инвестиционным фондом, который чуть не вложил значительные средства в технологический стартап. Компания показывала впечатляющий рост выручки – более 300% за два года. Но детальный анализ выявил, что большая часть этой выручки была фиктивной: компания продавала услуги своим же дочерним структурам, а те, в свою очередь, оплачивали эти услуги деньгами, полученными в виде займов

от материнской компании. Классическая схема «нарисованной выручки», которая рано или поздно приводит к краху.

Совет для бизнеса

Внедрите систему внутреннего контроля с чётким разделением полномочий. Регулярно проводите внутренний аудит и ротацию ключевых сотрудников, ответственных за финансовые решения. Создайте защищённый канал для сообщений о нарушениях (whistleblowing), который позволит сотрудникам анонимно информировать руководство о подозрительных действиях коллег.

Мошенничество в сфере услуг: плата за пустоту

Сфера услуг – благодатная почва для мошенников, ведь здесь зачастую сложно оценить качество результата или даже факт его наличия.

Псевдоэксперты: репутация напрокат

В мире, где экспертное мнение ценится на вес золота, звание «эксперта» стало разменной монетой. Появились целые индустрии псевдоэкспертов: от финансовых гуру, предсказывающих движение рынков (с точностью не выше подбрасывания монетки), до коучей личностного роста без профильного образования.

Я наблюдал за «инвестиционным советником», который продавал подписку на свою рассылку за 500 евро в месяц, обещая *«инсайдерскую информацию»* о движении рынков. Анализ его предсказаний за год показал, что их точность составляла около 50% – как при случайном угадывании. При этом у него было более 1,000 подписчиков, что приносило ему не менее 500,000 евро в год.

Образовательные аферы: дорога в никуда

Образование – одна из самых уязвимых для мошенничества сфер, ведь результат здесь отложен во времени, а критерии успешности размыты. Мошенники предлагают курсы и тренинги, обещающие золотые горы, но не дающие реальных знаний и навыков.

Типичный пример – курсы *«Как заработать миллион на криптовалютах за месяц»* или *«Станьте топовым дизайнером за 2 недели»*. Они редко стоят дешевле 1,000 евро и часто представляют собой набор общедоступной информации, упакованной в красивую обертку «эксклюзивных знаний».

Я встречал людей, потративших десятки тысяч евро на образовательные программы, которые не дали им ничего, кроме красочных сертификатов. В то же время существуют действительно качественные курсы и программы, в том числе бесплатные, от ведущих университетов мира.

Ремонт и строительство: классика жанра

Мошенничество в сфере ремонта и строительства существует, наверное, с тех самых пор, как человек начал строить первые жилища. Схемы здесь разнообразны: от банального использования некачественных материалов до сложных махинаций с проектной документацией.

Один из моих клиентов обратился ко мне после того, как заплатил строительной компании аванс в размере 30% за ремонт офиса (около 15,000 евро). Компания начала работы, демонтировала старую отделку и... исчезла. Расследование показало, что эта же компания под разными названиями провернула аналогичную схему в нескольких городах страны.

Как защититься:

При выборе поставщика услуг не ориентируйтесь только на красивый сайт и отзывы в интернете (их легко подделать). Запрашивайте референсы – контакты предыдущих клиентов, с которыми можно поговорить лично. Не платите большие авансы – разбивайте оплату на этапы, привязанные к конкретным результатам. И обязательно заключайте подробный договор с чётким описанием объёма работ, сроков и ответственности сторон.

Психология бытового мошенничества: почему мы так доверчивы?

В основе большинства описанных выше схем лежит наша естественная склонность доверять людям и системам. И этим активно пользуются мошенники.

«Эффект статуса»: костюм решает всё

Мы склонны доверять людям, которые выглядят представительно и говорят уверенно. Мошенник в дорогом костюме, с визитками солидной (часто несуществующей) компании и уверенной манерой общения вызывает гораздо больше доверия, чем обычный человек.

Я проводил эксперимент, когда один и тот же человек предлагал прохожим инвестировать в несуществующий проект. В первом случае он был одет в потертые джинсы и футболку, во втором – в деловой костюм. В первом случае его предложение не заинтересовало никого, во втором – контакты оставили почти 30% людей.

Вера в «официальные бумаги»

Мы привыкли доверять документам, особенно если они выглядят официально: с печатями, подписями, на фирменных бланках. Эта вера настолько сильна, что даже очевидные нестыковки в содержании могут быть проигнорированы, если форма кажется правильной.

Эффект «всех кинуть невозможно»

Многие жертвы массовых мошеннических схем – например, финансовых пирамид – руководствуются простой логикой: *«Не могут же они обмануть такое количество людей»*. Увы, могут и регулярно это делают. Масштаб операции не гарантирует ее честности.

Что делать?

Бытовое и корпоративное мошенничество многолико и постоянно эволюционирует. Но основные принципы защиты остаются неизменными:

1. **Проверяйте всё.** Не верьте на слово, даже если перед вами человек в дорогом костюме с внушительным титулом. Проверяйте документы, удостоверения личности, лицензии, отзывы (из разных источников).

2. **Помните: бесплатный сыр только в мышеловке.** Если предложение кажется слишком выгодным – вероятно, вам показывают не всю картину.

3. **Не спешите.** Мошенники почти всегда создают иллюзию срочности. Настоящие возможности редко исчезают за одну ночь.

4. **Консультируйтесь с профессионалами.** Перед крупными сделками (покупка недвижимости, инвестиции, дорогостоящие услуги) проконсультируйтесь с независимым специалистом.

5. **Доверяйте, но проверяйте.** Даже если поставщик услуг или товаров пришёл по рекомендации знакомых, это не гарантирует его честности. Люди меняются, компании тоже.

6. **Читайте мелкий шрифт.** В договорах, особенно финансовых, самое важное часто пишется самым мелким шрифтом в конце документа.

7. **Используйте защищённые способы оплаты.** По возможности избегайте предоплаты. Используйте платежные системы с функцией возврата средств или условного депонирования (escrow).

8. **Доверяйте своей интуиции.** Если что-то кажется подозрительным, скорее всего, так оно и есть. Не позволяйте убедить себя в обратном, даже если не можете точно сформулировать, что именно вас смущает.

Мошенники существовали всегда, но сегодня они эволюционировали, освоили новые технологии и психологические приёмы. Однако их цель остается неизменной – завладеть вашими деньгами или ценностями. И лучшая защита от них – это здоровый скептицизм, внимательность и готовность потратить время на проверку, прежде чем отдавать деньги или подписывать документы.

Как говорил мой дед: *«Если на секунду представить, что все люди вокруг – мошенники, мир покажется мрачным местом. Но если хотя бы иногда примерять эту мысль к тем, кто предлагает вам сделку, вы сохраните и деньги, и веру в человечество»*.

Часть 3

Технологии и будущее мошенничества

Глава 7. Цифровые двойники: ИИ как оружие мошенников

Вы думаете, что разговариваете с внуком по телефону? С начальником в мессенджере? С банковским сотрудником в видеочате? Уверены? А что, если это не они?

Помню, как в начале моей карьеры в кибербезопасности мы работали с примитивными программами подмены голоса. Это была скорее забава, чем реальная угроза – синтезированный голос звучал как робот из дешёвой научной фантастики 90-х. Сегодня искусственный интеллект может клонировать голос вашей матери по 30-секундной аудиозаписи так, что вы не заметите разницы.

В XXI веке мы стали свидетелями очередной технологической революции. Искусственный интеллект перестал быть прерогативой научных лабораторий и стал доступен каждому, у кого есть смартфон или ноутбук. То, что ещё недавно казалось невозможным, сегодня доступно по подписке всего за несколько долларов в месяц. И, как и всегда бывает с новыми технологиями, мошенники оказались в первых рядах их «пользователей».

Голосовой deepfake: когда звонит «бабушка»

Однажды мне поступил звонок от клиента – крупной страховой компании. Их директор по безопасности был в панике: *«Виктор, нам нужна ваша экспертиза. Мы потеряли 320,000*

евро на трансфере, который подтвердил наш финансовый директор. Но он утверждает, что никогда не давал такого разрешения».

Я прибыл в офис компании через час. Выяснилось, что финансовый отдел получил звонок от генерального директора с просьбой срочно перевести деньги на счет в Сингапуре. Звонивший объяснил это экстренной сделкой, которая должна была состояться буквально через несколько часов. Голос был идентичен голосу генерального директора, включая характерные речевые обороты и даже легкий акцент.

Мы провели расследование и обнаружили следующее:

1. Злоумышленники записали голос генерального директора во время его публичного выступления на отраслевой конференции.
2. Они использовали нейросеть для анализа речевых паттернов и создания цифровой модели его голоса.
3. Во время звонка они просто вводили текст, который хотели «произнести», а ИИ преобразовывал его в почти идеальную имитацию голоса директора.

То, что раньше требовало месяцев работы целой команды звукорежиссеров, теперь можно сделать за несколько часов с помощью общедоступных инструментов.

Этот случай – не исключение. По данным исследования компании McAfee за 2023 год, около 15% всех телефонных мошенничеств уже использовали элементы синтезированного голоса. А к 2024 году эта цифра выросла до 27%.

Вот как работает стандартная схема голосового deepfake:

1. Мошенник звонит бабушке от имени «внука» и сообщает о проблеме: *«Бабушка, я попал в аварию. Мне срочно нужны деньги на адвоката/лечение/залог»*.

2. Когда бабушка слышит голос, идентичный голосу внука, сомнения отпадают.

3. Эмоциональное давление (*«нужно срочно»*, *«я в опасности»*) блокирует критическое мышление.

4. Перевод денег происходит в течение минут, и вернуть их практически невозможно.

Как не стать жертвой:

- Установите с родственниками кодовое слово или фразу для экстренных ситуаций.
- Всегда перезванивайте на известный вам номер, даже если звонящий настаивает на немедленном решении.
- Задавайте вопросы, ответы на которые знаете только вы и ваш близкий человек.
- Если вам звонит «родственник» с просьбой о финансовой помощи, сказать, что вам нужно перезвонить через минуту – в 98% случаев мошенники сразу бросают трубку.

