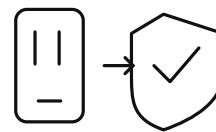


ПАМЯТКА 15



Пауза → проверка → действие

Требуют оплатить доставку или штраф

Проверяйте заказ или начисление в самостоятельно открытом официальном сервисе. Логотип, правильная фамилия и небольшая сумма не подтверждают подлинность сообщения или страницы оплаты.

Цифровая безопасность · Иван Юрьевич · Версия 1.0 · Редакционная проверка: 2026-10-26

Версия для чёрно-белой печати

Как понять, что случилось

- Вас торопят оплатить повторную доставку, пошлину, штраф или комиссию по ссылке из SMS. Обещают блокировку, потерю посылки либо увеличение суммы, если не сделать это сразу.
- Адрес отличается от привычного, ссылка сокращена, платёж предлагают на карту физического лица или за пределами приложения. Иногда данные заказа выглядят правдоподобно, поэтому одного совпадения недостаточно.

Что сделать сейчас

1. Не открывайте платёж из сообщения. Самостоятельно зайдите в приложение перевозчика, маркетплейса или официальный кабинет организации и найдите свой заказ либо начисление.
2. Сравните получателя, назначение и сумму внутри проверенного сервиса. При сомнениях обратитесь в поддержку оттуда, не используя телефон и чат из подозрительного сообщения.
3. Если только открыли ссылку, закройте её и уточните, вводили ли данные и запускали ли файлы. Открытие, передача пароля, кода и установка приложения требуют разных действий.
4. Если ввели данные карты, подтвердили платёж или уже перевели деньги, немедленно свяжитесь со своим банком официальным способом. Не ждите разбирательства с доставкой.

Что дальше

- Сохраните сообщение, адрес и данные операции для поддержки или банка. Для фишингового письма используйте встроенную жалобу почтового сервиса; не пересылайте активную ссылку всем знакомым.
- Если раскрыт пароль, смените его в настоящем сервисе и в других местах, где он повторялся. Проверьте сеансы и контакты восстановления с безопасного устройства.
- Проверьте подписки и последующие списания, если подозрительный платёж всё же прошёл. Настройте уведомления банка и оплачивайте заказы через выбранные заранее каналы.

Чего не делать

- Не переводите деньги для «возврата ошибочного штрафа» и не сообщайте код для «отмены доставки». Код может подтверждать вход, платёж или иной доступ, а не отмену.
- Не считайте HTTPS, красивую страницу и первое место в поиске доказательством честности. Не вводите реквизиты на сайте, пока не проверили его независимо от присланной ссылки.

Ваш вариант ситуации

Посылка действительно ожидается

- Всё равно проверьте сообщение через приложение перевозчика или маркетплейса. Совпадение события повышает убедительность приманки, но не доказывает принадлежность страницы.

Государственное начисление

- Проверьте его на самостоятельно открытом официальном портале соответствующего ведомства. Если данных нет, уточните вопрос через его справку; не оплачивайте по телефонному требованию.

Официальная помощь

- Google: поддельные письма и сайты support.google.com
- МВД: ложные сообщения Госуслуг mvdmedia.ru

Версия 1.0. Редакционная проверка 2026-10-26. Читайте эту памятку на learn.ivan-it.net/memos/delivery-fine-payment.

Связанные уроки: Ссылки, сайты и QR; Покупки, платежи и заработок; Проверьте сообщение о Госуслугах без спешки.

Источники: Google: Как защититься от фишинга и пожаловаться на него (проверка 2026-10-26); МВД России: Проверяйте подлинность сообщений от имени Госуслуг (проверка 2026-10-26); Т-Банк: Что делать, если перевели деньги мошенникам (проверка 2026-10-26).

Возможности сервисов меняются; результат восстановления и возврат денег не гарантируются. При риске денег немедленно обращайтесь в свой банк. Учебный сайт не заменяет официальную поддержку.