

ВИКТОРИЯ КАБАНЕЦ

КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ

50 СХЕМ ОБМАНА

В ИНТЕРНЕТЕ, БАНКАХ,
МАРКЕТПЛЕЙСАХ
И МЕССЕНДЖЕРАХ —
И СПОСОБЫ ЗАЩИТИТЬ
СВОИ ДЕНЬГИ



БАНКОВСКИЕ МОШЕННИКИ

ЗВОНКИ, ФЕЙКОВЫЕ
СОТРУДНИКИ, СПИСАНИЕ ДЕНЕГ



МАРКЕТПЛЕЙСЫ

ПОДДЕЛЬНЫЕ ТОВАРЫ,
ЛОЖНЫЕ ПРОДАВЦЫ



МЕССЕНДЖЕРЫ

ВЗЛОМ АККАУНТОВ,
ФАЛЬШИВЫЕ ССЫЛКИ



ФЕЙКОВЫЕ ВАКАНСИИ

ОБЕЩАНИЯ ЛЁГКОГО
ЗАРАБОТКА



КРИПТОМОШЕННИКИ

ЛОЖНЫЕ ИНВЕСТИЦИИ,
ФАЛЬШИВЫЕ ПЛАТФОРМЫ



СОЦИАЛЬНЫЕ СЕТИ

ВЗЛОМ, ОБМАН,
ПСЕВДОДРУЗЬЯ



НОВЫЕ СХЕМЫ

ИИ-ГОЛОСА, ПОДДЕЛЬНЫЕ
ВИДЕО, ДИПФЕЙКИ



ФАЛЬШИВЫЙ БАНК

ВАШ АККАУНТ
ЗАБЛОКИРОВАН

ВЫ ВЫИГРАЛИ
ПРИЗ!

ПЕРЕВЕДИТЕ
ДЕНЬГИ

ЗНАНИЯ,
КОТОРЫЕ
СОХРАНЯТ
ВАШИ
ДЕНЬГИ

Лучше
проверить,
чем потерять
деньги

Проверяй всегда:

- ☒ Кто написал?
- ☒ Настоящий ли сайт?
- ☒ Куда ведёт ссылка?
- ☒ Не передаю ли свои данные?
- ☒ Слишком невыгодное предложение?
- ☒ Что говорят отзывы?

ПРАКТИЧЕСКОЕ РУКОВОДСТВО
С РЕАЛЬНЫМИ ПРИМЕРАМИ, ПРОВЕРЕННЫМИ СОВЕТАМИ
И ЧЕК-ЛИСТАМИ ДЛЯ ВАШЕЙ БЕЗОПАСНОСТИ

Виктория Кабанец

**Как не попасться на
уловки мошенников**

«Автор»

2026

Кабанец В. В.

Как не попасться на уловки мошенников / В. В. Кабанец —
«Автор», 2026

Мошенники становятся всё изобретательнее. Как распознать обман и защитить свои деньги? В этой книге Виктория Кабанец разбирает 50 распространённых схем мошенничества: от банковских звонков и поддельных интернет-магазинов до обмана в Telegram, на маркетплейсах и с помощью искусственного интеллекта. Вы узнаете, как замечать тревожные сигналы, проверять подозрительные предложения и действовать, если вы уже столкнулись с мошенниками. Внутри — понятные примеры, практические советы, готовые шаблоны и чек-листы для вашей безопасности. **Научитесь распознавать обман до того, как потеряете деньги!**

© Кабанец В. В., 2026

© Автор, 2026

Содержание

Введение	7
Пять правил, которые стоит запомнить	8
Как устроена каждая глава	9
Часть. Банки и платежи	10
Схема 1. Звонок из «службы безопасности банка»	11
Как это выглядит	11
На чём строится обман	12
Главный тревожный сигнал	13
Что делать	14
Если вы уже отреагировали	15
Проверка на практике	16
Схема 2. «Безопасный счёт»	17
Как это выглядит	17
На чём строится обман	18
Главный тревожный сигнал	19
Что делать	20
Если вы уже отреагировали	21
Проверка на практике	22
Схема 3. Поддельное приложение банка	23
Как это выглядит	23
На чём строится обман	24
Главный тревожный сигнал	25
Что делать	26
Если вы уже отреагировали	27
Проверка на практике	28
Схема 4. Подмена номера банка	29
Как это выглядит	29
На чём строится обман	30
Главный тревожный сигнал	31
Что делать	32
Если вы уже отреагировали	33
Проверка на практике	34
Схема 5. Ложная блокировка карты	35
Как это выглядит	35
На чём строится обман	36
Главный тревожный сигнал	37
Что делать	38
Если вы уже отреагировали	39
Проверка на практике	40
Схема 6. Фальшивое возмещение комиссии	41
Как это выглядит	41
На чём строится обман	42
Главный тревожный сигнал	43
Что делать	44
Если вы уже отреагировали	45
Проверка на практике	46