Визуальные подделки: когда нельзя верить глазам

«Привет, как дела? Посмотри, у меня новое хобби. Что скажешь?» – такое сообщение пришло моему коллеге от его брата в Instagram. К сообщению было прикреплено видео, где его брат

рассказывал о новом способе заработка на криптовалюте, который *«уже принес ему 50,000 долларов за две недели»*.

Мой коллега чуть не перевёл деньги, но что-то его насторожило: брат никогда раньше не интересовался криптовалютами. Он позвонил ему и выяснил, что аккаунт был взломан, а видео – полностью сгенерировано с помощью технологии deepfake.

Deepfake-видео – это следующий этап эволюции визуального мошенничества. Еще в 2019 году для создания правдоподобной подделки требовалось специальное оборудование и навыки. Сегодня существуют мобильные приложения, которые могут преобразовать фотографию человека в видео, где этот человек говорит текст, написанный мошенником.

Распространенные сценарии использования поддельных видео:

1. **Фишинг с «доверенными лицами»**: видео с известным человеком (CEO компании, знаменитостью), рекламирующим инвестиционную возможность или криптовалютный проект.
2. **Компрометирующие материалы**: создание фейкового видео интимного характера для шантажа.
3. **Политическое манипулирование**: подделка выступлений политиков для создания скандалов или манипуляции общественным мнением.

В 2022 году мэр одного из европейских городов чуть не перевел 300,000 евро из городского бюджета после видеоконференции, где ему казалось, что он разговаривает с коллегой из другого города. На самом деле это был deepfake, созданный мошенниками.

Как защититься:

- Проверяйте информацию через официальные каналы. Если CEO вашей компании внезапно просит перевести деньги через видеозвонок, свяжитесь с ним по официальному телефону.
- Обратите внимание на нестандартные запросы. Если человек, даже знакомый, просит сделать что-то необычное — это повод для беспокойства.
- Используйте дополнительные каналы связи для верификации. Один звонок по стационарному телефону может спасти от миллионных потерь.

Текстовые имитации: когда ИИ пишет вместо человека

В гонке за технологическим совершенством мы нередко забываем, что самый простой инструмент может быть самым эффективным. Современные языковые модели, такие как GPT-4 или Anthropic Claude, могут имитировать стиль письма конкретного человека с пугающей точностью.

«Привет, это Анна из бухгалтерии. Не мог бы ты подтвердить эти платежи? Нужно срочно, я в отпуске и не могу зайти в систему». Такое сообщение получил финансовый директор одной из компаний-клиентов. Он был готов подтвердить транзакции, но что-то показалось ему странным: Анна никогда не обращалась к нему с подобными просьбами во время отпуска.

Расследование показало, что мошенники использовали ИИ для анализа писем Анны (полученных из взломанной

почты) и создания текста, идентичного ее стилю. Они даже включили характерные для неё словечки и шутки.

Современные генеративные модели могут:

- Имитировать стиль конкретного человека;
- Поддерживать логичный диалог;
- Адаптироваться к новой информации в реальном времени;
- Преодолевать языковые барьеры через мгновенный перевод.

Один из самых распространенных сценариев – рассылка писем от имени руководителя с просьбой о срочном переводе средств или покупке подарочных карт для «важных клиентов».

Что делать:

- Внедрите дополнительные протоколы подтверждения для финансовых операций.
- Используйте двухфакторную аутентификацию для корпоративной почты.
- Настройте серверы для проверки DKIM и SPF записей, чтобы минимизировать шансы подделки отправителя.
- Если не уверены – позвоните человеку напрямую.

ИИ как инструмент автоматизации мошенничества

Раньше для организации массовой фишинговой кампании требовалась команда из нескольких человек: кто-то создавал сайты-подделки, кто-то писал тексты, кто-то собирал базы

данных потенциальных жертв. Сегодня все это может делать один человек с ноутбуком и доступом к нескольким ИИ-сервисам.

Я недавно анализировал фишинговую кампанию, нацеленную на клиентов крупного скандинавского банка. Мошенники использовали ИИ для:

- Генерации персонализированных писем (с учётом имени, данных о последних транзакциях и т.д.);
- Создания клона официального сайта банка с автоматическим обновлением;
- Анализа и сортировки украденных данных;
- Автоматического обхода капчи и других защитных механизмов.

Массовость и автоматизация – вот что делает ИИ идеальным инструментом для мошенников. Если раньше они могли отправить 100 писем в день, то теперь – миллионы. Если раньше их письма были полны ошибок и выглядели подозрительно, то теперь они грамматически и стилистически безупречны.

Как защититься:

- Используйте современные антивирусы с функцией анализа поведения сайтов.
- Не переходите по ссылкам в письмах – вводите адрес банка вручную или используйте закладки.
- Внимательно проверяйте URL – мошенники часто используют похожие домены (например, *sw3dbank.com* вместо *swedbank.com*).

- Помните, что банки никогда не запрашивают полные данные карты или пароли по электронной почте.

Что нас ждет завтра?

Мне часто задают вопрос: *«Виктор, какие новые угрозы принесет развитие ИИ?»* Я не хочу выступать в роли пророка апокалипсиса, но некоторые тенденции очевидны:

1. **Мультимодальные deepfake**: комбинации голоса, видео и текста для создания идеальной подделки.
2. **ИИ-аватары для общения с жертвами**: виртуальные операторы поддержки, которые могут вести беседу часами, не вызывая подозрений.
3. **Автоматизированные системы для обхода биометрической защиты**: уже сейчас существуют алгоритмы, способные обмануть системы распознавания лиц.
4. **Массовая персонализация атак**: ИИ анализирует ваши социальные сети и создает идеальную приманку именно для вас.

Лучший способ не потерять деньги – это поверить, что их у вас могут украсть. Да, это параноидально. Но в мире, где технологии развиваются быстрее, чем наша способность к адаптации, здоровая паранойя – это не диагноз, а стратегия выживания.

Если вы думаете, что ваша бабушка никогда не переведёт деньги мошенникам, вспомните: современные технологии позволяют создать идеальную копию голоса и внешности её внука. В этом новом мире скептицизм – не недостаток, а необходимое качество.

И помните: самая эффективная защита – это знание. Расскажите о современных угрозах своим родным и близким. Ведь мошенники рассчитывают именно на то, что жертва не будет знать о возможностях современных технологий.

Глава 8. Цифровое золото для цифровых пиратов: криптовалюты в арсенале мошенников

Когда я впервые услышал о Bitcoin в 2011 году, это казалось чем-то из области научной фантастики: деньги, существующие только в цифровом виде, без контроля правительств и банков. *«Революция в финансах!»* – кричали первые энтузиасты. *«Инструмент для преступников!»* – возражали скептики. Как часто бывает, правы оказались и те, и другие.

Через десять лет после своего появления, криптовалюта превратилась одновременно и в легитимный финансовый инструмент, и в любимую игрушку мошенников по всему миру. Я уже упоминал криптовалютные пирамиды и фейковые ICO в главе о финансовом мошенничестве, но сейчас поговорим о другом: почему цифровые деньги стали идеальным инструментом для жуликов и как именно они их используют?

Криптовалюты: почему мошенники их любят

«Виктор, меня обманули! Я перевел 50,000 евро в Bitcoin какому-то брокеру. Он обещал утроить сумму за месяц, но теперь не отвечает. Можете помочь вернуть деньги?» – подобные звонки я получаю почти каждый месяц.

И почти всегда мой ответ начинается с тяжёлого вздоха. Не потому, что я не хочу помочь, а потому что в 99% случаев

деньги уже невозможно вернуть. Криптовалюты создавались как система, где главной ценностью является анонимность и отсутствие центрального регулятора. Именно эти особенности делают их привлекательными для мошенников:

1. **Необратимость транзакций**: после подтверждения перевода в блокчейне его невозможно отменить. Это, как если бы вы передали наличные из рук в руки – никакой банк не поможет вернуть средства.

2. **Псевдонимность**: криптовалютные кошельки не привязаны к реальным личностям. Вы отправляете деньги не *«Джону Доу»*, а на адрес вида *«1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa»*. Кто стоит за этим адресом – остается загадкой.

3. **Глобальный характер**: ваш мошенник может находиться на другом конце земного шара. И даже если вы определите страну, проблемы с юрисдикцией и международным сотрудничеством правоохранительных органов делают преследование почти невозможным.

4. **Скорость**: перевод миллионов долларов занимает минуты, а не дни, как в традиционной банковской системе. Мошенник получает деньги раньше, чем жертва понимает, что ее обманули.

Однажды я заказал аудит системы безопасности для компании, торгующей криптовалютой. Генеральный директор встретил меня с гордостью: *«У нас современные протоколы проверки пользователей, двухфакторная аутентификация, защита от DDOS-атак. Мы неуязвимы!»*.

«А как вы защищаетесь от схемы с подменой адреса?» – спросил я.

«Какой еще подмены?» – удивился он.

Я попросил разрешения провести эксперимент и установил на один из компьютеров компании простейшую вредоносную программу, которая отслеживала буфер обмена. Когда сотрудник копировал криптовалютный адрес получателя, программа заменяла его на другой – принадлежащий «злоумышленнику» (в данном случае – мне). Таким образом, человек думал, что отправляет деньги на нужный адрес, но в реальности они уходили совсем другому получателю.

За 15 минут эта элементарная программа могла бы украсть несколько миллионов долларов, и никто бы даже не заметил подмены, пока не стало бы слишком поздно.

Фишинг на новом уровне: охота за криптокошельками

В 2017 году, на пике криптовалютного бума, я наблюдал рождение новой формы фишинга: охоты за ключами от криптокошельков.

Представьте: вы увлечённый криптоинвестор. Однажды вы получаете электронное письмо от «техподдержки» популярной биржи Binance. В письме говорится о необходимости срочно подтвердить аккаунт из-за «подозрительной активности». Вы переходите по ссылке, видите точную копию интерфейса Binance и вводите свои учётные данные.

Через минуту ваш кошелёк пуст.

