

OSINT и ЗАЩИТА ОТ МОШЕННИКОВ:

Как проверять подозрительные
сайты и предложения



и

Дмитрий Соколов

Дмитрий Соколов

OSINT и защита от

мошенников. Как

проверять подозрительные

сайты и предложения

<https://litres.ru/74594754>

SelfPub; 2026

Аннотация

«Вам обещают возврат — подтвердите заявку до вечера». Сумма знакома, сообщение выглядит правдоподобно, собеседник торопит. Как понять, можно ли доверять предложению?

Книга предлагает практическую систему проверки. Вы научитесь искать сведения в открытых источниках, беречь личные данные, проверять домен и историю сайта, сверять контакты, документы, реквизиты, отзывы, изображения и тексты. Узнаете, как оценить продавца и его представителя, условия сделки и получателя оплаты, распознать давление и подмену личности. Практические разборы магазина, вакансии и инвестиционного предложения покажут, как сопоставлять факты и учитывать, чего проверка не может доказать.

Книга для тех, кто покупает онлайн, ищет работу или рассматривает вложения. Она не даст волшебного теста на

мошенника, но поможет остановиться, проверить информацию независимо, сохранить доказательства и действовать без чужой спешки.

Содержание

Почему мы верим мошенникам:	6
психологические уловки и признаки давления	
Безопасная проверка: как не раскрыть свои	17
данные и не навредить устройству	
Основы OSINT: как искать и сопоставлять	28
сведения из открытых источников	
Первичная проверка предложения: быстрый	41
список тревожных признаков	
Конец ознакомительного фрагмента.	52

Дмитрий Соколов OSINT и защита от мошенников. Как проверять подозрительные сайты и предложения

OSINT и защита от мошенников: Как проверять подозрительные сайты и предложения

Дмитрий Соколов

Почему мы верим мошенникам: психологические уловки и признаки давления

В половине шестого вечера Ольга стояла в очереди за продуктами, одной рукой придерживая корзину, другой отвечая на рабочее сообщение. День выдался длинным: встреча за встречей, недочитанные письма, звонок из школы. Телефон коротко завибрировал.

«Ольга, по вашему старому страховому договору обнаружена переплата — 31 840 #. Чтобы получить возврат, подтвердите заявку сегодня до 19:00. Специалист уже готов помочь».

Она не помнила такого договора. Но несколько лет назад действительно оформляла страховку вместе с кредитом. Сумма была приятной — и вполне правдоподобной. Следом позвонил мужчина, представился сотрудником отдела возвратов и спокойно объяснил: деньги положены по новому порядку, заявка почти готова, осталось подтвердить личность. «Давайте быстро, чтобы не потерять очередь, — сказал он. — У нас сегодня закрывается реестр».

Ольга была не наивной. Она руководила командой, проверяла договоры и учила подростка не открывать подозрительные ссылки. Но сейчас у неё болела голова, продукты

тянули руку, а в мессенджере уже ждал начальник. Внимание было занято, а сообщение обещало не риск, а приятную неожиданность. В голове мелькнуло: *Если это правда, будет обидно упустить*. Мужчина говорил уверенно. Он назвал её имя и часть данных о старом договоре.

— Сейчас придёт код. Просто продиктуйте его, чтобы подтвердить заявку, — сказал он.

Ольга открыла сообщение. На экране появилась короткая инструкция, которую в спешке легко было прочитать не до конца. Палец завис над цифрами.

Именно здесь расходятся две версии одного вечера.

Две версии одной сцены

В первой версии Ольга решает, что раз уж начала, нужно довести дело до конца. Она диктует код. Мужчина благодарит её и говорит, что возврат поступит в течение дня. Через несколько минут приходит настоящее уведомление от банка: выполнено действие, которого Ольга не собиралась совершать. Она звонит в банк, блокирует доступ, пытается понять, что именно произошло. Вечер теперь занят не покупками и ужином, а тревогой, звонками и восстановлением контроля.

Во второй версии всё происходит почти так же. То же сообщение, тот же усталый день, тот же уверенный голос. Но после слов про код Ольга замечает не только сумму возврата, но и собственное состояние: она торопится и боится упустить выгоду. Это не доказывает, что перед ней мошенник. Но означает, что сейчас ей сложнее спокойно оценить прось-

бу.

Она не диктует код и не продолжает разговор. Вместо этого говорит: «Я проверю информацию самостоятельно и, если она подтвердится, свяжусь с вами». Затем завершает звонок. Не нажимает на присланную ссылку, а ищет номер страховщика в старом договоре и звонит туда сама. Ей сообщают, что никаких возвратов по её договору не оформлено. Ольга не совершает необратимого действия — и возвращает себе самое важное: возможность решать без чужого сценария.

Вторая версия не требует особой проницательности. Ей достаточно одного промежутка между требованием и ответом. Пауза не сделала Ольгу подозрительной ко всему миру. Она просто дала ей время подумать.

Почему разумный человек может поверить

Мошенничество редко начинается с вопроса: «Хотите ли вы добровольно отдать свои деньги?» Оно начинается с предложения, проблемы или обязанности: вернуть переплату, защитить счёт, получить редкую скидку, не пропустить важное. Собеседник старается не просто сообщить факты, а направить ваше внимание — к выгоде, угрозе или дедлайну. Чем уже становится внимание, тем меньше места остаётся для проверки.

Это не недостаток характера. Мы все пользуемся быстрыми умственными сокращениями: доверяем знакомому названию, прислушиваемся к уверенным людям, сильнее реагируем на срочные угрозы. Обычно это помогает не тра-

тить силы на каждое решение. Но в ситуации давления привычный способ принимать решения может сработать против нас. Усталость, многозадачность и тревога дополнительно затрудняют внимательную оценку: человеку приходится одновременно слушать, читать, вспоминать и решать.

Важно отделять психологическое объяснение от установленного факта. Давление повышает риск ошибиться, но само по себе **не доказывает**, что предложение мошенническое. У настоящих организаций тоже бывают сроки, а уверенный тон не всегда означает обман. Но настойчивость и доверие к собеседнику не заменяют проверку. Особенно когда от вас требуют денег, кодов, доступа к аккаунту или решения, которое трудно отменить.

Шесть способов подтолкнуть вас к решению

1. Срочность: «Нужно сейчас». «Осталось десять минут», «заявка закроется до конца дня», «немедленно подтвердите операцию». Реальный срок иногда существует. Но когда собеседник не просто называет дату, а требует действовать прямо во время звонка, возникает важный вопрос: почему нельзя прервать разговор и проверить информацию самостоятельно?

Срочность отнимает время не только у проверки, но и у внутреннего вопроса: *Понимаю ли я, на что соглашаюсь?* Поэтому полезно насторожиться не только из-за конкретных слов, но и из-за темпа: вам задают вопросы один за другим, перебивают, не дают спокойно прочитать сообщение.

