ПРАКТИЧЕСКАЯ ПСИХОЛОГИЯ ДЛЯ РЕАЛЬНОЙ ЖИЗНИ

КНИГА II

ГДЕ НАС ОБМАНЫВАЮТ

Как распознавать скрытое влияние в общении, продажах и повседневных сценариях

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

УЧИТЕСЬ ВИДЕТЬ ЛОЖЬ, ДАВЛЕНИЕ, ИМИТАЦИЮ ЗАБОТЫ И СКРЫТЫЕ СХЕМЫ

АНТОН КРАВЧЕНКО

ДИАЛОГИ, РАЗБОРЫ, ТИПОВЫЕ СЦЕНАРИИ

Антон Кравченко

Где нас обманывают?

https://litres.ru/74087479
SelfPub; 2026

Аннотация

Обман редко выглядит как грубая ложь. Чаще он приходит через «срочное» сообщение, звонок из «банка», тревожную новость, давление близкого человека, красивую рекламу или просьбу, от которой неудобно отказаться.

«Где нас обманывают» — вторая книга практического справочника о манипуляциях. Она показывает, как работают мошеннические звонки, письма, SMS, QR-коды, мессенджеры, поддельные сайты, давление в отношениях, медийные ловушки, слухи, паника и цифровые схемы доверия.

Книга помогает не жить в подозрительности, а спокойно проверять ситуацию: где остановиться, что перепроверить, какие признаки риска заметить и как не отдать деньги, данные, доступ, репутацию и самостоятельность.

Для тех, кто хочет видеть обман раньше, чем он станет потерей.

Содержание

Антон Кравченко
Где нас обманывают?

Книга II. Карта опасностей: сценарии манипуляций в жизни, цифровой среде и медиа

Антон Кравченко

Введение. Где начинается обман

Телефон вибрирует вечером, когда вы уже устали. Сообщение короткое: «Оплата не прошла. Посылка вернётся отправителю. Подтвердите данные по ссылке».

Ссылка похожа на настоящую. Логотип знакомый. Время будто заканчивается. В голове мелькает простая мысль: «Лучше быстро проверить, чем потерять заказ». Именно здесь и начинается обман — не с грубой лжи, а с правдоподобной истории.

Главная цель манипулятора — заставить вас совершить поспешный шаг. Вас подводят к тому, чтобы вы нажали кнопку, назвали секретный код, подтвердили вход в личный кабинет, перевели деньги, открыли присланный файл, установили сомнительную программу или промолчали, когда вам навязывают ложную секретность.

В итоге вы сами выполните действие, которого от вас добиваются. Поэтому в этой книге мы смотрим не на красивую легенду, а на действие, к которому вас ведут.

Манипуляция редко начинается с приказа. Обычно человек сталкивается с ней в привычной ситуации: приходит короткое сообщение, раздаётся неожиданный звонок, появляется письмо от сервиса, просьба в рабочей переписке или бытовое объявление. Вам не дают спокойно проверить информацию, усиливают тревогу и подталкивают к поспешно-

му решению.

Книга показывает места, где обман прячется под обычную жизнь: звонки, письма, сообщения, QR-коды, мессенджеры, поддельные сайты, покупки, работа, отношения, медиа и цифровые сервисы.

Задача не в том, чтобы подозревать всех подряд. Задача — вовремя остановиться, прервать навязанный разговор, открыть официальный источник самостоятельно и только после этого решить, что делать.

Если действие связано с деньгами, кодом, доступом, документом, установкой программы или срочным согласием, сначала нужна пауза. Не спор. Не оправдание. Пауза и проверка.

Правило безопасности. Если контакт требует код, пароль, подтверждение во всплывающем уведомлении, перевод, установку программы или переход по присланной ссылке, немедленно прекратите общение. Проверяйте только через официальный сайт, приложение или уже известный номер, который вы набрали самостоятельно.

Как устроена эта книга

Каждая глава начинается с места, где ловушка выглядит обычной: звонок, личный кабинет, сайт, отзыв, мессенджер, работа, отношения, медиа. Затем вы видите, какую легенду вам предлагают, какое чувство пытаются вызвать и какого действия добиваются.

После сцены разбирается безопасный порядок действий: в какой момент остановиться, что проверить, какой официальный источник открыть самостоятельно и когда прекратить разговор.

Маршрут книги

Маршрут начинается с быстрых каналов обмана: звонков, сообщений, ссылок, QR-кодов и поддельных страниц. Дальше идут более сложные зоны: покупки, работа, отношения, медиа, благотворительность и инвестиции. Чем привычнее ситуация, тем меньше мы ждём подвоха.

Вторая книга учит начинать проверку до действия, а не после потери денег, доступа или времени.

Часть I. Социальная инженерия и мошеннические сценарии

Звонок может длиться две минуты. Сообщение — занимать одну строку. Но за ними часто стоит цепочка: источник кажется настоящим, история кажется правдоподобной, а сильное чувство заставляет торопиться, а нужное действие уже подготовлено.

Эта часть показывает, как обман собирается в живой сценарий. В нём есть источник, легенда, канал, эмоция, срочность, запрет проверки и действие, которого от вас добиваются. Разбор ведётся только с защитной стороны: как увидеть структуру контакта, остановить давление и проверить источник до денег, данных, подписи или доступа.

На что смотреть в жизни. Вспомните странное сообщение,

звонок, объявление или просьбу. Какую легенду вам предлагали принять за правду? Какого действия от вас ждали?

Главный принцип этой части: социальная инженерия опасна не отдельной фразой, а последовательностью. Сначала человек принимает источник за настоящий. Потом пугается, торопится и перестаёт проверять детали. После этого он делает то, чего от него добивались: сообщает код, переходит по ссылке, открывает файл, переводит деньги, меняет реквизиты, подтверждает доступ или распространяет сообщение.

Главный способ проверки: подозрительный контакт почти всегда строится из четырёх деталей — доверенный источник, проблема или приз, давление действовать немедленно и требование конкретного шага. Если в одном сообщении есть срочность, запрет проверки и просьба о деньгах, коде, ссылке, файле или доступе, контакт нужно остановить и проверить самостоятельно.

Раздел 1. Базовая модель социальной инженерии и первичная защита

Чтобы не тонуть в деталях каждой схемы, сначала нужна простая модель. Любой подозрительный контакт можно разложить на узлы: кто говорит, какую историю предлагает, чем торопит, какой канал удерживает и какого действия добивается.

Первый раздел Части I вводит диагностическую модель социально-инженерного контакта. В ней любой подозрительный контакт разбирается по восьми узлам: источник, легенда, канал, эмоция, срочность, запрет проверки, действие, которого добиваются и можно ли отменить последствия.

Как проверить ситуацию

Сначала проверьте источник: кто обращается и как подтверждён его статус.

Спросите себя: Кто обращается и как подтверждён его статус?

Тревожный признак: новый номер, похожий домен, «служба безопасности», «руководитель», «поддержка» без независимого подтверждения.

Что делать: прервите разговор и проверьте ситуацию через официальный номер, приложение, сайт или ранее из-

вестный контакт.

Затем проверьте легенду: какую историю предлагают принять за исходную реальность.

Спросите себя: Какую историю предлагают принять за исходную реальность?

Тревожный признак: авария, взлом, срочная проверка, выигрыш, штраф, личный кабинет, «важный документ».

Что делать: попросите письменную основу, номер обращения, официальный источник и время на проверку.

Посмотрите на способ связи: почему разговор ведут именно здесь.

Спросите себя: Почему контакт идёт именно здесь?

Тревожный признак: перевод из официального канала в мессенджер, звонок вместо письма, письмо вместо внутренней системы.

Что делать: вернуться в штатный канал, где уже есть история, права доступа и регламент.

Назовите чувство, которое пытаются вызвать до проверки фактов.

Спросите себя: Какое какое чувство пытаются вызвать до проверки фактов?

Тревожный признак: страх, чувство вины, надежда, жадность, срочность, сочувствие, стыд.

Что делать: назовите эмоцию и отделите её от факта и действия.

Проверьте срочность: почему вам не дают времени поду-

мать.

Спросите себя: Почему нельзя проверить позже?

Тревожный признак: «Пять минут», «сейчас закроется», «не кладите трубку», «иначе потеряете доступ».

Что делать: заранее введите правило паузы. Важные действия не выполняются в режиме срочности.

Отдельно отметьте запрет проверки: кому запрещают звонить и что запрещают уточнять.

Спросите себя: Кому запрещают звонить или что запрещают уточнять?

Тревожный признак: «Никому не говорите», «это конфиденциально», «проверка сорвётся».

Что делать: посчитайте запрет проверки самостоятельным красным флагом высокого риска.

В конце назовите нужное действие: что конкретно от вас хотят получить.

Спросите себя: Что конкретно от меня хотят?

Тревожный признак: код, пароль, ссылка, файл, перевод, смена реквизитов, подпись, подтверждение доступа.

Что делать: не выполнять действие до проверки через официальный сайт, приложение или уже известный контакт и письменной фиксации.

Оцените, можно ли отменить последствия, если вы ошибётесь.

Спросите себя: Можно ли безопасно отменить последствия?

Тревожный признак: деньги, доступ, персональные данные, подпись, публикация, удаление файлов.

Что делать: если действие нельзя быстро отменить, считайте риск высоким и не совершайте его без проверки.

Глава 1. Социальная инженерия как сценарная атака

Сообщение начинается спокойно: «Это служба поддержки, нужно уточнить пару данных». Через минуту появляется срочность, потом ссылка, потом просьба подтвердить доступ. Ловушка не в одной фразе, а в цепочке. Безопасный шаг — прервать навязанный разговор и перейти в официальный сайт, приложение или уже известный контакт самому.

Живой разбор приёма

Социальная инженерия — это обманный сценарий, в котором человека пытаются обманом, давлением или имитацией доверенного контекста привести к действию, выгодному атакующему: раскрытию информации, переводу денег, установке доступа, открытию файла или обходу нормальной процедуры.

Социальная инженерия существовала задолго до цифровой среды: поддельные представители власти, ложные сборы, мошеннические письма, фиктивные посредники и «про-

веряющие» использовали доверие и срочность. Цифровая среда усилила масштаб, скорость и правдоподобность таких сценариев: теперь письмо, звонок, сайт, мессенджер и поддельный профиль могут работать как единая цепочка.

Механизм строится на том, что человеку предлагают готовую историю вместо самостоятельной проверки. Человек не анализирует событие с нуля, а принимает предложенную подачу: «это банк», «это руководитель», «это сервисный кабинет», «это знакомый», «это срочная проблема». После этого человек думает только о требуемом действии и хуже проверяет факты.

Под стрессом и срочностью усиливается реакция тревоги и готовность быстро понять, что происходит. Это не означает автоматической потери контроля, но ухудшает качество проверки, особенно когда сообщение одновременно включает угрозу, авторитет и конкретную инструкцию.

Финансовые звонки и сообщения.

Корпоративная переписка и сценарии подмены деловой переписки.

Поддельная техническая поддержка.

Личный кабинет, маркетплейсы и сервисные уведомления.

Социальные сети и мессенджеры.

Офлайн-контакты под видом сотрудников служб.

Работает потому, что человек обычно доверяет узнаваемым ролям, старается быстро снять угрозу и не хочет нару-

шить социальную норму помощи, подчинения или лояльности. Мошенники используют не «глупость», а обычное доверие и желание помочь.

Определить источник: кто обращается и как он подтверждён.

Выделить легенду: какая история должна быть принята без проверки.

Найти ожидаемое действие: код, деньги, файл, ссылка, доступ, подпись.

Проверить наличие срочности и запрета проверки.

Оценить, можно ли отменить последствия.

Перенести проверку в официальный источник или уже известный контакт для проверки.

Принять решение только после остановки и проверки.

Как опознать

Ситуация начинается с проблемы, угрозы, выигрыша или срочной возможности.

Роль источника звучит важнее фактов.

Контакт удерживают в одном канале.

Сначала нужно действие до проверки.

Действие имеет необратимые последствия.

Как это выглядит в жизни

«Не кладите трубку»

«Никому не говорите»
«Сейчас потеряете доступ»
«Это поручение руководителя»
«Код нужен для отмены операции»
«Ссылка только для вас»

Красный флаг и безопасная проверка

Прервать навязанный разговор.

Не использовать номера и ссылки из подозрительного сообщения.

Самостоятельно открыть официальный сайт или приложение.

Связаться с известным контактом через прежний канал.

Зафиксировать запрос письменно.

При деньгах, данных и доступах использовать правило двух проверок.

Не всякая срочность — мошенничество. Реальные службы тоже могут сообщать о проблемах. Отличие безопасного процесса в том, что он допускает независимую проверку и не требует секретного действия в новом канале.

Пример 1. Человеку звонят «из банка» и говорят, что операция уже идёт. Верно так: завершить разговор и самостоятельно открыть приложение или позвонить по номеру с карты.

Пример 2. Поставщик присылает письмо о новых рекви-

зитах и просит оплатить сегодня, пока «не ушёл счёт». Верно так: открыть старый договор, позвонить по прежнему номеру и провести платёж только после второй подписи.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. сообщение о взломе аккаунта требует ввести одноразовый пароль.

Вывод простой: действие, которого добиваются — передать фактор доступа.

Ситуация. «сервисный кабинет» просит доплатить небольшую сумму по ссылке.

Вывод простой: малая сумма снижает критичность, но ссылка может вести к краже карты.

Разберите любое подозрительное сообщение по восьми узлам сценария.

Составьте личную фразу для прекращения разговора без объяснений.

Что является главным признаком сценарной атаки?

Почему официальный источник или уже известный контакт важнее уверенности в голосе или логотипе?

Социальная инженерия начинается там, где человека втягивают в чужой сценарий быстрее, чем он успевает проверить источник, цель и последствия.

Глава 2. Предлог и легенда как вход в контакт

Вам пишут: «Посылка задержана, нужна небольшая доплата». История похожа на правду, особенно если вы действительно ждёте заказ. Ловушка в том, что реальное ожидание снижает настороженность и мешает проверить сообщение. Безопасный шаг — не нажимать ссылку, а открыть приложение магазина или службы доставки самостоятельно.

Живой разбор приёма

Предлог — это объяснение, почему контакт происходит именно сейчас и почему человек должен включиться в ситуацию. Легенда — более широкая история, которая связывает источник, проблему, срочность и требуемое действие.

Предлоги использовались в классических мошеннических схемах: «проверка счётчика», «ошибка в документах», «родственник попал в беду», «вы выиграли приз». В цифровой среде они превратились в уведомления о доставке, безопасности, налогах, подписках, платёжах, заказах и корпоративных поручениях.

Предлог уменьшает сопротивление, потому что даёт готовое объяснение необычному запросу. Человек думает не «почему меня обманывают?», а «как решить предложенную

проблему?».

Когда ситуация выглядит как срочная проблема, человек стремится быстро вернуть ощущение контроля. Легенда с понятной ролью и простым действием снижает неопределённость и поэтому может восприниматься как облегчение.

Звонки от имени банка или госоргана.

Сообщения о доставке и заказах.

Корпоративные просьбы «от руководителя»

Романтические и благотворительные схемы.

Поддельная поддержка сервисов.

Офлайн-визиты под видом проверок.

Легенда работает, если она совпадает с реальной жизненной вероятностью: человек действительно ждёт доставку, пользуется банком, работает с документами, общается с коллегами или переживает за близких.

Записать легенду одной фразой.

Проверить, какие факты подтверждены независимо.

Отделить событие от инструкции: проблема может быть реальной, но инструкция — поддельной.

Проверить, почему выбран именно этот канал.

Найти, что случится при остановке.

Проверить через официальный источник.

Отказаться от действий, если легенда держится только на срочности.

Как опознать

Есть связная история с ролью и проблемой.

Подробности создают правдоподобие, но не проверяемость.

Контакт привязан к реальной ситуации человека.

История сразу ведёт к действию.

Как это выглядит в жизни

Предлог меняется при уточняющих вопросах.

Источник раздражается из-за проверки.

Объяснение слишком драматично.

Есть требование секретности.

Официальный источник якобы «не работает»

Красный флаг и безопасная проверка

Попросить номер обращения или официальный документ.

Проверить событие отдельно от инструкции.

Не переходить по ссылкам из сообщения.

Самостоятельно открыть сервис.

Сравнить легенду с известными регламентами.

Даже правдоподобная легенда не доказывает, что запрос настоящий. Но сама по себе легенда ещё не доказывает мо-

шенничество: решает проверяемость.

Пример 1. «Ваш заказ задержан, оплатите повторную доставку». Проверка: открыть приложение магазина самостоятельно, а не ссылку.

Пример 2. «Я новый бухгалтер поставщика, реквизиты изменились». Проверка: звонок по старому известному номеру и подтверждение через договорной канал.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. человек действительно ждал посылку, поэтому поверил SMS о доплате.

Вывод простой: совпадение с ожиданием усилило легенду.

Ситуация. сотрудник получил письмо с темой старого проекта.

Вывод простой: знание контекста повысило доверие.

Выпишите три распространённые легенды, которые могут сработать лично на вас.

Для каждой легенды составьте путь проверки.

Чем предлог отличается от доказательства?

Почему совпадение с реальной жизненной ситуацией не отменяет проверку?

Предлог — это входная дверь сценария. Защита начинается с вопроса: «Какие факты подтверждены вне этой истории?»

Глава 3. Имитация доверенного источника

На экране знакомый логотип, в письме правильное имя, в телефоне уверенный голос. Именно это и снижает критичность. Ловушка работает через узнаваемость. Безопасный шаг — проверить источник через старый известный номер или договорной контакт, а не через ссылку, номер или чат из нового сообщения.

Живой разбор приёма

Имитация доверенного источника — это попытка выдать себя за банк, руководителя, коллегу, госорган, сервис, родственника, службу поддержки или известную организацию, чтобы получить доверие до проверки.

Раньше имитация строилась на форме, печати, визитке или телефонном представлении. Сегодня она включает похожие домены, поддельные профили, логотипы, номера с подменой, переписку из взломанных аккаунтов и копирование стиля реального человека.

Человек склонен переносить доверие к роли или бренду на конкретный контакт. Если «банк» говорит о деньгах, а «руководитель» — о задаче, критичность снижается, потому что запрос кажется соответствующим роли.

Узнаваемые сигналы статуса и привычные привычные модели общения уменьшают неопределённость. При эмоциональном давлении мозг может опираться на узнавание, а не на проверку подлинности.

Поддельные банковские звонки.

подмена реквизитов и письма от имени контрагента.

Фишинговое письмо от имени сервиса.

Ложная техническая поддержка.

Поддельные аккаунты знакомых.

Сообщения от имени курьерских и государственных служб.

Работает потому, что в нормальной жизни доверие к ролям экономит время. Проблема появляется, когда роль имитируется, а человек не отделяет «заявленную роль» от «подтверждённой идентичности».

Определить заявленную роль источника.

Проверить канал: совпадает ли он с обычным способом связи.

Проверить домен, номер, профиль, историю переписки, стиль и контекст.

Не отвечать на запрос внутри подозрительного канала.

Связаться с источником через известный официальный источник или уже известный контакт.

Подтвердить запрос вторым фактором: документ, внутренний заявка, договор, регламент.

При расхождении прервать навязанный разговор и зафик-

сировать инцидент.

Как опознать

Используется громкая роль или бренд.

Контакт приходит из нового или непривычного канала.

Сообщение содержит просьбу об исключении из обычной процедуры.

Источник торопит и требует доверия.

Как это выглядит в жизни

Адрес похож на настоящий, но отличается одной буквой.

Номер не совпадает с официальным.

Профиль создан недавно.

«Руководитель» просит секретность.

«Служба» требует код или пароль.

Красный флаг и безопасная проверка

Не доверять роли без проверки канала.

Использовать официальный сайт, приложение или внутренний справочник.

Не перезванивать на номер из сообщения.

Ввести правило обратный звонок для платёжей и изменений реквизитов.

Обучить себя фразе: «Я подтвержу через штатный канал»

Иногда настоящий источник действительно использует новый канал, но это не отменяет проверки. Чем выше цена действия, тем строже должна быть идентификация.

Пример 1. Письмо с логотипом банка просит обновить данные. Проверка: не нажимать ссылку, открыть банк самостоятельно.

Пример 2. Сообщение от имени знакомого просит срочно занять деньги. Проверка: голосовой звонок или другой известный канал.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. взломанный аккаунт знакомого просит перевести деньги.

Вывод простой: источник выглядит реальным, но запрос нетипичен.

Ситуация. «CEO» пишет с личной почты.

Вывод простой: роль высокая, канал слабый.

Составьте таблицу: роль источника — допустимый канал — недопустимое действие без проверки.

Проверьте один официальный сервис: где у него реальные домены и контакты.

Почему логотип не доказывает подлинность?

Что важнее: уверенный тон или официальный источник или уже известный контакт?

Имитация источника ломается не спором, а процедурой: роль признаётся только после проверки канала и полномо-

чий.

Глава 4. Удержание на связи и перевод общения в навязанную связь

Если вас переводят из привычного канала в новый чат, ссылку или звонок, сначала вернитесь в официальный путь связи. Там есть история, правила и возможность проверки.