Что произошло? Вы попали на сайт-клон, созданный мошенниками. Такие сайты часто имеют домены, отличающиеся

от оригинала всего одной буквой: *bínance.com* вместо *binance.com* (заметили разницу в первой букве «i»?).

За 2023 год только через подобные фишинговые атаки было украдено криптовалют на сумму более 500 миллионов долларов.

Но мошенники не останавливаются на имитации веб-сайтов. Они создают поддельные приложения для управления криптовалютой, фальшивые расширения для браузеров, якобы облегчающие работу с криптокошельками.

Один из моих клиентов, инвестор из Стокгольма, установил расширение, обещавшее *«автоматическую оптимизацию газа»*[14] для транзакций Ethereum (технически звучит как полезная функция). На следующий день его кошелек со 120 ETH (около 300,000 евро на тот момент) был полностью опустошён. Расширение содержало скрытый код, который отправлял приватные ключи на сервер мошенников.

Как защититься:

- Всегда проверяйте URL-адреса криптовалютных сайтов, особенно внимательно изучайте символы (некоторые буквы могут быть заменены похожими из других алфавитов).
- Используйте аппаратные кошельки для хранения значительных сумм.

[14] ***Газ (Gas)*** *в криптовалютных транзакциях – это комиссия, которую пользователь платит за выполнение операций в блокчейне. Эти средства идут валидаторам (майнерам или нодам) как вознаграждение за обработку транзакций и поддержку сети.*

- Никогда не передавайте никому свои «seed-фразы»[15] и приватные ключи – легитимные сервисы никогда их не запрашивают.
- Установите закладки для криптобирж в браузере вместо перехода по ссылкам из писем.

NFT и метавселенные: новые горизонты для старых схем

Если бы мне в 2019 году кто-то сказал, что люди будут платить миллионы долларов за цифровые картинки обезьян, я бы рассмеялся. А если бы мне сказали, что на этом будут зарабатывать миллиарды мошенники – попросил бы показать сценарий этого научно-фантастического фильма.

Но реальность оказалась странней любой фантастики.

NFT (невзаимозаменяемые токены) – цифровые сертификаты о владении уникальными объектами – открыли новую эру цифрового коллекционирования. И, разумеется, новую главу в истории мошенничества.

Как-то раз меня пригласили проконсультировать коллекционера, который потерял NFT стоимостью более 1 миллиона долларов. История оказалась банальной: он получил сообщение о том, что его NFT номинировано на престижную премию в области цифрового искусства. Для «подтверждения участия»

[15] ***Seed-фраза (сид-фраза)*** *– это уникальная последовательность слов (обычно от 12 до 24), которая используется для генерации и восстановления приватных ключей в криптовалютных кошельках.*

требовалось подключить кошелёк к сайту премии. После подключения все его токены мгновенно перешли к мошенникам.

Вот несколько популярных схем мошенничества в мире NFT:

1. **Rug pull** (*«выдёргивание коврика»*): создатели проекта собирают деньги инвесторов, а затем исчезают вместе с ними.
2. **Фальшивые коллекции**: мошенники создают копии популярных NFT-проектов, обманывая невнимательных покупателей.
3. **Фишинг с помощью смарт-контрактов**: жертву заставляют подписать смарт-контракт, который передаёт все её NFT мошенникам.

В 2022 году я исследовал случай, когда мошенники создали копию популярного проекта Bored Ape Yacht Club. Они даже запустили сайт с почти идентичным дизайном, но с другим доменным именем. Путём агрессивной рекламы в социальных сетях они убедили множество людей «минтить» (покупать при первом выпуске) поддельные NFT. За один день они собрали около 4 миллионов долларов и исчезли.

Как защититься:

- Проверяйте адреса смарт-контрактов коллекций на официальных площадках.
- Никогда не подписывайте транзакции, в которых не уверены.
- Используйте отдельный кошелёк для взаимодействия с новыми проектами.

• Помните: если предложение кажется слишком хорошим, чтобы быть правдивым, вероятно, это мошенничество.

Криптоджекинг: когда вы майните[16] для мошенников

Представьте: вы не вкладываете в криптовалюты, не имеете кошельков, даже не интересуетесь этой темой. Значит, вы в безопасности от криптомошенников? К сожалению, нет.

В 2018 году я заметил странное поведение своего ноутбука: вентиляторы постоянно работали на полную мощность, система тормозила, батарея разряжалась за час. Диагностика показала, что процессор загружен на 100%. Я запустил мониторинг задач и обнаружил неизвестный процесс, потребляющий все ресурсы. Это был криптоджекинг – скрытая программа, которая использовала мощности моего компьютера для майнинга криптовалюты в пользу мошенников.

Криптоджекинг – это процесс скрытого использования чужого компьютера для добычи криптовалюты. Заражение может произойти через фишинговые письма, взломанные веб-сайты или даже через общественный Wi-Fi.

По оценкам экспертов, к началу 2024 года около 8% всей вычислительной мощности, используемой для майнинга криптовалют, приходилось на заражённые компьютеры обычных пользователей.

---

[16] ***Майнить*** *(от англ. to mine – «добывать») – это процесс добычи криптовалюты путем решения сложных математических задач с использованием вычислительных мощностей (CPU, GPU, ASIC или FPGA).*

Признаки криптоджекинга:

- Компьютер работает значительно медленнее обычного.
- Вентиляторы постоянно работают на высокой скорости даже без запуска ресурсоёмких программ.
- Батарея ноутбука разряжается быстрее обычного.
- Повышенное потребление электроэнергии (актуально для стационарных компьютеров).

Как защититься:

- Установите надёжный антивирус с функцией блокировки майнеров.
- Используйте блокировщики скриптов в браузере (например, NoScript или uBlock Origin).
- Регулярно проверяйте список запущенных процессов на подозрительную активность.
- Не открывайте вложения из непроверенных источников.

Смарт-контракты – не всегда умные решения

«Красота смарт-контрактов в том, что они исключают посредников и гарантируют выполнение условий!» – восторженно рассказывал мне разработчик одного блокчейн-проекта.

«А что, если в коде контракта изначально заложена уязвимость?» – спросил я.

«Ну... это проблема, да», – нехотя признал он.

Смарт-контракты – самоисполняющиеся алгоритмы на блокчейне – часто преподносятся как панацея от мошенничества. Но правда в том, что они так же уязвимы, как и любой другой код, написанный человеком.

В 2016 году проект The DAO потерял около 60 миллионов долларов из-за ошибки в коде смарт-контракта. В 2021 году взлом крипто-мостов (протоколов для перевода активов между блокчейнами) привел к потере более 1 миллиарда долларов.

Я регулярно провожу аудит смарт-контрактов для блокчейн-проектов и почти всегда нахожу потенциальные уязвимости. Некоторые из них достаточно серьёзны, чтобы позволить злоумышленнику украсть все средства проекта.

Распространённые проблемы со смарт-контрактами:

1. **Переполнение счётчика**: когда контракт не может корректно обработать очень большие числа.
2. **Ошибки округления**: незначительные неточности, которые в масштабе могут привести к крупным потерям.
3. **Логические ошибки**: неверные условия выполнения операций.
4. **Front-running**: когда злоумышленник видит транзакцию до её подтверждения и использует эту информацию для своей выгоды.

Как защититься:

- Доверяйте только проверенным и аудированным смарт-контрактам.
- Начинайте с небольших сумм при взаимодействии с новыми протоколами.

- Следите за обновлениями безопасности проектов, с которыми взаимодействуете.
- Используйте инструменты для анализа смарт-контрактов перед крупными вложениями.

Будущее криптовалютного мошенничества

Когда речь заходит о будущем криптовалютного мошенничества, я предпочитаю быть реалистом, а не оптимистом. С ростом регулирования и развитием технологий некоторые старые схемы станут менее эффективными, но появятся новые, более изощренные.

Вероятные тенденции ближайших лет:

1. **Квантовая угроза**: с развитием квантовых компьютеров многие криптографические алгоритмы, лежащие в основе блокчейнов, могут стать уязвимыми.
2. **Атаки на «оракулы»**: смарт-контракты часто полагаются на внешние источники данных – «оракулы». Манипуляция этими источниками может привести к новым видам мошенничества.
3. **Социальная инженерия 2.0**: мошенники будут всё чаще использовать искусственный интеллект и deepfake для создания убедительных сценариев обмана.
4. **Гибридные атаки**: комбинации технических уязвимостей и социальной инженерии, направленные на обход многоуровневой защиты.

Я часто говорю клиентам: *«Не важно, насколько вы технически подкованы. Важно, насколько вы осторожны»*. В мире

криптовалют правило простое: если вы не понимаете, как работает технология или протокол – не вкладывайте в него деньги.

Как сказал один из моих коллег: *«В традиционных финансах вы доверяете институтам. В криптовалютах вы доверяете математике и коду. Но в обоих случаях вы должны доверять своей интуиции»*.

Если предложение звучит слишком хорошо, чтобы быть правдой, скорее всего, это скам. Даже если оно завёрнуто в блестящую бумажку блокчейна, смарт-контрактов и децентрализации.

Глава 9. За горизонтом обмана: мошенничество будущего

Когда меня спрашивают, победим ли мы когда-нибудь мошенничество, я вспоминаю свой разговор с легендарным специалистом по кибербезопасности, который сейчас консультирует крупнейшие технологические компании мира.

«Виктор, – сказал он мне, – представь эволюционную гонку между гепардом и антилопой. Антилопа становится быстрее, потому что выживают самые быстрые. Но и гепард становится быстрее по той же причине. Эта гонка никогда не закончится».

Так и с мошенничеством. Мы создаём защиту, мошенники ищут обходные пути. Мы совершенствуем технологии, они адаптируются и используют их против нас. Вечный танец жертвы и хищника.

В этой главе я хочу заглянуть за горизонт и обсудить, какие угрозы ждут нас в ближайшем будущем. Не для того, чтобы напугать, а чтобы подготовить. Знание – по-прежнему лучшая защита.

Метавселенные: новая территория без законов

В 2021 году Марк Цукерберг объявил о переименовании Facebook в Meta и о создании метавселенной – виртуального пространства, где люди будут работать, общаться и

развлекаться. С тех пор термин «метавселенная» стал одним из самых обсуждаемых в технологическом мире.