2. Дефицит: «Только для вас и только сегодня». «Последнее место», «осталось два билета», «мы выбрали всего десять клиентов». Ограниченное предложение может казаться ценнее именно потому, что его будто бы вот-вот не станет. Появляется страх упустить не просто покупку, а *особенный шанс*. В такой момент легко начать объяснять себе, почему предложение выгодно, и забыть проверить, кто его сделал.

Посмотрите, что именно подтверждает дефицит. Не скриншот таймера, присланный продавцом, и не его слова, а независимый источник. Если предложение настоящее, возможно, его удастся найти через официальный сайт или подтвердить по номеру, который вы нашли сами.

3. Запугивание: «Если не сделаете — будет хуже». «Счёт заблокируют», «начислят штраф», «вас привлекут к ответственности», «вы потеряете доступ». Страх заставляет стремиться прежде всего прекратить неприятное ощущение. Человек делает то, что обещает быструю развязку: следует инструкции, отвечает на вопросы, подтверждает действие. Однако угроза, произнесённая по телефону, ещё не является доказательством полномочий собеседника. Попросите сообщить, где и как можно проверить её независимо, и не выполняйте указания только ради того, чтобы звонящий перестал вас пугать.

4. Авторитет: «Я специалист, я знаю порядок». Собеседник может назвать себя сотрудником банка, госслуж-

бы, полиции, известной компании или «службы безопасности». Он может использовать профессиональные слова, говорить размеренно и звучать так, словно процедура ему хорошо знакома. Это влияет на доверие, но роль и компетентность нельзя подтвердить одним уверенным голосом, логотипом в сообщении или отображаемым именем звонящего.

Задайте себе вопрос: *Я проверяю полномочия человека или просто реагирую на то, как он себя представил?* Безопаснее завершить разговор и связаться с организацией по номеру из договора, приложения или официального сайта, открытого самостоятельно.

5. Лесть и ощущение исключительности: «Мы выбрали именно вас». «Видно, что вы человек подготовленный», «такие условия доступны только надёжным клиентам», «вам можно доверить решение». Лесть приятна — и в этом нет ничего постыдного. Но после неё просьба может выглядеть не как рискованное действие, а как подтверждение вашей компетентности. Отказ будто бы ставит под сомнение то, чем вас только что похвалили.

Заметьте, когда вас приглашают не просто оценить условия, а поверить в собственную исключительность. Можно быть компетентным человеком и всё равно попросить письменные условия, взять время на проверку или сказать «нет».

6. Взаимность: «Я уже для вас постарался». «Я лично придержал место», «уже подготовил документы», «добился для вас исключения». Здесь включается естественное жела-

ние ответить на услугу услугой и не показаться неблагодарным. Но если вы ничего не просили, а «услуга» появилась вместе с давлением, вы не обязаны платить за неё согласием. Подготовленный кем-то документ не создаёт у вас обязанности его подписать.

Иногда эти приёмы соединяются. Сначала вам говорят, что вы избраны, затем сообщают о последнем свободном месте, потом пугают потерей выгоды и предлагают подтвердить всё немедленно. Каждый отдельный шаг может выглядеть небольшим. Вместе они образуют коридор, в конце которого от вас ждут действия.

«Пауза на три вопроса»

Когда разговор ускоряется, не пытайтесь мгновенно разгадать, мошенник перед вами или нет. Сначала остановите движение к действию и спросите себя:

1. Что от меня требуют?

Не «подтвердить заявку», а конкретно: перевести деньги, назвать код, перейти по ссылке, сообщить данные, установить программу, согласиться с договором? Переведите красивую формулировку в простое описание поступка.

2. Почему именно сейчас?

Что случится, если я завершу звонок и проверю информацию позже? Кто установил срок и могу ли я найти подтверждение этому сроку независимо от собеседника?

3. Что случится, если я откажусь или подожду?

Речь идёт о реальной и проверяемой процедуре или о на-

казании, которое мне только обещают? Могу ли я обратиться в организацию самостоятельно, посоветоваться с близким или прочитать условия без того, чтобы за мной наблюдали и подгоняли?

Три вопроса не дают мгновенного ответа на всё. Их задача проще: вернуть вам право распоряжаться своим вниманием. Если человек отказывается дать время, запрещает советоваться, требует сохранять разговор в тайне или настаивает, чтобы вы действовали только по его инструкции, это весомый повод остановиться. Не окончательный вердикт о том, кто перед вами, а достаточная причина не продолжать действие в текущем разговоре.

Для этого не требуется оправдываться. Подойдут короткие фразы:

- «Я не принимаю решения во время входящего звонка».
- «Я проверю информацию самостоятельно и свяжусь с вами, если понадобится».
- «Не присылайте мне ссылку: я найду официальный контакт сам».
- «Я не буду сообщать коды и выполнять действия, смысла которых не понимаю».

Не нужно убеждать собеседника, что вы правы. Чем дольше спор, тем больше возможностей снова втянуть вас в его темп. Можно просто закончить разговор.

Короткий тест: на меня давят или дают время подумать?

Ответьте «да» или «нет»:

- Меня торопят и требуют решения прямо сейчас.
- Последствия отказа описывают так, что я пугаюсь.
- Мне предлагают особые условия, но мешают проверить

их независимо.

- Меня просят никому не рассказывать или не советовать-ся.

- Я не могу простыми словами объяснить, какое действие сейчас совершаю.

- Собеседник раздражается, когда я прошу время или другой способ связи.

Любой ответ «да» — повод сделать паузу. Если речь идёт о деньгах, коде, пароле или доступе к устройству, пауза должна предшествовать действию, а не следовать за ним. При этом тест не устанавливает, мошенник ли перед вами: он помогает заметить условия, в которых риск ошибиться возрастает.

Теперь небольшое упражнение. Вспомните предложение, звонок или сообщение, которое недавно вызвало сильную реакцию. Запишите три вещи:

- **Что я почувствовал(а)?** Страх, азарт, жадность, облегчение, стыд, любопытство, обязанность?

- **Что от меня хотели получить?** Какое конкретное действие скрывалось за формулировкой?

- **Какой проверочный шаг вернёт мне контроль?** Например, закончить звонок, найти контакт организации само-

стоятельно, перечитать договор, спросить человека, которому доверяю, или просто не отвечать до утра.

Называние эмоции не отменяет её и не делает предложение ложным. Оно помогает отделить чувство от факта: *я боюсь потерять доступ* — это описание моего состояния; *доступ действительно заблокируют через десять минут* — утверждение, которое нужно проверить.