Живой разбор приёма

Удержание на связи — это удержание человека в таком способе связи, где атакующий контролирует темп, эмоцию, доступ к ссылкам, документам, номерам и инструкциям.

В телефонных мошенничествах каналом был непрерывный разговор. В современных сценариях каналом может быть мессенджер, поддельный сайт, удалённый доступ, чат поддержки, видеозвонок, QR-код или цепочка писем.

Когда человек остаётся внутри канала давления, он видит только ту информацию, которую даёт источник. Возможность сравнения, консультации и остановки снижается.

Непрерывный поток инструкций поддерживает возбуждение и снижает вероятность остановки. Переключение канала на независимый ресурс помогает вернуть исполнительный контроль.

Звонки «не кладите трубку»

Перевод в мессенджер.

Ссылки на поддельные сайты.

Удалённая помощь с демонстрацией экрана.

QR-коды для оплаты.

Цепочки писем с изменёнными реквизитами.

Работает потому, что канал задаёт ритм решения. В чужом канале легче навязать срочность, скрыть альтернативы и подменить проверку инструкцией.

Понять, кто контролирует канал.

Проверить, запрещают ли переключиться в официальный источник.

Определить, есть ли непрерывные инструкции.

Найти, какие данные видит или может получить источник.

Прервать канал до действия.

Открыть официальный источник самостоятельно.

Возобновлять контакт только после проверки.

Как опознать

Контакт удерживает на линии.

Источник сам присылает все ссылки и номера.

Предлагают установить приложение удалённого доступа.

Просят демонстрировать экран.

Убеждают не закрывать чат.

Как это выглядит в жизни

«Если отключитесь, операция пройдёт»
«Перейдите только по этой ссылке»
«Не открывайте приложение самостоятельно»
«Сейчас я вас проведу по шагам»
«Включите демонстрацию экрана»

Красный флаг и безопасная проверка

Положить трубку.

Закрыть ссылку.

Не устанавливать удалённый доступ по просьбе звонящего.

Не демонстрировать экран с кодами и банковскими приложениями.

Самостоятельно перейти в официальный сервис.

Некоторые законные службы поддержки тоже ведут человека по шагам. Разница: настоящая поддержка не требует секретных кодов, платёжей в странный способ и не запрещает самостоятельную проверку.

Пример 1. «Специалист» просит установить программу для защиты счёта. Чтобы вернуть контроль, не устанавливать и обратиться в банк самостоятельно.

Пример 2. В письме есть номер «службы поддержки». Чтобы вернуть контроль, не звонить по нему, найти номер

на официальном сайте.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. человек не положил трубку 40 минут и выполнил инструкции.

Вывод простой: канал удерживал внимание и ритм.

Ситуация. короткая ссылка на поддельной квитанции ведёт на форму оплаты.

Вывод простой: канал подменил официальный путь.

Составьте список каналов, в которых вы не выполняете финансовые действия.

Пропишите правило: какие действия нельзя делать при демонстрации экрана.

Почему канал влияет на качество решения?

Какой первый шаг при фразе «не кладите трубку»?

Канал — это часть воздействия. Вернуть себе канал значит вернуть себе время, проверку и автономию.

Глава 5. Срочность, страх и запрет проверки

Фраза «только сейчас» — сигнал остановки. Спросите, чем подтверждён срок, кто его установил и что изменится, если вы проверьте условия позже.

Живой разбор приёма

Срочность и запрет проверки — центральная связка социально-инженерного давления: человека убеждают, что задержка опасна, а проверка через официальный сайт, приложение или уже известный контакт сорвёт спасение или усилит проблему.

В традиционных мошеннических схемах использовались «последний шанс», «родственник в беде», «штраф сегодня», «выигрыш с ограниченным сроком». В цифровых сценариях это стало таймерами, блокировками аккаунта, угрозами списания, ложными уведомлениями безопасности и дедлайнами платёжей.

Страх сужает внимание, а срочность переносит решение из режима анализа в режим исполнения. Запрет проверки блокирует главный защитный механизм — обращение к независимому источнику.

В тревожном состоянии человек стремится быстро прекратить неопределённость. Если источник одновременно предлагает простое действие, оно может восприниматься как путь к безопасности, хотя именно оно создаёт риск.

Банковские звонки.

Поддельные уведомления безопасности.

Корпоративные платёжи.

Сообщения о штрафах.

Медицинские и семейные тревожные сценарии.

Ложные розыгрыши и призы.

Работает потому, что проверка требует времени, а страх требует немедленного облегчения. Манипулятор выигрывает, если человек выбирает облегчение вместо проверки.

Назвать срочность: «меня торопят».

Определить, что именно станет хуже при остановке.

Проверить, объяснена ли срочность докувнутренно.

Выделить запрет проверки как отдельный сигнал риска.

Ввести минимальную время на проверку.

Проверить через независимый источник.

Действовать только при подтверждённой угрозе.

Как опознать

Короткий дедлайн.

Страх потери денег или доступа.

Давление голосом.

Угроза наказания за бездействие.

Секретность.

Как это выглядит в жизни

«У вас две минуты»

«Если проверите, будет поздно»

«Не сообщайте никому, даже сотрудникам банка»

«Код нужен для отмены»

«Иначе счёт заблокируют»

Красный флаг и безопасная проверка

Использовать правило: «чем сильнее срочность, тем обязательнее пауза на проверку»

Не передавать коды и пароли.

Не переводить деньги на «безопасные счета»

Не менять реквизиты без второго подтверждения.

Фиксировать разговор и обращаться в официальный сайт, приложение или уже известный контакт.

Бывают реальные аварийные ситуации. Но даже в них безопасная система допускает подтверждение личности и не требует раскрытия секретных данных неизвестному источнику.

Пример 1. «Сейчас спишут деньги, назовите код». Чтобы вернуть контроль, коды не называют никогда; проверка только через банк.

Пример 2. «Поставщик ждёт оплату до 17:00, реквизиты изменились». Чтобы вернуть контроль, обратный звонок по старому номеру и письменное подтверждение.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. таймер на сайте заставляет купить «за минуту».

Вывод простой: срочность замещает сравнение условий.

Ситуация. звонящий запрещает говорить с родственника-

ми.

Вывод простой: запрет проверки повышает риск до красного.

Выпишите пять фраз срочности и для каждой напишите защитный ответ.

Сформулируйте личное правило остановки для денег, доступа и документов.

Почему запрет проверки опаснее самой срочности?

Как отличить реальный дедлайн от манипулятивного?

Срочность безопасна только тогда, когда проверяема. Если срочность запрещает проверку, это не аргумент, а сигнал остановки.

Глава 6. Выуживание информации без прямого запроса

Собеседник не просит пароль прямо. Он уточняет «безобидные» детали: где вы работаете, каким банком пользуетесь, кто руководитель, когда вы дома. Эти куски потом собираются в схему. Безопасный шаг — не отвечать на вопросы, смысл которых вам не ясен.

Живой разбор приёма

Выуживание информации — это получение полезных сведений через разговор, уточнения, дружелюбие, мнимую по-

мощь или бытовые вопросы без прямого требования «сообщите секрет».

В разведывательных, мошеннических и корпоративных сценариях ценная информация часто собиралась не через взлом, а через обычный разговор: кто отвечает за платёжи, кто в отпуске, какой сервис используется, как зовут руководителя, когда будет перевод.

Люди охотно помогают, исправляют ошибки собеседника и заполняют пробелы. Если вопрос выглядит безобидно, защитная реакция не возникает.

Социальная кооперация и желание поддержать разговор снижают вероятность жёсткого фильтра. Особенно это заметно при дружелюбном тоне, комплименте, общей принадлежности или просьбе «просто уточнить».

Телефонные разговоры.

Социальные сети.

Корпоративная переписка.

Собеседования и деловые встречи.

Службы поддержки.

Офлайн-разговоры у стойки или входа.

Работает потому, что отдельный фрагмент кажется безопасным, но несколько фрагментов собираются в карту доступа: имена, роли, расписания, привычки, поставщики, номера заказов, внутренние процедуры.

Определить, какую информацию пытаются уточнить.

Проверить, зачем собеседнику это знать.

Оценить, можно ли использовать ответ для доступа, платёжа или имитации доверия.

Не исправлять подозрительные «ошибки» собеседника.

Отвечать общими формулировками или переводить в официальный запрос.

Фиксировать повторяющиеся вопросы.

Сообщать ответственным при признаках сбора информации.

Как опознать

Вопросы кажутся бытовыми, но касаются ролей, графиков, систем или процедур.

Собеседник просит подтвердить детали.

Вопросы распределены по разным каналам.

Источник ссылается на знакомых или общий проект.

Как это выглядит в жизни

«А кто у вас обычно согласует платёжи?»

«Руководитель сейчас на месте?»

«Какая у вас система входа?»

«Просто подтвердите последние цифры»

«Я, кажется, ошибся в адресе, подскажите правильный»

Красный флаг и безопасная проверка

Не подтверждать внутренние сведения неизвестным источникам.

Переносить запрос в официальный сайт, приложение или уже известный контакт.

Использовать минимально достаточный ответ.

Не публиковать лишние рабочие сведения в открытом доступе.

Обучить команду правилу: безобидные детали тоже могут быть чувствительными.

Не каждый уточняющий вопрос опасен. Риск зависит от контекста, идентификации источника и потенциальной полезности ответа для обхода процедур.

Пример 1. «Подскажите, Иван сегодня в офисе?» — безопаснее ответить: «Передайте запрос на общий адрес, его обработают».

Пример 2. «Какая у вас CRM?» — для внешнего собеседника это может быть избыточная информация.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. мошенник узнал имя бухгалтера из сайта и использовал его в письме.

Вывод простой: открытая информация стала элементом доверия.

Ситуация. сотрудник подтвердил отпуск руководителя.

Вывод простой: это помогло сценарию срочного платёжа.

Проведите аудит открытых сведений о себе или компании.

Составьте список информации, которую нельзя подтверждать неизвестным людям.

Почему «безобидная» информация может быть опасной?

Чем подтверждение отличается от раскрытия?

Выуживание редко выглядит как атака. Его защита — не подозрительность ко всем, а правило минимального раскрытия и официального канала.

Глава 7. Перенаправление на ожидаемое действие

В начале говорят о проблеме, помощи или выгоде, но всё постепенно сводится к одному действию: перевести, нажать, подписать, отправить код, промолчать. Безопасный шаг — задать главный вопрос: «Что конкретно от меня хотят прямо сейчас?»

Живой разбор приёма

Перенаправление на действие, которого добиваются — это момент, когда весь собеседник сводится к конкретному шагу: сообщить код, перейти по ссылке, открыть файл, опла-

тить, изменить реквизиты, установить приложение, подтвердить вход или передать доступ.

В старых схемах нужным действием были наличные, подпись, передача документа или устное согласие. В цифровой среде оно часто принимает форму клика, ввода кода, разрешения доступа, установки приложения или подтверждения операции.

Человек может спорить о легенде, но пропустить момент действия. Манипуляция становится опасной именно тогда, когда обсуждение превращается в выполнение.

При длительном напряжении простая инструкция даёт ощущение выхода. Чем дольше человек удерживался в сценарии, тем привлекательнее становится «сделайте один шаг, и всё закончится».

Коды подтверждения и одноразовый код.

Ссылки на формы.

Вложения и архивы.

Удалённый доступ.

Платежи и переводы.

Изменение реквизитов.

Подписание документов.

Работает потому, что ожидаемое действие часто выглядит маленьким: один код, одна ссылка, одна галочка, одна доплата. Но именно этот шаг может открыть доступ или создать необратимые последствия.

Спросить: «Что конкретно от меня хотят сделать?»

Классифицировать действие: деньги, доступ, данные, подпись, файл, публикация.

Оценить обратимость.

Проверить источник и необходимость действия.

Отделить проблему от предложенного способа решения.

При красном уровне риска не выполнять действие вообще.

Возвращаться только к штатному процессу.

Как опознать

После длинного объяснения появляется простая инструкция.

Шаг подаётся как формальность.

Действие выполняется в нестандартном канале.

Последствия объяснены размыто.

Как это выглядит в жизни

«Просто назовите код»

«Просто откройте файл»

«Просто подтвердите вход»

«Просто оплатите 1 рубль»

«Просто установите приложение»

Красный флаг и безопасная проверка

Коды и пароли не передаются никому.

Ссылки открываются только из официального приложения или сайта.

Вложения проверяются через источник и безопасность.

Доступы выдаются только по регламенту.

Платежи и реквизиты проверяются через обратный звонок и второе лицо.

Некоторые требуемые действия действительно могут быть законными и нужными. Поэтому задача не в том, чтобы отказываться от всего, а в том, чтобы каждое необратимое действие проходило проверку источника, канала и основания.

Пример 1. «Для отмены перевода назовите код». На самом деле код может подтверждать вход или перевод.

Пример 2. «Откройте счёт во вложении». Вложение может быть техническим входом в компрометацию устройства.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. человек ввёл код на сайте, похожем на банк.

Вывод простой: действие, которого добиваются было замаскировано под проверку.

Ситуация. сотрудник изменил реквизиты поставщика по письму.

Вывод простой: действие требовало второго подтвержде-

ния.

Составьте список действий, которые вы никогда не делаете из входящего сообщения.

Для каждого действия определите официальный путь выполнения.

Почему важно искать ожидаемое действие?

Какие действия требуют красного уровня проверки?

Сценарий можно слушать, но действие нельзя выполнять без проверки. Защита фокусируется на моменте перехода от слов к шагу.

Глава 8. Порядок действий проверки через официальный сайт, приложение или уже известный контакт

Когда история звучит убедительно, хочется проверить её прямо в том же чате. Это ошибка: канал уже может быть частью ловушки. Безопасный шаг — прервать разговор и проверить через источник, который вы нашли сами.

Живой разбор приёма

Порядок действий проверки через официальный сайт, приложение или уже известный контакт — это заранее установленная последовательность действий, которая позволяет проверить источник, событие и запрос вне канала давления.

В корпоративной безопасности проверка через официальный сайт, приложение или уже известный контакт давно используется для платёжей, доступа и изменений реквизитов. В бытовой защите тот же принцип применим к банкам, онлайн-сервисам, родственникам, объявлениям, госуслугам и онлайн-покупкам.

Готовый порядок действий снижает нагрузку на человека в стрессе. Не нужно заново придумывать ответ: есть правило, которое автоматически разрывает сценарий.

Предварительное правило помогает перевести поведение из режима поспешного ответа в заранее заданный. Оно снижает зависимость от сильные чувства момента и возвращает контроль через заранее выбранную последовательность.

Подозрительные звонки.

Сообщения о деньгах.

Ссылки и вложения.

Изменение реквизитов.

Запросы кода или доступа.

Срочные просьбы знакомых.

Корпоративные поручения.

Работает потому, что атакующий рассчитывает на импровизацию жертвы, а порядок действий убирает импровизацию. Решение принимает не испуганный человек в моменте, а заранее установленное правило.

Прервать навязанный разговор.

Не использовать ссылки, номера и реквизиты из сообще-

ния.

Найти официальный источник самостоятельно.

Проверить событие: существует ли проблема, платёж, заказ, запрос.

Проверить источник: имеет ли человек или организация право требовать действие.

Проверить действие: нужно ли оно и обратимо ли оно.

Возобновить процесс только в штатном канале или отказаться.

Как опознать

Проверка возможна через независимый источник.

Официальный источник подтверждает или опровергает событие.

Источник не возражает против остановки.

Действие можно выполнить безопасным способом.

Как это выглядит в жизни

Источник злится на время на проверку.

Официальный источник не подтверждает событие.

Просят вернуться в подозрительный канал.

Контакты в сообщении отличаются от официальных.

Действие нужно выполнить «секретно»

Красный флаг и безопасная проверка

Создать личные правила для денег, документов и доступов.

Хранить официальные контакты отдельно.

Использовать двухканальное подтверждение для платёжей.

Не делать исключений из-за статуса собеседника.

После инцидента обновлять правила.

Порядок действий не гарантирует стопроцентной защиты, если официальный источник уже скомпрометирован или человек сам нарушает правило. Поэтому для крупных рисков нужен второй независимый человек или формальный регламент.

Пример 1. Входящий звонок «из банка» завершается, затем человек сам открывает приложение и проверяет уведомления.

Пример 2. Письмо об изменении реквизитов проверяется звонком по старому номеру договора и подтверждением вторым сотрудником.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. человек не перезванивает по номеру из письма, а открывает сайт самостоятельно.

Вывод простой: канал отделён от источника.

Ситуация. компания вводит правило двух подписей для новых реквизитов.

Вывод простой: подмену деловой переписки удаётся остановить.

Напишите собственный порядок действий проверки для банка, работы, маркетплейса и родственников.

Составьте список доверенных контактов, которые не берутся из входящего сообщения.

Почему порядок действий должен быть заранее?

Какой канал считается независимым?

Проверка через официальный сайт, приложение или уже известный контакт — основной защитный механизм Части I. Она не спорит с легендой, а выводит решение из среды, где человек действует внутри навязанной истории.

Сводная матрица раздела 1

Сценарный элемент: Легенда

Что делает атакующий: Создаёт объяснение контакта и срочности.

Что делает защищающийся: Проверяет факты вне легенды.

Уровень риска: Средний/высокий

Сценарный элемент: Имитация источника

Что делает атакующий: Использует роль, бренд, должность или знакомство.

Что делает защищающийся: Проверяет канал и полномочия.

Уровень риска: Высокий

Сценарный элемент: Удержание на связи

Что делает атакующий: Удерживает в звонке, чате, ссылке или поддельной форме.

Что делает защищающийся: Прерывает канал и переходит в официальный путь.

Уровень риска: Высокий

Сценарный элемент: Эмоциональная срочность

Что делает атакующий: Создаёт страх потери, штрафа, блокировки или упущения.

Что делает защищающийся: Вводит время и проверку.

Уровень риска: Высокий

Сценарный элемент: Запрет проверки

Что делает атакующий: Требует секретности или запрещает консультацию.

Что делает защищающийся: Считает это красным флагом.

Уровень риска: Красный

Сценарный элемент: Выуживание сведений

Что делает атакующий: Собирает маленькие фрагменты контекста.

Что делает защищающийся: Отвечает минимально и через официальный сайт, приложение или уже известный контакт.

Уровень риска: Средний

Сценарный элемент: Нужное действие

Что делает атакующий: Сводит сценарий к коду, ссылке, платёжу, доступу.

Что делает защищающийся: Не выполняет до проверки через официальный сайт, приложение или уже известный контакт.

Уровень риска: Красный

Сценарный элемент: Проверка через официальный сайт, приложение или уже известный контакт

Что делает атакующий: Пытается вернуть в свой канал.

Что делает защищающийся: Использует заранее установленный порядок действий.

Уровень риска: Защитный круг

Блок кейсов к разделу 1

Ситуация 1. Человеку звонят «из банка» и требуют назвать код для отмены операции.

Вывод простой: заявленный источник не подтверждён, действие, которого добиваются — передать фактор доступа, риск красный.

Ситуация 2. Письмо от «поддержки маркетплейса» просит оплатить 49 рублей по ссылке.

Вывод простой: малая сумма снижает критичность, но канал оплаты поддельный.

Ситуация 3. «Руководитель» пишет в мессенджере и просит срочно перевести деньги партнёру.

Вывод простой: высокая роль, новый канал, нарушение

платёжного регламента.

Ситуация 4. «Поставщик» сообщает об изменении реквизитов за час до платёжа.

Вывод простой: ожидаемое действие необратимо, нужно обратный звонок по старому номеру.

Ситуация 5. Поддельная поддержка просит установить программу удалённого доступа.

Вывод простой: канал контроля передаётся источнику.

Ситуация 6. Сообщение от знакомого аккаунта просит занять деньги.

Вывод простой: аккаунт может быть взломан, нужна проверка голосом или старым каналом.

Ситуация 7. На сайте появляется таймер «аккаунт будет удалён через 10 минут».

Вывод простой: срочность подталкивает к вводу данных.

Ситуация 8. В офис звонят и спрашивают, кто согласует платёжи.

Вывод простой: выуживание контекста для дальнейшего сценария.

Ситуация 9. В письме есть вложение «акт сверки».

Вывод простой: ожидаемый документ не отменяет проверки отправителя и канала.

Ситуация 10. «Госслужба» сообщает о штрафе и просит оплатить через поддельную кнопку оплаты.

Вывод простой: официальный статус должен проверяться через официальный портал.

Ситуация 11. В мессенджере предлагают инвестицию «только для своих».

Вывод простой: эксклюзивность, срочность, обещание выгоды и перевод вне регламента.

Ситуация 12. Красный флаг: «Сотрудник безопасности» запрещает говорить с банком.

Вывод простой: запрет проверки — самостоятельный красный флаг.

Ситуация 13. Под видом опроса собирают название банка, оператора и дату рождения.

Вывод простой: фрагменты могут использоваться для следующего контакта.

Ситуация 14. «Коллега» просит прислать файл с клиентской базой на личную почту.

Вывод простой: роль знакомая, канал и действие нештатные.