Но что такое метавселенная с точки зрения безопасности? Это новый дикий запад – территория, где правила ещё не установлены, а полиции попросту нет.

Недавно я участвовал в расследовании первого крупного мошенничества в метавселенной. Компания-разработчик привлекла более 60 миллионов долларов на создание виртуального мира с возможностью покупки «цифровой земли». Тысячи инвесторов вложили деньги в участки, которые, по обещаниям создателей, должны были расти в цене по мере развития проекта.

Через шесть месяцев основатели исчезли вместе с деньгами, а инвесторы остались с бесполезными NFT, которые невозможно было ни продать, ни использовать.

Это лишь начало. Вот что нас ждёт в ближайшие годы:

1. Виртуальное имущество и виртуальные кражи

В метавселенных люди будут владеть цифровыми активами: землёй, домами, одеждой для аватаров, виртуальными предметами искусства. Стоимость некоторых цифровых предметов уже сейчас достигает сотен тысяч долларов. Естественно, где есть ценность, там появляются и похитители.

Механизмы кражи виртуального имущества будут разнообразны:

- Фишинг для получения доступа к цифровым кошелькам;
- Эксплойты в коде метавселенных;
- Социальная инженерия внутри виртуальных миров.

Представьте: ваш аватар встречает в виртуальном мире «сотрудника техподдержки», который предлагает помощь в настройке безопасности. Вы предоставляете доступ, и через минуту ваша коллекция виртуальных предметов исчезает.

2. Виртуальная недвижимость и мошеннические застройщики

В популярных метавселенных уже сейчас торгуется виртуальная земля. Люди покупают участки рядом с «престижными локациями», рассчитывая на рост их стоимости.

Скоро мы увидим целые инвестиционные схемы вокруг виртуальной недвижимости. *«Купите участок в нашем виртуальном районе сейчас, и через год его цена утроится!»* Как и с реальной недвижимостью, многие такие проекты окажутся пирамидами.

Однажды в Стокгольме я консультировал венчурный фонд, собиравшийся инвестировать в компанию, создающую «элитную недвижимость» в одной из популярных метавселенных. На презентации основатели показали красивые рендеры виртуальных небоскребов и обещали 300% возврата инвестиций за два года.

Проведя расследование, я обнаружил, что за компанией стояли те же люди, которые ранее были связаны с несколькими криптовалютными скамами. Техническая документация проекта была скопирована с других источников, а показанные рендеры были созданы с помощью шаблонов.

Фонд отказался от инвестиций, а через четыре месяца компания-разработчик объявила о «технических сложностях» и закрылась, оставив частных инвесторов ни с чем.

3. Виртуальная идентичность и её кража

В метавселенных нашей основной точкой взаимодействия с миром станут аватары. Они будут представлять нас в виртуальных офисах, на встречах, в развлекательных пространствах. И, как это всегда бывает, появятся люди, желающие украсть чужую идентичность.

Представьте сценарий: злоумышленник создаёт копию вашего аватара, входит в виртуальный офис вашей компании и проводит «экстренное совещание», на котором просит коллег перевести средства на определенный счёт. Если метавселенная не имеет надежной системы верификации личности, такое мошенничество может оказаться успешным.

Как защититься:

- Выбирайте метавселенные с надежными системами верификации и безопасности;
- Используйте двухфакторную аутентификацию для доступа к своему аватару;
- Не храните ценные виртуальные активы на основном аккаунте – используйте отдельные кошельки;
- Сохраняйте здоровый скептицизм к инвестициям в виртуальную недвижимость.

Умный дом, умный город... умный мошенник

IoT (Internet of Things) – интернет вещей – стремительно меняет нашу повседневную жизнь. Умные холодильники, термостаты, системы безопасности, медицинские устройства... По прогнозам, к 2030 году среднестатистическое домохозяйство будет иметь более 50 подключенных устройств.

И все они потенциально могут стать мишенью для хакеров и мошенников.

В 2022 году я расследовал случай, когда группа злоумышленников взломала несколько десятков умных термостатов в элитном жилом комплексе. Они повысили температуру до максимума и заблокировали управление, а затем потребовали выкуп в криптовалюте. Жители оказались перед выбором: платить или терпеть невыносимую жару.

Этот случай – лишь вершина айсберга. Вот что нам предстоит:

1. Умный дом как заложник

Представьте: вы возвращаетесь домой и обнаруживаете, что не можете войти – умные замки заблокированы. На экране вашего смартфона появляется сообщение: *«Перечислите 0.1 Bitcoin на этот адрес, чтобы вернуть контроль над своим домом»*.

Или другой сценарий: ваша система безопасности взломана, и злоумышленники угрожают отключить её, если не получат выкуп. Фактически, вам придется заплатить за то, чтобы ваш дом не был ограблен.

2. Манипуляции с умными городскими системами

Концепция «умного города» предполагает интеграцию множества систем: светофоров, энергосетей, водоснабжения, видеонаблюдения. Компрометация этих систем может привести к хаосу.

В 2021 году я участвовал в тестировании безопасности систем управления дорожным движением в одном европейском городе. Мы обнаружили уязвимость, позволяющую удаленно менять режим работы светофоров. К счастью, это была санкционированная проверка, а не реальная атака.

3. Медицинские устройства и шантаж

Это самый тревожный сценарий. Умные инсулиновые помпы, кардиостимуляторы, слуховые аппараты – все эти устройства могут иметь уязвимости.

В 2018 году FDA (Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США) выпустило предупреждение об уязвимостях в определенных моделях кардиостимуляторов, которые теоретически позволяли хакерам менять настройки устройства.

Сценарий шантажа с использованием медицинских устройств пока остаётся теоретическим, но технически возможным.

Как защититься:

- Регулярно обновляйте программное обеспечение всех умных устройств;

- Используйте сложные пароли для IoT-устройств и меняйте заводские настройки;
- Сегментируйте домашнюю сеть – отделяйте критически важные устройства от остальных;
- Приобретайте устройства только от проверенных производителей с хорошей репутацией в сфере безопасности.

Биометрический обман: когда ваше лицо и голос больше не принадлежат только вам

«Смотрите мне в глаза, и банковское приложение откроется автоматически», – с гордостью демонстрировал новую функцию своего смартфона мой друг-банкир.

«А что, если кто-то использует твою фотографию?» – спросил я.

«Система определяет, живой человек перед ней или изображение», – ответил он уверенно.

«А если это будет реалистичная 3D-модель твоего лица?» – не унимался я.

Он замолчал.

Биометрическая аутентификация стремительно входит в нашу жизнь. Отпечатки пальцев, распознавание лица, голосовая идентификация, сканирование сетчатки – всё это должно сделать нашу жизнь безопаснее и удобнее. Но в руках мошенников эти технологии могут обернуться против нас.

1. Обман систем распознавания лиц

Уже сейчас существуют технологии, способные обмануть системы распознавания лиц:

- 3D-маски, созданные на основе фотографий;
- Deepfake-видео с имитацией движений головы и моргания;
- Проекция изображения лица на специальную маску.

В 2022 году на конференции по кибербезопасности в Барселоне я наблюдал демонстрацию: исследователь смог обмануть систему распознавания лиц крупного банка с помощью маски, напечатанной на 3D-принтере. Стоимость создания такой маски – менее 200 евро, а потенциальный ущерб – неограничен.

2. Подделка голоса и голосовые deepfakes

Я уже рассказывал о синтезе голоса в главе про искусственный интеллект, но технологии развиваются ещё быстрее, чем мы думаем. Сейчас для создания реалистичной голосовой модели достаточно всего нескольких секунд записи голоса человека.

Это открывает новые возможности для мошенничества:

- Обход голосовой аутентификации в банковских системах;
- Авторизация голосовых транзакций;
- Поддельные голосовые сообщения с просьбами о помощи.

3. Подделка отпечатков пальцев

Мало кто знает, но отпечаток пальца можно подделать, имея лишь его четкую фотографию. Исследователи из Токийского университета продемонстрировали, как можно воссоздать отпечаток с фотографии, сделанной с расстояния трех метров обычной камерой смартфона.

А сколько раз вы оставляли отпечатки на стаканах в кафе или на документах в офисе?

Как защититься:

- Используйте многофакторную аутентификацию – не полагайтесь только на биометрию;
- Будьте осторожны с публикацией чётких фотографий своего лица в социальных сетях;
- По возможности используйте дополнительные проверки при авторизации критически важных операций;
- Следите за развитием технологий защиты – производители постоянно совершенствуют алгоритмы противодействия обману.

Нейроинтерфейсы: когда взламывают уже не компьютер, а мозг

Технологии нейроинтерфейсов – устройств, позволяющих напрямую взаимодействовать с компьютером посредством мозговой активности – уже не фантастика. Компании вроде Neuralink Илона Маска активно работают над созданием имплантов, которые позволят парализованным людям управлять

компьютерами, а в будущем, возможно, дадут и здоровым людям новые способности.

Но вместе с новыми возможностями приходят и новые риски.

Представьте: ваш банковский аккаунт привязан к нейроинтерфейсу. Для перевода денег достаточно подумать о сумме и получателе. Что произойдет, если хакеры получат доступ к вашему нейроинтерфейсу? Или смогут подделать сигналы, которые он отправляет?

Это не сюжет фантастического фильма, а вполне реальная угроза будущего.

В 2022 году команда исследователей из Калифорнийского университета опубликовала работу, в которой продемонстрировала возможность извлечения конфиденциальной информации (такой как пароли) из сигналов мозга, зафиксированных коммерчески доступными электроэнцефалографами.

Нейрохакинг может принимать различные формы:

- Кража данных, считанных напрямую из мозга;
- Манипуляция входящими сигналами для создания ложных восприятий;
- Внедрение подсознательных команд или желаний;
- Шантаж с использованием личных данных, полученных через нейроинтерфейс.

Как защититься:

- Относитесь к безопасности нейроинтерфейсов так же серьёзно, как к безопасности компьютера – возможно, даже серьёзнее;
- Используйте только проверенные устройства от надёжных производителей;
- Следите за законодательством в этой области – нам нужны чёткие правила защиты нейроданных;
- Будьте особенно осторожны с технологиями, которые могут записывать или интерпретировать ваши мысли.

