Приложение

**Данные, которые нельзя сообщать никому и никогда.**

* В киберпространстве действует простое правило: чем меньше личной информации вы раскрываете, тем труднее вас обмануть. Даже один невинный ответ может стать началом цепочки мошенничества. Ниже — перечень ключевых данных, которые всегда должны оставаться при вас.
* Финансовая информация:

– номер карты, срок действия, CVC/CVV-код, логины и пароли от интернет-банка, коды из SMS, пуш-уведомления подтверждения.

- пример: вам заказное письмо, для подтверждения доставки, отправьте код из SMS.

* Персональные документы:

– паспортные данные, ИНН, СНИЛС, фото документов.

– пример: подтвердите личность для доставки — отправьте фото паспорта.

* Аутентификационные коды:

– любые разовые пароли из SMS, push-коды, QR-коды подтверждения. Никому и ни при каких условиях.

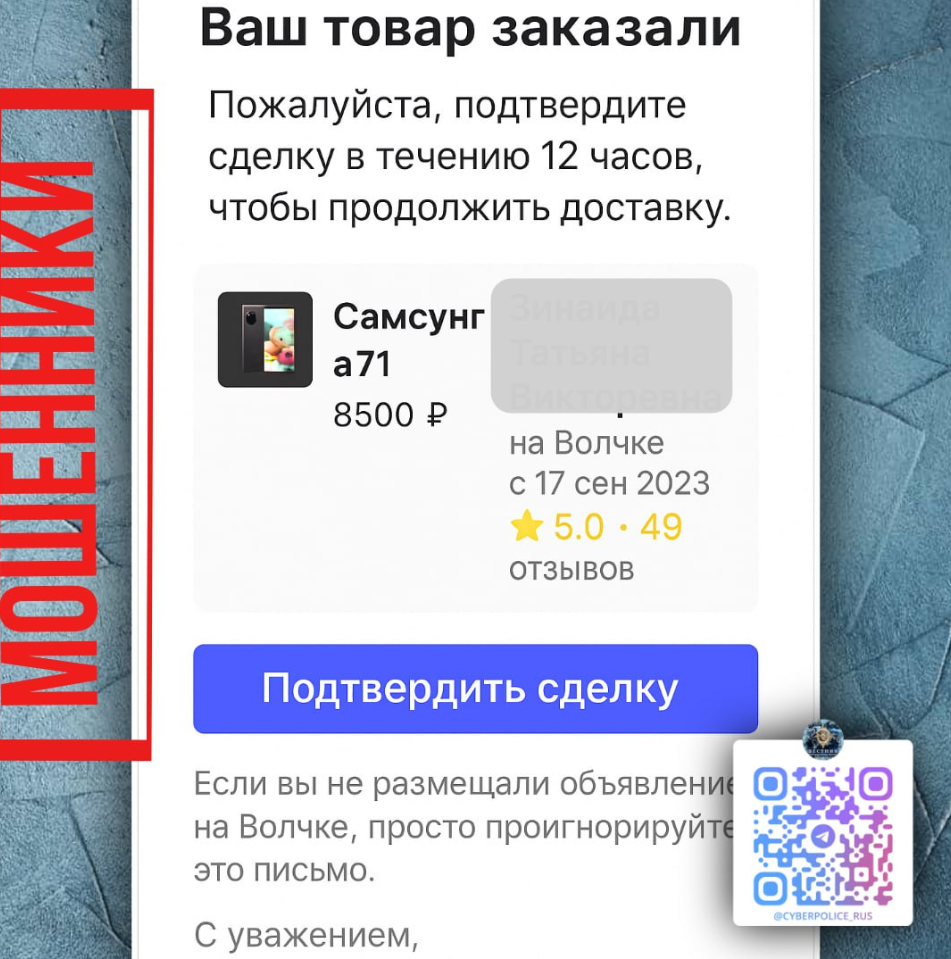
* Приватная информация:

– адрес, номера родственников, маршрут поездки, точное местоположение в режиме реального времени. Особенно — в открытых аккаунтах.

* Комбинации данных:

– имя + дата рождения + номер телефона — уже достаточно для подбора пароля, входа в почту или оформления кредита.

**Помните:** никто из официальных структур — ни банк, ни «Госуслуги», ни полиция — не попросит у вас коды доступа или паспорт по телефону или в чате. Ваши данные — ваша зона ответственности. Бережное отношение к ним — лучший вклад в безопасность вас и ваших близких.



**❗Одна из схем обмана продавцов на площадках объявлений.**

Гражданин размещает объявление о продаже чего-нибудь на популярной платформе.

☎«Покупатель» выходит на связь, уговаривает отправить ему фото товара в мессенджер под предлогом того, что фото в приложении не загружается. Перенос общения в мессенджеры необходим мошеннику, чтобы обойти встроенные в популярные приложения системы защиты и обеспечить себе дополнительную анонимность.  
  
После обсуждения предмета сделки, «покупатель» заявляет, что уже оплатил товар через площадку и продавцу нужно просто «подтвердить получение средств».

📥На электронную почту или в мессенджер пользователя поступит сообщение, максимально точно копирующее официальный стиль площадки (пример на скриншоте).

🔗Ссылка ведёт на поддельную страницу, где ввод карты и SMS-код приводит к краже денег.

✅Чтобы защититься, рекомендуется использовать официальные приложения площадок для всех операций. Не переходите по ссылкам из писем и мессенджеров. Проверяйте адрес сайта — даже мелкие отличия могут быть признаком подделки.



**❓Как понять, что тебя втягивают в преступление?**

Не все «дропы» осознают противоправный характер деятельности. И этим пользуются мошенники. Организаторы преступных схем ищут молодых — тех, кто не боится рисковать, хочет лёгких денег и не думает, что за «доставку» можно реально стать фигурантом уголовного дела.

Вот самые главные «красные флаги»:

1. Вместо собеседования — ссылка на Telegram-чат. Никаких HR, никаких офисов — сразу «в работу».

2. Никаких звонков, только текст. Чтобы соискатель не запомнил голос и не задал лишних вопросов.

3. Соискатель не знает, кто «работодатель». Только ник в мессенджере и аватарка из «нейронки».

4. Слишком лёгкие деньги. 5–10% от суммы, "за одну доставку — 7к".

5. «Крипта» и «наличка». Настоящие компании так не работают. Переводы через биткоин и «забери пакет в подъезде» — это всегда криминал.

6. Пожилые люди отдают деньги. Даже если соискатель не знает, что стало причиной: «спасение внука» или «угроза счетам» — он участвует в схеме.

7. Говорят: «Если откажешься — сядешь». Запугивание — популярный инструмент.

**Что будет, если согласиться на предложение?**

✅Ты — не помощник, ты — соучастник. Даже если «всего лишь забрал конверт».

✅Организаторов «достать» сложнее, а вот твои данные, фото и маршруты - легко.

✅Каждое следующее «задание» - новый эпизод дела. Больше «заданий» — серьезнее ответственность.

✅Вернёшь все деньги. Суд взыщет ущерб в полном размере. А твоего процента никто не вспомнит.

✅Реальное лишением свободы. А если ты помогал не мошенникам, а террористам?