Ситуация 15. «Маркетплейс» присылает ссылку для возврата средств.

Вывод простой: возврат должен проверяться в приложении, а не по входящей ссылке.

Ситуация 16. «Юрист» обещает срочно снять арест за предоплату.

Вывод простой: страх и надежда соединены с быстрым платёжом.

Ситуация 17. Звонящий знает имя и адрес, поэтому кажется настоящим.

Вывод простой: знание деталей не доказывает полномочия.

Ситуация 18. В чате проекта появляется новый участник и просит доступ к папке.

Вывод простой: нужно проверка через владельца проекта.

Ситуация 19. «Сервис подписки» сообщает о списании и предлагает отменить по ссылке.

Вывод простой: тревога о потере денег переводит в поддельный канал.

Ситуация 20. Человек прекращает разговор, открывает официальное приложение и не находит проблемы.

Вывод простой: проверка через официальный сайт, приложение или уже известный контакт разорвала сценарий.

Блок упражнений к разделу 1

Разберите последнее подозрительное SMS, письмо или сообщение по восьми узлам: источник, легенда, канал, эмоция, срочность, запрет проверки, действие, которого добиваются, обратимость.

Составьте личный список действий, которые нельзя выполнять из входящего сообщения: коды, ссылки, файлы, платёжи, реквизиты, доступы.

Опишите путь проверки для банка, маркетплейса, работы, родственников и госуслуг.

Напишите три фразы для безопасного прекращения звонка без спора и объяснений.

Сделайте таблицу «роль источника — допустимое под-

тверждение — недопустимое действие без проверки».

Проведите аудит открытых данных о себе: какие сведения могут помочь имитации доверенного контакта.

Смоделируйте безопасную проверку изменения реквизитов поставщика.

Потренируйтесь отделять событие от инструкции: проблема может быть реальной, но предложенный способ решения — опасным.

Составьте порядок действий остановки для ситуаций красного риска.

После каждого подозрительного контакта делайте послесценарный разбор: где был вход, где эмоция, где ожидаемое действие.

Блок быстрой проверки к разделу 1

Что такое социальная инженерия в защитной логике?

Почему социальная инженерия опасна не фразой, а сценарием?

Какие восемь узлов входят в базовую модель сценария?

Чем заявленный источник отличается от подтверждённого источника?

Почему логотип, номер или уверенный голос не являются доказательством?

Что такое предлог?

Чем легенда отличается от факта?

Почему совпадение с реальной ситуацией усиливает риск?

Что такое удержание на связи?

Почему нельзя пользоваться номером или ссылкой из подозрительного сообщения?

Почему срочность требует не ускорения, а остановки?

Почему запрет проверки — красный флаг?

Что такое выуживание информации?

Почему маленькие фрагменты сведений могут быть опасны?

Что считается нужным действием?

Какие нужные действия относятся к красному уровню риска?

Что такое официальный источник или уже известный контакт для проверки?

Почему обратный звонок должен идти по старому известному номеру?

Как заранее установленный порядок действий снижает риск?

Какой главный вывод раздела 1 Части I?

Чек-лист первичной защиты от социально-инженерного контакта

Я знаю, кто обращается, или только верю заявленной роли?

Контакт пришёл через обычный штатный канал или через новый путь?

Есть ли срочность, страх, чувство вины, секретность или запрет проверки?

Какая конкретная инструкция дана: код, ссылка, файл, пе-

ревод, доступ, подпись?

Что будет, если я возьму время на проверку на 10–30 минут?

Можно ли проверить событие через официальный источник, не используя данные из сообщения?

Есть ли необратимые последствия: деньги, данные, доступ, документы?

Нарушает ли просьба обычный регламент?

Нужна ли вторая проверка через официальный сайт, приложение или уже известный контакт?

Если источник сопротивляется проверке, почему?

Защитные формулы раздела 1

«Я не выполняю действия из входящего сообщения. Проверю самостоятельно».

«Я завершаю разговор и сам свяжусь с организацией через официальный сайт, приложение или уже известный контакт».

«Коды, пароли и доступы я никому не сообщаю».

«Изменение реквизитов подтверждается только по старому известному контакту».

«Если проверка запрещена, действие не выполняется».

«Срочность не отменяет регламент».

«При деньгах, доступах и документах нужна вторая проверка».

«Вернёмся к вопросу после письменной фиксации и проверки источника».

Дополнение к мини-глоссарию

Социальная инженерия: Сценарное обманное воздействие на человека для получения информации, доступа, денег или выполнения действия.

Предлог: Объяснение, почему контакт происходит и почему человек должен включиться.

Легенда: Связная история, которая задаёт роль источника, проблему, срочность и действие.

Имитация источника: Выдача себя за доверенное лицо, организацию или сервис.

Удержание на связи: Удержание контакта в среде, где атакующий контролирует темп и инструкции.

Выуживание информации: Получение полезных сведений через косвенные, бытовые или дружелюбные вопросы.

Нужное действие: Конкретный шаг, ради которого построен сценарий: код, ссылка, платёж, доступ, файл, подпись.

Проверка через официальный сайт, приложение или уже известный контакт: Проверка источника и события через канал, не предоставленный подозрительным сообщением.

Источники и опорные материалы

CISA. Материалы о социальной инженерии и фишинг: контакт использует доверие, срочность и знакомые формы общения, чтобы получить информацию или доступ.

Здесь важно увидеть точку входа в обман: nIST CSRC Glossary. Social engineering: an attempt to trick someone into

revealing information that can be used to attack systems or networks.

NIST CSRC Glossary. Фишинг: цифровая форма социальной инженерии, где поддельные письма или сайты выглядят правдоподобно и выманивают информацию.

Руководство NIST Phish Scale: метод оценки того, насколько человеку трудно распознать фишинговое письмо и признаки социальной инженерии.

FTC Consumer Advice. Рекомендации FTC: мошенники часто выдают себя за доверенные организации, говорят о проблеме или призе, давят срочностью и требуют конкретный перевод, код или иное действие.

FBI. Рекомендации по подмене деловой переписки: проверять изменения реквизитов и платёжные запросы по известным контактам, настороженно относиться к секретности и давлению срочностью, использовать двухэтапное подтверждение переводов.

Что будет дальше

Дальнейшая логика Части I переходит от общей модели социальной инженерии к конкретным мошенническим каналам: телефонные звонки, SMS, мессенджеры, электронная почта, поддельные сайты, короткая ссылка, удалённый доступ и физический контакт. Для каждого канала нужно сохранять защитный фокус: распознавание, тревожные признаки, безопасная пауза на проверку, проверка через официальный сайт, приложение или уже известный контакт и отказ

от необратимых действий до подтверждения.

Дополнение к разделу. Российские антифрод-барьеры: когда банк и связь помогают остановиться

Мошеннический перевод редко выглядит как преступление в моменте. Человек может сам нажать кнопку, сам назвать данные, сам подтвердить доступ и только потом понять, что его вели через страх. Поэтому часть защиты теперь строится не только на внимательности человека, но и на задержках, банковских предупреждениях и проверках связи. Эти барьеры не заменяют личную паузу, но дают шанс остановиться до потери денег.

Что важно знать читателю

С 1 января 2026 года Банк России расширил признаки мошеннических переводов с шести до двенадцати. Запоминать номера признаков не нужно. Важна логика: банк смотрит не только на получателя денег, но и на странности вокруг действия — необычный платёж, подозрительный получатель, резкий рост звонков и сообщений перед переводом, смену телефона в онлайн-банке или на Госуслугах, признаки удалённого доступа к устройству, быстрый перевод через СБП самому себе и попытку сразу отправить крупную сум-

му новому человеку.

Если получатель денег уже есть в базе Банка России по мошенническим переводам, банк обязан приостановить перевод на два дня и предупредить человека. Это не наказание и не «ошибка банка». Это время на проверку. Но важно не путать: не каждый подозрительный признак сам по себе означает автоматическую остановку на два дня. По другим признакам банк предупреждает о риске, а дальше порядок зависит от вида операции, получателя и правил закона.

Отдельно с 1 сентября 2025 года банки проверяют снятие наличных в банкомате на признаки давления. Если срабатывает хотя бы один признак, банк вводит временный лимит на снятие через банкомат: до 50 тысяч рублей в сутки на 48 часов. Более крупную сумму в этот период можно получить в отделении. Смысл простой: если человека держат на линии и ведут к банкомату, у него появляется время выйти из чужого темпа.

По кредитам и займам с 1 сентября 2025 года действует период охлаждения: при сумме от 50 до 200 тысяч рублей деньги становятся доступны через 4 часа, а при сумме свыше 200 тысяч рублей — через 48 часов. Если кредит оформляют под давлением, эта задержка может стать спасительной паузой: не надо «дожимать» получение денег, надо проверить, кто и зачем торопит.

Для звонков тоже появляются защитные признаки. Официальный звонок от организации должен быть проверяемым:

название, номер, причина обращения, возможность перезвонить самостоятельно. Если вам звонят якобы из банка, ведомства или полиции через мессенджер и разговор касается денег, кредита, карты, доступа или «безопасного счёта», безопасный поступок одно: закончить разговор и открыть официальный источник самостоятельно. Сотрудники Банка России, банков и госорганов не должны вести финансовые вопросы через иностранные мессенджеры.

Маркировка бизнес-звонков помогает отличать обычный коммерческий контакт от безымянного вызова, но не превращает экран телефона в абсолютное доказательство. Нет метки — не значит автоматически мошенник. Есть метка — не значит автоматически безопасно. Надёжный критерий другой: можно ли завершить разговор, открыть официальный сайт или приложение самому и проверить обращение без давления.

Как опознать

Перед переводом резко выросло количество звонков, SMS или сообщений в мессенджерах.

Вас держат на линии и одновременно требуют перевести деньги, снять наличные, назвать код или установить приложение.

Недавно сменился номер телефона в онлайн-банке или на Госуслугах, а вас уже подталкивают к переводу.

Вас просят быстро перевести крупную сумму новому человеку после перевода самому себе через СБП.

Вас ведут к банкомату после кредита, закрытия вклада или разговора о «защите денег».

Банк остановил перевод или ограничил снятие, а собеседник требует «срочно пройти заново» или «не обращать внимания на предупреждение».

Красный флаг и безопасная проверка

Не спорьте с предупреждением банка. Считайте его защитной паузой.

Закончите текущий разговор. Не оставайтесь на линии с тем, кто объясняет, как обойти предупреждение.

Откройте приложение банка самостоятельно или позвоните по номеру с карты, договора или официального сайта.

Проверьте получателя: имя, банк, реквизиты, основание платёжа, старый договор, прежний номер поставщика или знакомого.

Если речь о кредите, снимите давление с времени: «Я не беру деньги в разговоре. Проверю условия и вернусь к вопросу позже».

Если вас вели к банкомату, отойдите от устройства, положите телефон в карман, зайдите в отделение или позвоните в банк самостоятельно.

Если вы уже нажали перевод или передали код, сразу об-

ратитесь в банк, заблокируйте карту или доступ, сохраните переписку и звонки, затем подайте заявление через официальный порядок.

Карта красных флагов

«Я не перевожу деньги в разговоре. Проверю всё сам через приложение».

«Назовите номер обращения. Я перезвоню по официальному номеру».

«Если банк остановил платёж, я не буду его проталкивать. Сначала проверка».

«Я не называю коды, не ставлю программы и не подтверждаю доступ по звонку».

«Я прекращаю разговор. Дальше — только официальный источник».

Кейс

— Антон, платёж не прошёл, потому что система безопасности банка сработала ошибочно. Сейчас главное — не сбрасывайте вызов. Откройте приложение, повторите перевод и подтвердите, что это вы. Если появится предупреждение, нажимайте «всё равно отправить». Мы сопровождаем операцию до конца, иначе деньги зависнут.

В этой фразе опасна не техническая деталь, а попытка заставить человека обойти защитный барьер своими руками.

Правильный ход — не спорить, а остановиться: завершить разговор, открыть банк самостоятельно, проверить получателя и не повторять перевод под диктовку.

Что именно от меня хотят: перевод, наличные, код, доступ, кредит, установка программы?

Почему действие нужно сделать прямо сейчас?

Почему я должен оставаться на связи с этим человеком?

Как я проверю это без ссылки, номера и инструкций из текущего контакта?

Что я потеряю, если подожду 30 минут и открою официальный источник сам?

Антифрод-барьер работает только тогда, когда человек не помогает мошеннику его обойти. Если банк, телефон или приложение дают паузу, используйте её: не вводите код, не нажимайте повторный перевод, не снимайте наличные под диктовку, не ставьте программу удалённого доступа и не доказывайте незнакомому голосу, что «операция ваша».

Раздел 2. Каналы мошеннического контакта: электронная почта,

SMS

, звонок, мессенджер, сайт и ссылка

Этот блок продолжает Часть I и переводит общую модель социальной инженерии в практическую диагностику каналов. Один и тот же собеседник может быть доставлен через письмо, SMS, голосовой звонок, мессенджер, поддельную страницу, поддельную кнопку оплаты или деловую пере-

писку. Суть меняется мало: источник имитирует доверие, создаёт повод, ускоряет реакцию и ведёт к нужному действию. Меняется только поверхность атаки: где человек видит сообщение, каким способом отвечает и какие признаки проверки доступны.

Защитный принцип раздела: канал не доказывает подлинность. Письмо может выглядеть официально, SMS может прийти в той же цепочке, что и настоящие сообщения сервиса, голос может звучать уверенно, сайт может иметь аккуратный дизайн, QR-код оплаты может быть наклеен на реальный объект, а деловое письмо может использовать знакомый стиль. Поэтому проверять нужно не впечатление от канала, а независимые признаки: кто инициировал контакт, какое действие нужно, почему срочно, можно ли проверить через ранее известный канал и что будет потеряно при остановке.

CISA описывает фишинг как форму социальной инженерии и отдельно выделяет SMS-фишинг. FTC описывает фишинговые сообщения как письма и уведомления, которые выглядят как сообщения от знакомой или доверенной компании и требуют перейти по ссылке, открыть вложение или предоставить данные. FBI в рекомендациях по подмене деловой переписки подчёркивает: платёжные запросы и изменения реквизитов нужно проверять через личный контакт или звонок по известному номеру, а не по данным из подозрительного письма.

Как проверить ситуацию

Фишинговое письмо: массовое или целевое письмо, которое имитирует сервис, организацию, коллегу или уведомление.

Целевое фишинговое письмо: персонализированное письмо с использованием контекста человека, должности, проекта, покупки или отношений.

Мошенническое SMS: SMS или короткое сообщение с ложной проблемой, ссылкой, кодом, доставкой, оплатой или подтверждением.

Мошеннический звонок: голосовой звонок, голосовое сообщение или звонок через мессенджер с давлением и управлением темпом.

Мессенджеры и соцсети: подмена знакомого, работодателя, поддержки, покупателя, продавца или участника окружения.

Поддельные сайты и формы входа: внешне похожая страница, собирающая логины, коды, данные карты или документы.

QR-фишинг: перевод проверки из видимого текста в код, который скрывает адрес и действие до сканирования.

подмена деловой переписки: деловая переписка, где меняют реквизиты, инициируют перевод или заставляют нарушить финансовый регламент.

Электронная почта часто маскируется под счёт, уведомление маркетплейса, документ, приглашение или сообщение о безопасности. Опасность в том, что письмо похоже на официальный шаблон. Не открывайте вложение и не переходите по кнопке, пока не проверите домен, отправителя и причину обращения через уже известный источник.

SMS давит краткостью и срочностью: «посылка», «штраф», «банк», «код», «запись», «маркетплейс». Цель — заставить вас нажать ссылку, оплатить или подтвердить действие. Не переходите из сообщения. Откройте нужный сервис самостоятельно.

Звонок чаще всего прикрывается авторитетом банка, полиции, службы безопасности или руководителя. Вас удерживают в разговоре, торопят и ведут к одному из действий: назвать код, перевести деньги или установить приложение. Завершите разговор и перезвоните по официальному номеру.

В мессенджере обман держится на доверии к аватару, имени и прошлой переписке. Сообщение может выглядеть как просьба знакомого, покупателя, продавца или HR-специалиста. До перевода денег, отправки кода, открытия файла или передачи данных проверьте личность человека другим способом.

Поддельный сайт или форма входа обычно прикрываются словами «авторизация», «оплата», «проверка аккаунта». Вас ведут к вводу логина, пароля, данных карты или кода. Проверьте адрес вручную и переходите только через закладку,

поиск или официальное приложение.

QR-код опасен тем, что адрес не виден до сканирования. Его могут наклеить на оплату парковки, меню, анкету, объявление или страницу маркетплейса. Перед вводом любых данных проверьте домен и закройте страницу, если адрес выглядит чужим.

Подмена деловой переписки маскируется под изменение реквизитов, срочный счёт или уточнение платёжа. Опасность в деловом контексте: письмо выглядит привычно, а просьба будто вписана в работу. Любое изменение реквизитов подтверждайте по старому известному контакту и проводите только после второго согласования.

Глава 9. Фишинговое письмо: имитация официального контакта

Здесь важно увидеть точку входа в обман: письмо выглядит официально: логотип, подпись, срочная тема, кнопка «подтвердить». Но подлинность письма не доказывается оформлением. Безопасный шаг — не нажимать кнопку, а открыть сервис вручную и проверить уведомления внутри аккаунта.

Живой разбор приёма

Фишинговое письмо — это сообщение, которое выглядит

как письмо от сервиса, банка, работодателя, поставщика, госоргана или знакомого лица и подталкивает человека к ссылке, вложению, ответу или раскрытию данных.

Откуда это появилось?

Фишинговые письма развивались вместе с электронной почтой: от грубых массовых рассылок до хорошо оформленных писем с логотипами, персональными данными, деловым контекстом и вложениями. По мере улучшения фильтров выросла роль психологических признаков: срочности, предлога, доверия и похожести на привычные уведомления.

Письмо использует доверие к шаблону и привычку быстро обрабатывать уведомления. Человек видит знакомый бренд, счёт, файл, приглашение или предупреждение и реагирует на сценарий, не проверяя технические детали и реальный контекст.

Срочное предупреждение создаёт ощущение угрозы и снижает склонность к вдумчивой проверке. Знакомые визуальные элементы уменьшают ощущение риска, а рабочий поток повышает вероятность автоматического клика.

Рабочая почта, личная почта, рассылки сервисов, документы, счета, уведомления маркетплейса, безопасность аккаунтов, поддельные приглашения и файлы.

Потому что письмо выглядит как обычная часть деловой или бытовой рутины. Чем больше оно похоже на ожидаемый

формат, тем меньше человек воспринимает его как отдельное решение.

Как схема развивается?

Распознать канал контакта и отделить его от реального источника.

Определить действие, которого добиваются: данные, деньги, код, файл, доступ, подпись или переход.

Проверить, есть ли срочность, секретность, запрет проверки или эмоциональное давление.

Сравнить запрос с обычным регламентом, прежней историей отношений и независимыми данными.

При риске остановить действие и перейти к проверке через заранее известный официальный источник.

Как опознать

Адрес отправителя похож на настоящий, но не совпадает.

Текст требует перейти по ссылке или открыть файл.

Есть неожиданное вложение.

Письмо имитирует счёт, блокировку или безопасность.

Обращение общее или контекстно неточное.

Как это выглядит в жизни

Тревожный признак: неожиданное письмо с требованием

срочного действия, ссылка на вход в аккаунт, вложение без предварительной договорённости, ошибка в домене, просьба отключить проверки или обойти регламент.

Красный флаг и безопасная проверка

Не входить в аккаунт по ссылке из письма. Открывать сервис вручную через сохранённый адрес или приложение. В рабочей среде проверять вложения, домен, контекст и отправителя через установленный регламент.

Не всякое письмо со ссылкой опасно. Но подлинность письма нельзя доказывать дизайном, логотипом или уверенным тоном.

Письмо «ваш аккаунт будет заблокирован» ведёт на страницу входа.

Письмо от «поставщика» содержит новый счёт с нетипичным вложением.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Бухгалтер получил письмо с темой «Срочно оплатить до 16:00» и вложенным счётом.

Человек получил уведомление о входе в аккаунт и ссылку «проверить активность».

Возьмите пример сообщения и выпишите: источник, предлог, эмоцию, действие, канал проверки.

Сформулируйте ответ, который не спорит, но переносит

решение в независимую проверку.

Какое действие хотят получить?

Почему действие нужно выполнить именно сейчас?

Каким независимым каналом можно проверить запрос?

Фишинговое письмо опасно не только ссылкой, а сочетанием знакомого формата, срочности и привычки действовать внутри почтового потока.

Глава 10. Целевой фишинг: письмо под конкретного человека

Живой разбор приёма

Целевой фишинг — это письмо, где сообщение подстраивается под конкретного человека, должность, проект, организацию, покупку, событие или публично доступную информацию.

Откуда это появилось?

С ростом открытых данных, соцсетей и корпоративных следов персонализация стала сильнее: злоумышленник может использовать имя руководителя, контекст сделки, вакансии, конференции, документы, поставщика или публичную роль человека.

Персонализация снижает критичность: если сообщение содержит реальные детали, человек ошибочно переносит правдивость деталей на правдивость всего запроса.