Заключение: готовы ли мы к будущему мошенничества?

Технологии развиваются с головокружительной скоростью. То, что казалось научной фантастикой десять лет назад, сегодня доступно каждому. И, к сожалению, в том числе мошенникам.

Означает ли это, что нам нужно бояться технологического прогресса? Конечно, нет. Новые технологии делают нашу жизнь лучше, удобнее, интереснее. Но мы должны быть готовы к рискам, которые они несут.

Лучшая защита – это знание и здоровый скептицизм. Задавайте вопросы. Проверяйте информацию. Не торопитесь принимать решения, особенно если они касаются ваших денег или личных данных.

Я часто повторяю своим клиентам: *«Параноик – это не тот, кто думает, что за ним следят. Это тот, кто думает, что*

за ним следят только его враги». В мире современных технологий небольшая доля паранойи – это просто здравый смысл.

Помните, главное преимущество мошенников – это наша неосведомленность и наивность. Вооружившись знаниями о потенциальных угрозах, вы снижаете свои шансы стать жертвой в разы.

И последнее: делитесь своими знаниями с другими. Особенно с теми, кто может быть наиболее уязвим – пожилыми родственниками, детьми, людьми, далекими от технологий. Образование – наше главное оружие в борьбе с мошенниками будущего.

Технологии будут развиваться. Мошенничество будет эволюционировать вместе с ними. Но если мы будем готовы к этим изменениям, если будем оставаться на шаг впереди мошенников, мы сможем наслаждаться всеми преимуществами технологического прогресса, минимизировав его риски.

В конце концов, будущее – это не то, что с нами просто случается. Это то, что мы создаём своими действиями и решениями сегодня.

Часть 4

Как защититься?

Глава 10. В голове у жертвы: психологические ловушки мошенничества

«Мошенники не взламывают компьютеры. Они взламывают людей, которые пользуются компьютерами»

В предыдущих главах мы разобрали десятки схем мошенничества – от древних трюков с фальшивыми монетами до современных deepfake-атак. Но есть одна вещь, которая остаётся неизменной на протяжении тысячелетий: психология жертвы. Как ни странно, наш мозг практически не эволюционировал с точки зрения устойчивости к обману.

Я часто слышу от людей фразу*: «Со мной такого никогда не случится, я слишком умный»*. И знаете что? Именно эти люди чаще всего и оказываются в моём офисе, рассказывая, как потеряли все сбережения на «гарантированных инвестициях».

В этой главе мы посмотрим на мошенничество глазами нейробиологии и психологии. Я покажу вам, почему даже профессора университетов и топ-менеджеры попадаются на примитивные уловки. И, что важнее, – научу, как превратить свой мозг из пособника мошенников в детектор лжи.

Почему мы так легко верим?

Когда я только начинал карьеру журналиста, меня поразила история одного профессора психологии, который перевёл

50,000 евро нигерийским мошенникам. Казалось бы – человек, который сам читает лекции о когнитивных искажениях! Как такое возможно?

Чтобы понять это, нужно разобраться в нескольких ключевых психологических особенностях нашего мышления:

1. Эвристика доступности

Наш мозг оценивает вероятность событий по тому, насколько быстро мы можем вспомнить примеры. Чем легче мы можем представить ситуацию, тем более вероятной она нам кажется.

Мошенники мастерски используют эту особенность. Например, фразой *«ваша карта заблокирована»* они мгновенно активируют все истории о блокировках карт, которые вы когда-либо слышали. И в момент стресса мозг цепляется именно за эти воспоминания, а не за статистику мошенничества.

Однажды в Стокгольме я наблюдал, как женщина с двумя учеными степенями и IQ выше 130 отдавала все данные своей карты по телефону «сотруднику банка». Когда я спросил её позже, почему она это сделала, она сказала: *«У меня раньше действительно блокировали карту из-за подозрительных транзакций, это показалось логичным»*.

2. Синдром упущенной выгоды (FOMO)

Страх что-то упустить – мощнейший психологический триггер. Когда мошенник говорит *«только сегодня»* или *«осталось 2 места»*, в нашем мозгу активируется древний инстинкт дефицита.

Я сам чуть не попался на это, когда мне предложили «эксклюзивное» участие в ICO криптовалюты с «гарантированной доходностью». Мысль о том, что завтра эта возможность исчезнет, буквально отключила мой критический анализ. К счастью, я взял паузу на 24 часа – и за это время обнаружил, что проект был полной фикцией.

3. Эффект авторитета

Мы запрограммированы доверять авторитетам. Исследования Милграма показали, что люди готовы выполнять даже сомнительные действия, если команда исходит от человека в белом халате.

Мошенники используют эту уязвимость, представляясь сотрудниками банков, полиции или государственных служб. Даже минимальные атрибуты власти – официальный тон, правильная терминология – заставляют наш мозг автоматически снижать критичность.

В моей практике был случай, когда опытный финансист перевел 200,000 евро на «безопасный счёт», потому что звонивший представился «старшим инспектором кибербезопасности Европола» и использовал профессиональный жаргон.

4. Когнитивная нагрузка

Мошенники обожают создавать ситуации, когда жертве нужно быстро принимать решения в состоянии стресса. Это не случайно – под давлением префронтальная кора, отвечающая за критическое мышление, практически отключается, а контроль переходит к более примитивным структурам мозга.

Вспомните типичный звонок лжесотрудника банка: *«Срочно, с вашей карты пытаются списать деньги! У нас есть только 3 минуты, чтобы остановить транзакцию!»* В такой ситуации даже самый разумный человек может действовать импульсивно.

Психологические профили жертв

Вопреки распространенному мнению, на удочку мошенников попадаются не только пожилые люди или технически неграмотные. За годы работы я выделил несколько психологических профилей, наиболее уязвимых для разных типов мошенничества:

1. «Эксперт»

Это может показаться парадоксальным, но люди с высоким уровнем знаний в определённой области часто становятся жертвами именно в этой сфере. Феномен называется «проклятием знания» – эксперты настолько уверены в своей компетентности, что теряют бдительность.

Я консультировал IT-директора крупной компании, который попался на примитивный фишинг. На вопрос *«как это произошло?»* он ответил*: «Я был уверен, что распознал бы настоящий фишинг. Это было слишком просто, поэтому я решил, что это настоящее письмо»*.

2. «Искатель справедливости»

Этот тип особенно уязвим для мошенничества, апеллирующего к чувству справедливости. Например, финансовые

пирамиды часто маскируются под «народные» проекты, борющиеся с «несправедливостью банковской системы».

Статистика показывает, что около 35% жертв инвестиционного мошенничества привлекает не только потенциальная выгода, но и идеологическая составляющая – возможность «бросить вызов системе».

3. «Одинокий благодетель»

Исследования показывают, что люди, испытывающие одиночество, на 30% более уязвимы для мошенничества. Причина проста – мошенники предлагают не только финансовую выгоду, но и эмоциональную связь, внимание, благодарность.

Именно поэтому аферы с *«помощью попавшим в беду за границей»*, романтические схемы и благотворительные мошенничества так успешны – они заполняют эмоциональный вакуум.

4. «Игрок»

Люди с повышенной склонностью к риску чаще становятся жертвами инвестиционного мошенничества. Их мозг буквально «подсаживается» на дофамин от ожидания выигрыша, что приводит к принятию иррациональных решений.

Нейробиологические исследования показывают, что в момент обещания большой прибыли в мозгу активируются те же центры удовольствия, что и при употреблении наркотиков. Неудивительно, что критическое мышление отключается.

Как мошенники управляют нашими эмоциями

Профессиональные мошенники – это не просто технические эксперты. Прежде всего, они мастера эмоциональных манипуляций. Вот основные техники, которые они используют:

1. Эмоциональные качели

Мошенники намеренно создают эмоциональные контрасты: сначала вызывают страх или тревогу, а затем предлагают облегчение.

Классический пример – звонок о «проблемах с банковским счётом», за которым следует успокаивающее *«мы можем всё исправить, просто следуйте инструкциям»*. После пережитого стресса жертва испытывает такое облегчение, что готова некритично выполнять любые указания.

2. Постепенная эскалация

Опытные мошенники никогда не просят о крупных суммах сразу. Они используют технику «нога в дверях» – сначала маленькая просьба, затем чуть больше, и так до тех пор, пока жертва не окажется глубоко вовлеченной.

В моей практике был случай с человеком, который в итоге перевел мошенникам более 300,000 евро. А начиналось всё с «пробной инвестиции» в 100 евро, которая действительно принесла прибыль.

3. Срочность и дефицит

«У вас есть только 15 минут, чтобы принять решение» – типичная тактика мошенников. Цейтнот не даёт жертве возможности обдумать ситуацию, проконсультироваться с близкими или провести собственное расследование.

И, как я уже писал в начале книги, создание иллюзии дефицита – один из старейших приемов. *«Только сегодня»*, *«последний токен по этой цене»*, *«осталось 2 места»* – все эти фразы активируют страх упустить выгоду.

4. Эффект «свой-чужой»

Мошенники адаптируются к профилю жертвы, создавая впечатление «своего человека». Они могут имитировать акцент, использовать профессиональный жаргон или делиться якобы личными историями, похожими на опыт жертвы.

«Я тоже из России, переехал в 90-е» – эта фраза однажды чуть не стоила мне нескольких тысяч евро, когда я общался с «инвестиционным консультантом». Мозг автоматически повышает доверие к «своим», даже если эта общность иллюзорна.

Что делать?

Теперь, когда мы разобрали психологические механизмы, давайте поговорим о защите. Хорошая новость в том, что знание этих механизмов уже делает вас менее уязвимыми.

1. Правило 24 часов

Внедрите в свою жизнь простое правило: никогда не принимайте финансовых решений в тот же день, особенно если вас торопят. Даже если предложение кажется идеальным, дайте себе 24 часа на размышление.