Схема 7. Звонок о кредите на ваше имя	47
Как это выглядит	47
На чём строится обман	48
Главный тревожный сигнал	49
Что делать	50
Если вы уже отреагировали	51
Проверка на практике	52
Схема 8. Поддельный платёжный QR-код	53
Как это выглядит	53
На чём строится обман	54
Главный тревожный сигнал	55
Что делать	56
Если вы уже отреагировали	57
Проверка на практике	58
Схема 9. Ложное сообщение о штрафе	59
Как это выглядит	59
На чём строится обман	60
Главный тревожный сигнал	61
Что делать	62
Если вы уже отреагировали	63
Проверка на практике	64
Схема 10. Просьба установить удалённый доступ	65
Как это выглядит	65
На чём строится обман	66
Главный тревожный сигнал	67
Что делать	68
Если вы уже отреагировали	69
Проверка на практике	70
Часть. Покупки и объявления	71
Схема 11. Несуществующий интернет-магазин	72
Как это выглядит	72
На чём строится обман	73
Главный тревожный сигнал	74
Что делать	75
Если вы уже отреагировали	76
Проверка на практике	77
Схема 12. Предоплата продавцу без защиты	78
Как это выглядит	78
На чём строится обман	79
Главный тревожный сигнал	80
Что делать	81
Конец ознакомительного фрагмента.	82

Виктория Кабанец

Как не попасться на уловки мошенников

Как не попасться на уловки мошенников

50 схем обмана в интернете, банках, маркетплейсах и мессенджерах — и способы защитить свои деньги

Виктория Кабанец

Практическое руководство • 2026

Введение

Современные мошенники используют не только технологии, но и человеческие чувства: страх, срочность, доверие, надежду на выгодную покупку и желание помочь близкому. Чтобы защититься, не нужно разбираться во всех компьютерных программах. Гораздо важнее научиться замечать давление, проверять информацию независимо и не совершать необратимых действий в спешке.

Эта книга объясняет пятьдесят распространённых сценариев обмана. Мы не приводим технические инструкции, которые помогли бы злоумышленникам, а сосредоточиваемся на признаках риска и безопасных действиях. Названия площадок и сервисов приведены как примеры: сам факт упоминания не означает, что площадка поддерживает мошенничество.

Пять правил, которые стоит запомнить

- Не сообщайте коды из СМС, пароли и данные входа посторонним.
- Не переводите деньги на «безопасные счета» по указанию звонящего.
- Проверяйте сведения через самостоятельно открытые официальные сайты и приложения.
- Не устанавливайте программы удалённого доступа по просьбе незнакомца.
- При подозрении на обман прекращайте разговор и сохраняйте доказательства.

Как устроена каждая глава

Сначала показана типичная ситуация. Затем объясняется психологический приём, перечисляются признаки опасности и конкретные шаги защиты. После этого дано небольшое упражнение: его можно выполнить заранее, до столкновения с мошенниками.

Внимание: юридические процедуры, сроки оспаривания переводов и способы обращения зависят от страны, банка, договора и обстоятельств. Проверяйте актуальные правила в официальных источниках. Эта книга не заменяет консультацию специалиста.

Часть. Банки и платежи

В этой части рассматриваются ситуации, где злоумышленники используют знакомые сервисы и привычные действия. Основной принцип защиты — проверка по независимому каналу и отказ от решений под давлением.

Схема 1. Звонок из «службы безопасности банка»

Как это выглядит

Незнакомец сообщает о подозрительном переводе и требует назвать код из СМС.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Код подтверждения нужен собеседнику для доступа или операции, а не для проверки вашей личности.

Что делать

Прекратите разговор и сами позвоните в банк по номеру с карты или официального сайта.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 2. «Безопасный счёт»

Как это выглядит

Вас убеждают перевести накопления на якобы защищённый счёт.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Банк не защищает средства переводом на неизвестные реквизиты.