Выберите своё правило паузы

Полезно придумать правило заранее, когда на вас не давят. Например: «Я не совершаю финансовых действий по неожиданному входящему звонку. Сначала завершаю разговор, затем проверяю предложение по независимому каналу». Для крупной покупки можно установить правило ночи: не принимать решение до следующего дня. Для просьб о коде, пароле или удалённом доступе правило может быть ещё проще: не сообщать и не предоставлять их по указанию незнакомого собеседника.

Пауза — это не автоматический отказ. Это защита пространства, в котором отказ и согласие становятся вашими решениями, а не ответами на чужую спешку. Настоящее предложение может выдержать проверку. А если после нескольких минут ожидания вам всё ещё не хватает данных, значит, данных пока недостаточно.

Люди верят мошенникам не потому, что им недостаёт ума или жизненного опыта. Мы откликаемся на знакомые человеческие потребности: избежать беды, получить выгоду,

оправдать доверие, не упустить шанс, ответить на доброту. Именно поэтому защитой становится не стыд и не обещание «больше никогда не ошибаться», а простой навык замечать давление и возвращать себе время.

Если вас торопят, пугают или запрещают советоваться, безопаснее остановиться и проверить предложение независимо. Доверие и настойчивость собеседника не заменяют проверки. Сначала — пауза и решение, что именно вы проверяете. Затем — аккуратная проверка, не раскрывающая лишних данных и не подвергающая риску ваше устройство.

Безопасная проверка: как не раскрыть свои данные и не навредить устройству

В 8:12 Ирина ставит чайник и одной рукой ищет в сумке ключи, другой пытается ответить на рабочее сообщение. Телефон вибрирует: «Вам положен возврат переплаты — 18 460 рублей. Подтвердите заявку до 9:00, иначе сумма будет аннулирована». Ниже — логотип знакомой компании и ссылка. Через минуту звонит «специалист отдела выплат»: голос спокойный, уверенный, будто Ирина задерживает нечто давно ей причитающееся.

Ирина не наивна. Она руководит отделом закупок, читает договоры, замечает несостыковки. И всё же предложение попадает в удачный момент: сумма приятная, а недавно она действительно меняла тариф. В голове быстро складывается удобная версия: «Наверное, переплату пересчитали. Надо только подтвердить».

Представим, что дальше утро пошло по двум разным сценариям.

Одно сообщение — два утра

В первой версии Ирина нажимает на ссылку. Страница открывается быстро, логотип на месте, цвета знакомые, рядом с адресом браузера есть значок замка. Адрес сайта

она не рассматривает: телефонный экран маленький, а звонящий уже объясняет, что процедура займёт «меньше минуты».

На странице просят ввести номер телефона и пароль от личного кабинета. Потом приходит одноразовый код — якобы для подтверждения возврата. Ирина вводит и его. Следующий шаг — установить приложение «для зачисления выплаты». Тут она наконец останавливается: почему для получения денег нужно ставить неизвестную программу? Она закрывает страницу, но уже передала данные, которые могли дать постороннему доступ к её аккаунту.

Не обязательно именно так закончится каждый подобный эпизод. Но если отдать кому-то пароль, одноразовый код или доступ к устройству, последствия могут выйти далеко за пределы одного «возврата». Важно не искать виноватую в этой истории. Ирина действовала не глупо — она действовала в условиях, специально созданных для поспешного решения.

Во второй версии Ирина замечает, что у неё участилось дыхание: радостное предвкушение смешалось с тревогой опоздать. Она не нажимает на ссылку и задаёт себе три вопроса:

1. Что от меня требуют? Ввести пароль и код, а возможно, установить программу.

2. Почему именно сейчас? Потому что так написано в сообщении, но независимого объяснения срочности пока нет.

3. Что случится, если я откажусь или подожду? Возможно, никакого возврата не будет. Но это можно проверить, не рискуя аккаунтом.

Ирина закрывает сообщение, открывает приложение компании привычным способом — через значок на телефоне — и ищет уведомление там. Его нет. Затем она звонит по номеру из договора, а не по номеру из сообщения. Служба поддержки подтверждает: подобной акции нет. Ирина сохраняет сообщение, отправляет его на проверку через предусмотренный сервис жалоб и блокирует отправителя.

Дело не в том, что всякое неожиданное предложение обязательно мошенническое. Давление само по себе не доказывает обман. Но оно повышает вероятность ошибки — и является достаточной причиной остановиться. Настойчивость собеседника, знакомый логотип и приятная сумма не заменяют независимой проверки.

Почему рассудительные люди тоже торопятся

Мошеннические и просто манипулятивные сообщения не рассчитаны на особый тип людей. Они используют обычные человеческие реакции.

Срочность превращает решение в забег: «Ответьте в течение десяти минут», «Окно подтверждения закрывается». Когда внимание занято дедлайном, на проверку как будто не остаётся места.

Дефицит и страх потери делают предложение ценнее: «Осталось два места», «После полуночи скидка исчезнет»,

«Иначе потеряете начисление». Мы часто сильнее переживаем из-за возможной утраты, чем радуемся сопоставимой выгоде. Это не недостаток характера, а знакомая особенность принятия решений.

Запугивание заставляет подчиниться ради облегчения. «Ваш счёт заблокируют», «Посылка будет уничтожена», «На вас оформлен долг». В этот момент человек может стремиться не к лучшему решению, а просто к прекращению тревоги.

Авторитет маскирует просьбу под распоряжение: «Я из службы безопасности», «Поручение от руководства», «Государственная программа». Должность, форма, логотип и уверенный тон могут выглядеть убедительно, но не удостоверяют ни личность собеседника, ни правдивость его слов.

Лесть и исключительность подталкивают принять предложение, чтобы не потерять статус: «Вас выбрали как надёжного клиента», «Только для постоянных покупателей».

Взаимность действует иначе: «Мы уже подготовили выплату — осталось только подтвердить» или «Вот вам подарок, оплатите лишь доставку». Возникает ощущение, будто отказ будет неблагодарностью.

Исследования принятия решений показывают: стресс и перегрузка могут сужать внимание и затруднять удержание нескольких условий в уме. Мы цепляемся за главное — «вернуть деньги», «не потерять доступ», «успеть» — и хуже замечаем побочные просьбы: ввести код, открыть вложение, включить демонстрацию экрана. Это не означает, что чело-

век теряет рассудок. Скорее, ему предлагают решать сложную задачу на бегу, пока кто-то намеренно подталкивает его в неверную сторону.

Проверяйте предложение, не подвергая проверке себя

Безопасная проверка начинается не с поиска улики, а с ограничения риска. Представьте неизвестное сообщение как конверт с тонкой щелью: сначала решите, что не станете через неё передавать, — и лишь затем изучайте содержание.