Я видел, как это правило сэкономило миллионы евро моим клиентам. Удивительно, но за эти 24 часа «невероятные возможности» часто обнаруживают свою мошенническую природу.

2. Встройте сомнение в принятие решений

Выработайте привычку задавать себе три вопроса перед любым финансовым решением:

- Почему именно я получил это предложение?
- Что произойдёт, если я откажусь или отложу решение?
- Как бы я объяснил это решение скептически настроенному другу?

Эти простые вопросы активируют критическое мышление и часто выявляют нестыковки в схемах мошенников.

3. Создайте эмоциональный буфер

Научитесь распознавать эмоциональные манипуляции. Если вы чувствуете сильную тревогу, страх или, наоборот, эйфорию от потенциальной возможности – это сигнал остановиться.

Я рекомендую технику «эмоционального шага назад»: представьте, что ситуация происходит не с вами, а с вашим

другом, и вы даёте ему совет. Такая дистанция помогает увидеть манипуляции.

4. Проверяйте, даже если стыдно

Многие жертвы признавались мне, что не перепроверили информацию, потому что *«было неудобно показаться недоверчивым»* или *«не хотелось тратить время оператора»*.

Запомните: лучше минута неловкости, чем годы финансовых проблем. Положите трубку и перезвоните в банк по официальному номеру. Проверьте компанию в реестрах. Поищите отзывы (не на сайте компании, а на независимых ресурсах).

5. Развивайте осознанное отношение к риску

Поймите свой психологический профиль и уязвимости. Если вы «игрок» – осознайте, что высокая доходность всегда сопряжена с высоким риском, а *«гарантированная высокая доходность»* – это оксюморон и красный флаг.

Если вы «эксперт» – напоминайте себе, что даже профессионалы могут ошибаться. Иногда самые примитивные схемы работают именно на опытных людях, уверенных в своей неуязвимости.

Заключение

Психология мошенничества – это не просто академическая область. Это практический инструмент выживания в современном цифровом мире.

Я всегда говорю своим клиентам: мошенники не волшебники. Они просто хорошо понимают, как работает человеческий мозг, и используют эти знания против нас. Но эту же информацию можно использовать для защиты.

Помните: самый надежный фаервол против мошенничества – это не антивирус или сложный пароль. Это ваш критически настроенный мозг, осознающий свои когнитивные слабости.

Когда мы с женой покупали нашу квартиру в Стокгольме, агент по недвижимости пытался давить на нас тактикой срочности: *«Другая пара готова подписать контракт через час»*. Я улыбнулся и сказал: *«Отлично, пусть подписывают. Мы примем решение завтра»*. В итоге квартира досталась нам, причём на 5% дешевле первоначальной цены.

Иногда лучшая защита – это готовность упустить возможность. Потому что настоящие возможности редко исчезают за 15 минут, а вот деньги – очень даже могут.

Глава 11. Цифровой иммунитет: техническая защита от мошенников

«Мошенники – как вирусы: постоянно мутируют, чтобы обойти защиту. Но в отличие от вирусов, их можно победить не только антибиотиками, но и знаниями»

Если предыдущая глава была о защите вашего мозга от психологических манипуляций, то эта – о создании цифрового щита вокруг ваших данных и денег. Я называю это *«цифровым иммунитетом»* – способностью технически противостоять атакам мошенников.

Представьте, что ваша цифровая жизнь – это средневековый замок. Психологическая защита – это тренированные солдаты гарнизона. А техническая защита – это стены, рвы и подъёмные мосты. Даже если враг очень убедителен в переговорах, хорошие стены не дадут ему проникнуть внутрь.

В моей практике я видел сотни случаев, когда даже самые простые технические меры спасали людей от огромных потерь. И наоборот – как отсутствие элементарной цифровой гигиены приводило к катастрофам.

Важно понимать: идеальной защиты не существует. Но ваша задача – сделать атаку на вас настолько сложной и невыгодной, чтобы мошенник просто переключился на более легкую цель. Помните старую шутку про двух туристов и медведя? *«Мне не нужно бежать быстрее медведя. Мне нужно бежать быстрее тебя»*.

Итак, давайте построим ваш цифровой замок.

Основы цифровой гигиены

Начнём с базовых вещей, которые должны стать для вас такой же привычкой, как чистка зубов. Эти меры не требуют глубоких технических знаний, но критически важны:

1. Пароли: ваши цифровые ключи

Если бы я получал по евро каждый раз, когда слышу *«у меня один пароль на все сайты, так проще запомнить»* – я бы уже купил яхту. И если бы получал ещё по евро за каждую историю взлома такого человека – купил бы две.

Вот правила, которые не обсуждаются:

- **Никогда не используйте один пароль для разных сервисов.** Когда (не если, а именно когда) один из сайтов будет взломан, мошенники получат доступ ко всем вашим аккаунтам.
- **Используйте менеджер паролей.** LastPass, 1Password, Bitwarden, KeePass – выбор большой. Вам нужно запомнить только один мастер-пароль, а менеджер сгенерирует и сохранит сложные уникальные пароли для всех сайтов.
- **Создавайте сложные пароли.** Минимум 12 символов, комбинация букв разного регистра, цифр и специальных символов. И нет, *«Password123!»* – это не сложный пароль.
- **Регулярно меняйте пароли к критически важным сервисам.** Банки, электронная почта, мессенджеры – раз в 3–6 месяцев.

Я консультировал руководителя IT-компании, чей аккаунт электронной почты был взломан. Знаете, как? Он

использовал один и тот же пароль для рабочей почты и для регистрации на каком-то форуме по рыбалке. Форум взломали, базу паролей слили, и через несколько дней злоумышленники получили доступ к его корпоративной переписке. Цена ошибки – около 50,000 евро.

2. Двухфакторная аутентификация (2FA)

Если пароль – это ключ от замка, то 2FA – это дополнительная охрана, которая проверяет ваш документ на входе. Даже если злоумышленник узнает пароль, без второго фактора он не сможет войти в аккаунт.

Варианты 2FA по уровню защиты (от лучшего к худшему):

- **Аппаратные ключи** (YubiKey, Titan Security Key) – физические устройства, которые нужно подключить к компьютеру или смартфону. Наиболее надежный вариант.
- **Приложения-аутентификаторы** (Google Authenticator, Microsoft Authenticator, Authy) – генерируют временные коды на вашем смартфоне.
- **SMS-коды** – наименее надежный вариант из-за возможности перехвата SMS или подмены SIM-карты. Но всё равно лучше, чем ничего.

Включите 2FA везде, где это возможно, особенно для электронной почты, социальных сетей, банковских приложений и облачных хранилищ.

Один из моих клиентов установил 2FA для своего аккаунта Gmail после того, как чуть не потерял доступ к почте. Через неделю в логах Gmail он увидел 17 неудачных попыток входа с

IP-адресов из трёх разных стран. Мошенники знали его пароль, но не смогли пройти дальше.

3. Обновления ПО: латаем дыры в крепостной стене

Каждое обновление операционной системы, браузера или приложения – это не просто новые функции. В первую очередь, это исправление уязвимостей безопасности, которые уже обнаружены.

- **Включите автоматические обновления** для операционной системы и браузера.
- **Регулярно обновляйте приложения** на смартфоне и компьютере.
- **Особое внимание – роутеру.** Большинство людей настраивают роутер раз в жизни и забывают о нём. А ведь это – главные ворота в вашу домашнюю сеть.

Помню случай с семьей из Стокгольма, которая игнорировала обновления ПО на своем смарт-телевизоре. В результате телевизор был взломан и использовался для майнинга криптовалюты. Они заметили проблему, только когда устройство начало сильно перегреваться и тормозить.

Распознаём цифровые ловушки

Теперь, когда мы укрепили базовую защиту, давайте научимся распознавать наиболее распространенные технические ловушки.

1. Фишинг: волк в овечьей шкуре

В главе 5 мы подробно разбирали, что такое фишинг. Теперь поговорим, как технически его распознать:

- **Проверяйте URL-адреса.** Фишинговые сайты часто используют похожие, но не идентичные адреса: *swedbank-secure.com* вместо *swedbank.com* или *amazon.com* (с кириллической «а») вместо *amazon.com*.
- **Используйте закладки для важных сайтов.** Не переходите на банковские сайты по ссылкам из писем или SMS.
- **Обращайте внимание на HTTPS.** Отсутствие защищённого соединения (зеленый замок в адресной строке) – серьёзный повод для беспокойства. Но помните: наличие HTTPS не гарантирует, что сайт настоящий!
- **Установите антифишинговое расширение для браузера.** Например, Web of Trust, PhishDetector или встроенную защиту в современных браузерах.

Один из сотрудников нашей компании едва не ввел корпоративные логин и пароль на поддельном сайте Microsoft 365. Сайт был идеальной копией оригинала, но в URL вместо «microsoft» было «rnicrosoft» с кириллической «г». Спасло его только то, что менеджер паролей не предложил автозаполнение, что показалось подозрительным.

2. Вредоносное ПО: троянский конь цифрового века

Вот как защититься от вредоносных программ:

- **Используйте антивирус.** Да, даже на Мас. Да, даже если вы *«очень осторожны»*.

- **Не скачивайте программы с неофициальных источников.** Торренты со взломанными программами и игры с *«бесплатной активацией»* – это классический способ распространения вредоносного ПО.
- **Будьте осторожны с расширениями для браузера.** Они имеют доступ ко всему, что вы делаете в интернете. Устанавливайте только те, что действительно необходимы и имеют хорошую репутацию.
- **Регулярно сканируйте систему на вредоносное ПО.** Некоторые современные вирусы настолько продвинуты, что могут месяцами оставаться незамеченными.

На одной из конференций по кибербезопасности я познакомился с человеком, который оплатил полную версию какого-то видеоредактора со скидкой 90% через подозрительный сайт. Через месяц с его банковского счёта исчезли все деньги. Вредоносная программа тихо собирала его банковские данные все это время.

Настройки безопасности в социальных сетях и приложениях

Социальные сети и приложения – это не просто развлекательные платформы. Это настоящие сокровищницы ваших личных данных. Вот как максимально их защитить:

1. Аудит приватности

- **Проверьте настройки приватности.** Кто может видеть ваши посты, фотографии, список друзей? Ограничьте доступ до минимально необходимого круга людей.