Узнавание своего контекста вызывает чувство релевантности и снижает ощущение случайности. Человек быстрее принимает сообщение как «относящееся ко мне», особенно при рабочей нагрузке.

Корпоративная переписка, HR, продажи, закупки, юридические документы, инвестиционные предложения, деловые конференции, фриланс и проекты.

Потому что точные детали создают иллюзию проверенности источника. Человек думает: «они знают контекст, значит, это свои».

Как схема развивается? Как опознать

Сообщение слишком хорошо попадает в текущий контекст.

Просят выполнить нетипичный шаг.

Ссылаются на реальных людей, но не дают обычный канал подтверждения.

Предлагают срочно открыть файл или дать доступ.

Стиль слегка отличается от привычного.

Как это выглядит в жизни

Тревожный признак: реальная деталь плюс необычное действие; просьба «не беспокоить руководителя»; изменение обычного процесса; новое вложение или ссылка в знакомом рабочем контексте.

Красный флаг и безопасная проверка

Проверять не только детали, но и действие. Если запрос нетипичен, подтверждать его через ранее известный канал, внутреннюю систему задач или прямой контакт.

Сильная персонализация может выглядеть убедительно даже для опытного человека; поэтому защита должна быть процедурной, а не основанной только на внимательности.

Письмо от имени партнёра с упоминанием реального договора просит открыть «обновлённую спецификацию».

Сообщение от имени HR использует название вакансии и просит заполнить форму с документами.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Менеджер получил письмо с упоминанием реального клиента и просьбой срочно отправить коммерческие данные.

Сотруднику прислали «обновление регламента» от имени знакомого отдела.

В целевом фишинге опасны правдивые детали: они слу-

жат не доказательством подлинности, а приманкой для снижения проверки.

Глава 11. Мошенническое SMS: SMS и короткие сообщения как канал срочного действия

Живой разбор приёма

Мошенническое SMS — это социальная инженерия через SMS или короткие сообщения, где человека подталкивают к ссылке, оплате, подтверждению, звонку или раскрытию данных.

Откуда это появилось?

SMS долго воспринимались как служебный канал банков, маркетплейса, госуслуг и операторов. Это сделало короткое сообщение удобным инструментом для ложных уведомлений о заказах, штрафах, платёжах и кодах.

Краткость SMS не оставляет места для аргументов, зато усиливает импульсивность. Человек видит маленькое сообщение, короткую ссылку и срочный повод, поэтому действие кажется незначительным.

Мобильное уведомление вызывает быстрый ориентиро-

вочный рефлекс. Малый формат снижает ощущение риска: кажется, что «просто проверить ссылку» не является полноценным решением.

Маркетплейс, банки, штрафы, записи к врачу, маркетплейсы, службы такси, операторы связи, подтверждение входа, «ошибочные» коды.

Потому что SMS появляется в личном устройстве и выглядит как техническое уведомление, а не как убеждающее сообщение.

Как схема развивается? Как опознать

Короткая ссылка.

Сообщение о проблеме с доставкой, оплатой или аккаунтом.

Просьба оплатить небольшой сбор.

Запугивание блокировкой.

Номер или цепочка сообщений выглядят знакомо, но действие нетипично.

Как это выглядит в жизни

Тревожный признак: ссылка из SMS для оплаты, ввод карты или кода, «последний день», «заказ задержан», «подтвердите сейчас», отсутствие возможности проверить без ссыл-

ки.

Красный флаг и безопасная проверка

Не открывать сервис из SMS. Проверять доставку, банк или аккаунт через официальное приложение, сайт, закладку или номер с карты/договора.

Настоящие сервисы тоже отправляют SMS. Но подлинность события нужно проверять отдельно, а не через ссылку в сообщении.

SMS «заказ задержан, оплатите 49 рублей» ведёт на форму карты.

Сообщение «ваш аккаунт будет удалён» просит срочно войти по ссылке.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Покупатель ждёт доставку и получает SMS с оплатой «таможенного сбора».

Человек получает сообщение о штрафе с короткой ссылкой.

Мошенническое SMS использует личный характер телефона и малый формат сообщения: защита начинается с отказа переходить по ссылкам из SMS.

Глава 12. Мошеннический звонок: голосовой звонок и управление темпом

В атласе обмана этот фрагмент проверяется через источник, канал и действие: голос в трубке звучит уверенно, а фон похож на офис. Но голос не является доказательством. Безопасный шаг — завершить звонок и перезвонить самому по официальному номеру.

Живой разбор приёма

Мошеннический звонок — это голосовая социальная инженерия: звонок, голосовое сообщение или разговор в мессенджере, где источник имитирует роль и управляет эмоцией, временем и действиями человека.

Откуда это появилось?

Телефонные мошеннические сценарии существовали до цифровой эпохи, но усилились за счёт подмены номеров, утечек данных, мессенджеров и возможности быстро переводить деньги или устанавливать приложения.

Голос создаёт ощущение живого контакта и социального обязательства отвечать. Звонящий контролирует темп, перебивает сомнения, задаёт последовательность шагов и удер-

живает человека в канале.

Живой голос усиливает социальное присутствие и реакцию на авторитет. Срочный тон активирует стрессовую реакцию, при которой человек хуже удерживает сложные проверки в памяти.

Банк, полиция, служба безопасности, техподдержка, работодатель, родственник, курьер, покупатель, продавец, оператор связи.

Потому что в разговоре сложнее поставить время на проверку. Человек чувствует необходимость отвечать и боится выглядеть подозрительным, грубым или некомпетентным.

Как схема развивается? Как опознать

Звонящий требует не класть трубку.
Диктует действия пошагово.
Просит код, перевод, установку приложения или доступ.
Ссылается на угрозу счёту, делу или родственнику.
Сопротивляется самостоятельному перезвону.

Как это выглядит в жизни

Тревожный признак: запрет завершить разговор, перевод на «безопасный счёт», требование кода, установка приложения удалённого доступа, секретность, давление «сейчас или

потеряете деньги».

Красный флаг и безопасная проверка

Завершить разговор. Самостоятельно связаться с организацией по номеру из официального источника. Не сообщать коды и не выполнять финансовые действия в режиме входящего звонка.

Некоторые настоящий службы звонят клиентам. Но нормальная организация не должна запрещать независимую проверку или требовать секретных кодов.

«Служба безопасности банка» удерживает человека на линии и просит перевести деньги.

«Сотрудник поддержки» просит установить приложение для диагностики.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Пенсионеру звонит «следователь» и требует срочно помочь сохранить деньги.

Предпринимателю звонит «банк» и просит подтвердить платёж кодом.

Мошеннический звонок опасен управлением темпом. Главная защита — физически разорвать канал, потому что спор внутри звонка часто усиливает давление.

Глава 13. Мессенджеры и соцсети: подмена знакомого и доверительной среды

Ловушка часто начинается с канала: вас переводят туда, где быстрее отвечают и хуже проверяют. В новом окне, чате или звонке исчезают привычные правила. Безопасный шаг — вернуться в официальный сайт, приложение или уже известный контакт самому, без ссылок и номеров из сообщения.

Живой разбор приёма

Это сценарии, где контакт приходит через мессенджер, социальную сеть, группу, чат продажи, рабочий канал или личный аккаунт и использует доверие к профилю, аватару, истории переписки или группе.

Откуда это появилось?

По мере ухода общения в мессенджеры мошеннические сценарии стали имитировать родственников, коллег, продавцов, покупателей, HR, администраторов групп и службу поддержки платформ.

Мессенджер воспринимается как личная среда. Аватар,

имя и прежняя переписка создают ощущение знакомого человека, даже если аккаунт взломан, скопирован или используется похожий профиль.

Личная переписка активирует доверие и привычку быстро отвечать. Короткие реплики и уведомления удерживают человека в эмоциональном цикле «вопрос — ответ».

Telegram, WhatsApp, VK, Instagram, рабочие чаты, объявления, маркетплейсы, окружения района, районные чаты, фриланс и вакансии.

Потому что человек проверяет не запрос, а знакомость интерфейса и имени. Если сообщение пришло «от своего», критичность падает.

Как схема развивается? Как опознать

Знакомый внезапно просит деньги или код.
Покупатель/продавец уводит в другой чат.
Ссылка на оплату или доставку приходит вне платформы.
Профиль новый или похожий, но не тот.
Стиль общения отличается.

Как это выглядит в жизни

Тревожный признак: срочная просьба от знакомого, отказ созвониться, просьба кода, перевод вне платформы, файл от

неожиданного контакта, «я потом объясню».

Красный флаг и безопасная проверка

Проверить личность вторым каналом: звонок, голосовая фраза, личный вопрос, старый номер, контакт вне мессенджера. По сделкам не уходить с защищённой платформы.

Мессенджер удобен и для настоящих просьб. Но любые деньги, доступы, коды и документы требуют отдельной проверки личности.

«Друг» просит срочно занять деньги, но не может говорить.

«Покупатель» предлагает оформить доставку по ссылке вне площадки.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

В рабочий чат добавляют похожий аккаунт контрагента и просят срочно сменить реквизиты платёжа.

Продавцу на Авито присылают ссылку «получить деньги за товар».

В мессенджерах нужно проверять не только профиль, но и владение личностью: знакомое имя не равно проверенному источнику.

Глава 14. Поддельные сайты, формы входа и платёжные страницы

Сообщение звучит убедительно: деньги под угрозой, решение нужно сейчас, а проверка якобы только всё испортит. В такой сцене человек защищает не счёт, а тревогу. Безопасный шаг — прекратить контакт и проверить ситуацию через официальный сайт, приложение или уже известный контакт, найденный самостоятельно.

Живой разбор приёма

Это сценарий, где человека приводят на страницу, похожую на настоящий сайт сервиса, банка, магазина, маркетплейса или корпоративной системы, чтобы получить логины, пароли, коды, данные карты или документы.

Откуда это появилось?

Фальшивые сайты эволюционировали от грубых копий до аккуратных страниц с адаптивным дизайном, HTTPS, похожими доменами, локализацией и логикой реального сервиса.

Внешнее сходство снижает проверку. Человек видит знакомый дизайн и воспринимает форму как продолжение известного сервиса, особенно если попал туда из письма, SMS

или рекламы.

Визуальная узнаваемость запускает привычку мышления знакомости. Состояние срочности снижает внимание к адресной строке, мелким символам домена и несоответствию процесса.

Авторизация, маркетплейс, маркетплейсы, банки, облачные сервисы, корпоративные порталы, госуслуги, оплата брони, штрафы, подписки.

Потому что дизайн часто воспринимается как доказательство подлинности, хотя его можно имитировать.

Как схема развивается? Как опознать

Домен похож, но имеет лишние символы.

Страница просит лишние данные.

Форма пришла из внешней ссылки.

Нет нормального пути с главной страницы сервиса.

После ввода данных появляется новая просьба о коде или карте.

Как это выглядит в жизни

Тревожный признак: вход по ссылке из сообщения, ввод кода подтверждения на странице, просьба карты для «получения денег», странный домен, давление таймером.

Красный флаг и безопасная проверка

Открывать сервис вручную, через приложение, закладку или официальный поиск. Перед вводом данных проверять домен, назначение формы, необходимость действия и наличие события в настоящем аккаунте.

HTTPS и красивый дизайн не гарантируют безопасность. Сертификат подтверждает соединение с доменом, но не то, что домен принадлежит нужной организации.

Страница маркетплейса просит карту для получения денег от покупателя.

Форма «безопасности аккаунта» просит логин, пароль и код.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Человек входит в «корпоративную почту» по ссылке из письма и вводит пароль.

Продавец вводит данные карты на странице «получения оплаты».

Поддельная страница работает за счёт визуальной привычки. Защита — не доверять виду страницы и входить в сервис только независимым маршрутом.

Глава 15. Поддельная ссылка: скрытая ссылка в физическом или цифровом коде

Живой разбор приёма

QR-фишинг — это использование кода для перехода на скрытую ссылку, форму оплаты, страницу входа, приложение или инструкцию, где реальный адрес не виден до сканирования.

Откуда это появилось?

короткая ссылка стали привычными для меню, парковок, платёжей, билетов, объявлений, доставок и авторизации. Это создало канал, где проверка ссылки затруднена: человек видит квадратный код, но не видит адрес.

поддельная кнопка оплаты переносит доверие с места размещения на содержимое ссылки. Если код наклеен на терминал, стол, объявление или документ, человек предполагает, что он относится к реальному объекту.

Физический контекст создаёт ощущение подлинности. Сканирование кажется техническим действием, а не решением перейти на неизвестный ресурс.

Кафе, парковки, подъезды, объявления, документы, презентации, письма, платёжи, билеты, Wi-Fi-доступ, анкеты и акции.

Потому что адрес скрыт до момента сканирования, а доверие часто переносится с окружающей среды на код.

Как схема развивается? Как опознать

Форма наклеен поверх другого кода.
Код ведёт на сокращённую или странную ссылку.
После сканирования просят карту, логин или код.
Нет альтернативного официального способа.
Код связан с оплатой или доступом.

Как это выглядит в жизни

Тревожный признак: физическая наклейка без признаков организации, ссылка не похожа на официальный домен, запрос платёжа или логина, срочная скидка или штраф, отсутствие проверки через приложение.

Красный флаг и безопасная проверка

После сканирования смотреть домен до ввода данных. Для оплаты и входа использовать официальное приложение или ручной переход на сайт. Не вводить карты и коды на

странице, открытой из неизвестной ссылки.

форма оплаты сами по себе нейтральны. Риск возникает, когда они скрывают адрес и обходят привычную проверку ссылки.

На парковочном автомате наклеен код на экране, ведущий на фальшивую оплату.

В письме «от IT» форма ведёт на страницу входа в корпоративный аккаунт.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Посетитель кафе сканирует ссылка-меню и видит просьбу зарегистрироваться картой.

Жилец сканирует объявление об оплате коммунальной услуги по код на экране.

Фишинг через форму опасен тем, что адрес скрыт до сканирования. Защита — считать сканирование началом проверки, а не доказательством подлинности.

Глава 16. Подмена деловой переписки: как меняют реквизиты и финансовое решение

Здесь важно увидеть точку входа в обман: высокая доходность часто подаётся ярко, а риски — мелким шрифтом или вообще не называются. Безопасный шаг — проверить лицензии, комиссии, сценарий убытка и возможность выхода до

перевода денег.

Живой разбор приёма

Подмена деловой переписки — это деловой обман, где через поддельное или взломанное письмо инициируют перевод, изменение реквизитов, покупку, выдачу данных или обход финансового регламента.

Откуда это появилось?

Подмена деловой переписки стала особенно опасной из-за цифровизации документооборота, удалённой работы, сложных цепочек поставщиков и привычки согласовывать платёжи по электронной почте и мессенджерам.

собеседник использует деловой контекст, авторитет должности, знакомые имена, реальный проект и давление сроком. Цель — заставить сотрудника выполнить действие как часть обычного процесса, но с изменёнными реквизитами или нарушенным контролем.

Рабочая роль усиливает автоматическое следование процедуре и авторитету. Давление дедлайна и страх сорвать задачу уменьшают вероятность поднять вопрос о проверке.

Бухгалтерия, закупки, продажи, недвижимость, юридические сделки, подрядчики, фриланс, HR, зарплатные данные, счета и реквизиты поставщиков.

Потому что запрос выглядит не как мошенничество, а

как рабочая задача от поставщика, партнёра или внутренней службы.

Как схема развивается? Как опознать

Появились новые реквизиты.

Платёж стал срочным.

Просят сохранить конфиденциальность.

Ответственный человек якобы недоступен.

Коммуникация идёт с похожего адреса или через новый канал.

Как это выглядит в жизни

Тревожный признак: изменение реквизитов по электронной почте, срочный перевод без стандартного согласования, секретность, обход второго подтверждения, давление статусом, невозможность проверить старым каналом.

Красный флаг и безопасная проверка

Любые изменения реквизитов подтверждать через старый известный номер или договорной контакт, а крупные платёжи — через двухкругное согласование. Не использовать телефоны и ссылки из подозрительного сообщения.

Подмена деловой переписки может использовать реаль-

ные взломанные ящики; поэтому даже настоящий адрес не отменяет регламент финансовой проверки.

«Поставщик» присылает письмо о смене банковских реквизитов.

«Поставщик» просит срочно оплатить счёт по новым реквизитам и никому не звонить до вечера.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Бухгалтер получил письмо из существующей цепочки с новым счётом.

Менеджер по закупкам получил срочную просьбу изменить платёжные данные подрядчика.

Подмена деловой переписки ломает не внимание, а процесс. Поэтому защита должна быть не индивидуальной догадкой, а обязательным финансовым регламентом проверки.

Блок кейсов раздела 2

Ситуация 1. Человек получил письмо «ваш аккаунт заблокирован» и перешёл по ссылке.

Вывод простой: источник имитирует сервис, эмоция — тревога, действие — вход, защита — открыть сервис вручную.

Ситуация 2. Бухгалтер получил счёт от знакомого поставщика, но реквизиты изменились.

Вывод простой: риск подмены деловой переписки, защита — подтверждение по старому известному телефону и второй подписью.

Ситуация 3. SMS о задержке заказа просит оплатить 79 рублей.

Вывод простой: малый платёж снижает критичность, защита — проверка в приложении маркетплейса.

Ситуация 4. Звонящий из «банка» требует не класть трубку.

Вывод простой: удержание на связи, защита — завершить звонок и перезвонить по номеру с карты.

проверка личности- Ситуация 5. «Друг» в мессенджере просит срочно занять деньги и не может говорить.

Вывод простой: проверка личности через голосовой звонок или официальный источник или уже известный контакт для проверки.

Ситуация 6. Покупатель на площадке отправляет ссылку «получить оплату».

Вывод простой: уход с платформы, защита — не вводить карту для получения денег.

Ситуация 7. ссылка в сообщении на парковке ведёт на сайт с похожим доменом.

Вывод простой: физический контекст не доказывает подлинность, защита — официальное приложение парковки.

Ситуация 8. HR-претендент получает форму с просьбой загрузить паспорт до интервью.

Вывод простой: персонализированный контекст, защита — проверить домен и канал работодателя.

Ситуация 9. В рабочую переписку приходит «обновлён-

ный договор» с макросами.

Вывод простой: вложение без проверки, защита — спросить отправителя старым каналом.

Ситуация 10. Руководитель якобы просит купить подарочные карты «для клиентов».

Вывод простой: давление авторитетом и секретностью, защита — финансовый регламент.

Ситуация 11. SMS о штрафе содержит короткую ссылку.

Вывод простой: штраф проверяется только через официальный сервис или приложение.

Ситуация 12. Голосовой бот сообщает о «подозрительной операции» и переводит на оператора.

Вывод простой: автоматизация доверия, защита — не продолжать сценарий.

Ситуация 13. Письмо с короткая ссылка для «обновления пароля» обходит видимую ссылку.

Вывод простой: скрытие адреса, защита — портал открыть вручную.

Ситуация 14. В соцсети появляется копия профиля родственника.

Вывод простой: похожий аватар не равен личности, защита — проверка по старому контакту.

Ситуация 15. Поставщик просит срочно оплатить новый счёт до закрытия банка.

Вывод простой: дедлайн и изменение реквизитов, защита — пауза на проверку и подтверждение.

Ситуация 16. Мошенник в чате аренды присылает ссылку на «безопасную бронь».

Вывод простой: поддельная платёжная страница, защита — платить только внутри платформы.

Ситуация 17. Поддержка сервиса просит подтверждение во всплывающем уведомлении «для отмены операции».

Вывод простой: код — это доступ, защита — никому не сообщать.

Ситуация 18. В письме есть имя реального клиента и ссылка на «файл проекта».

Вывод простой: при целевом фишинге нужно проверять действие, а не только детали.

Ситуация 19. ссылка на объявлении в подъезде обещает перерасчёт платёжей.

Вывод простой: скрытая ссылка и финансовый мотив, защита — официальный сайт управляющей организации.

Ситуация 20. Сотрудник получает письмо от «IT» с просьбой срочно подтвердить вход.

Вывод простой: имитация внутренней службы, защита — заявка или контакт через корпоративный портал.

Блок упражнений раздела 2

Разберите любое входящее письмо по схеме: канал, источник, предлог, эмоция, действие, проверка через официальный сайт, приложение или уже известный контакт.

Составьте личный список сервисов, в которые вы никогда не входите по ссылкам из сообщений.

Напишите три фразы для завершения подозрительного звонка без объяснений и спора.

Потренируйтесь проверять домен: найдите отличия между похожими адресами и официальным доменом.

Создайте правило для денежных просьб в мессенджерах: как именно вы проверяете личность.

Опишите регламент проверки изменения реквизитов для бизнеса или личных платёжей.

Сделайте таблицу: какие данные нельзя сообщать по телефону, в SMS, в чате и на неизвестной странице.

Разберите поддельная кнопка оплаты без ввода данных: что нужно проверить до любого платёжа или авторизации.

Сравните два сообщения: массовое фишинговое письмо и персонализированный фишинг. Найдите общие элементы.

Сформулируйте «правило остановки»: при каких признаках вы прекращаете контакт сразу.

