

Доставка с подвохом: как мошенники обманывают покупателей и продавцов

Мы заказываем товары онлайн, продаем вещи через сайты объявлений и получаем посылки практически не задумываясь. Привычным сценарием доставки все чаще пользуются и мошенники: представляются курьерами, присылают ссылки на «безопасную доставку», требуют код из SMS или используют возврат для подмены товара.

Цель одна — заставить человека действовать быстро и не проверять информацию: сообщить секретный код, перейти по фишинговой ссылке, перевести деньги или невнимательно принять возврат.

«Подтвердите доставку»: что скрывается за просьбой назвать код

Это одна из самых простых и при этом эффективных схем. Человеку звонят или пишут якобы из службы доставки, интернет-магазина или маркетплейса и сообщают, что на его имя оформлена посылка. Ее нужно подтвердить, отменить или перенести на другое время.

Иногда мошенники заранее знают имя человека и другие базовые сведения. Это создает ощущение, что звонок действительно связан с реальным заказом. Затем следует просьба: «Для подтверждения доставки назовите код из SMS».

На самом деле SMS-код может подтверждать вовсе не получение посылки, а вход в аккаунт, изменение настроек или другую операцию. Передав его постороннему, человек фактически сам подтверждает действие, которого не совершал. Полученный доступ злоумышленники могут использовать для дальнейших мошеннических действий.

О подобных схемах в июле 2026 года отдельно предупреждала Генеральная прокуратура Казахстана.

Сценарий может быть и другим. Например, «курьер» сообщает, что доставка задержана, посылка находится на складе или за повторную отправку необходимо внести небольшую сумму. Для оплаты человеку присылают ссылку на страницу, внешне похожую на сайт известной службы доставки. На самом деле это фишинговый ресурс, созданный для получения платежных данных.

Используются не только ссылки. В сообщении о «пропущенной доставке» может находиться QR-код с предложением оплатить повторную отправку. После сканирования пользователь также попадает на поддельную страницу, где его просят ввести данные банковской карты.

Поэтому QR-код из неизвестного сообщения следует воспринимать так же осторожно, как незнакомую ссылку.

Если вы действительно ждете заказ, не продолжайте разговор по сценарию звонящего. Самостоятельно откройте приложение или официальный сайт магазина либо службы доставки и проверьте информацию там. А если ничего не заказывали, тем более не подтверждайте «посылку» и не называйте никаких кодов.

«Оформим доставку через специальный сервис»

Еще одна распространенная схема начинается с обычного объявления о продаже. Выставляете вещь на торговой площадке, и вскоре появляется заинтересованный покупатель. Он сообщает, что находится в другом городе и предлагает воспользоваться доставкой. На первый взгляд все логично: покупатель оплачивает товар, а курьер забирает его у продавца.

Но затем появляется ссылка: «Здесь оформите доставку», «По этой ссылке получите оплату», «Введите данные карты, чтобы зачислить деньги».

Страница может практически полностью копировать известную торговую площадку или службу доставки. На ней продавца просят указать номер карты, срок ее действия, код с обратной стороны либо SMS-код.

Вместо получения оплаты человек рискует передать мошенникам платежные данные и столкнуться с несанкционированными операциями. О фальшивых сервисах доставки, которые злоумышленники используют под видом покупателей, также предупреждал KZ-CERT.

Иногда мошенники обходятся без фишингового сайта. Под видом оформления сделки они требуют сначала оплатить «комиссию за получение денег», «страховку», «резервирование доставки» или другой обязательный платеж. После перевода собеседник исчезает.

Важно понимать: сама доставка не является проблемой. Опасность возникает, когда неизвестный человек уводит сделку за пределы официальной площадки, присылает стороннюю ссылку или требует неожиданный платеж.

Если сервис объявлений предусматривает встроенную оплату или доставку, используйте их и следуйте инструкциям самой площадки. А если «покупатель» торопит, настаивает на переходе по его ссылке или убеждает, что деньги можно получить только после оплаты комиссии, — это серьезный повод остановить сделку и все проверить.