Что делать

Ничего не переводите; самостоятельно свяжитесь с банком.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 3. Поддельное приложение банка

Как это выглядит

Ссылка ведёт на страницу установки похожего приложения.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Проверяйте издателя приложения и адрес источника.

Что делать

Не устанавливайте файл из сообщения; используйте официальные каналы банка.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 4. Подмена номера банка

Как это выглядит

На экране отображается знакомый номер, но звонит мошенник.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Номер на экране не доказывает личность звонящего.

Что делать

Не доверяйте отображаемому номеру; перезвоните сами.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 5. Ложная блокировка карты

Как это выглядит

Сообщение требует срочно перейти по ссылке и ввести данные карты.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Срочность и ссылка на сторонний домен — тревожные признаки.

Что делать

Откройте приложение банка самостоятельно.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 6. Фальшивое возмещение комиссии

Как это выглядит

Обещают вернуть удержанную комиссию после оплаты «активации».

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Настоящее возмещение не требует перевода на личную карту незнакомца.

Что делать

Проверяйте право на возврат напрямую у организации.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 7. Звонок о кредите на ваше имя

Как это выглядит

Пугают оформлением займа и предлагают «отменить» его встречным кредитом.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Не оформляйте кредит по инструкции звонящего.

Что делать

Проверьте информацию через банк и официальные кредитные сведения.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 8. Поддельный платёжный QR-код

Как это выглядит

QR-код ведёт на страницу оплаты другого получателя.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

QR-код — только способ передачи реквизитов, не знак надёжности.

Что делать

Проверяйте имя получателя и назначение перед подтверждением.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 9. Ложное сообщение о штрафе

Как это выглядит

Приходит требование оплатить штраф по короткой ссылке.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Не вводите платёжные данные на сайте из сообщения.

Что делать

Проверьте начисление через официальный государственный сервис.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 10. Просьба установить удалённый доступ

Как это выглядит

«Специалист» просит включить демонстрацию экрана или программу управления.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Доступ к экрану может раскрыть коды и личные данные.

Что делать

Отключите сеанс, удалите подозрительное ПО и свяжитесь с банком.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Часть. Покупки и объявления

В этой части рассматриваются ситуации, где злоумышленники используют знакомые сервисы и привычные действия. Основной принцип защиты — проверка по независимому каналу и отказ от решений под давлением.

Схема 11. Несуществующий интернет-магазин

Как это выглядит

Красивый сайт предлагает популярный товар по необычно низкой цене.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Скидка сама по себе не доказательство мошенничества, но требует проверки.

Что делать

Проверьте сведения о продавце, независимые отзывы и условия возврата.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.
- Сообщите о подозрительном аккаунте в поддержку площадки через официальный интерфейс.

Если вы уже отреагировали

Сразу прекратите контакт. Если раскрыты банковские данные или переведены средства — немедленно свяжитесь с банком по официальному номеру и уточните блокировку, оспаривание операции и другие доступные меры. Если передан пароль — измените его с доверенного устройства, завершите посторонние сеансы и включите дополнительную защиту. При угрозах или хищении обратитесь в компетентные органы.

Проверка на практике

Представьте, что сообщение пришло вашему близкому. Какой независимый канал проверки вы предложите? Какое действие нужно отложить до подтверждения? Запишите короткую фразу для отказа.

Моя безопасная фраза: «Я проверю информацию самостоятельно через официальный канал. Сейчас ничего не перевожу и никаких кодов не называю».

Мои

действия:

Схема 12. Предоплата продавцу без защиты

Как это выглядит

Продавец настаивает на переводе вне платформы.

На чём строится обман

Собеседник пытается сократить время на размышление и заставить вас доверять сообщению больше, чем собственным проверкам. Часто используется авторитет организации, эмоциональная история или обещание выгоды. Отдельный признак ещё не доказывает мошенничество, но сочетание давления, непрозрачных условий и просьбы о деньгах требует остановиться.

Главный тревожный сигнал

Переход в сторонний мессенджер может лишить защиты площадки.

Что делать

Используйте предусмотренные площадкой способы оплаты и доставки.

- Не выполняйте указания из неожиданного сообщения, пока не проверите источник.
- Не передавайте секретные коды, пароли и полный доступ к устройству.
- Сохраните ссылку, время, скриншоты и сведения о платеже, если контакт уже состоялся.

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.