Не переходите по ссылкам из неожиданного сообщения, даже если оно пришло в знакомом мессенджере и оформлено безупречно. Не сканируйте QR-код, который обещает получить выплату или отменить блокировку. Не открывайте вложения и не включайте макросы в документах по просьбе неизвестного отправителя. Если предложение настоящее, его обычно можно проверить другим путём.

Не звоните по номеру из сообщения. Найдите контакт в приложении, договоре, на банковской карте или на официальном сайте, который открыли самостоятельно. Если нужно проверить уведомление от банка, войдите в приложение привычным способом или позвоните на номер с карты. Если речь о работодателе — свяжитесь с коллегой через уже известный рабочий канал, а не отвечайте на адрес, указанный в подозрительном письме.

При самостоятельном поиске не считайте первую строку в поисковой выдаче гарантией подлинности: там могут быть

рекламные результаты. Не переходите по ним автоматически. Введите знакомый адрес сайта сами или используйте сохранённую закладку. Если не уверены, спросите у организации через канал, который нашли независимо от сообщения.

Замок в адресной строке — не знак честности. Он показывает, что соединение с сайтом зашифровано, но не подтверждает, что сайт принадлежит нужной компании. Страница мошенника тоже может иметь замок. Название организации в адресе может отличаться всего одним символом или быть частью длинного незнакомого адреса. Поэтому не нужно пытаться распознать каждый сайт с первого взгляда: безопаснее вообще не вводить личные данные на странице, открытой по неожиданной ссылке.

Сервисы проверки адресов и файлов могут дать дополнительную подсказку, но не гарантируют безопасности. И не вставляйте в такие сервисы персональную ссылку из письма, если в ней есть ваш номер, токен или другой уникальный фрагмент: проверяемый адрес сам может содержать данные, позволяющие получить доступ к аккаунту.

Особое правило — **не сообщайте посторонним пароли, PIN-коды, коды из СМС и пуш-уведомлений, резервные коды восстановления.** Одноразовый код — не формальность, а временный ключ. Сообщение вроде «диктуйте код, чтобы отменить операцию» — повод немедленно остановить разговор. Одобряйте вход или платёж только в том случае, если сами начали это действие и понимаете, что

именно подтверждаете.

То же относится к просьбам показать экран, установить программу удалённого доступа или «помощник». Не устанавливайте приложения и расширения по ссылке из сообщения, не скачивайте файлы приложений напрямую с неизвестного сайта. Не разрешайте незнакомой программе доступ к уведомлениям, функциям управления устройством или экрану. Не включайте демонстрацию экрана по просьбе «службы поддержки». В добросовестной помощи не должно быть необходимости отдавать собеседнику управление вашим телефоном.

Если сервис действительно просит ввести платёжные данные — например, при обычной покупке, — делайте это только на странице, которую открыли самостоятельно и проверили, а не на странице из внезапного сообщения. По возможности используйте уведомления о транзакциях, лимиты и отдельную карту для интернет-покупок. Это не отменяет проверки, но уменьшает возможный ущерб.

Полезный защитный слой — уникальные пароли и менеджер паролей: он обычно не подставляет сохранённые данные на похожем, но чужом домене. Это не безошибочный детектор, а дополнительный сигнал. Обновляйте операционную систему и браузер, загружайте приложения из проверенных магазинов и смотрите на имя разработчика. Но и магазин приложений не освобождает от внимания: похожее название ещё не означает, что приложение выпущено нужной

компанией.

Если вы уже нажали

Один клик не равен катастрофе. Не ругайте себя и не пытайтесь в панике «исправить всё» первой же программой, которую предложит всплывающее окно.

Если вы только открыли страницу, ничего не скачивали, не вводили данные и не выдавали разрешений — закройте вкладку. Не нажимайте появившиеся кнопки «очистить устройство» или «срочно проверить вирусы». Обновите браузер и систему. При необходимости выполните проверку встроенными средствами защиты устройства.

Если вы ввели пароль, смените его **самостоятельно открыв официальный сайт или приложение**. Сделайте это с устройства, которому доверяете. Выйдите из других активных сеансов, включите или перенастройте многофакторную защиту и проверьте, не изменились ли резервная почта и номер телефона. Если такой же пароль использовался на других сайтах, замените его и там.

Если вы сообщили банковский код, данные карты или подтвердили операцию, немедленно свяжитесь с банком по номеру на карте или через официальное приложение. Попросите проверить операции и принять необходимые меры. Если установили неизвестную программу или дали кому-то управлять устройством, прекратите пользоваться им для банковских операций и свяжитесь со службой поддержки с другого, безопасного устройства. Для рабочего телефо-

на или компьютера сообщите специалистам своей организации.

Сохраните сообщение, время звонка и скриншоты, предварительно закрыв личные сведения, если собираетесь пересылать их кому-то для консультации. Не публикуйте в открытом доступе коды, номер карты, адрес аккаунта и персональные ссылки. Не отправляйте полные документы незнакомому «эксперту по безопасности»: желание проверить не должно превращаться в новую утечку.

Упражнение: «На меня давят или дают время подумать?»

В следующий раз, когда предложение покажется одновременно выгодным и срочным, не пытайтесь сразу решить, настоящее оно или нет. Сначала определите, что происходит с вами.

Шаг первый. Назовите эмоцию. Не просто «я нервничаю», а точнее: «я боюсь потерять выплату», «мне приятно, что меня выбрали», «я тороплюсь прекратить тревогу». Такое название не выключит эмоцию, но поможет заметить её, прежде чем она станет командой к действию.

Шаг второй. Ответьте на три вопроса:

- Что от меня требуют сделать прямо сейчас?
- Почему это нужно сделать именно сейчас?
- Что случится, если я откажусь или подожду и проверю информацию другим способом?

Шаг третий. Выберите один безопасный провероч-

новый шаг: открыть официальное приложение самостоятельно, позвонить по известному номеру, обратиться к руководителю через рабочий канал. Не нужно выполнять просьбу, чтобы выяснить, заслуживает ли она доверия.

Мини-тест «На меня давят или дают время подумать?» — это не способ вынести вердикт, а способ заметить риск. Отметьте, если в предложении:

- есть жёсткий срок, который нельзя спокойно проверить;
- требуют пароль, код, платёж или установку программы;
- запрещают советоваться или обращаться в официальную поддержку;

- собеседник сам предлагает единственный «правильный» канал связи;

- отказ или пауза описаны как немедленная катастрофа.

Чем больше таких сигналов, тем важнее сделать паузу. Даже один сигнал, связанный с паролем, одноразовым кодом, доступом к устройству или переводом денег, — достаточная причина не продолжать действие, пока вы не проверили его независимо.

