

УНИВЕРСАЛЬНЫЕ ЭТАПЫ МОШЕННИЧЕСКИХ СХЕМ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ



@CYBERPOLICE_RUS

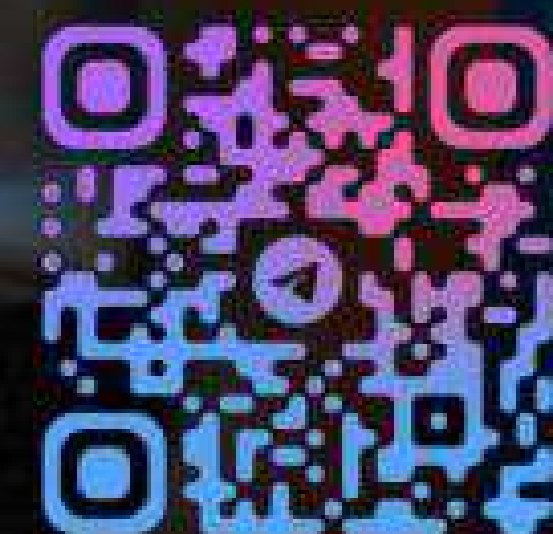
АНАЛИЗ УГОЛОВНЫХ ДЕЛ ПОКАЗЫВАЕТ, ЧТО СХЕМЫ МОШЕННИКОВ ПРИ ВСЕМ ИХ РАЗНООБРАЗИИ ОЧЕНЬ ПОХОЖИ. НЕЗАВИСИМО ОТ ПЛАТФОРМЫ ИЛИ СПОСОБА ОБМАНА, ИХ ДЕЙСТВИЯ МОЖНО РАЗДЕЛИТЬ НА ПЯТЬ ПОСЛЕДОВАТЕЛЬНЫХ ЭТАПОВ — ОТ ВЫБОРА ЖЕРТВЫ ДО ПОЛУЧЕНИЯ ДОСТУПА К ДЕНЬГАМ ИЛИ ДАННЫМ.

ЭТАП РЕКОГНОСЦИРОВКИ



ПОДГОТОВКА И ПОИСК ЦЕЛИ

Мошенники сознательно выбирают те онлайн-платформы, где чаще всего общаются дети и подростки. Они активно действуют в социальных сетях, мессенджерах, а также в чатах игровых сервисов и на сайтах с объявлениями. Эти места удобны для контакта с молодыми пользователями, где злоумышленники могут выдать себя за сверстников, продавцов или модераторов, чтобы завоевать доверие и обмануть.