- **Контролируйте, какие приложения имеют доступ к вашим аккаунтам.** Регулярно проверяйте список подключенных приложений в Facebook, Google и других сервисах. Удаляйте те, которыми не пользуетесь.
- **Отключите геолокацию** для приложений, которым она не нужна. Зачем калькулятору знать, где вы находитесь?

После того, как один из моих клиентов столкнулся с шантажом, мы провели аудит его социальных сетей. Оказалось, что из-за неправильных настроек приватности любой человек мог увидеть его отпускные фотографии, информацию о дорогих покупках и даже точный адрес дома (он был указан в метаданных фотографий).

2. Безопасность банковских приложений

- **Используйте отдельный E-mail для финансовых сервисов.** Не тот, который вы указываете на сайтах, форумах или в социальных сетях.
- **Включите уведомления обо всех операциях.** Чем быстрее вы заметите подозрительную активность, тем больше шансов остановить мошенников.
- **Используйте виртуальные карты для онлайн-покупок.** Многие банки позволяют создавать временные виртуальные карты с ограниченным балансом для онлайн-платежей.
- **На общедоступных Wi-Fi не проводите финансовые операции.** Либо используйте VPN, либо мобильный интернет.

Я сам стал параноиком в этом вопросе после того, как услышал историю коллеги. Он проверил баланс карты, подключившись к бесплатному Wi-Fi в кафе. На следующий день

обнаружил списание всех средств. Как выяснилось, кто-то в том же кафе создал поддельную точку доступа с похожим названием.

Инструменты проверки

Существует множество сервисов, которые помогут вам проверить подозрительные сайты, письма или файлы:

1. Проверка веб-сайтов

- **WHOIS-сервисы** (*whois.net*, *whois.domaintools.com*) – показывают, когда был зарегистрирован домен и кем. Сайт, созданный неделю назад, вряд ли принадлежит *«известному банку с 30-летней историей»*.
- **VirusTotal** – сканирует ссылки на предмет вредоносного содержимого.
- **ScamAdviser** – оценивает надежность интернет-магазинов.
- **Web of Trust (WOT)** – показывает репутацию сайта на основе отзывов пользователей.

2. Проверка электронных писем

- **Mail-Tester** – анализирует техническую структуру письма на признаки спама.
- **DMARC Inspector** – позволяет проверить подлинность отправителя.
- **Расширения для проверки ссылок в Gmail и Outlook.**

3. Проверка номеров телефонов

- **GetContact, TrueCaller** – показывают, как номер помечен у других пользователей (например, «Мошенники Банк»).
- **Официальные базы мошеннических номеров** от телеком-операторов и банков.

Я регулярно пользуюсь этими инструментами, и они не раз спасали меня от неприятностей. Например, однажды я чуть не кликнул на ссылку в письме от «службы доставки». Проверка на VirusTotal показала, что ссылка ведёт на фишинговый сайт, имитирующий страницу оплаты.

Шифрование – ваш последний рубеж защиты

Даже если все предыдущие меры не сработали, шифрование может стать последним барьером между вашими данными и мошенниками:

- **Шифруйте важные файлы** с помощью встроенных средств (BitLocker в Windows, FileVault в macOS) или специальных программ (VeraCrypt, AxCrypt).
- **Используйте защищённые мессенджеры** с end-to-end шифрованием (Signal, Telegram в секретных чатах, WhatsApp).
- **Для особо чувствительных данных рассмотрите вариант «холодного» хранения** – на отключённых от интернета устройствах или даже на бумаге.

Я знаю бизнесмена, который потерял доступ к своему компьютеру из-за программы-вымогателя. Все файлы были зашифрованы, кроме одной папки – в ней хранились наиболее важные

документы, которые он заранее зашифровал сам. Мошенники получили доступ к компьютеру, но не к этим критически важным данным.

Что делать?

В качестве заключения, вот мой чек-лист технической безопасности. Распечатайте его и повесьте рядом с компьютером:

1. Ежемесячно:

- Меняйте пароли к критически важным аккаунтам.
- Проверяйте активность в банковских приложениях.
- Сканируйте устройства на вредоносное ПО.
- Очищайте браузер от ненужных расширений и cookies.

2. Ежеквартально:

- Проводите аудит настроек приватности в социальных сетях.
- Проверяйте список приложений, имеющих доступ к вашим аккаунтам.
- Обновляйте прошивку роутера и других сетевых устройств.

3. Ежегодно:

- Создавайте резервные копии важных данных.
- Пересматривайте стратегию безопасности – появляются новые угрозы и новые инструменты защиты.

- Повышайте свою техническую грамотность – читайте блоги по кибербезопасности, слушайте подкасты, посещайте вебинары.

Я начинал эту главу с метафоры замка. Закончу другой: техническая безопасность – это не спринт, а марафон. Мошенники постоянно придумывают новые способы обойти защиту, и вам нужно постоянно адаптироваться.

Помните: безопасность – это процесс, а не результат. В цифровом мире нет абсолютной защиты, но есть разница между лёгкой мишенью и крепостью, которую сложно взломать.

Я надеюсь, что эта глава поможет вам стать крепостью. В конце концов, мошенники – как вода: всегда текут по пути наименьшего сопротивления. Убедитесь, что этот путь не проходит через вас.

Глава 12. После удара: что делать, если вы стали жертвой мошенников

«Быть обманутым – не повод для стыда. Стыдно – не извлечь из этого уроки и не помочь другим»

За годы работы в сфере кибербезопасности мне приходилось видеть самые разные реакции людей, столкнувшихся с мошенничеством. Кто-то впадал в отчаяние, кто-то испытывал парализующий стыд, некоторые переходили к яростному отрицанию, а другие начинали одержимо искать виноватых – банки, интернет-провайдеров, государство.

Все эти реакции я понимаю. Но ни одна из них не поможет вам вернуть деньги, восстановить репутацию или просто пережить случившееся с минимальными потерями.

В прошлых главах мы говорили о том, как не стать жертвой. Но что делать, если самое страшное уже произошло? Если вы читаете эту главу после того, как столкнулись с мошенничеством – не отчаивайтесь. То, что вы видите перед собой эту книгу, уже говорит о вашем желании разобраться и двигаться дальше. И я помогу вам в этом.

Первые 48 часов: время решает всё

Когда дело касается мошенничества, время – ключевой фактор. Разница между действиями в первый час и через

неделю может определить, вернёте ли вы свои деньги или хотя бы часть из них.

Вот пошаговый план действий, который должен стать вашей «аварийной инструкцией»:

1. Немедленно прекратите взаимодействие с мошенниками

Это кажется очевидным, но психология жертвы такова, что многие продолжают общаться с мошенниками, надеясь «договориться» или «вразумить» их. Резко обрывайте любой контакт. Блокируйте номера, удаляйте из друзей, игнорируйте сообщения.

Один из моих клиентов, осознав обман, решил «перехитрить» мошенников и притвориться, что всё еще верит им. В результате он потерял ещё 5,000 евро, пока мы убеждали его просто прекратить общение.

2. Документируйте всё

Прежде чем блокировать или удалять контакты мошенников, сделайте скриншоты всей переписки, сохраните историю звонков, запишите все детали взаимодействия. Зафиксируйте:

- Имена и никнеймы, которые использовали мошенники;
- Номера телефонов и адреса электронной почты;
- Названия компаний и веб-сайтов;
- Реквизиты счетов, куда переводились деньги;
- Скриншоты сайтов с датой и временем.

Это критически важные доказательства, которые помогут не только при обращении в правоохранительные органы, но и при попытке возврата денег через банк.

3. Свяжитесь с банком

Если вы перевели деньги или передали данные карты:

- Немедленно позвоните на горячую линию вашего банка и сообщите о мошеннической операции;
- Заблокируйте карту, с которой производилась оплата;
- Попросите отменить транзакцию (если прошло менее 24 часов, шансы выше);
- Подайте заявление о несогласии с операцией (chargeback).

Важно: каждая минута промедления уменьшает шансы на возврат средств. Деньги могут быстро перемещаться между счетами или конвертироваться в криптовалюту.

У меня была клиентка, которая позвонила в банк через 15 минут после перевода мошенникам. Банку удалось заморозить и вернуть 80% суммы. Её подруга с идентичной ситуацией обратилась через два дня – и не вернула ничего.

4. Обратитесь в правоохранительные органы

- Подайте заявление в полицию по месту жительства;
- Обратитесь в специализированные подразделения по борьбе с киберпреступностью (контакты можно найти на официальных сайтах правоохранительных органов вашей страны);

- При трансграничном мошенничестве обратитесь в Интерпол или Европол.

Не позволяйте отговорить себя от подачи заявления фразами вроде *«это бесполезно»* или *«вы сами добровольно перевели деньги»*. Настаивайте на принятии заявления. Даже если ваш случай не раскроют немедленно, информация может помочь в выявлении крупных мошеннических сетей.

5. Измените пароли и усильте безопасность

Если мошенники получили доступ к вашим личным данным:

- Смените пароли на всех аккаунтах, начиная с электронной почты и банковских приложений;
- Включите двухфакторную аутентификацию везде, где это возможно;
- Проверьте устройства на наличие вредоносного ПО;
- Проверьте, нет ли подозрительной активности в ваших аккаунтах.

Возврат денег: возможные пути

Вопреки распространенному мнению, деньги, потерянные из-за мошенничества, иногда можно вернуть. Шансы зависят от многих факторов, включая:

- Тип мошенничества;
- Время, прошедшее с момента перевода;
- Метод оплаты;
- Ваши действия после обнаружения обмана.

Банковские переводы и карточные платежи

Если вы оплачивали товар или услугу банковской картой:

- Visa и Mastercard имеют процедуру chargeback, позволяющую оспорить транзакцию в течение 120 дней;
- Для переводов через систему SWIFT иногда возможен отзыв платежа, если получатель ещё не забрал деньги;
- Некоторые банки предлагают страхование от мошенничества, покрывающее часть потерь.