Блок быстрой проверки раздела 2

Почему канал сообщения не доказывает подлинность источника?

Чем массовый фишинг отличается от целевого?

Почему SMS-ссылка особенно опасна при ожидании маркетплейса?

Какая главная защита при подозрительном звонке?

Почему нельзя использовать номер телефона из подозрительного письма для проверки?

Почему настоящий или взломанный электронная почта не

отменяет финансовый регламент?

Какие признаки указывают на сценарий подмены деловой переписки?

Что проверять перед вводом данных на странице входа?

Почему HTTPS не является достаточным доказательством подлинности?

Какая особенность форма оплаты усложняет проверку?

Как проверить просьбу о деньгах от знакомого в мессенджере?

Почему срочность повышает риск ошибки?

Что значит «проверять действие, а не только детали»?

Какие данные нельзя сообщать по входящему звонку?

Почему уход с торговой платформы в отдельный чат рискован?

Красный флаг и безопасная проверка при просьбе изменить реквизиты поставщика?

Какой официальный источник или уже известный контакт подходит для проверки банка?

Какое действие требуется от вас в фишинговом письме?

Почему поддельные сайты часто выглядят убедительно?

Как сформулировать безопасную время на проверку при любом подозрительном канале?

Чек-лист защиты по каналам

Я не перехожу по ссылкам из входящих сообщений для входа в важные аккаунты.

Я не сообщаю коды, пароли, seed-фразы, данные карты и

удалённый доступ по телефону или в чате.

Я проверяю денежные просьбы от знакомых вторым каналом.

Я проверяю изменение реквизитов только через старый известный номер или договорной контакт.

Я не оплачиваю и не авторизуюсь на страницах, открытых из неизвестной ссылки в сообщении.

Я не использую контактные данные из подозрительного сообщения для проверки этого же сообщения.

Я прекращаю звонок, если мне запрещают положить трубку или проверить информацию.

Я рассматриваю срочность как повод остановиться, а не ускориться.

Я сохраняю финансовые решения в письменном регламенте и не меняю его под давлением.

Я считаю красивый дизайн, логотип и знакомый стиль недостаточными доказательствами подлинности.

Защитные формулы раздела 2

«Я не открываю ссылки из входящих сообщений. Проверю через приложение или официальный сайт».

«Я завершаю звонок и сам перезвоню по номеру из официального источника».

«Коды и пароли я никому не сообщаю, включая сотрудников банка и поддержки».

«Изменение реквизитов подтверждается только через прежний известный канал».

«Я не перехожу в сторонний чат и не оформляю оплату вне платформы».

«Короткая ссылка не является доказательством подлинности. Сначала проверю адрес».

«Если запрос срочный, он тем более требует проверки».

«Направьте запрос по официальному регламенту, после этого он будет рассмотрен».

Дополнение к мини-глоссарию

Фишинг: поддельное сообщение, которое имитирует доверенный источник и ведёт к ссылке, вложению, форме или раскрытию данных.

Целевой фишинг: персонализированное письмо под конкретного человека, роль, проект или организацию.

Мошенническое SMS: Социальная инженерия через SMS или короткие сообщения.

Мошеннический звонок: Голосовая социальная инженерия через телефонный звонок, голосовое сообщение или звонок в мессенджере.

Поддельная форма входа: Страница, похожая на настоящий сервис, но собирающая учётные данные или коды.

QR-фишинг: использование QR-кода для скрытого перехода на опасную ссылку или форму.

деловой сценарий подмены платёжа, реквизитов, поручения или доступа через переписку.

Независимый маршрут входа: Переход в сервис через приложение, закладку, официальный сайт или заранее извест-

ный адрес, а не через входящее сообщение.

Источники и опорные материалы

CISA. Предотвращение социальной инженерии и фишинга: фишинг является формой социальной инженерии; SMS-мошенничество использует текстовые сообщения; атаки строятся на доверии, срочности и каналах связи.

CISA. Распознавание фишинга и сообщение о нём: подозрительные сообщения нужно передавать на проверку, а не переходить по неожиданным ссылкам и просьбам.

FTC Consumer Advice. Как распознавать фишинг: такие сообщения могут выглядеть как письма известных компаний и просить перейти по ссылке, открыть вложение или передать личные данные.

FTC Consumer Advice. Как избегать мошенничества: мошенники выдают себя за доверенные организации, создают проблему или обещают приз, давят срочностью и требуют конкретный перевод или другое действие.

FBI. Рекомендации по подмене деловой переписки: проверять платёжные и закупочные запросы лично или по известному номеру; отдельно подтверждать изменения реквизитов; настороженно относиться к секретности и давлению срочностью.

NIST Phish Scale User Guide: метод оценки того, насколько человеку трудно распознать фишинговое письмо и признаки социальной инженерии в электронной почте.

OCC. Предотвращение фишинговых атак: не передавать

личные данные в ответ на неожиданные запросы и не доверять внешнему виду страницы, потому что подделка может выглядеть убедительно.

Что будет дальше

Дальнейшая логика Части I переходит от каналов контакта к типовым мошенническим сценариям по жизненным ситуациям: банк, маркетплейс, маркетплейс, аренда, работа, инвестиции, романтическая переписка, техподдержка, госуслуги и благотворительность. Важно показывать не только признаки, но и полный сценарный путь: вход, легенда, эмоция, ожидаемое действие, точка разрыва и безопасная проверка.

Раздел 3. Типовые мошеннические сценарии по жизненным ситуациям

Этот блок переводит анализ каналов в анализ жизненных сценариев. На практике человек редко видит «фишинговое письмо» как абстрактную угрозу. Он видит банковскую проблему, посылку, покупателя на онлайн-сервис, квартиру, вакансию, инвестиционную возможность, романтическую переписку или предупреждение техподдержки. Именно житейская правдоподобность делает сценарий сильнее технических признаков.

Защитный принцип раздела: проверять нужно не только сообщение, но и сюжет. Если история построена вокруг срочной проблемы, неожиданной выгоды, редкой возможности, доверенного лица или нужности обойти обычный порядок, это уже отдельный объект проверки. Канал может быть любым: письмо, SMS, мессенджер, звонок, сайт, форма оплаты или личная встреча. Но сценарная структура остаётся узнаваемой: предлог, эмоция, действие, которого добиваются, сужение проверки и фиксация результата.

FTC в материалах для потребителей описывает повторяемую схему мошенничества как сочетание имитации доверенного источника, проблемы или приза, давления действовать немедленно и требования определённого способа действия или оплаты. FBI в материалах по подмена деловой пе-

переписки отдельно подчёркивает проверку платёжных запросов и изменений реквизитов через личный контакт или заранее известный номер. CISA рассматривает фишинг как форму социальной инженерии, а NIST связывает социальную инженерию с попыткой обманом заставить человека раскрыть информацию или совершить действие.

Как проверить ситуацию

Банковский сценарий: «подозрительная операция», «защита счёта», «безопасный счёт», «код отмены» или «проверка клиента».

Интернет-магазин и уведомления: заказ, таможенный сбор, изменение адреса, оплата хранения, фальшивый трек-номер.

Торговая площадка и объявления: уход из платформы, фальшивая безопасная сделка, поддельный покупатель или продавец.

Аренда и недвижимость: слишком выгодный объект, невозможность показа, предоплата до проверки, давление спросом.

Работа и HR: вакансия, тестовое задание, документы, оплата обучения, доступ к аккаунтам или «служебное» приложение.

Инвестиции и быстрый доход: гарантированная доходность, инсайдерский доступ, криптовалюта, наставник, за-

крытый клуб.

Романтическая переписка: доверие, эмоциональная близость, кризис, просьба о деньгах или перевод к инвестициям.

Техническая поддержка: вирус, блокировка, удалённый доступ, «диагностика», платное исправление или кража данных.

Банк.

Как выглядит: говорят о подозрительной операции, защите денег или «безопасном счёте».

На что давят: на страх потери и доверие к авторитету.

К чему ведут: коду, переводу, удалённому доступу или данным карты.

Что делать: завершите контакт и откройте банк через приложение или номер с карты.

Доставка и интернет-магазин.

Как выглядит: пишут, что посылка не доставлена, адрес нужно уточнить или требуется небольшой сбор.

На что давят: на ожидание заказа и малую сумму платёжа.

К чему ведут: ссылке, данным карты или персональным данным.

Что делать: проверьте заказ в официальном приложении или на сайте службы.

Покупка или безопасная сделка.

Как выглядит: говорят о безопасной сделке, брони, онлайн-сервисе или быстром покупателе.

На что давят: на выгоду и страх потерять сделку.

К чему ведут: переходу из платформы, оплате или ссылке.

Что делать: не уходите из платформы и не вводите данные вне неё.

Аренда.

Как выглядит: предлагают выгодную квартиру и пугают высоким спросом.

На что давят: на дефицит и надежду быстро найти жильё.

К чему ведут: задатку, отправке документов или переводу.

Что делать: проверьте объект, адрес, право сдачи и договор до оплаты.

Работа.

Как выглядит: предлагают вакансию, оформление, обучение или тестовое задание.

На что давят: на надежду, статус и желание быстрее устроиться.

К чему ведут: документам, оплате, установке приложения или выдаче доступа.

Что делать: проверьте работодателя, договор и способ связи.

Инвестиции.

Как выглядит: обещают закрытую возможность и высокую доходность.

На что давят: на жадность, надежду и страх упустить шанс.

К чему ведут: пополнению счёта, криптопереводу или выдаче доступа.

Что делать: проверьте лицензию, риск, порядок вывода средств и независимые источники.

Романтическая переписка.

Как выглядит: быстро создают близость, говорят о кризисе или совместном будущем.

На что давят: на привязанность и чувство вины.

К чему ведут: деньгам, подарочным картам или инвестициям.

Что делать: не отправляйте деньги человеку без проверки личности вне переписки.

Техническая поддержка.

Как выглядит: пугают вирусом, блокировкой, ошибкой или «срочной диагностикой».

На что давят: на панику и зависимость от «специалиста».

К чему ведут: удалённому доступу, оплате или кодам.

Что делать: не давайте удалённый доступ по входящему контакту.

Глава 17. Банковский сценарий: «спасение денег» и безопасный счёт

В атласе обмана этот фрагмент проверяется через источник, канал и действие: чем ярче выгода, тем спокойнее должна быть проверка: документ, источник, полная стоимость и возможность отступить.

Живой разбор приёма

Банковский сценарий — это мошенническая история, где источник имитирует банк, службу безопасности, полицию, регулятора или специалиста и убеждает человека срочно «защитить» деньги, передать код, установить приложение или перевести средства.

Откуда это появилось?

Телефонные и цифровые банковские схемы развивались от простых просьб сообщить данные карты до сложных сценариев с несколькими ролями, поддельными документами, звонками «из банка», «от полиции» и инструкциями по переводу средств.

собеседник соединяет авторитет, страх потери и срочность. Человек не воспринимает перевод или код как отдачу денег, потому что действие упаковано как защита от внешней угрозы.

Страх финансовой потери активирует быструю защитную реакцию. Под давлением угрозы сужается внимание, возрастает зависимость от «инструктора», а проверка откладывается как риск задержки.

Телефонные звонки, SMS, мессенджеры, поддельные страницы банка, письма о блокировке, ложные уведомления о входе, сценарии «безопасного счёта».

Потому что банк воспринимается как авторитетный защитник, а человек в состоянии тревоги пытается выполнить инструкции, чтобы быстро снять угрозу.

Как схема развивается?

Назвать жизненный сценарий: банк, интернет-магазин, покупка, аренда, работа, инвестиции, отношения или техподдержка.

Определить предлог: какая проблема, выгода, угроза или возможность предъявляется.

Выделить ожидаемое действие: деньги, код, доступ, документ, переход, перевод, подпись или личные данные.

Проверить признаки давления: срочность, секретность, запрет остановки, уход из платформы, обход регламента.

Перейти к независимой проверке через официальный сайт, приложение, прежний известный контакт, договор или личный осмотр.

Как опознать

Говорят о подозрительной операции.

Просят не класть трубку.

Требуют код или установку приложения.

Предлагают перевести деньги для защиты.

Запрещают самостоятельно звонить в банк.

Как это выглядит в жизни

Тревожный признак: «безопасный счёт», «код отмены», «служба безопасности», «не кладите трубку», «операция уже идёт», просьба установить удалённый доступ или перевести деньги.

Красный флаг и безопасная проверка

Прекратить входящий контакт. Открыть банк самостоятельно через приложение или позвонить по номеру с карты. Не сообщать коды, не устанавливать программы по инструкции звонящего, не переводить деньги для «защиты».

Настоящий банк может предупреждать о риске, но не должен требовать секретные коды, удалённый доступ или перевод средств на «защитный» счёт.

Звонящий сообщает о кредите, оформленном мошенниками, и просит «отменить» операцию кодом.

Псевдоспециалист службы безопасности убеждает перевести деньги на «резервный счёт».

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. человеку звонят после онлайн-покупки и называют последние цифры карты.

Вывод простой: реальная деталь усиливает доверие, но не доказывает источник.

Ситуация. «следователь» подключается после «банка» и усиливает запрет на разглашение.

Вывод простой: многоэтапный авторитет.

Разберите похожий реальный сценарий по пяти пунктам: предлог, эмоция, действие, канал, проверка.

Сформулируйте безопасную фразу отказа, которая не спорит с историей, но возвращает решение в регламент.

Какой собеседник разыгрывается?

Какое действие, которого добиваются нужно?

Какая проверка через официальный сайт, приложение или уже известный контакт разрушает сценарий?

В банковском сценарии защита проста и жёстка: входящий контакт не управляет деньгами, кодами и устройством.

Глава 18. Торговая площадка и заказ: мелкий платёж как вход к карте

Живой разбор приёма

Сценарий цифровая витрина использует ожидание заказа, трек-номер, изменение адреса, таможенный сбор, оплату хранения или «повторную доставку», чтобы перевести человека на поддельную страницу оплаты или сбора данных.

Откуда это появилось?

Рост интернет-торговли сделал доставку универсальным бытовым контекстом. Мошеннику не нужно знать точный заказ: вероятность, что человек ждёт посылку, достаточно высока, а небольшая сумма снижает бдительность.

Малый платёж кажется неопасным, а ожидание заказа создаёт готовое объяснение. Человек проверяет не источник, а «как быстрее получить заказ».

Ожидание вознаграждения и раздражение от задержки повышают импульсивность. Малый размер платёжа снижает субъективный риск, хотя вводятся полноценные платёжные данные.

SMS, электронная почта, мессенджеры, ссылка в сообщении на уведомлениях, поддельные сайты служб сервис покупки, объявления о «посылке на складе».

Потому что собеседник совпадает с бытовой рутиной и не выглядит как крупное финансовое решение.

Как схема развивается? Как опознать

Сообщают о задержке или невозможности онлайн-сервис.

Просят оплатить небольшой сбор.

Ссылка ведёт на форму карты.

Адрес страницы похож на доставку, но не официальный.

Нет проверки в приложении службы.

Как это выглядит в жизни

Тревожный признак: короткая ссылка, просьба оплатить 1-100 рублей, требование полного номера карты и кода, сообщение о срочной утилизации или возврате заказа.

Красный флаг и безопасная проверка

Открыть приложение или официальный сайт поддержки интернет-магазин вручную. Не вводить карту по ссылке из SMS. Проверить трек-номер в независимом источнике.

Иногда поддержки торговая площадка действительно берут доплаты, но это проверяется только внутри официального личного кабинета или через известный канал.

SMS «заказ не может быть доставлен, оплатите повторную доставку».

Email «обновите адрес цифровая витрина» ведёт на фальшивую форму.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. человек ждёт сервис покупки-заказ и получает SMS с оплатой «хранения».

Вывод простой: совпадение ожидания и ложного предлога.

Ситуация. форма на двери подъезда предлагает «получить посылку».

Вывод простой: скрытый адрес и доверие к месту.

Сценарий онлайн-сервис опасен мелкостью: небольшая сумма служит не целью, а входом к карте и данным.

Глава 19. Интернет-магазин и объявления: уход из безопасной платформы

Обман редко начинается с фразы «я мошенник». Обычно он начинается с обычной детали: уведомления, просьбы, ссылки, имени знакомого или срочного предупреждения. Дальше разберём, где именно появляется давление и какой шаг возвращает вам контроль.

Живой разбор приёма

Сценарий торговая площадка или объявления подталкивает продавца или покупателя уйти из защищённой площадки в сторонний чат, ссылку, фальшивую доставку, поддельную безопасную сделку или внешний платёж.

Откуда это появилось?

С развитием C2C-площадок мошенники стали копиро-

вать интерфейсы безопасной сделки, цифровая витрина, бронирования и оплаты. Главная цель — вынести операцию из среды, где есть правила, арбитраж и контроль платёжа.

Выгода сделки, быстрый покупатель или редкий товар создают страх потерять возможность. Ссылка выглядит как продолжение платформы, хотя фактически переводит человека в контролируемую среду.

Предвкушение сделки и страх упущения ускоряют согласие. Человек сосредотачивается на продаже или покупке, а не на проверке платёжного маршрута.

Авито-подобные площадки, сервисах покупки, чаты, объявления, аренда вещей, онлайн-сервис товаров, поддельные формы оплаты и получения денег.

Потому что сделка кажется уже почти завершённой, и сопротивление платформенному обходу воспринимается как риск сорвать продажу.

Как схема развивается? Как опознать

Покупатель или продавец уводит в мессенджер.

Присылают ссылку на оплату или получение денег.

Говорят, что «так безопаснее»

Просят данные карты для получения платёжа.

Торопят из-за другого покупателя.

Как это выглядит в жизни

Тревожный признак: внешняя ссылка на «безопасную сделку», просьба ввести карту для получения денег, отказ работать через платформу, курьерская легенда вне правил площадки.

Красный флаг и безопасная проверка

Не уходить из платформы для оплаты, интернет-магазин и подтверждения сделки. Проверять правила площадки. Не вводить данные карты на внешней странице.

Общение вне платформы само по себе не всегда мошенничество, но финансовое действие вне регламента резко повышает риск.

Покупатель присылает ссылку «получить оплату».

Продавец редкого товара просит предоплату в мессенджере, потому что «много желающих».

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. продавец получает ссылку на фальшивое получение денег.

Вывод простой: получение платёжа превращено во ввод карты.

Ситуация. покупателя просят оплатить доставку по ссылке вне площадки.

Вывод простой: уход из защищённого круга.

Главная защита на площадках — не переносить деньги и подтверждения в чужой сценарий.

Глава 20. Аренда и недвижимость: выгодный объект до проверки

Во второй книге этот риск рассматривается как место обмана: смотрите не только на слова. Важнее увидеть темп, скрытую цель, цену ошибки и возможность спокойно отказаться.

Живой разбор приёма

Арендный собеседник использует привлекательный объект, низкую цену, срочность, высокий спрос и невозможность полноценного показа, чтобы получить предоплату, документы или персональные данные до проверки.

Откуда это появилось?

Фальшивые объявления об аренде появились вместе с массовыми онлайн-досками. Мошенники копируют реальные фотографии, адреса и описания, меняют цену и контакт, затем давят на быстрый перевод.

собеседник соединяет дефицит, надежду и страх потерять

жильё. Человек начинает конкурировать за объект, который ещё не проверен.

Дефицит жилья и срочность вызывают стрессовую оценку: «если не сейчас, упущу». В этом состоянии предоплата кажется способом закрепить возможность.

Сайты объявлений, соцсети, мессенджеры, окружения аренды, краткосрочная аренда, бронирование комнат и квартир.

Потому что квартира или помещение — значимый ресурс, а выгодная цена создаёт эмоциональное давление быстрее фактической проверки.

Как схема развивается? Как опознать

Цена заметно ниже рынка.
Собственник «в другом городе»
Показ невозможен до оплаты.
Торопят из-за очереди желающих.
Просят перевод, криптовалюту или подарочные карты.

Как это выглядит в жизни

Тревожный признак: предоплата без показа и договора, отказ видеосвязи или документов, слишком хорошая цена, копии фото из других объявлений, давление «забронировать

сейчас».

Красный флаг и безопасная проверка

Проверить адрес, фотографии, право сдачи, договор, личность собственника и возможность осмотра. Не отправлять деньги до базовой проверки объекта и условий.

Иногда бронь действительно применяется, но она должна быть оформлена через проверяемый договор, платформу или юридически понятный порядок.

«Собственник за границей» просит депозит, чтобы снять объявление.

Объект с низкой ценой публикуется в нескольких городах с разными контактами.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. арендатору предлагают скидку за оплату до просмотра.

Вывод простой: цена используется как давление.

Ситуация. фотографии квартиры найдены в старом объявлении другого агентства.

Вывод простой: копирование доверительных материалов.

В аренде защита строится вокруг проверки объекта, права распоряжения и договора до денег.

Глава 21. Работа и HR: вакансия как вход к документам, оплате или доступу

временный пароль часто называют «кодом отмены», «проверкой» или «подтверждением личности». На деле это ключ к вашему доступу. Безопасный шаг — не диктовать коды, пароли и подтверждения во всплывающем уведомлении никому, даже если собеседник представился банком или поддержкой.