«Возврат» с неприятным сюрпризом

Мошенническая схема может возникнуть и тогда, когда товар уже продан.

Представим обычную ситуацию: продавец отправил товар через торговую площадку, покупатель получил его, а затем оформил возврат. Псылка возвращается, но внутри оказывается уже другая, более дешевая или неисправная вещь. Если товары внешне похожи, подмену можно заметить не сразу.

Например, продавец отправил исправный смартфон, а при возврате получил похожее устройство с другим серийным номером или неисправный товар.

У крупных торговых площадок обычно предусмотрены механизмы разрешения споров и защиты участников сделки. Но подтвердить свою позицию гораздо проще, если заранее сохранить доказательства того, что именно было отправлено и в каком состоянии.

Поэтому при продаже дорогой техники или других ценных вещей сделайте фотографии или видео товара, зафиксируйте его внешний вид, комплектацию и серийный номер, если он имеется. Полезно также снять процесс упаковки перед передачей посылки службе доставки.

При получении возврата не спешите подтверждать завершение сделки. Проверьте товар и его комплектацию. Если обнаружили подмену, повреждения или другие несоответствия, сразу зафиксируйте их на фото или видео и обратитесь в службу поддержки площадки.

Не стоит переводить спор исключительно в личную переписку с покупателем. Если сделка проходила через маркетплейс, используйте предусмотренный им механизм обращения и сохраняйте сведения о заказе, переписку, документы об отправке, фотографии и видеозаписи до окончательного разрешения ситуации.

Почему мошенники используют именно доставку

Причина проста: доставка дает естественный повод неожиданно связаться с человеком. Звонок «из банка» многие уже воспринимают настороженно, а сообщение «от курьера» кажется обычным. Тем более человек действительно может ждать заказ, возврат или оплату за проданную вещь. Поэтому фразы «ваша посылка задержана», «курьер не смог доставить заказ», «подтвердите получение» легко воспринимаются как часть реальной сделки.

Для убедительности мошенники используют логотипы известных компаний, копируют оформление сайтов, создают похожие адреса страниц и могут располагать некоторыми персональными данными человека. Но внешнее сходство еще не подтверждает подлинность сообщения или сайта.

Запомните три простых правила:

- Код из SMS — не пароль для курьера.
- Данные карты — не способ получить оплату от покупателя.
- А присланная ссылка или QR-код — не доказательство того, что перед вами официальный сервис.

Как защитить себя при покупке и продаже онлайн

1. **Не сообщайте секретные данные.** SMS-коды, пароли, PIN-коды и другие конфиденциальные сведения нельзя передавать посторонним, кем бы они ни представлялись.
2. **Проверяйте заказ самостоятельно.** Откройте официальное приложение или сайт магазина, маркетплейса либо службы доставки и посмотрите статус отправления.
3. **Не переходите по неожиданным ссылкам и QR-кодам.** Особенно если через них предлагают подтвердить доставку, получить деньги или оплатить небольшую комиссию.
4. **Не выводите сделку за пределы площадки.** При продаже через сервис объявлений используйте встроенные инструменты оплаты и доставки, если они предусмотрены.
5. **Не оплачивайте внезапные «комиссии».** «Страховка», «резерв», «активация получения денег» и другие платежи, появившиеся только по просьбе незнакомого человека, должны насторожить.
6. **Фиксируйте дорогие отправления.** Сохраняйте фото и видео товара, его состояния, комплектации, серийного номера и упаковки, а также документы и переписку до полного завершения сделки.
7. **Если данные уже переданы мошенникам — действуйте сразу.** Свяжитесь с банком через официальный канал, примите меры для защиты счета и при необходимости обратитесь в правоохранительные органы.

Если для получения посылки или денег за проданную вещь вас просят выйти за пределы официального сервиса, сообщить SMS-код, перейти по неизвестной ссылке или срочно что-то оплатить, остановитесь и проверьте информацию самостоятельно. Это поможет вам сохранить не только деньги, но и доступ к банковским и другим цифровым аккаунтам.