Заранее придумайте личное правило, чтобы не сочинять его в самый напряжённый момент. Например: **«По неожиданным ссылкам я не захожу в аккаунты и не подтверждаю операции. Любое предложение, где просят код, деньги или установку приложения, я проверяю через официальный канал. Сначала пауза — потом решение».** Можно добавить конкретный срок: пятнадцать минут

без переписки и один звонок по известному номеру. Настоящее предложение выдержит проверку; если вопрос действительно не терпит отлагательства, вы сможете связаться с организацией безопасным способом.

Проверка — не проявление подозрительности и не экзамен на сообразительность. Это способ вернуть себе выбор, когда кто-то пытается сделать его за вас. Чем меньше вы раскрываете до подтверждения, тем меньше риск потерять: не только деньги, но и доступ к аккаунтам, приватность и контроль над устройством. Сначала остановитесь, назовите, что от вас требуют, и найдите независимый путь проверки. Доверие может быть началом разговора, но не заменой фактам.

Основы OSINT: как искать и сопоставлять сведения из открытых источников

Марина уже видела такое сообщение: аккуратный логотип, имя знакомого работодателя, вежливое обращение. Она действительно недавно откликнулась на вакансию — и теперь ей обещали прислать договор. Остался один шаг: открыть ссылку, скачать документ и войти в «защищённый кабинет». Внизу стояло предупреждение: «Подтвердите данные сегодня, иначе предложение будет передано другому кандидату».

Палец почти коснулся экрана. Но Марина остановилась. Она не стала отвечать отправителю, переходить по ссылке или скачивать файл. Вместо этого посмотрела на то, что уже было перед глазами: адрес отправителя, формулировки, название компании и срок, которым её торопили. Затем нашла официальный сайт работодателя самостоятельно и проверила контакты на нём. Через указанный там номер ей подтвердили: сообщение не имеет отношения к компании.

Марина не взломала мошенников, не установила специальную программу и не устроила цифровую погоню. Она просто отделила проверку от взаимодействия. Это и есть хорошее начало OSINT — поиска и сопоставления сведений

из открытых источников.

Что значит «проверить по открытым источникам»

OSINT часто представляют как набор хитрых технических приёмов. В действительности основа метода куда проще: сформулировать вопрос, найти доступные сведения, оценить их происхождение и сопоставить независимые источники.

«Открытый» здесь не означает «безопасный», «точный» или «разрешённый для любого использования». Это означает, что сведения доступны без обхода защиты и без взлома. Официальный сайт компании, государственный реестр, опубликованные контакты, сообщения надзорного органа, открытая новость — примеры таких источников. Чужой личный кабинет, закрытая переписка и база данных, добытая незаконным способом, к ним не относятся.

Цель проверки тоже важна. Не нужно собирать всё, что можно найти о неизвестном отправителе, — это и лишнее, и потенциально вредное для чужой приватности. Достаточно ответить на конкретные вопросы:

- Существует ли организация, от имени которой мне пишут?
- Подтверждает ли она именно это предложение?
- Совпадает ли адрес сайта со ссылкой, указанной на её официальных страницах?
- Есть ли независимые сведения, которые поддерживают или опровергают заявление отправителя?

OSINT — не коллекционирование подозрительных деталей, а аккуратная работа с доказательствами. Представьте, что вы раскладываете на столе несколько кусочков карты. Один сам по себе почти ничего не объясняет. Но когда кусочки происходят из разных мест и складываются в одну картину, уверенности становится больше.

Безопасная дистанция: контрольная точка до проверки

Перед любым поиском сделайте короткую паузу. Не нужно быть специалистом по кибербезопасности, чтобы начать с четырёх запретов:

Не переходить по ссылке. Не скачивать файл. Не вводить секреты. Не раскрывать персональные данные.

Под «секретами» понимаются пароли, коды из SMS и приложений, PIN-коды, данные банковской карты, фразы восстановления криптокошелька. Персональные данные — не только паспортный номер. Это также адрес, дата рождения, рабочая почта, сведения о родственниках и фотографии документов.

Никакого способа пользоваться интернетом совсем без цифровых следов не существует: поисковая система может сохранить запрос, сайт — записать обращение к нему, приложение — собирать данные в соответствии со своими настройками. Здесь задача скромнее и практичнее: **не оставлять следов на подозрительном ресурсе и не давать**

его создателям новых сведений о себе. Для этого не вводите в поиск содержание закрытого сообщения, свои данные или уникальный код из ссылки. Ищите только то, что необходимо для проверки.

Если в сообщении уже видны текст, адрес сайта или номер телефона, их часто достаточно, чтобы начать. Не открывайте ссылку «просто посмотреть». Даже загрузка страницы может сообщить её владельцу технические сведения о вашем устройстве или подтвердить, что адресат активен. А форма, похожая на знакомую страницу входа, может быть создана именно для кражи пароля.

Пошаговая проверка без контакта с отправителем

Шаг первый. Зафиксируйте то, что уже получили.

Сохраните сообщение или сделайте снимок экрана, если это нужно для последующего обращения в компанию или банк. Не пересылайте его без необходимости: в нём могут быть личные данные, а некоторые ссылки содержат индивидуальные идентификаторы. Не отвечайте отправителю даже для того, чтобы спросить, настоящее ли это сообщение. Ответ подтвердит, что адрес или номер действующий, а объяснение мошенника не станет независимой проверкой.

Шаг второй. Сформулируйте вопрос, а не обвинение.

«Это точно обман» — уже готовый вывод. Он может заставить нас замечать только то, что его подтверждает. Лучше спросить: «Могу ли я независимо подтвердить, что компания отправила мне именно эту ссылку и просит выполнить

именно эти действия?» Так вы не подгоняете сведения под заранее выбранный ответ.

Психологи давно изучают, как срочность и эмоциональное возбуждение мешают обдуманному выбору. Когда человек боится потерять деньги, работу или доступ к аккаунту, его внимание сужается: он сосредоточен на кнопке «срочно подтвердить» и меньше замечает детали. Повторение знакомого названия или логотипа тоже способно создать ощущение достоверности, хотя само по себе оно ничего не доказывает. Пауза — не формальность, а способ вернуть себе возможность рассуждать.

Шаг третий. Отделите видимое имя от настоящего адреса. Имя отправителя в почте или мессенджере можно выбрать произвольно. Поэтому смотрите не только на подпись «Служба поддержки» или название компании, но и на фактический адрес отправителя, если приложение его показывает.

С адресами сайтов действует похожее правило: важна не знакомая часть где-то посередине, а основной домен. Например, в условном адресе `login.bank.example.attacker.test` слова `bank.example` могут быть приманкой, а сайт размещён на домене `attacker.test`. Поддомены читаются слева направо, но границу основного домена нужно определять справа налево. Адрес с названием фирмы и дополнительным словом вроде `secure`, `help` или `career` не становится её официальным только из-за этих слов.