Живой разбор приёма

HR-собеседник использует интерес к работе, статус вакансии, удалённое оформление, тестовое задание или обучение, чтобы получить документы, деньги, доступ к аккаунтам, установить приложение или вовлечь человека в незаконные действия.

Откуда это появилось?

Удалённая работа, фриланс и цифровой найм расширили возможности поддельных вакансий. Сценарии стали включать фальшивые HR-профили, собеседования, тесты, «обучение», оплату оборудования и крипто/платёжные операции.

Надежда на доход и статус снижает критичность. Кандидат находится в роли просителя и чаще выполняет инструкции работодателя, чтобы не потерять шанс.

Ожидание вознаграждения усиливает мотивацию к сотрудничеству. Авторитет работодателя и страх потерять возможность делают нетипичные требования менее заметными.

Сайты вакансий, мессенджеры, соцсети, электронная почта, фриланс-площадки, удалённое оформление, «международные компании», поддельные рекрутеры.

Потому что трудоустройство уже предполагает передачу данных и выполнение заданий; мошенник расширяет эту норму за безопасные пределы.

Как схема развивается? Как опознать

Предлагают высокую оплату без проверки квалификации.
Просят оплатить обучение или оборудование.
Требуют документы до договора.
Дают странные финансовые поручения.
Просят установить неизвестное приложение.

Как это выглядит в жизни

Тревожный признак: предоплата за работу, просьба принять/перевести деньги, оформление через личный аккаунт,

отсутствие юридического лица, давление срочно подписать или отправить документы.

Красный флаг и безопасная проверка

Проверять работодателя, домен, юридические данные, договор, реальные контакты и характер задачи. Не платить за трудоустройство и не выполнять финансовые операции для неизвестной компании.

Некоторые работодатели действительно собирают документы, но только после понятного процесса, договора и проверяемой идентичности организации.

«Работодатель» просит оплатить доступ к обучению перед началом работы.

Кандидату предлагают принимать платёжи клиентов на личную карту.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. удалённая вакансия обещает высокий доход за пересылку денег.

Вывод простой: возможное вовлечение в обналичивание.

Ситуация. рекрутер просит паспорт до собеседования.

Вывод простой: преждевременный сбор данных.

Вакансия не отменяет личную безопасность: документы, деньги и доступ передаются только после проверки работодателя и договора.

Глава 22. Инвестиции и быстрый доход: гарантированная прибыль как наживка

Живой разбор приёма

Инвестиционный собеседник обещает высокую или гарантированную доходность, закрытый доступ, инсайдерскую возможность, быстрый вывод прибыли, криптовалютную схему или «наставника», чтобы получить перевод и удержать человека в цепочке пополнений.

Откуда это появилось?

Инвестиционные мошенничества эволюционировали от финансовых пирамид и псевдоброкеров к криптосхемам, поддельным приложениям, соцсетевым «экспертам», романтическо-инвестиционным сценариям и имитации лицензированных платформ.

собеседник использует надежду, жадность, FOMO и социальное доказательство. Маленькая начальная «прибыль» может служить ценовой зацепкой доверия и подготовкой к крупному пополнению.

Ожидание выигрыша активирует систему вознаграждения. Когда человек уже вложил деньги, эскалация обяза-

тельств мешает остановиться и признать риск.

Соцсети, мессенджеры, поддельные брокеры, криптоплатформы, инвестиционные клубы, каналы сигналов, романтические переписки, фальшивые приложения.

Потому что обещание контроля над будущим и быстрый рост денег перекрывают проверку лицензий, рисков и механики вывода.

Как схема развивается? Как опознать

Обещают гарантированную высокую доходность.
Торопят войти до роста.
Демонстрируют чужие успехи.
Вывод прибыли затруднён комиссиями.
Просят пополнить ещё для разблокировки.

Как это выглядит в жизни

Тревожный признак: гарантия прибыли, отсутствие лицензии, криптопереводы неизвестным лицам, «налог/комиссия для вывода», давление наставника, запрет сомнений.

Красный флаг и безопасная проверка

Проверить лицензию, юридическое лицо, регуляторный статус, условия вывода, риск потери и независимые отзывы.

Не переводить деньги на личные кошельки и не увеличивать взнос ради «разблокировки».

Реальные инвестиции тоже несут риск. Ключевое отличие мошеннического сценария — обещание гарантии, непрозрачность и давление на пополнение.

«Брокер» показывает рост баланса, но требует оплатить налог до вывода.

«Наставник» в мессенджере предлагает закрытую криптостратегию.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. первая маленькая выплата убеждает вложить больше.

Вывод простой: демонстрационная прибыль как доверительный крючок.

Ситуация. вывод блокируется до нового платёжа.

Вывод простой: эскалация потерь.

В инвестиционных сценариях Если оставить одну мысль, то высокая гарантированная прибыль и невозможность свободного вывода — не возможность, а красный флаг.

Глава 23. Романтическая переписка: близость, доверие и денежная просьба

Собеседник кажется «своим»: понимает, улыбается, говорит похожими словами. Симпатия снижает проверку усло-

вий. Безопасный шаг — оценивать предложение отдельно от человека, который его подаёт.

Живой разбор приёма

Романтический собеседник строит эмоциональную близость и доверие через переписку, затем вводит кризис, совместное будущее, инвестиционную возможность или просьбу о деньгах.

Откуда это появилось?

Онлайн-знакомства и соцсети сделали романтические схемы масштабируемыми. Сценарии могут длиться недели и месяцы, использовать фото, голос, видеозаписи, подарки, обещания встречи и постепенное вовлечение в финансовые действия.

Доверие создаётся не аргументами, а регулярным вниманием, признанием, интимностью и обещанием уникальной связи. Денежная просьба появляется как тест заботы или шаг к совместному будущему.

Эмоциональная привязанность снижает критичность к противоречиям. Страх потерять связь и желание помочь активируют уступчивость даже при отсутствии офлайн-проверки личности.

Сайты знакомств, соцсети, мессенджеры, игровые сообщества, международные переписки, романтическо-инвести-

ционные схемы.

Потому что человек принимает решение не в режиме сделки, а в режиме отношений, где отказ воспринимается как холодность или предательство.

Как схема развивается? Как опознать

Быстрое усиление близости.
Откладывание реальной встречи.
История кризиса.
Просьба о деньгах, подарочных картах или крипто.
Перевод в инвестиции или «совместный проект»

Как это выглядит в жизни

Тревожный признак: просьба денег от человека, которого вы не встречали; невозможность видео/встречи; драматические препятствия; секретность; инвестиционный совет от романтического контакта.

Красный флаг и безопасная проверка

Не отправлять деньги и не инвестировать по просьбе онлайн-партнёра без проверки через официальный сайт, приложение или уже известный контакт личности и истории. Обсудить ситуацию с внешним человеком, не вовлечённым

эмоционально.

Настоящие отношения тоже включают помощь, но финансовая помощь без проверенной личности и офлайн-контекста это зоной высокого риска.

Онлайн-партнёр просит оплатить билет, но встреча постоянно срывается.

После недель переписки человек предлагает «семейную» инвестицию в криптовалюту.

обязательство- Ситуация: просьба о деньгах оформлена как доказательство любви.

Вывод простой: чувство превращено в обязательство.

Ситуация. романтический контакт ведёт на инвестиционную платформу.

Вывод простой: смесь близости и финансовой наживки.

Романтический такая схема опасна тем, что финансовое действие маскируется под эмоциональную верность.

Глава 24. Техническая поддержка: вирус, удалённый доступ и платное спасение

Живой разбор приёма

Сценарий техподдержки убеждает человека, что устройство заражено, аккаунт заблокирован, данные под угрозой

или нужно срочная диагностика, после чего просит удалённый доступ, оплату, код или установку программы.

Откуда это появилось?

Технические мошенничества начались с холодных звонков и всплывающих предупреждений, затем расширились через поисковую рекламу, поддельные сайты поддержки, звонки от «Microsoft/Apple/оператора/банка» и удалённые инструменты.

собеседник использует техническую неопределённость: человек не может быстро оценить проблему и передаёт контроль «специалисту». Паника и непонимание делают инструкции авторитетными.

Техническая тревога вызывает зависимость от внешнего эксперта. Чем непонятнее проблема, тем сильнее стремление быстро передать управление тому, кто говорит уверенно.

Всплывающие окна, поисковые объявления поддержки, входящие звонки, мессенджеры, удалённый доступ, поддельные страницы антивируса или системной ошибки.

Потому что человек хочет сохранить устройство и данные, но не знает, как отличить реальную ошибку от театра угрозы.

Как схема развивается? Как опознать

Экран блокируется предупреждением.

Дают номер «поддержки»

Просят установить удалённый доступ.

Показывают обычные системные события как доказательство вируса.

Требуют оплату немедленно.

Как это выглядит в жизни

Тревожный признак: входящий «специалист», удалённый доступ без вашей заявки, требование кодов, угроза потери данных, оплата подарочными картами/крипто/переводом.

Красный флаг и безопасная проверка

Не звонить по номеру из всплывающего окна. Не давать удалённый доступ по входящему контакту. Закрыть страницу, отключить сеть при нужности, обратиться в официальную поддержку или к доверенному специалисту.

Реальная поддержка может использовать удалённый доступ, но только после вашей инициативы, через проверенный канал и с понятным ограничением прав.

В браузере появляется окно «ваш компьютер заражён, по-

звоните срочно».

Звонящий «из поддержки» просит установить AnyDesk/TeamViewer.

Дальше важно увидеть не саму легенду, а действие, к которому вас подводят.

Ситуация. мошенник показывает журнал событий Windows как доказательство взлома.

Вывод простой: поток непонятных технических слов превращён в угрозу.

Ситуация. «поддержка» просит код из приложения-аутентификатора для восстановления.

Вывод простой: код — это доступ, а не диагностикой.

В техподдержке базовое правило: удалённый доступ и коды не передаются по сценарию, который начался не с вашей проверенной заявки.

Блок кейсов раздела 3

Ситуация 1. «Банк» сообщает, что на имя клиента оформляют кредит.

Вывод простой: страх долга и ложная срочность; защита — завершить звонок и проверить банк самостоятельно.

изоляция- Ситуация 2. «Сотрудник полиции» запрещает рассказывать родственникам.

Вывод простой: секретность как изоляция; защита — не выполнять инструкции и обращаться в официальный орган самостоятельно.

Ситуация 3. сообщение от торговая площадка просит под-

твердить возврат по ссылке.

Вывод простой: малый платёж как вход к карте; защита — открыть заказ внутри официального приложения цифровая витрина.

Ситуация 4. Покупатель на площадке присылает ссылку «получить деньги».

Вывод простой: подмена получения платёжа вводом карты; защита — не уходить из платформы.

Ситуация 5. Продавец редкого товара требует предоплату, потому что «через час заберут».

Вывод простой: дефицит и FOMO; защита — безопасная сделка по правилам площадки.

Ситуация 6. Арендодатель просит депозит до просмотра квартиры.

Вывод простой: выгодная цена и высокий спрос; защита — осмотр, документы, договор.

Ситуация 7. Фото квартиры найдено на другом сайте с другой ценой.

Вывод простой: копирование доверительного материала; защита — обратный поиск и проверка адреса.

Ситуация 8. Вакансия обещает высокий доход без опыта и просит оплатить обучение.

Вывод простой: надежда и предоплата; защита — не платить за трудоустройство.

Ситуация 9. Работодатель просит принять деньги на личную карту.

Вывод простой: риск вовлечения в незаконную операцию; защита — отказ и проверка компании.

Ситуация 10. «Брокер» показывает рост баланса, но не даёт вывести деньги без комиссии.

Вывод простой: эскалация обязательств; защита — не пополнять ради разблокировки.

Ситуация 11. Инвестиционный наставник просит перейти в закрытый чат.

Вывод простой: изоляция от внешней проверки; защита — проверка через официальный сайт, приложение или уже известный контакт лицензии и условий.

Ситуация 12. Онлайн-партнёр просит деньги на билет.

Вывод простой: близость и кризис; защита — не отправлять деньги без проверки личности.

Ситуация 13. Романтический контакт предлагает криптоинвестиции.

Вывод простой: pig-butchering-сценарий; защита — разделить отношения и финансовые действия.

Ситуация 14. В браузере появляется окно «компьютер заражён».

Вывод простой: техническая паника; защита — не звонить по номеру в окне.

Ситуация 15. «Техподдержка» просит удалённый доступ.

Вывод простой: передача контроля; защита — не устанавливать инструменты по входящему контакту.

Ситуация 16. «Госорган» сообщает о компенсации и про-

сит оплатить комиссию.

Вывод простой: приз плюс плата; защита — официальная проверка через сайт органа.

Ситуация 17. Курьер просит код подтверждения по телефону.

Вывод простой: код как доступ; защита — коды не сообщаются внешним лицам.

Ситуация 18. HR отправляет файл «тестового задания» с макросами.

Вывод простой: вакансия как предлог для файла; защита — не открывать рискованные вложения.

Ситуация 19. «Служба безопасности» просит установить приложение для защиты.

Вывод простой: защита подменена удалённым доступом; защита — официальный сайт, приложение или уже известный контакт банка.

Ситуация 20. Арендодатель отказывается показывать объект и просит криптоперевод.

Вывод простой: невозможность возврата и проверки; защита — не платить.

Блок упражнений раздела 3

Составьте таблицу из восьми сценариев раздела и впишите для каждого: предлог, эмоцию, действие, проверку.

Разберите одно подозрительное сообщение о банке по схеме: кто пишет, что требует, почему срочно, как проверить.

Сформулируйте личное правило: какие действия с бан-

ком вы никогда не выполняете по входящему звонку.

Опишите безопасный маршрут проверки сервис покупки без перехода по SMS-ссылке.

Составьте правило для онлайн-сервисах: когда нельзя уходить в мессенджер и что нельзя вводить по внешней ссылке.

Создайте чек-лист проверки аренды: адрес, собственник, документы, показ, договор, платёжный маршрут.

Проверьте любую вакансию по признакам риска: предоплата, слишком высокая оплата, странные финансовые действия, документы до договора.

Разберите инвестиционное предложение: лицензия, риск, вывод, гарантии, кто получает деньги, где хранятся средства.

Сформулируйте фразу для романтического контакта: «финансовые вопросы я не обсуждаю до личной проверки личности».

Опишите порядок действий при всплывающем окне «ваш компьютер заражён», не переходя к номеру из этого окна.

Блок быстрой проверки раздела 3

Почему жизненный сценарий опаснее отдельного канала?

Какие признаки банковского сценария являются сигнала остановкими?

Почему «безопасный счёт» это красным флагом?

Почему малый платёж по внешней ссылке может быть опасен?

Что означает уход из платформы в интернет-мага-

зин-сделке?

Почему слишком выгодная аренда требует усиленной проверки?

Какие документы и действия нельзя передавать до проверки работодателя?

Чем инвестиционное мошенничество отличается от обычного инвестиционного риска?

Почему «гарантированная доходность» опасна?

Как романтическая близость превращается в финансовое обязательство?

Почему просьба денег от онлайн-партнёра это высоким риском?

Что нельзя делать при входящем контакте «техподдержки»?

Почему удалённый доступ опаснее устной консультации?

Какой официальный источник или уже известный контакт использовать для проверки банка?

Как проверить заказ без ссылки из сообщения?

Как проверить аренду до предоплаты?

Какие признаки указывают на поддельную вакансию?

Почему комиссия для вывода инвестиционной прибыли это красным флагом?

Красный флаг и безопасная проверка, если мошеннический сценарий уже начался и вы успели вовлечься?

Какая универсальная фраза возвращает любой сценарий в безопасную проверку?

Чек-лист сценарной защиты

Я называю сценарий до действия: банк, торговая площадка, покупка, аренда, работа, инвестиции, отношения или техподдержка.

Я ищу ожидаемое действие: деньги, код, доступ, документ, ссылка, перевод, подпись или данные.

Я считаю срочность поводом остановиться, а не ускориться.

Я не использую контакты, ссылки и номера, присланные в подозрительном сообщении, для проверки этого же сообщения.

Я не перевожу деньги для «защиты», «разблокировки», «вывода прибыли» или «брони» без проверки через официальный сайт, приложение или уже известный контакт.

Я не сообщаю коды, пароли, данные карты, seed-фразы и не даю удалённый доступ по входящему контакту.

Я не ухожу из безопасной платформы в сторонний чат для оплаты или подтверждения сделки.

Я не плачу за трудоустройство и не выполняю финансовые поручения неизвестного работодателя.

Я не отправляю деньги человеку из романтической переписки без реальной проверки личности.

Я фиксирую правило заранее: важные решения проходят время на проверку, документ и официальный источник или уже известный контакт.

Защитные формулы раздела 3

«Я не решаю банковские вопросы по входящему звонку. Проверю через приложение или номер с карты».

«Я не ввожу карту по ссылке из сообщения. Открою заказ в официальном приложении».

«Оплата и цифровая витрина остаются внутри платформы. Внешние ссылки не использую».

«До осмотра, договора и проверки документов предоплату не перевожу».

«За трудоустройство я не плачу и финансовые операции через личные счета не выполняю».

«Гарантированную доходность и вывод через дополнительный платёж я не рассматриваю».

«Финансовую помощь в онлайн-отношениях я не оказываю до проверки через официальный сайт, приложение или уже известный контакт личности и ситуации».

«Удалённый доступ по входящему звонку или всплывающему окну я не предоставляю».

«Если запрос срочный, он требует не скорости, а проверки».

«Пришлите официальный запрос по проверяемому каналу, я вернусь после анализа».

Дополнение к мини-глоссарию

Банковский сценарий: мошенническая история о защите денег, подозрительной операции, кредите или «безопасном счёте».

Безопасный счёт: ложная конструкция, где перевод денег

мошеннику представляется как защита средств.

Сценарий сервис покупки: мошенничество вокруг заказа, трек-номера, сбора, адреса или повторной онлайн-сервис.

Уход из платформы: перенос сделки из защищённой среды интернет-магазин в сторонний чат, ссылку или платёжный маршрут.

Арендная приманка: слишком выгодный объект или бронь, используемые для получения предоплаты до проверки.

Поддельная вакансия: рабочий сценарий, где кандидат платит, раскрывает лишние данные или выполняет рискованные действия.

Инвестиционная ловушка: обещание высокой или гарантированной прибыли с непрозрачным выводом средств.

Романтическое мошенничество: построение близости и доверия для финансовой просьбы или инвестиционного вовлечения.

Техподдержка-мошенничество: сценарий технической угрозы, ведущий к удалённому доступу, оплате, кодам или краже данных.

Разбор ситуации по шагам: проверка не отдельной фразы, а всей истории, роли источника, чувства, требуемого действия и способа проверки.

Источники и опорные материалы

FTC Consumer Advice. Как избегать обмана с подставным лицом: не переходить по ссылкам и не звонить по номерам из

неожиданных сообщений; проверять историю через заранее известные контакты.

FTC Consumer Advice. Как избегать мошенничества: типовой собеседник включает подмену личности, проблему или приз, давление срочностью и требование конкретного перевода или действия.

FTC Consumer Advice. Мошенничество с арендой: поддельные объявления могут обещать низкую цену, отличные условия, недоступного владельца и требование перевести деньги до осмотра жилья.

FTC Consumer Advice. Спам-SMS и фишинг: поддельные сообщения пытаются выманить пароли, номера счетов и другие личные данные.

FBI. Рекомендации по подмене деловой переписки: проверять платёжные и закупочные запросы лично или по известному номеру; отдельно подтверждать изменения реквизитов.

FBI. Романтическое мошенничество: преступники используют поддельные онлайн-личности, входят в доверие, затем манипулируют жертвой и просят деньги.

CISA. Предотвращение социальной инженерии и фишинга: атаки маскируются под доверенные источники и используют привычные каналы связи.

NIST SP 800-63B-4 и NIST Phish Scale: устойчивые к фишингу способы входа и сложность распознавания фишинга важны для защиты аккаунтов и учётных данных.

USPIS. Мошенническое SMS: Мошеннические сообщения о доставке: SMS о посылках могут вести на поддельные ссылки.

CFTC. Рекомендации по романтическому и инвестиционному мошенничеству: романтические и инвестиционные легенды могут сочетаться через приложения знакомств, соцсети и обещания цифровых активов.

Что будет дальше

Дальнейшая логика Части I переходит от бытовых сценариев к многошаговым мошенническим цепочкам: первичный контакт, прогрев доверия, подтверждающая роль второго лица, перенос в закрытый канал, тестовое действие, эскалация суммы, удержание жертвы и постфактум-додавливание. Задача раздела — показать, как отдельные техники объединяются в последовательную операцию и где эту операцию можно разорвать минимальным безопасным действием.

Раздел 4. Многошаговые мошеннические цепочки: прогрев, подтверждение, захват действия и вывод

Назначение раздела — показать социальную инженерию не как отдельную подозрительную фразу, а как цепочку последовательных шагов. В реальном мошенническом сценарии опасность часто возникает не в первом сообщении, а в накоплении доверия, вторичных подтверждений, срочности, контролируемого канала, подмены проверки и постепенно сужающегося выбора.

