

Мошенники создают поддельные домовые чаты!

Цель — выманить персональные и платёжные данные, коды из SMS, доступ к аккаунтам, либо заставить сделать срочный перевод.

Как распознать поддельный домовой чат:

- **Вас неожиданно добавили в группу**, а вы не запрашивали вступление.
- **Название похоже на официальное**, но отличается парой символов (например, «Наш Дом 123» вместо «Наш Дом-123»).
- **В описании нет конкретики**: нет адреса дома, названия УК, контактов старшего по дому.
- **Администраторы анонимны** или их профили выглядят подозрительно (нет фото, мало активности).
- **Срочность и давление**: «сегодня последний день», «иначе отключат», «нужно прямо сейчас».
- **Просят перейти по ссылке**, установить приложение, ввести код

из SMS, прислать фото документа.

- **Предлагают перевод на карту физлица** вместо официальных реквизитов УК.
- **Запрещают обсуждать тему вне чата** или «жаловаться».

Главные правила безопасности:

1. **Не переходите по ссылкам** из домовых чатов, даже если они выглядят знакомо.
2. **Никогда не сообщайте**:
 - коды из SMS и push-уведомлений;
 - пароли и логины;
 - данные банковской карты (номер, срок, CVV);
 - фото документов (паспорт, СНИЛС и т. д.).
3. **Не устанавливайте приложения** по просьбе неизвестных в чате.
4. **Проверяйте информацию**:
 - позвоните в управляющую компанию по номеру



**ПРОКУРАТУРА
ОРЛОВСКОЙ ОБЛАСТИ**
предупреждает

**ОСТРОЖНО!
МОШЕННИКИ!**

**НЕ ДАЙТЕ ОБМАНУТЬ СЕБЯ
И СВОИХ БЛИЗКИХ!**

2026 год

официального сайта или квитанции;

- спросите у старшего по дому или подъезду, которого вы знаете лично;
- сверьте объявления на доске в подъезде и на сайте УК.

5. Не сканируйте QRкоды с листовок в подъезде, если на них нет полного адреса, названия УК и контактов.

Если вы уже вступили в подозрительный чат:

!Не выполняйте никаких действий по просьбам из чата.

!Выйдите из группы и заблокируйте подозрительных пользователей.

!Если вы уже перешли по ссылке и вводили данные:

- смените пароли от почты, банка, Госуслуг;
- включите двухфакторную аутентификацию;
- при подозрении на компрометацию банковской

карты – заблокируйте её, обратитесь в банк

Что делать, если вы уже стали жертвой мошенничества:

1. **Срочно свяжитесь с банком и заблокируйте карты/доступ к счёту.**
2. **Смените пароли от всех важных аккаунтов.**
3. **Обратитесь в полицию (позвоните на номер 112 или 102) и подайте заявление.**
4. **Предупредите соседей и старшего по дому о мошенническом чате.**

Объясните пожилым родственникам, что никто из управляющих организаций, банков и госорганов не просит коды из SMS в чатах.



**ПРОКУРАТУРА
ОРЛОВСКОЙ ОБЛАСТИ
предупреждает**

**ОСТОЖНО!
МОШЕННИКИ!**

**НЕ ДАЙТЕ ОБМАНУТЬ СЕБЯ
И СВОИХ БЛИЗКИХ!**

2026 год