Если ссылка скрыта за кнопкой, не обязательно извлекать её любой ценой. Безопаснее найти официальный сайт организации самостоятельно и проверить, какой портал она указывает в разделе контактов, вакансий или помощи. На телефоне не удерживайте палец на сомнительной ссылке, если не знаете, как именно ваше приложение показывает её адрес: можно случайно открыть предварительный просмотр или саму страницу.

Шаг четвёртый. Начинайте с источника, независимого от сообщения. Если вам пишут из банка — используйте номер на банковской карте или в официальном приложении. Если сообщение якобы от работодателя — найдите сайт компании сами, введя её название в поиске или используя уже сохранённый адрес. Если речь о финансовой организации, лицензии или государственном органе — ищите сведения в реестре соответствующего регулятора.

Не пользуйтесь телефонным номером, кнопкой «поддержка» или ссылкой, предложенными в подозрительном сообщении. Это всё части одной истории, и они не могут независимо подтвердить друг друга. По той же причине логотип на странице, аккуратный дизайн и значок замка в браузере не доказывают, что вы на настоящем сайте. HTTPS означает, что соединение шифруется; он не удостоверяет честность владельца ресурса.

Шаг пятый. Сопоставьте сведения, а не просто посчитайте сайты. Поиск по названию компании и конкрет-

ному домену может обнаружить предупреждения, новости или разборы. Но результат в поисковой выдаче — не экспертиза. Рекламная ссылка может стоять выше официальной; отзыв может быть поддельным; предупреждение — устаревшим. Проверяйте, кто именно опубликовал сведения и когда.

Особенно полезны источники, которые возникли независимо друг от друга. Если пять сайтов перепечатали один и тот же пресс-релиз, это не пять подтверждений, а один источник, размноженный на пяти страницах. Спросите себя: «Откуда автор это узнал? Указывает ли он документы, собственное расследование или только пересказывает чужой текст?»

Официальный сайт хорошо подтверждает собственные контакты и правила компании. Государственный реестр — существование юридического лица или лицензии. Независимая новостная публикация может дать контекст. Но даже наличие настоящей компании не доказывает, что конкретное сообщение отправлено ею: мошенники часто используют реальные названия организаций.

Шаг шестой. Отметьте, что известно, а что только предполагается. Можно сделать простую таблицу из трёх колонок:

Утверждение	Источник
-------------	----------

Что это подтверждает

Компания существует
Государственный реестр
Юридическое лицо зарегистрировано

На официальном сайте указан другой портал для кандидатов

Сайт компании

Предложенная ссылка не совпадает с опубликованным адресом

Незнакомцы жалуются на домен

Отзывы или публикации

Есть повод для осторожности, но нужна оценка качества источников

Такой формат помогает не перепутать факт с выводом. «Компания существует» — факт, если вы проверили реестр. «Значит, письмо от неё настоящее» — уже вывод, причём необоснованный. Незнание тоже можно честно записать: «Не удалось подтвердить». Отсутствие найденных предупреждений не превращает ссылку в безопасную.

Вернёмся к Марине. Она проверила компанию через официальный сайт и обнаружила, что настоящий портал для кандидатов имеет другой адрес. Это не было математическим

доказательством, что каждый участник переписки — мошенник. Но для решения «скачивать ли файл и вводить пароль» доказательств достаточно: независимое подтверждение не получено, а риск неоправдан. Марина позвонила по номеру с официального сайта и остановилась.

Ошибки, которые превращают проверку в риск «Открою только на секунду». Страница может начать загрузку, запустить автоматическую переадресацию или предложить разрешение на уведомления. Если вопрос можно решить через официальный сайт или звонок, нет причины проверять его на подозрительной странице.

«Загружу файл в бесплатный онлайн-анализатор». Некоторые сервисы проверки ссылок и файлов сохраняют переданные материалы или показывают результаты другим пользователям. Не отправляйте туда приватные ссылки с токенами доступа, одноразовыми кодами или персональными данными. Не загружайте чужие документы и конфиденциальные файлы в публичные сканеры. Если файл прислан по рабочему каналу, следуйте правилам организации и обратитесь в IT-службу. Неизвестный файл не нужно открывать «в изоляции» или запускать в специальной среде — это создаёт дополнительные риски, не обязательные обычному пользователю.

«Введу вымышленные данные и посмотрю, что будет». Такой опыт всё равно означает взаимодействие с формой. Она может собирать сведения об устройстве, закрепить

сессию или переключиться на настоящий сценарий кражи данных. Не проверяйте подозрительные формы собственными экспериментами.

«На сайте есть замок — значит, всё хорошо». Шифрование защищает передачу данных между браузером и сайтом, но не говорит, честен ли сайт. Мошеннический ресурс тоже может использовать защищённое соединение.

«Номер звонившего выглядит знакомым». Номер на экране можно подменить. Завершите разговор и перезвоните по номеру, который самостоятельно нашли на официальном сайте, карте или в приложении. Не используйте номер из SMS о «блокировке счёта», даже если он оформлен убедительно.

Обычная цифровая гигиена — часть расследования

Для проверки не требуется специальное устройство, но важно, чтобы ваш телефон или компьютер был в обычном рабочем состоянии. Устанавливайте обновления операционной системы и браузера: они закрывают известные уязвимости. Используйте блокировку экрана, а для разных сервисов — разные пароли, сохранённые в надёжном менеджере паролей. Менеджер помогает заметить подмену домена: часто он не предложит сохранённый пароль на похожем, но чужом сайте.

Включите многофакторную аутентификацию там, где она доступна; предпочтительны способы, устойчивые к фишин-

гу, например ключи доступа, если сервис их поддерживает. Делайте резервные копии важных данных и проверяйте, что они действительно доступны. В настройках телефона время от времени просматривайте разрешения приложений: доступ к контактам, микрофону, камере и геолокации должен соответствовать назначению программы. Не устанавливайте приложение, которое вам прислали ссылкой, только потому, что отправитель назвал его «защитным», «служебным» или «обязательным».

Эти меры не заменяют осторожность, но уменьшают цену ошибки. Проверка подозрительного предложения безопаснее на устройстве, которое обновлено, защищено блокировкой и не переполнено программами неизвестного происхождения.

Если подозрительное уже произошло

Если вы ввели пароль, смените его с доверенного, обновлённого устройства — не по ссылке из сообщения, а через официальный сайт или приложение. Если этот пароль использовался где-то ещё, замените его и там. Завершите активные сеансы, если сервис предоставляет такую возможность, и включите или перепроверьте многофакторную защиту.