Практическая задача раздела — научиться разрывать цепочку на раннем этапе: до передачи денег, кодов, документов, доступа к устройству, данных карты, учётных записей, криптовалюты, реквизитов или корпоративной информации.

Ключевое правило раздела: мошенническая цепочка опасна не отдельным звеном, а тем, что каждое следующее звено делает предыдущее психологически «разумным». Поэтому защитный анализ должен проверять не только сообщение, но и путь, по которому человека ведут.

Как проверить ситуацию

Первичный контакт. Атакующий собеседник действует так: Создаёт повод для внимания: проблема, выгода, статус, просьба, угроза. Опасность — Человек вступает в общение без проверки источника. Защитный разрыв: Не переходить к действию; определить, кто пишет и чего хочет.

Прогрев доверия. Атакующий собеседник действует так: Добавляет детали, имена, документы, эмоции, «узнаваемые» элементы. Опасность — Детализация принимается за доказательство подлинности. Защитный разрыв: Проверять не подробность, а независимые подтверждения.

Вторичное подтверждение. Атакующий собеседник действует так: Вводит другого человека, сайт, чат, письмо, номер или «специалиста». Опасность — Ложная проверка внутри той же схемы воспринимается как безопасность. Защитный разрыв: Проверять через канал, выбранный самим человеком.

Захват действия. Атакующий собеседник действует так: Подводит к переводу, коду, установке, подписи, входу или раскрытию данных. Опасность — Психологический фокус смещается с проверки на выполнение инструкции. Защитный разрыв: Назвать действие, которого добиваются и остановить сценарий.

Закрепление. Атакующий собеседник действует так: До-

бивается необратимого действия и удерживает человека от обращения за помощью. Опасность — Потеря денег, доступа, аккаунта, документов или времени. Защитный разрыв: Фиксация фактов, блокировка каналов, обращение в официальные службы.

Глава 25. Первичный крючок: проблема, выгода или тревожный сигнал

Для темы «Первичный крючок: проблема, выгода или тревожный сигнал» главный тест простой: что произойдёт, если вы не ответите сразу? Если пауза на проверку вызывает злость, угрозы или запрет на проверку, перед вами уже не объяснение, а давление.

Живой разбор приёма

Первичный крючок — это первый элемент цепочки, который заставляет человека обратить внимание и вступить в контакт: сообщение о проблеме, обещание выгоды, срочное уведомление, просьба о помощи, угроза потери или статусное обращение.

Откуда это появилось?

Крючок возник задолго до цифровых каналов: в уличном

мошенничестве, поддельных письмах, телефонных сценариях и коммерческом давлении. В цифровой среде он стал масштабируемым: одно и то же сообщение может быть отправлено тысячам людей, а персонализированная версия используется против конкретной цели.

Механизм строится на ориентировочном рефлексе: человек автоматически выделяет сигнал, который связан с угрозой, деньгами, статусом, близкими людьми или личной выгодой. Если крючок попадает в текущую тревогу человека, критическое мышление включается позже, чем эмоциональная реакция.

Угрожающие и значимые стимулы быстрее захватывают внимание через системы оценки значимости, включая миндалевидное тело, островковую кору и сети внимания. Это не означает полного отключения разума, но снижает качество первой оценки и ускоряет готовность отвечать.

Email, SMS, звонки, мессенджеры, соцсети, объявления, поддельные уведомления банков, сервисов торговая площадка, цифровых витринах, госорганов, работодателей и технической поддержки.

Крючок работает, потому что человек сначала реагирует на смысл «что-то произошло», а уже потом проверяет источник. Особенно опасны крючки, совпадающие с реальными ожиданиями: человек ждёт посылку, оплату, звонок, ответ по вакансии или банковскую операцию.

Как схема развивается?

Выбрать тему, которая вероятна для человека.

Сформулировать событие: проблема, шанс, ошибка, долг, блокировка, выигрыш или просьба.

Добавить элемент срочности или значимости.

Перевести человека в ответ, клик, звонок или чат.

Не дать ему выйти в независимую проверку.

Признаки применения и тревожные признаки

Сообщение пришло неожиданно.

Источник требует быстрый ответ.

Есть ссылка, номер или вложение внутри сообщения.

Тема вызывает страх, жадность, вину или сильное любопытство.

Проверка предлагается через тот же канал.

Красный флаг и безопасная проверка

Назвать крючок вслух: «Меня сейчас вводят в контакт через тему X». Затем не отвечать по присланному маршруту, а самостоятельно открыть официальный сайт, приложение, договор, личный кабинет или известный номер.

Не каждый неожиданный контакт является мошенничеством. Но любое неожиданное сообщение с требованием действия должно считаться непроверенным до подтверждения по независимому каналу.

SMS о посылке с требованием оплатить маленький сбор.

Письмо «службы безопасности» о подозрительной операции.

Сообщение от якобы знакомого с просьбой срочно занять денег.

Кейсы для самостоятельного разбора

Для этой главы используйте общий раздел с кейсами раздела 4 ниже: определите звено цепочки, ожидаемое действие, эмоциональный рычаг и безопасный разрыв.

Практические упражнения по технике включены в общий блок упражнений раздела 4. При выполнении обязательно фиксируйте, на каком звене цепочки возник риск.

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Первичный крючок не нужно «разгадывать». Его нужно остановить: пока источник не проверен, действие не выполняется.

Глава 26. Прогрев доверия через детали, совпадения и псевдодостоверность

Здесь важно увидеть точку входа в обман: смотрите не только на слова. Важнее увидеть темп, скрытую цель, цену ошибки и возможность спокойно отказаться.

Живой разбор приёма

Прогрев доверия — это накопление деталей, которые создают ощущение подлинности: имя, город, номер заказа, должность, логотип, фрагмент реального события, документы, скриншоты, корпоративный стиль или знание контекста.

Откуда это появилось?

В классических мошеннических схемах доверие строилось через одежду, речь и документы. В цифровой среде его создают скопированные шаблоны писем, домены, логотипы, утечки данных, открытые профили, данные из объявлений и массовая персонализация.

Человек склонен принимать подробность за достоверность. Если сообщение содержит реальные элементы его жизни, возникает ошибка: «раз они это знают, значит, источник настоящий». На самом деле знание части информации не доказывает право требовать действие.

Детали снижают неопределённость и создают ощущение знакомой, связной истории: человеку проще поверить рассказу, чем остановиться и проверить каждую часть. Чем лучше история «ложится» на ожидания, тем меньше сопротивление.

подмена деловой переписки, поддельные письма от руководителя, фальшивые вакансии, аренда, сервисах покупки,

романтические сценарии, банковские звонки, псевдоюридические и псевдогосударственные обращения.

Прогрев работает, потому что человеку трудно отделить подлинность отдельных деталей от подлинности всего сценария. Реальный номер заказа не делает ссылку безопасной; имя руководителя не доказывает письмо; логотип банка не подтверждает звонок.

Как схема развивается?

Собрать доступные детали о цели или ситуации.

Встроить их в правдоподобную историю.

Добавить визуальные или статусные маркеры.

Добиться, чтобы человек сам достроил недостающую достоверность.

Перейти к нужному действию после снижения настороженности.

Признаки применения и тревожные признаки

Источник знает некоторые детали, но требует непривычное действие.

Детали используются как замена официальной проверке.

Документы представлены картинками, скриншотами или ссылками без независимой проверки.

История становится всё более убедительной, но проверяемый канал не появляется.

Возникает мысль: «слишком много деталей, чтобы быть

обманом».

Красный флаг и безопасная проверка

Разделить «деталь верна» и «запрос законен». Проверять полномочия, канал, реквизиты и действие отдельно, а не принимать всю историю пакетом.

Подробность может быть нормальной частью настоящий процесса. Риск возникает там, где подробность подталкивает к действию без проверки через официальный сайт, приложение или уже известный контакт.

Письмо с именем реального поставщика и срочной просьбой оплатить счёт по новым реквизитам.

Звонок с упоминанием последних цифр карты.

Арендодатель присылает «паспорт» и видео квартиры, но требует бронь до просмотра.

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Детали повышают правдоподобие, но не доказывают законность. Защита проверяет полномочия, а не впечатление.

Глава 27. Ложное вторичное подтверждение

Мошеннику не нужно, чтобы вы поверили во всё. Ему до-

статочно, чтобы вы поверили на несколько минут — до кода, перевода, файла или подписи. Дальше разберём, где именно появляется давление и какой шаг возвращает вам контроль.

Живой разбор приёма

Ложное вторичное подтверждение — это создание дополнительного «источника», который якобы подтверждает первый: второй звонок, другой сотрудник, чат поддержки, сайт проверки, поддельный договор, «юрист», «служба безопасности» или «гарант сделки».

Откуда это появилось?

Многоступенчатые мошеннические схемы давно используют сообщников. В цифровом виде роль сообщника может выполнять другой аккаунт, поддельный сайт, бот, письмо с похожего домена, фальшивый отзыв или имитация официального интерфейса.

Человек успокаивается, когда получает подтверждение из «ещё одного места». Ошибка возникает, если второе место контролируется тем же сценарием. Психологически это выглядит как проверка, но фактически остаётся внутри ловушки.

Подтверждение снижает тревогу и уменьшает потребность в дополнительном анализе. Социальное доказательство и авторитет второго источника создают ощущение за-

вершённой проверки.

Поддельные сайты оплаты, фальшивые гаранты сделок, «второй специалист поддержки», чат поддержки, поддельные отзывы, фейковые страницы онлайн-сервис, техническая поддержка, инвестиционные платформы.

Ложное подтверждение работает, потому что человек путает количество сигналов с независимостью сигналов. Два источника не являются двумя источниками, если оба пришли из одного сценария.

Как схема развивается?

Создать первый контакт.

Предложить «проверку» через удобный канал.

Подключить вторую роль или интерфейс.

Подтвердить историю первого источника.

Использовать ощущение безопасности для получения действия.

Признаки применения и тревожные признаки

Второй источник предложен первым источником.

Проверка ведёт на присланный сайт, номер, чат или короткая ссылка.

У второго источника тот же стиль речи, срочность или цель.

Нельзя самостоятельно выбрать официальный сайт, приложение или уже известный контакт.

После подтверждения сразу требуют действие.

Красный флаг и безопасная проверка

Правило: проверка должна быть независимой не по форме, а по происхождению. Человек сам выбирает сайт, номер, приложение, контакт в договоре или офлайн-встречу.

В реальных процессах могут быть несколько сотрудников и каналов. Но если все маршруты проверки даёт инициатор контакта, независимости нет.

Звонящий переключает на «специалиста ЦБ».

Продавец на интернет-магазин даёт ссылку на «безопасную доставку».

Инвестплатформа показывает «проверенный» кабинет и чат аналитика.

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Проверка внутри сценария не является проверкой. Защита строится на независимом канале, выбранном самим человеком.

Глава 28. Докумысленный и технический предлог

Живой разбор приёма

Докумысленный или технический предлог — это объяснение, почему нужно подписать, скачать, установить, подтвердить, перейти, открыть файл, назвать код, предоставить доступ или загрузить документ.

Откуда это появилось?

Раньше технический предлог был связан с бумажными бланками и физическим доступом. Сейчас он часто принимает вид PDF, архива, формы входа, обновления, удалённой поддержки, облачной ссылки, поддельная кнопка оплаты, проверки личности или электронного договора.

Документ и техническая процедура создают ощущение формальности. Человек начинает воспринимать действие как часть процесса, а не как самостоятельный риск. Особенно опасны слова «стандартно», «для безопасности», «для подтверждения», «для закрытия заявки».

Формальные процедуры снижают эмоциональную настороженность и переводят внимание в исполнительный режим:

человек лучше шагам, а не пересматривает цель.

Вакансии, аренда, банковские сценарии, инвестиции, торговых площадках, техподдержка, корпоративные процессы, псевдогосуслуги, цифровая витрина и возвраты.

Предлог работает, потому что настоящий организации действительно используют документы и технические процедуры. Мошенническая схема копирует форму процесса, но меняет цель действия.

Как схема развивается?

Сформировать правдоподобную необходимость.

Назвать действие техническим или докувнутренным.

Снизить значимость риска: «это просто подтверждение».

Провести человека через шаги.

Получить данные, доступ, подпись, платёж или установку.

Признаки применения и тревожные признаки

Вас просят открыть файл или ссылку из неожиданного сообщения.

Просят установить программу удалённого доступа.

Код подтверждения в почте называют «отменой», «проверкой» или «защитой».

Документ нельзя проверить через официальный кабинет.

Процесс требует данных, которые нормальная организация не запрашивает в таком канале.

Красный флаг и безопасная проверка

Любое техническое действие переводится в вопрос: «Что именно изменится после этого шага?» Если ответ неясен, действие не выполняется. Документы проверяются через официальный сайт, кабинет, юриста, банк или известный контакт.

Многие реальные процессы требуют документов. Защитный критерий — не наличие документа, а происхождение канала, необходимость этих данных и обратимость действия.

«Для возврата денег установите приложение поддержки».

«Для договора аренды пришлите фото паспорта и предоплату».

«Для вывода прибыли пройдите проверку по ссылке».

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Докупсихологическая форма не равна безопасности. Технический шаг нужно проверять как отдельное действие с отдельным риском.

Глава 29. Платёжная развязка и необратимый маршрут

Живой разбор приёма

Платёжная развязка — это этап, где собеседник переводит доверие, тревогу или обязательство в денежное действие: перевод, предоплату, комиссию, криптовалюту, подарочную карту, ссылка-платёж, оплату сервис покупки, «налог», «страховой депозит» или «безопасный счёт».

Откуда это появилось?

Денежные развязки существовали в любых схемах обмана, но цифровые платёжи увеличили скорость и необратимость. Появились сценарии с криптовалютой, gift cards, мгновенными переводами, платёжными ссылками, форма оплаты и поддельными посредниками.

К моменту оплаты человек уже эмоционально вложен в сценарий. Он хочет завершить процесс, избежать потери, вернуть доступ, спасти деньги, закрепить выгоду или не выглядеть подозрительным. Это создаёт эффект «последнего шага».

Страх потери и ожидание выгоды усиливают импульсив-

ность. Системы вознаграждения и угрозы конкурируют с рациональной оценкой, особенно если введён дедлайн.

Инвестиционные схемы, аренда, онлайн-сервисах, интернет-магазин, романтические просьбы, подмена деловой переписки, техподдержка, криптовалютные сценарии, поддельные штрафы, гос- и банковские имитации.

Развязка работает, потому что платёж подаётся не как риск, а как способ решить уже созданную проблему. Мошенник продаёт не услугу, а снятие тревоги.

Как схема развивается?

Создать проблему, шанс или обязательство.

Подвести к «последнему» платёжному шагу.

Объяснить необычный способ оплаты срочностью или безопасностью.

Попросить не обсуждать и не задерживать действие.

После оплаты требовать новый платёж или исчезнуть.

Признаки применения и тревожные признаки

Просят оплатить gift cards, криптовалютой, переводом частному лицу или через непроверенную ссылку.

Требуют «комиссию для вывода прибыли».

Предоплата нужна до просмотра, договора или проверки.

Деньги якобы переводятся для защиты денег.

Способ оплаты необычен для заявленной организации.

Красный флаг и безопасная проверка

Правило: необычный способ оплаты — самостоятельный красный флаг. Перед платёжом нужно ответить на пять вопросов: кому, за что, по какому договору, как вернуть, через какой официальный сайт, приложение или уже известный контакт подтверждено.

Некоторые настоящий платёжи тоже могут быть срочными. Но настоящий получатель не запрещает проверку и не требует скрытности.

«Комиссия для вывода прибыли» на инвестиционной платформе.

«Страховой депозит» за квартиру до просмотра.

«Покупка криптовалюты в банкомате для защиты счёта».

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Деньги нельзя переводить для снятия тревоги. Деньги переводятся только после проверки получателя, основания, договора и обратимости.

Глава 30. Захват учётной записи и обход защиты через человека

Для карты мошеннических сценариев это звучит так:

смотрите не только на слова. Важнее увидеть темп, скрытую цель, цену ошибки и возможность спокойно отказаться.

Живой разбор приёма

Захват учётной записи — это сценарий, где человека подводят к раскрытию пароля, кода, ссылки входа, подтверждения во всплывающем уведомлении, токена, seed-фразы, данных восстановления или к установке программы, позволяющей получить контроль.

Откуда это появилось?

Сначала фишинг был массовым сбором логинов и паролей. Затем схемы стали обходить многофакторную защиту через человека: поддельные формы, просьбы подтвердить вход, социальное давление, SIM-сценарии, удалённый доступ и перехват восстановления.

Человек часто воспринимает код как «подтверждение разговора», а не как ключ к доступу. В всплывающие уведомлениях работает усталость и желание убрать раздражающий запрос. В техподдержке — доверие к инструкции.

При срочности исполнительный контроль сужается до выполнения ближайшего шага. Если источник выглядит авторитетным, человек меньше анализирует технический смысл действия.

Банки, почта, соцсети, мессенджеры, торговых площад-

ках, госуслуги, корпоративные системы, криптокошельки, облачные сервисы, SIM и аккаунты восстановления.

Захват работает, потому что защита часто рассчитана на технический барьер, а атакующий переносит атаку на поведение человека: «скажите код», «подтвердите», «перейдите», «установите», «введите».

Как схема развивается?

Создать повод для входа или подтверждения.

Направить на форму, звонок, приложение или всплывающее подтверждение.

Переопределить смысл кода или подтверждения.

Получить доступ или восстановление аккаунта.

Быстро сменить контакты, пароли, реквизиты или вывести средства.

Признаки применения и тревожные признаки

Просят код входа в личный кабинет, всплывающее уведомление или приложения.

Код называют «отменой операции».

Просят seed-фразу, резервные коды или ссылку восстановления.

Просят установить удалённый доступ.

Вход выполняется не через самостоятельно открытый официальный сайт или приложение.

Красный флаг и безопасная проверка

Код, всплывающее уведомление, seed-фраза и восстановление аккаунта считаются ключами, а не информацией для разговора. Никому не передавать. Входить только через самостоятельно открытое приложение или сайт. Для важных аккаунтов использовать дополнительную защиту входа, предпочтительно устойчивую к поддельным письмам, если доступно.

Службы поддержки могут присылать коды, но не должны просить назвать их оператору, если код открывает доступ или подтверждает действие.

«Назовите код, чтобы отменить заявку на кредит».

«Подтвердите всплывающее уведомление, это проверка безопасности».

«Введите seed-фразу для синхронизации кошелька».

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Защита аккаунта ломается не только взломом, но и инструкцией человеку. Любой код — это действие, а не разговорная информация.

Глава 31. Повторная эксплуатация жертвы и повторный обман под видом возврата денег

Живой разбор приёма

Повторная эксплуатация — это схема, где после первой потери человеку предлагают «вернуть деньги», «найти мошенника», «разблокировать активы», «ускорить расследование» или «вывести остаток» за новый платёж, данные или доступ.

Откуда это появилось?

Повторные схемы существовали в офлайн-мошенничестве как «помощь юриста» или «возврат через посредника». В цифровой среде они распространились вокруг криптовалюты, инвестиций, фальшивых брокеров, романтических схем и техподдержки.

После потери человек испытывает стыд, злость, надежду и желание исправить ошибку. Мошенник использует это состояние: обещает вернуть контроль и снять боль. Чем больше потеря, тем сильнее риск новой уступки.

Стресс и сожаление усиливают поиск быстрого восстанов-

ления. Мозг склонен предпочесть действие, которое обещает вернуть потери, даже если вероятность низкая и риск высок.

Криптовалютные схемы, фальшивые инвестиции, романтическое мошенничество, утечки данных, поддельные юридические услуги, фальшивые «службы возврата», поддельные сотрудники платформ.

Схема работает, потому что человек уже знает, что проблема реальна: деньги действительно потеряны. Поэтому новая легенда не должна доказывать наличие проблемы, она лишь обещает решение.

Как схема развивается?

Найти человека после потери или удержать его в старом канале.

Представиться специалистом по возврату, службой, юристом или платформой.

Попросить данные, оплату комиссии, доступ или новый перевод.

Объяснить срочность «окном возврата».

Получить вторую потерю или дополнительные данные.

Признаки применения и тревожные признаки

Вам обещают вернуть деньги за предоплату.

Просят оплатить налог, комиссию или юридический сбор до результата.

Контакт пришёл от неизвестного «специалиста по возвра-

ту».

Просят seed-фразу, доступ к кошельку или удалённый доступ.

Говорят, что нужно действовать тайно и быстро.

Красный флаг и безопасная проверка

После инцидента нельзя продолжать общаться в старом канале. Нужно фиксировать факты, блокировать доступы, обращаться в банк, платформу, официальные органы и проверенные юридические каналы. Возврат «за комиссию вперёд» считать высоким риском.

Реальное восстановление иногда возможно через банк, платёжную систему, платформу или правоохранительные органы. Но оно не требует seed-фраз, удалённого доступа и оплаты неизвестному посреднику.

«Мы нашли ваши украденные криптоактивы, оплатите газ-комиссию».

«Юрист вернёт деньги от брокера за аванс».