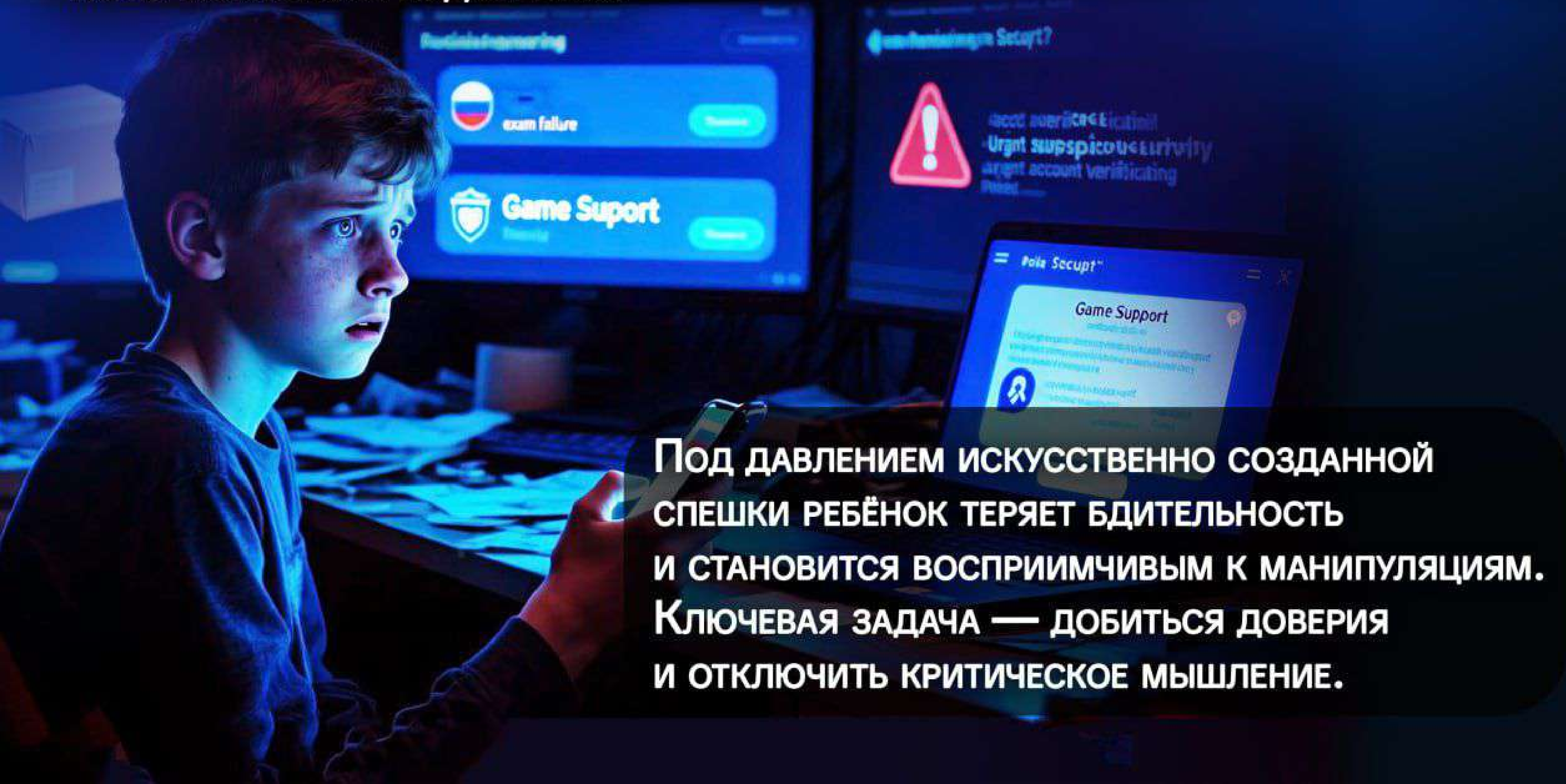


@CYBERPOLICE_RUS

УСТАНОВЛЕНИЕ КОНТАКТА И ФОРМИРОВАНИЕ ЛЕГЕНДЫ



Мошенник инициирует общение, представляясь доверенным лицом (сотрудником школы, курьером, техподдержкой). Он создаёт иллюзию срочной проблемы: угроза блокировки аккаунта, ошибка в доставке, регистрация в учебном сервисе. Легенда строится на повседневных ситуациях, чтобы исключить подозрения.



Под давлением искусственно созданной спешки ребёнок теряет бдительность и становится восприимчивым к манипуляциям. Ключевая задача — добиться доверия и отключить критическое мышление.

ЭСКАЛАЦИЯ ДАВЛЕНИЯ И ИЗОЛЯЦИЯ ЖЕРТВЫ



УСТАНОВИВ КОНТАКТ ЗЛОУМЫШЛЕННИК ИНИЦИИРУЕТ ПОЛУЧЕНИЕ ПЕРВИЧНЫХ ДАННЫХ (коды SMS, личная информация), ПОСЛЕ ЧЕГО СИТУАЦИЯ РЕЗКО «ОБОСТРЕАЕТСЯ». ПОД ПРЕДЛОГОМ УГОЛОВНОГО ДЕЛА ИЛИ АРЕСТА РОДИТЕЛЕЙ В РАЗГОВОР ВКЛЮЧАЮТСЯ ПСЕВДОСОТРУДНИКИ СИЛОВЫХ СТРУКТУР. ОБЩЕНИЕ ПЕРЕНОСИТСЯ В МЕССЕНДЖЕРЫ (TELEGRAM, WHATSAPP) ДЛЯ СКРЫТИЯ ОТ ОКРУЖЕНИЯ.



ЖЕРТВЕ ЗАПРЕЩАЮТ КОНТАКТИРОВАТЬ С СЕМЬЕЙ ПОД УГРОЗОЙ «СРЫВА ОПЕРАЦИИ». ОСНОВНАЯ ЦЕЛЬ — ПОЛНОЕ ПОДЧИНЕНИЕ И ЭМОЦИОНАЛЬНАЯ ЗАВИСИМОСТЬ.



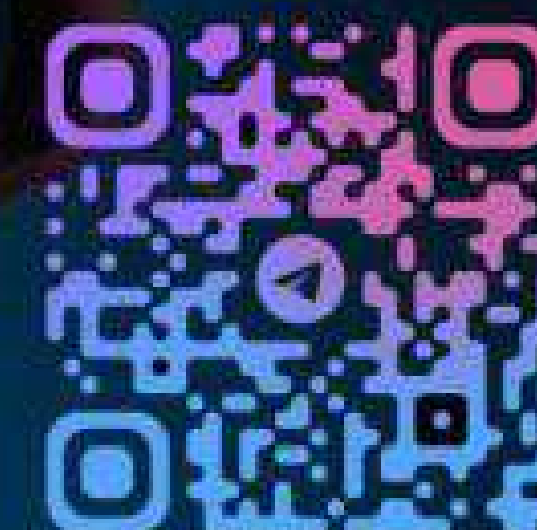
ИСПОЛНЕНИЕ: ПРИНУЖДЕНИЕ К ПЕРЕДАЧЕ СРЕДСТВ



Под непрерывным давлением в режиме реального времени (через видеозвонок или голосовую связь) мошенник принуждает жертву к действиям через ряд фиктивных предложений:



- «Декларирование средств родителей» — под видом проверки финансовой деятельности;
- «Дистанционный обыск» — с требованием перевода денег для «исключения компрометирующих находок»;
- Перевод на «безопасные счета» — якобы для защиты активов от «ареста» или «взлома».