Если вы сообщили данные карты, пароль от банка или одноразовый код, немедленно свяжитесь с банком через номер на карте или в официальном приложении. Если установили неизвестную программу, не вводите в ней новые данные; об-

ратитесь в официальную службу поддержки или к специалисту, которому доверяете. Не ругайте себя и не тратьте первые минуты на выяснение, как именно вас обманули. Сначала ограничьте возможный ущерб, затем сохраните сообщение и обратитесь туда, кто может помочь.

Ваш личный порядок действий

Потратьте несколько минут и запишите правила, которым сможете следовать, когда появится срочное сообщение:

- Если пришла ссылка:** не открываю; нахожу организацию независимо; проверяю опубликованный на её сайте адрес и связываюсь по известному официальному каналу.

- Если прислали файл:** не скачиваю и не запускаю неизвестное вложение; уточняю отправителя через другой канал; рабочие документы передаю на проверку по правилам своей организации.

- Если позвонили:** не сообщаю пароли и коды; завершаю разговор; сам набираю официальный номер.

- Если уже передал данные:** меняю пароль с доверенного устройства, закрываю активные сеансы и сразу связываюсь с банком или соответствующей службой.

Можно дополнить этот список ещё одним правилом: «Если меня торопят, я сначала проверяю, потом решаю». Так оно продолжает урок предыдущих глав и не требует каждый раз заново собираться с духом.

OSINT — это не соревнование в технической ловкости и не обещание безошибочно распознать любую уловку. Это

дисциплина спокойного внимания: заметить, что именно утверждается, найти сведения в источниках, не зависящих от подозрительного отправителя, и не выдавать предположение за факт. Проверять можно, не вступая в контакт с создателями сомнительного сообщения. Иногда лучший результат расследования — не полный портрет неизвестного человека, а ясное решение не нажимать кнопку и проверить предложение другим путём.

Первичная проверка предложения: быстрый список тревожных признаков

Вечером во вторник Марине попало предложение, которое казалось почти подарком: новая камера — на сорок процентов дешевле, чем в крупных магазинах. Сайт выглядел аккуратно, возле товара горели пять звёзд, а таймер обещал, что скидка закончится через девять минут. Внизу страницы значилось: «Официальный партнёр». Марина уже потянулась за картой, когда заметила, что продавец просит перевести деньги на счёт физического лица.

Это ещё не доказывало мошенничество. Но это меняло вопрос. Не «похоже ли предложение на настоящее?», а «какие его важные обещания подтверждаются независимо — и насколько надёжно?».

Публичные сведения о продавце часто напоминают россыпь пазлов на столе: регистрация компании, отзывы, страница в социальной сети, адрес, упоминание в каталоге. Сложность не в том, чтобы собрать как можно больше кусочков. Важно понять, какие из них относятся к делу, кто их опубликовал и подтверждают ли они друг друга.

Сразу обозначим границу: OSINT — это работа с законно доступной информацией. Не нужно взламывать аккаун-

ты, обходить ограничения доступа, выдавать себя за другого человека, преследовать владельца сайта или публиковать чьи-либо личные данные. Для проверки предложения достаточно открытых источников и безопасного поведения. Если сведения нельзя получить без нарушения приватности или правил сервиса, значит, это не подходящий способ проверки.

Быстрый список тревожных признаков

Начать можно с короткого просмотра. Он не выносит приговор, а помогает решить, стоит ли продолжать проверку.

- Торопят:** «только сейчас», «осталось одно место», «счёт заблокируют через десять минут».

- Обещают несоразмерно много:** доход без риска, необычайно низкую цену, гарантированный результат там, где он не может быть гарантирован.

- Просят секреты:** код из сообщения, пароль, данные карты, снимок документа или доступ к экрану — особенно под предлогом «подтверждения».

- Предлагают небезопасную схему оплаты:** перевод на чужую карту, криптовалюту или способ, при котором покупателю трудно оспорить платёж.

- Путают, кто именно продаёт:** на странице одна компания, в договоре другая, а деньги уходят третьему лицу.

- Ссылаются на известный бренд, но подтверждения связи нет:** логотип и слова «официальный партнёр» размещены самим продавцом, а независимый источник этого не подтверждает.

●**Скрывают базовые условия:** нет ясных правил возврата, доставки, отмены, контактов или сведений о юридическом лице там, где они должны быть доступны.

●**Отзывы выглядят однообразно:** похожие формулировки, одинаковый ритм публикаций, хвалебные тексты без конкретики.

●**Канал связи замкнут на отправителе:** вас просят не звонить в организацию обычным способом, а пользоваться только номером или ссылкой из сообщения.

●**Слова расходятся с действиями:** например, продавец говорит о защищённой оплате, но предлагает перевод без понятной защиты покупателя.

Один признак редко отвечает на вопрос «мошенничество или нет». У небольшого добросовестного магазина может быть мало отзывов; новый сайт не обязательно создан преступниками; необычный способ оплаты сам по себе не раскрывает намерений. Но несколько несостыковок — особенно вокруг личности продавца, денег и безопасности данных — достаточная причина не переходить к оплате, пока они не объяснены и не проверены.

Это важно ещё и потому, что давление меняет внимание. Когда перед глазами тикает таймер, человеку проще заметить скидку и труднее удерживать в уме условия оплаты, возврата и происхождения товара. Срочность — не доказательство обмана, но плохая обстановка для решения. Поэтому полезно сделать проверку отдельной задачей, а не частью пе-

реписки с продавцом.

Что именно мы пытаемся узнать

Перед поиском сформулируйте вопрос. Не «надёжный ли это сайт?» — слишком широко. Лучше так: «Подтверждается ли независимым источником, что компания X управляет сайтом Y и вправе продавать товар бренда Z?»

Точная формулировка помогает не подменить расследование впечатлениями. В нём полезно различать четыре вещи:

- **Факт** — непосредственно наблюдаемое обстоятельство: на странице указана такая-то цена; реестр показывает запись с таким-то названием.

- **Заявление** — то, что сообщает продавец или другой источник: «мы официальный партнёр», «работаем десять лет».

- **Интерпретация** — вывод из сведений: «платёж физическому лицу не согласуется с обещанием оплаты компании».

- **Гипотеза** — возможное объяснение: «сайт может использовать чужое название».

Эти категории легко смешать. Например: «В официальном реестре не нашлось компании с таким названием» — это результат конкретного поиска. «Значит, продавец мошенник» — уже вывод, который не следует из результата автоматически. Возможно, компания зарегистрирована в другой юрисдикции, использует иное юридическое название или поиск по реестру ограничен. Честная проверка не прячет та-

кие варианты.

Учебное расследование: камера со скидкой

Вернёмся к Марине. Назовём продавца «КамераЛайт», а производителя камеры — вымышленной компанией «Орбита». На странице магазина сказано: «Официальный партнёр “Орбиты”. Работаем семь лет. Более двух тысяч довольных клиентов. Оплата полностью защищена».