«Банк заблокировал перевод, но нужна новая операция для отмены».

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

После потери человек особенно уязвим. Первый шаг защиты — прервать навязанный разговор и перейти только в

официальные каналы.

Глава 32. Порядок действий разрыва мошеннической цепочки

Для карты мошеннических сценариев это звучит так: сначала разберитесь, что именно от вас хотят. Затем проверьте условия вне разговора и только после этого решайте.

Живой разбор приёма

Порядок действий разрыва цепочки — это последовательность безопасных действий, которая останавливает сценарий на любом этапе: контакт, прогрев, подтверждение, технический шаг, платёж, захват аккаунта или повторная эксплуатация.

Откуда это появилось?

В защитных практиках кибербезопасности и антифрода давно используется принцип проверки через официальный сайт, приложение или уже известный контакт, разделения ролей, остановки, двухкругного подтверждения, ограничений на платёжи и журналирования событий. В бытовой защите эти принципы переводятся в простые личные правила.

Порядок действий избавляет от необходимости импро-

визировать под давлением. Если правило известно заранее, человек не спорит со сценарием, а выполняет собственную процедуру безопасности.

Предварительно заданный алгоритм снижает нагрузку на внимание в стрессовой ситуации. Вместо поиска ответа человек выполняет привычную последовательность: остановить, назвать действие, проверить, решить.

Любые ситуации с деньгами, данными, доступом, документами, подписями, кодами, установкой программ, срочными просьбами и неожиданными контактами.

Порядок действий работает, потому что мошенническая цепочка зависит от движения вперёд. Если человек даёт время на проверку и независимую проверку, цепочка теряет управление.

Как схема развивается?

Остановить канал: не отвечать, не кликать, не переводить, не устанавливать.

Назвать действие, которого добиваются: что именно от меня хотят?

Назвать эмоцию: страх, выгода, чувство вины, стыд, срочность, доверие.

Определить источник: кто это и откуда я это знаю?

Проверить через независимый официальный сайт, приложение или уже известный контакт.

Оценить обратимость: можно ли отменить действие?

Принять решение только после остановки и фиксации условий.

Если действие уже сделано — немедленно перейти к ограничению ущерба.

Признаки применения и тревожные признаки

Любая просьба ускориться.

Любой запрет на обсуждение.

Любой код, платёж, доступ или документ.

Любой новый канал, предложенный инициатором.

Любое давление «сейчас или потеряете».

Красный флаг и безопасная проверка

Использовать правило: «Сначала проверка через официальный сайт, приложение или уже известный контакт, потом действие. Без проверки через официальный сайт, приложение или уже известный контакт действия нет». Для финансовых и учётных сценариев заранее настроить дополнительную защиту входа, лимиты, уведомления, отдельные каналы подтверждения и список доверенных контактов.

Порядок действий не устраняет все риски, но резко снижает вероятность импульсивного действия. В сложных случаях нужна помощь банка, платформы, юриста, ИБ-специалиста или правоохранительных органов.

Пауза на проверку при звонке из банка и самостоятельный

вход в приложение.

Проверка реквизитов поставщика по старому известному контакту.

Отказ от «помощи» после инвестиционной потери и обращение только в официальные каналы.

Кейсы для самостоятельного разбора

Контрольные вопросы по технике включены в общий блок быстрой проверки раздела 4.

Цепочка разрывается не спором с мошенником, а возвратом контроля над каналом, временем, источником и действием.

Сводная матрица многошаговых мошеннических цепочек

Цепочка: Контакт — тревога — ссылка.

Типичная легенда: Проблема с аккаунтом, штрафом, подпиской или платёжом.

Нужное действие: Клик, вход, оплата, данные.

Красный флаг: Ссылка внутри неожиданного сообщения.

Разрыв: Открыть официальный сайт самостоятельно.

Цепочка: Детали — доверие — просьба.

Типичная легенда: Источник знает имя, заказ, должность, событие.

Нужное действие: Перевод, документ, код, подпись.

Красный флаг: Детали заменяют проверку.

Разрыв: Проверить полномочия отдельно от деталей.

Цепочка: Первый источник — второй источник — действие.

Типичная легенда: Сотрудник переключает на другого специалиста.

Нужное действие: Подтверждение, перевод, установка.

Красный флаг: Второй канал дал инициатор.

Разрыв: Выбрать официальный источник или уже известный контакт самому.

Цепочка: Документ — форма — данные.

Типичная легенда: Договор, анкета, возврат, проверка.

Нужное действие: Паспорт, карта, пароль, код.

Красный флаг: Форма пришла по подозрительной ссылке.

Разрыв: Проверить кабинет, домен, получателя и цель.

Цепочка: Проблема — спасение — платёж.

Типичная легенда: Безопасный счёт, комиссия, налог, бронь.

Нужное действие: Денежный перевод.

Красный флаг: Платёж решает искусственно созданную тревогу.

Разрыв: Не платить до договора и проверки через официальный сайт, приложение или уже известный контакт.

Цепочка: Аккаунт — код — контроль.

Типичная легенда: Отмена операции, подтверждение личности, поддержка.

Нужное действие: SMS-код, всплывающее уведомление,

пароль, seed-фраза.

Красный флаг: Код просят назвать человеку.

Разрыв: Код не передавать; входить только самому.

Цепочка: Потеря — надежда — повторный платёж.

Типичная легенда: Возврат денег, поиск активов, юридическая помощь.

Нужное действие: Новая комиссия, доступ, данные.

Красный флаг: Обещание вернуть за предоплату.

Разрыв: Обращаться только в официальные каналы.

Цепочка: Сценарий — пауза на проверку — аудит.

Типичная легенда: Любая история с деньгами, доступом или документами.

Нужное действие: Любое необратимое действие.

Красный флаг: Срочность и запрет проверки.

Разрыв: Порядок действий: стоп, цель, эмоция, источник, проверка.

Блок кейсов раздела 4

Ситуация 1. сообщение сообщает о проблеме с аккаунтом и предлагает подтвердить данные по ссылке. Получатель действительно ждёт посылку. Разберите, почему совпадение ожидания не доказывает подлинность сообщения.

Ситуация 2. На рабочую почту приходит письмо от поставщика с просьбой срочно оплатить по новым реквизитам. В письме есть старый номер договора и знакомая подпись. Определите, какие детали могут быть правдивыми, а какие требуют проверки по прежнему номеру и через вторую под-

пись.

Ситуация 3. Покупателю на цифровая витрина продавец предлагает «безопасную доставку» по отдельной ссылке, потому что «так дешевле и быстрее». Найдите точку выхода из защищённой платформы.

Ситуация 4. Звонящий из «банка» знает последние цифры карты и просит назвать код для отмены подозрительной операции. Определите, где происходит подмена смысла кода.

Ситуация 5. Арендодатель присылает видео квартиры, фото паспорта и договор, но просит бронь до просмотра. Разберите, почему документы не заменяют проверку объекта и собственника.

Ситуация 6. Инвестиционный «аналитик» показывает кабинет с прибылью и просит оплатить налог для вывода средств. Определите платёжную развязку и признаки повторного платёжа.

Ситуация 7. После потери денег человеку пишет «служба возврата криптовалюты» и просит оплатить газ-комиссию. Разберите, почему это повторный обман под видом возврата денег.

Ситуация 8. В мессенджере якобы знакомый просит срочно перевести деньги, объясняя, что не может говорить по телефону. Найдите запрет на независимую проверку.

Ситуация 9. Поддержка «облачного сервиса» просит установить удалённый доступ для восстановления аккаунта.

Определите технический предлог и риск захвата.

Ситуация 10. HR-специалист предлагает работу и просит открыть счёт для тестовой финансовой операции. Разберите, почему рабочая легенда превращается в финансовую схему.

Ситуация 11. Письмо от поставщика сообщает о смене реквизитов и просит оплатить сегодня. Секретарь видит знакомый стиль письма. Определите, какие проверки нужны до оплаты.

Ситуация 12. Человек получает ссылка в сообщении для оплаты штрафа. Сообщение выглядит официально. Разберите, почему короткая ссылка не должен быть самостоятельным доказательством.

Ситуация 13. Романтический партнёр из переписки просит помочь с пошлиной для «освобождения груза». Найдите переход от близости к платёжной развязке.

Ситуация 14. На сайте появляется CAPTCHA, после которой предлагают выполнить странные действия в командной строке или установить файл. Определите технический предлог и безопасную остановку.

Ситуация 15. Человеку звонят из «службы безопасности» и говорят не класть трубку, пока он идёт к банкомату. Найдите удержание на связи и запрет проверки.

Ситуация 16. Клиенту присылают ссылку на «возврат средств» после отмены заказа. Форма просит данные карты и код. Разберите, какие данные не нужны для возврата.

Ситуация 17. Сотруднику пишет «юрист партнёра» и под-

тверждает срочность оплаты, но контакт появился из письма поставщика. Определите ложное вторичное подтверждение.

Ситуация 18. Пожилому человеку звонит «внук» в беде и передаёт трубку «следователю». Найдите эмоциональный крючок, вторичную роль и запрет проверки.

Ситуация 19. После подозрительного платёжа человек продолжает переписку с тем же «специалистом», надеясь исправить ситуацию. Разберите, почему нужно немедленно менять канал.

Ситуация 20. Команда получает срочный запрос на перевод денег от руководителя, который находится «на встрече и недоступен». Разработайте безопасный двухкругный порядок проверки.

Блок упражнений раздела 4

Блок быстрой проверки раздела 4

Почему мошенническую схему нужно анализировать как цепочку, а не как отдельную фразу?

Что такое первичный крючок?

Почему совпадение с реальным ожиданием не доказывает подлинность сообщения?

Чем подробность отличается от достоверности?

Почему знание последних цифр карты не доказывает полномочия звонящего?

Что такое ложное вторичное подтверждение?

Почему проверка по ссылке, присланной инициатором, не является независимой?

Какие действия относятся к техническому предлогу?

Почему удалённый доступ это высоким риском?

Почему временный пароль нельзя рассматривать как обычную информацию?

Что делает платёжную развязку особенно опасной?

Почему необычный способ оплаты это красным флагом?

Что такое «комиссия для вывода прибыли» в мошенническом сценарии?

Почему после первой потери человек становится уязвимее?

Что такое повторный обман под видом возврата денег?

Какие данные нельзя передавать для «возврата средств»?

Какие пять вопросов нужно задать перед любым платёжом?

Что означает «проверка должна быть независимой по происхождению»?

Какие шаги входят в порядок действий разрыва цепочки?

Красный флаг и безопасная проверка, если действие уже совершено и риск реализовался?

Чек-лист разрыва мошеннической цепочки

Я не считаю сообщение подлинным только потому, что оно совпало с моими ожиданиями.

Я отделяю правдивые детали от законности запроса.

Я не использую ссылку, номер, чат или поддельная кнопка оплаты из подозрительного сообщения для проверки этого же сообщения.

Я не передаю коды, пароли, seed-фразы, резервные коды и ссылки восстановления.

Я не устанавливаю программы удалённого доступа по входящему контакту.

Я не плачу комиссии, налоги, депозиты или сборы до проверки через официальный сайт, приложение или уже известный контакт основания.

Я не перевожу деньги на «безопасный счёт», криптокошелёк, gift card или частный счёт по срочной инструкции.

Я проверяю смену реквизитов поставщика через старый известный контакт, а не через письмо с новыми реквизитами.

Я прекращаю старый канал, если уже возник инцидент или подозрение.

Я фиксирую: кто обратился, что просил, какой канал, какие реквизиты, какие ссылки, какие действия уже сделаны.

Защитные формулы раздела 4

«Я не использую ссылку из сообщения. Проверю через официальный сайт или приложение».

«Детали могут быть верными, но запрос всё равно требует проверки через официальный сайт, приложение или уже известный контакт».

«Код, всплывающее уведомление и ссылка восстановления — это ключи доступа. Я их не передаю».

«Второй канал, который дал инициатор, не является независимым».

«Я не устанавливаю удалённый доступ по входящему звонку или сообщению».

«Необычный способ оплаты означает остановку и проверку».

«Перед оплатой мне нужны получатель, основание, договор, возвратность и официальный сайт, приложение или уже известный контакт».

«После потери я прекращаю этот канал и обращаюсь только в банк, платформу или официальный орган».

«Если меня торопят, я замедляюсь».

«Без проверки через официальный сайт, приложение или уже известный контакт действия нет».

Дополнение к мини-глоссарию

Первичный крючок: первое сообщение или событие, которое вводит человека в мошеннический контакт.

Прогрев доверия: накопление деталей и эмоциональных подтверждений, создающих ощущение подлинности.

Псевдодостоверность: впечатление правды, созданное частично верными деталями, документами, логотипами или совпадениями.

Ложное вторичное подтверждение: проверка, которая кажется независимой, но фактически контролируется тем же сценарием.

Докумысленный предлог: использование договора, анкеты, счёта, формы или документа как оправдания рискованного действия.

Технический предлог: использование обновления, установки, кода, удалённого доступа или формы входа как оправдания передачи контроля.

Платёжная развязка: этап сценария, где человека переводят к денежному действию.

Необратимый маршрут: способ действия, который трудно отменить: криптовалюта, gift cards, перевод частному лицу, удалённый доступ, раскрытие seed-фразы.

Захват учётной записи: получение контроля над аккаунтом через пароль, код, всплывающее уведомление, восстановление, токен или социальное давление.

Повторный обман после потери: повторная схема, где человеку после потери обещают вернуть деньги или активы за новый платёж, данные или доступ.

Разрыв цепочки: остановка сценария через время на проверку, независимую проверку и отказ от действия до подтверждения.

Источники и опорные материалы

FTC Consumer Advice. Как избегать мошенничества: не переходить по ссылкам из неожиданных сообщений, использовать доверенные сайты или известные номера и не поддаваться срочности.

FTC Consumer Advice. Как распознавать фишинг: описаны сообщения, которые просят перейти по ссылке, открыть вложение или передать данные; для защиты аккаунтов рекомендована дополнительная защита входа.

FTC Consumer Advice. Как распознавать и сообщать о спам-SMS: не переходить по подозрительным ссылкам и пересылать спам-сообщения на 7726.

FTC Consumer Advice. Как защищать личные данные: использовать надёжные пароли и дополнительную защиту входа для аккаунтов с личной информацией.

FBI. Рекомендации по подмене деловой переписки: проверять платёжные и закупочные запросы лично или по известному номеру и отдельно подтверждать изменения реквизитов.

FBI. Материалы о подмене деловой переписки: описывают требования секретности, давление срочностью и необходимость двухэтапной проверки банковских переводов.

CISA. Предотвращение социальной инженерии и фишинга: описывает попытки выглядеть доверенным источником и использовать привычные каналы связи.

NIST Phish Scale User Guide: даёт метод оценки сложности распознавания фишинговых сообщений и их признаков.

NIST SP 800-63B: для сред с повышенными требованиями выделяет способы входа, устойчивые к фишингу.

FTC Consumer Advice. Что знать о криптовалюте и мошенничестве: описывает признаки криптовалютных схем и способы сообщить о них.

Что будет дальше

Дальнейшая логика Части I переходит от многошаговых цепочек к постинцидентной защите: что делать, если че-

ловек уже кликнул, сообщил данные, назвал код, перевёл деньги, установил удалённый доступ или передал документы. Задача блока — построить порядок действий ограничения ущерба, восстановления контроля и фиксации доказательств без паники и повторной эксплуатации.

Мост внутри Книги II: от быстрых схем к сложным маскам

Сначала обман выглядит как короткое сообщение или звонок. Затем он становится сложнее: синтетический голос, взломанный аккаунт знакомого, персональная легенда, несколько каналов связи и ложное подтверждение. Здесь важно не учиться спорить с мошенником, а увидеть саму конструкцию ловушки.

Раздел 7. Мошеннические сценарии повышенной сложности: синтетические медиа, компрометированные каналы и персонализация

Этот блок завершает переход от классических мошеннических схем к современным сценариям, в которых злоумышленник может использовать синтетический голос, дипфейк-видео, реальный взломанный аккаунт, длинный прогрев, подмену нескольких каналов и персонализацию под конкретного человека. Материал подан с защитной стороны: цель не воспроизвести атаку, а научиться распознавать структуру доверия, разрывать сценарий и переводить решение из эмоционального канала в проверяемую процедуру.

Главный принцип раздела: чем правдоподобнее контакт, тем меньше нужно полагаться на субъективное ощущение узнавания и тем строже должна быть проверка через официальный сайт, приложение или уже известный контакт. Голос, лицо, аватар, реальная переписка и знакомый стиль письма больше не являются достаточным доказательством подлинности.

Как проверить ситуацию

Сценарий: Синтетический голос

Главная уязвимость: узнавание голоса близкого или руководителя

Типовой целевой результат: перевод, код, срочное действие

Защитная проверка: кодовая фраза, обратный звонок на старый номер, пауза на проверку

Сценарий: Дипфейк-видео

Главная уязвимость: доверие к визуальному присутствию

Типовой целевой результат: платёж, доступ, подтверждение решения

Защитная проверка: процедура вне видеозвонка, второй канал, письменный порядок действий

Сценарий: Взломанный аккаунт знакомого

Главная уязвимость: реальная история переписки

Типовой целевой результат: ссылка, просьба, деньги, документ

Защитная проверка: проверка через иной канал и прежний контакт

Сценарий: Алгоритмическая персонализация

Главная уязвимость: ощущение, что собеседник «знает меня.»

Типовой целевой результат: согласие без проверки

Защитная проверка: отделить знание фактов от полномочий

Сценарий: Поддельная проверка

Главная уязвимость: доверие к форме, документу, печати, интерфейсу

Типовой целевой результат: паспорт, селфи, карта, код

Защитная проверка: только официальный сайт/приложение, ручной ввод адреса

Сценарий: Мультиканальное подтверждение

Главная уязвимость: ложное усиление доверия несколькими каналами

Типовой целевой результат: ускоренное действие

Защитная проверка: проверка независимости каналов

Сценарий: Helpdesk/IT/HR-имитация

Главная уязвимость: доверие к внутренней роли

Типовой целевой результат: сброс доступа, токен, изменение реквизитов

Защитная проверка: регламент, заявка, known-good контакт

Сценарий: Порядок действий синтетического доверия

Главная уязвимость: сумма голос+лицо+контекст+срочность

Типовой целевой результат: любое критическое действие

Защитная проверка: решение только по процедуре, не по впечатлению

Глава 49. Синтетический голос и экстренная просьба от близкого или руководителя

Живой разбор приёма

Сценарий, в котором голосовое сообщение или звонок создают ощущение контакта с реальным знакомым человеком, но ключевое доказательство подлинности строится только на звучании голоса и срочности ситуации.

Откуда это появилось?

Раньше телефонное мошенничество опиралось на актёрскую игру, шум, стресс и короткий разговор. С развитием технологий подделки голоса риск сместился: человек может слышать голос, похожий на родственника, коллегу или руководителя, и считать само узнавание достаточной проверкой.

Работают узнавание, эмоциональная близость, страх за человека, роль помощи и запрет на рациональную время на проверку. Чем ближе предполагаемый источник, тем слабее потребность проверять формальные признаки.

Срочная просьба о помощи активирует быструю оценку угрозы, телесное напряжение и импульс спасения. Исполнительные функции могут временно уступать эмоциональной реакции: «сначала помогу, потом разберусь».

Семейные звонки, рабочие поручения, голосовые сообщения в мессенджерах, просьбы о переводе, «попал в беду», «нужно срочно закрыть вопрос».

Голос воспринимается как интимный и трудноподделываемый признак личности. Ошибка возникает там, где человек проверяет не полномочия и канал, а собственное ощущение узнавания.

Как схема развивается?

Появляется срочный голосовой контакт от «знакомого».

Формируется эмоциональный контекст: беда, секретность, нехватка времени.

Запрашивается действие, которое нельзя откладывать.

Любая проверка подаётся как вред или предательство.

После действия связь прекращается или лучше новая просьба.

Как опознать

Голос похож, но контакт новый.

Просьба срочная и финансовая.

Запрещают перезвонить.

Требуют код, перевод, криптовалюту или подарочную карту.

Объяснение построено на панике, а не на проверяемых деталях.

Как это выглядит в жизни

Высокий риск возникает, когда совпадают три элемента: узнаваемый источник, срочное действие и запрет нормальной проверки. В современных сценариях нельзя считать голос, лицо, реальный аккаунт или знание персональных деталей окончательным доказательством.

Красный флаг и безопасная проверка

Использовать семейную или корпоративную кодовую фразу.

Перезвонить на старый сохранённый номер, а не по входящему контакту.

Не обсуждать коды и деньги в том же канале.

Включить правило: «голос не подтверждает платёж».

Сообщить второму доверенному человеку до действия.

Кодовая фраза помогает только если она заранее известна ограниченному кругу и не публикуется в переписке. Для крупных решений нужна процедура, а не один контрольный вопрос.

«Мама, я попал в аварию, срочно переведи деньги адво-

кату».

«Это я от поставщика. Реквизиты новые, оплатите сейчас, потом пришлю подтверждение».

Конец ознакомительного фрагмента.