Безопасность аккаунта (политика и инструкция)

1. Минимальные требования безопасности

- пароль не короче 10 символов;
- запрет повторного использования последних 5 паролей;
- обязательное подтверждение входа при смене устройства.

Рекомендуется включить 2FA (двухфакторная аутентификация). Для продавцов с подключенными выплатами 2FA обязательна.

2. Признаки подозрительной активности

Система риска может сработать, если:

- вход из новой страны + попытка смены реквизитов выплат;
- 5 неудачных попыток входа подряд;
- массовое создание объявлений (10+ за 10 минут) в высокорисковых категориях;
- частые отмены заказов после оплаты.

3. Что происходит при подозрении на взлом

- аккаунт может быть временно “заморожен” (вход ограничен);
- выплаты приостанавливаются до проверки;
- пользователю отправляется уведомление в интерфейсе (без запросов кодов/паролей).

4. Как восстановить доступ

1. Нажмите “Не могу войти”.
2. Подтвердите номер телефона или почту (в зависимости от привязки).
3. Пройдите проверку устройства (если запрошено).
4. Задайте новый пароль.
   Если доступа к телефону/почте нет — обращение в поддержку с темой “Восстановление доступа”.

Поддержка может запросить:

- последние 2–3 объявления (что размещали);
- примерные даты последних входов;

- частичную информацию о последней оплате (дата/сумма/маска карты).
  Поддержка **никогда** не просит CVV, SMS-коды, полный номер карты.

5. Смена реквизитов выплат

Смена реквизитов — операция повышенного риска:

- требуется 2FA;
- действует “карантин” 24 часа до первой выплаты на новые реквизиты;
- при смене реквизитов в период активных споров выплаты могут быть продлены до завершения проверок.

6. Ответственность пользователя

Пользователь обязан:

- не передавать доступ третьим лицам;
- не использовать “общие” номера телефонов;
- не публиковать контакты и коды подтверждения в переписке.
  Если доказано, что пользователь сам передал коды/пароли, компенсации по спорным операциям могут быть отклонены.