В Швеции я столкнулся со случаем, когда клиент банка смог вернуть 12,000 евро через процедуру chargeback спустя почти два месяца после оплаты несуществующей инвестиционной услуги. Ключевым фактором успеха стали подробные доказательства обмана и настойчивость в общении с банком.

Криптовалютные платежи

С криптовалютой ситуация сложнее, но не безнадежна:

- Многие криптобиржи сотрудничают с правоохранительными органами и могут заморозить средства при наличии официального запроса;
- Существуют специализированные компании, занимающиеся отслеживанием криптовалютных транзакций и помогающие в возврате украденного;
- Некоторые страховые компании начали предлагать полисы, покрывающие потери от криптомошенничества.

Важно понимать: анонимность криптовалют преувеличена. Каждая транзакция записывается в блокчейн и теоретически может быть отслежена. Проблема в том, что для этого часто

требуются судебные решения и международное сотрудничество.

Юридические механизмы

В зависимости от юрисдикции, вы можете:

- Инициировать гражданский иск против мошенников (если их личности установлены);
- Присоединиться к коллективному иску против организаторов крупных схем;
- Взыскать компенсацию с посредников, способствовавших мошенничеству (например, платёжных систем, не соблюдавших процедуры проверки).

В моей практике был случай, когда группа инвесторов, пострадавших от одной и той же инвестиционной пирамиды, объединилась и наняла адвоката. Судебный процесс занял почти три года, но в итоге они вернули около 30% вложенных средств.

Психологическая реабилитация: как жить дальше

Финансовые потери – это только часть проблемы. Психологические последствия мошенничества могут быть не менее разрушительными. Чувство стыда, вины, потеря доверия к людям, постоянная тревога – всё это может преследовать жертву годами.

Принятие случившегося

Первый шаг к восстановлению – признать, что:

- Вы стали жертвой профессионалов, которые годами оттачивали мастерство обмана;
- Мошенники специально используют психологические триггеры, усыпляющие бдительность;
- В подобную ситуацию может попасть каждый, независимо от образования и социального статуса.

Когда я работал с группой поддержки для жертв мошенничества, один бизнесмен долго не мог принять факт обмана. *«Я веду компанию, принимаю стратегические решения каждый день. Как я мог попасться на такой простой развод?»* – повторял он. Принятие пришло только когда он осознал, что стал мишенью хорошо отработанной схемы, а не просто *«повёлся на развод»*.

Разговор с близкими

Многие жертвы мошенничества скрывают случившееся от семьи и друзей, боясь осуждения. Это усугубляет психологическую травму.

Советы по разговору с близкими:

- Выберите подходящее время и место для спокойного разговора;
- Заранее продумайте, какую информацию вы готовы раскрыть;
- Объясните, что вам нужна поддержка, а не осуждение или советы «задним числом»;

- Если финансовые потери затрагивают семейный бюджет, будьте готовы предложить план по минимизации последствий.

История одной из моих клиенток показательна: скрыв от мужа потерю семейных сбережений, она месяцами жила в постоянном стрессе, пытаясь самостоятельно решить проблему. Когда правда всё же открылась, ей пришлось иметь дело не только с финансовыми последствиями, но и с кризисом доверия в семье.

Профессиональная помощь

Не стесняйтесь обратиться к специалистам:

- Психологи, специализирующиеся на травматическом опыте и финансовых потерях;
- Группы поддержки для жертв мошенничества (онлайн и офлайн);
- Финансовые консультанты, помогающие разработать план восстановления.

В некоторых странах существуют государственные программы психологической поддержки жертв мошенничества – узнайте, доступны ли они в вашем регионе.

Превращение опыта в защиту: как помочь другим

Моя собственная история началась с того, что я сам чуть не стал жертвой хитроумного криптовалютного мошенничества. Этот опыт подтолкнул меня к изучению темы, а затем – к

созданию компании по консультированию и защите от мошенников.

Превратите негативный опыт в возможность:

- Расскажите свою историю друзьям и родственникам – предупреждён значит вооружён;
- Делитесь информацией в социальных сетях, помогая другим распознавать похожие схемы;
- Обращайтесь в СМИ, если ваша история может помочь в информировании широкой аудитории;
- Сотрудничайте с правоохранительными органами, предоставляя информацию для раскрытия схем.

Один из моих читателей после прочтения предыдущего издания книги создал популярный Telegram-канал, где публикует актуальные схемы мошенничества. Сегодня у канала более 200,000 подписчиков, и он помог предотвратить десятки случаев мошенничества.

Законодательство и его эволюция

Правовые механизмы борьбы с мошенничеством постоянно развиваются, хотя и не всегда поспевают за изобретательностью преступников:

Текущее состояние

- В большинстве стран ужесточаются наказания за киберпреступления;
- Совершенствуются механизмы международного сотрудничества в расследовании трансграничного мошенничества;

- Разрабатываются правовые рамки для регулирования новых технологий (криптовалюты, искусственный интеллект).

Будущие тенденции

- Расширение ответственности финансовых посредников за недостаточную проверку клиентов;
- Создание специализированных международных органов по борьбе с киберпреступностью;
- Внедрение технологических решений для проверки личности и предотвращения мошенничества на уровне инфраструктуры интернета.

Недавно Европейский союз принял директиву, обязывающую банки внедрять системы противодействия мошенничеству и компенсировать клиентам ущерб в случае недостаточных мер защиты. Это знаковый сдвиг, перекладывающий часть ответственности с потребителей на финансовые институты.

Заключение: жизнь после мошенничества

Если вы стали жертвой мошенников, знайте: это не конец света. Многие проходили через это и не просто восстанавливались, но становились сильнее и мудрее.

Мошенничество – это не только финансовый, но и жизненный опыт, который, как ни парадоксально, может принести и пользу:

- Вы становитесь более внимательными к деталям;
- Развиваете критическое мышление и интуицию;
- Учитесь лучше понимать психологию людей;

• Приобретаете ценный опыт, которым можете поделиться с другими.

И, что самое важное, – вы учитесь отличать настоящее от поддельного, не только в финансовых вопросах, но и в жизни в целом.

Мир мошенничества постоянно эволюционирует, и ни одна книга не может дать исчерпывающее руководство на все случаи жизни. Но я надеюсь, что, вооружившись знаниями из этих страниц, вы будете чувствовать себя увереннее в противостоянии обману.

Берегите себя и своих близких. И помните – знание сильнее обмана.

В следующий раз, когда вам позвонят из «службы безопасности банка», вы не только положите трубку, но и поможете кому-то из своих близких избежать той же ловушки. А это значит, что вы уже не просто выживший – вы боец на стороне правды в нескончаемой битве с мошенничеством.

Заключение

Когда я начинал писать эту книгу, мне задавали один и тот же вопрос: *«Есть ли вообще смысл бороться с мошенничеством? Разве это не бесконечная игра в кошки-мышки?»* Признаюсь, иногда я и сам задавался этим вопросом, особенно после очередного кейса, когда технологии, призванные нас защищать, становились инструментом обмана.

Но правда в том, что у этой игры есть правила. И тот, кто их знает, уже не просто мышь в лабиринте.

Мошенничество эволюционирует вместе с технологиями – от поддельных монет в Древнем Риме до дипфейков голоса ваших близких. Законодательство многих стран меняется, пытаясь догнать эту эволюцию. Мы видим появление специализированных подразделений киберполиции, ужесточение наказаний за цифровые преступления, межгосударственные соглашения по борьбе с мошенниками.

Но закон всегда будет на шаг позади. Настоящая защита – это осведомлённость каждого из нас.

Вспомните древнюю мудрость: *«Предупреждён – значит вооружён»*. В мире технологических афер эта фраза актуальна как никогда. Каждый раз, когда вы делитесь знаниями о новой схеме мошенничества с родственниками или проверяете подозрительную ссылку перед тем, как кликнуть – вы делаете мир безопаснее.

Победить мошенничество полностью? Возможно, нет. Но сделать его менее прибыльным – абсолютно реально. Когда большинство людей научится распознавать манипуляции,

когда технологические компании будут строить защиту на опережение, а не по факту взлома – мы увидим, как меняется баланс сил.

«Доверяй, но проверяй» – этот принцип должен стать такой же частью цифровой гигиены, как регулярное мытьё рук для профилактики болезней.

И помните: ваша бдительность – не паранойя. Это ваш цифровой иммунитет в мире, где технологии могут быть как лекарством, так и ядом.

Будьте здоровы. И в сети тоже.

Виктор Лансен

Об авторе

Виктор Лансен (42 года)

Виктор – эксперт по кибербезопасности, журналист-расследователь и один из самых востребованных спикеров по теме цифрового мошенничества в Европе. Родился в семье русских эмигрантов, переехавших в Швецию в 1990-х. Вырос в мультикультурной среде: говорил дома по-русски, на улице – по-шведски, а с интернетом – по-английски. С ранних лет хотел доказать, что может быть на шаг впереди – не только в языке, но и в технологиях.

В юности Виктор подрабатывал в службе IT-поддержки, где впервые столкнулся с тем, что позже назовёт «невидимой экономикой доверия». Позже стал журналистом, расследующим теневые схемы на стыке финансов и технологий, а затем перешёл в практику – в компанию по борьбе с фродом. Поворотным моментом стала его личная ошибка: покупка фейкового токена на красивом, но липовом криптосайте. Именно тогда он решил, что будет не только защищать, но и обучать.

Сегодня Виктор Лансен руководит консалтинговым агентством по цифровой безопасности, консультирует банки, стартапы и правоохранительные органы. Его выступления можно увидеть на TEDx, Black Hat и в крупнейших европейских медиа. Но главной своей миссией он считает просвещение обычных пользователей – тех, кто думает, что их не обманешь, пока не становится слишком поздно.

Виктор живёт в Стокгольме, любит цифровой детокс, собирает редкие книги о старинных аферах и искренне верит, что критическое мышление – это лучшая защита в мире, где правда и ложь стали неотличимы. Его стиль – смесь практичности,

иронии и настоящего журналистского чутья. Он пишет так, как будто ведёт читателя за руку сквозь минное поле цифрового доверия – и подсказывает, где именно не стоит наступать.