Проверять каждую фразу отдельно полезнее, чем пытаться определить, «настоящий» ли сайт целиком. Для этого нужен простой журнал. Вот его центральная таблица:

Утверждение

Источник

Независимое подтверждение

Ограничение

Уверенность

«КамераЛайт» — официальный партнёр «Орбиты»

Страница продавца

В публичном списке партнёров производителя такого названия нет

Список может быть неполным; магазин может фигурировать под юридическим названием

Не подтверждено; связь остаётся неясной

Компания работает семь лет

Раздел «О нас» на сайте

В доступном реестре найдена организация с похожим названием, но сайт не указывает её регистрационный номер

Совпадение названий не доказывает, что организация владеет сайтом

Низкая уверенность в заявленном стаже

У магазина более двух тысяч покупателей

Счётчик и отзывы на его страницах

На независимых площадках найдено лишь несколько отзывов

Отсутствие отзывов не доказывает отсутствие клиентов; площадки могут не охватывать рынок

Заявление независимо не подтверждено

Оплата полностью защищена

Текст на странице оформления заказа

В условиях платёжного сервиса не описана заявленная защита; магазин предлагает перевод частному лицу

Нужно проверить, кто именно получает перевод и какие правила применимы в этой стране

Серьёзная несостыковка; до выяснения не платить

Уверенность здесь относится к аккуратности вывода, а не к вероятности преступления. Например, можно быть уверенным, что в просмотренном списке партнёров нужного на-

звания нет, и при этом не быть уверенным, что продавец не авторизован: он мог быть указан иначе или список мог оказаться неполным. Это не уклончивость, а точность.

Обратите внимание на разницу между источниками. Сайт продавца и его же страница в социальной сети — не два независимых подтверждения. Владелец может контролировать обе площадки и перенести туда одно и то же утверждение. Подлинный каталог производителя, официальный реестр организаций и правила платёжного сервиса отвечают на другие вопросы и обычно не зависят от продавца. Но и они не всеисильны: реестр подтверждает существование юридической записи, а не честность каждого магазина, который на неё ссылается.

Как провести первичную проверку

1. Запишите, что именно обещают. Не ограничивайтесь ощущением «выгодное предложение». Выпишите конкретные утверждения: кто продавец, что продаёт, откуда товар, кто его доставит, как принимается оплата, какие гарантии даются. Чем конкретнее обещание, тем проще найти источник, который может его проверить.

2. Соберите минимум данных. Для первого прохода обычно достаточно названия магазина, адреса сайта, юридического названия, указанного контакта, условий оплаты и доставки. Не отправляйте продавцу свои документы или дополнительные сведения «для проверки». Не нужно собирать личную информацию о владельце: цель — оценить предло-

жение, а не разыскивать человека.

3. Ищите по нескольким независимым каналам. Проверьте сведения на самом сайте, затем отдельно — в источнике, который должен знать ответ. Статус партнёра проверяйте у производителя; регистрационные данные — в подходящем государственном реестре; условия оплаты — у платёжной организации, а не по обещанию магазина. Для репутации можно посмотреть несколько независимых площадок. Поиск по точной фразе из отзыва, адресу сайта, названию и официальному номеру компании иногда помогает найти повторяющиеся тексты или старые упоминания.

Поисковая система — это указатель, а не судья. Она может показывать устаревший фрагмент страницы, смешивать однофамильцев, поднимать популярный материал выше надёжного. Один результат поиска, один отзыв или одно совпадение названия не дают достаточного основания ни для доверия, ни для обвинения.

4. Сохраняйте происхождение сведений. В журнале проверки должны быть: вопрос, поисковый запрос, источник, дата доступа, что найдено, ограничение и следующий шаг. Например: «Вопрос — кто владеет сайтом? Запрос — название магазина и регистрационный номер. Источник — государственный реестр, дата — 14 мая. Найдено — юридическое лицо с похожим названием. Ограничение — на сайте магазина нет номера, поэтому связь не установлена. Следующий шаг — проверить сведения через официальный кон-

такт производителя или продавца, найденный независимо».

Запись даты важна: сайты меняют условия, компании переезжают, реестры обновляются. Данные, верные полгода назад, сегодня могут быть бесполезны. Учитывайте и юрисдикцию: реестры разных стран различаются, часть сведений может быть закрыта или индексироваться не полностью. «Не нашёл» означает «не нашёл в проверенном источнике по этому запросу на эту дату», а не «такого не существует».

5. Сопоставьте результаты, а не просто сложите их. Несколько источников полезны, если они действительно независимы и подтверждают один и тот же факт. Две статьи, скопировавшие пресс-релиз магазина, не становятся двумя подтверждениями. А вот сведения от производителя, платёжного сервиса и государственного реестра могут дать разные части картины. Ищите не только совпадения, но и противоречия: разные названия получателя платежа, адреса, сроки работы, условия возврата.

6. Выберите следующий шаг по уровню риска. Если ключевое обещание не подтвердилось, задайте продавцу конкретный вопрос — например, попросите указать юридическое название партнёра и регистрационный номер. Затем проверьте ответ через источник, найденный самостоятельно, а не по ссылке из того же сообщения. Если продавец уклоняется, усиливает давление, требует секретный код или предлагает обойти безопасный способ оплаты, прекращайте взаимодействие. Вам не требуется доказать мошенничество, что-

бы отказаться от сомнительной покупки.

Небольшая тренировка

Представьте предложение: «Годовая подписка на учебный сервис со скидкой 80%. Осталось три места. Для активации пришлите код из СМС. Мы официальный партнёр крупной платформы». На странице есть логотип платформы, но нет ясного названия юридического лица.

Разделите сведения на три группы:

Известно: продавец просит код из СМС; указывает ограничение по времени; заявляет о партнёрстве; юридическое лицо на странице не обозначено ясно.

Предполагается: возможно, скидка ненастоящая; возможно, логотип используется без разрешения. Пока это гипотезы.

Неизвестно: действительно ли продавец связан с платформой; кому принадлежит сайт; зачем нужен код и какое действие он подтверждает.

Следующий шаг не должен состоять в отправке кода «ради проверки». Нужно найти официальный сайт платформы самостоятельно, посмотреть перечень партнёров или обратиться в поддержку через опубликованный там контакт. А код не передавать: он может подтверждать вход или платёж, а не право на скидку.

Не искать абсолютную уверенность

Первичная проверка не превращает интернет в прозрачное стекло. Она не обещает узнать все намерения продавца

и не заменяет юридическую или техническую экспертизу. Её задача практичнее: отделить собственные слова продавца от независимых подтверждений, обнаружить важные несостыковки и понять, чего вы пока не знаете.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.