ЭТАП: ЗАВЕРШЕНИЕ



Мошенник получает сведения о количестве средств и организует их «вывод». Способы изъятия средств:

- ПЕРЕВОДЫ ЧЕРЕЗ ОНЛАЙН-БАНК;
- ПЕРЕДАЧА НАЛИЧНЫХ КУРЬЕРУ;
- ПРИОБРЕТЕНИЕ КРИПТОВАЛЮТЫ С ПЕРЕВОДОМ НА УКАЗАННЫЙ КОШЕЛЁК.

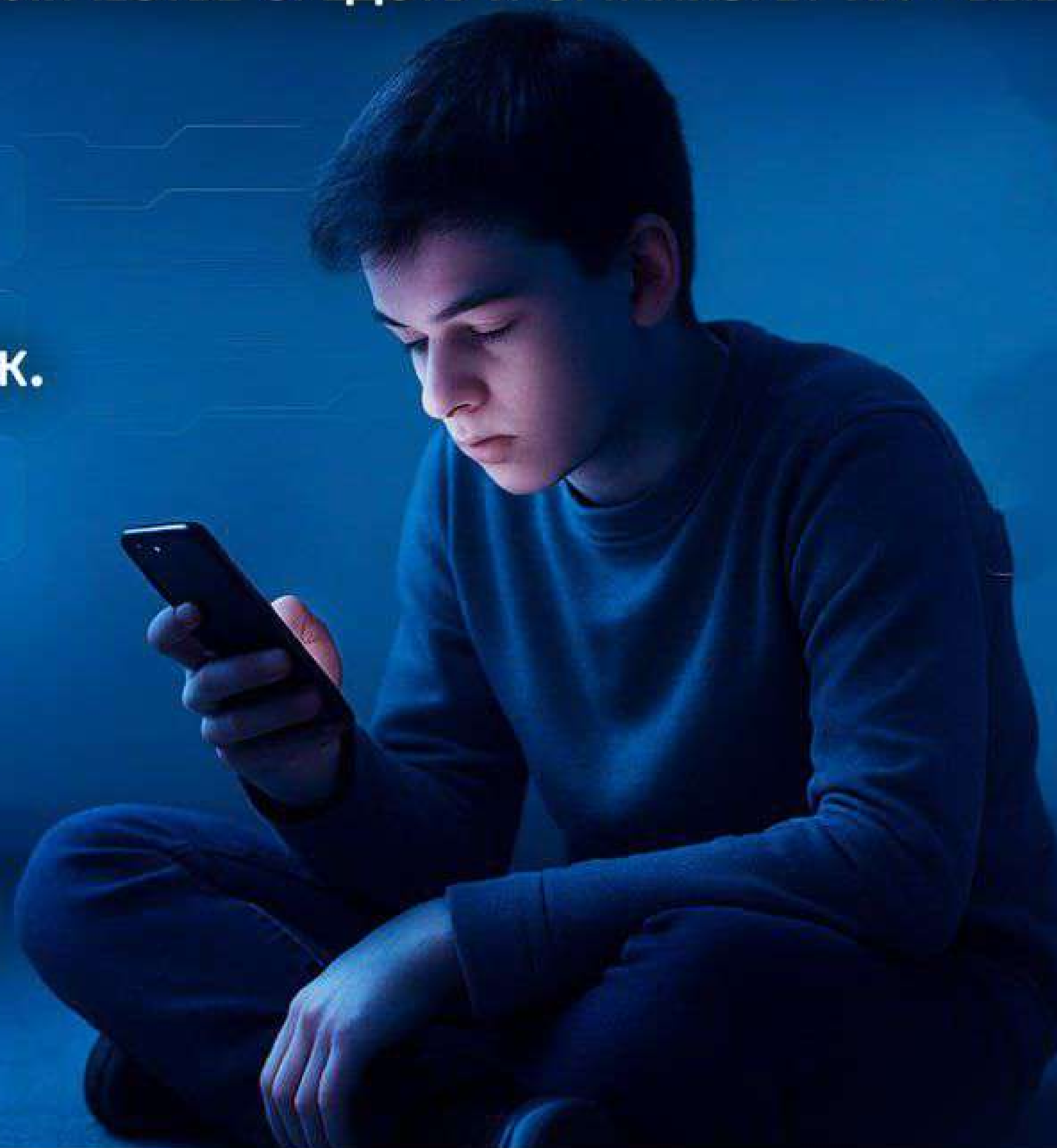
 НЕ ДОСТУПНО

НЕ ДОСТУПНО

НЕ ДОСТУПНО



@CYBERPOLICE_RUS

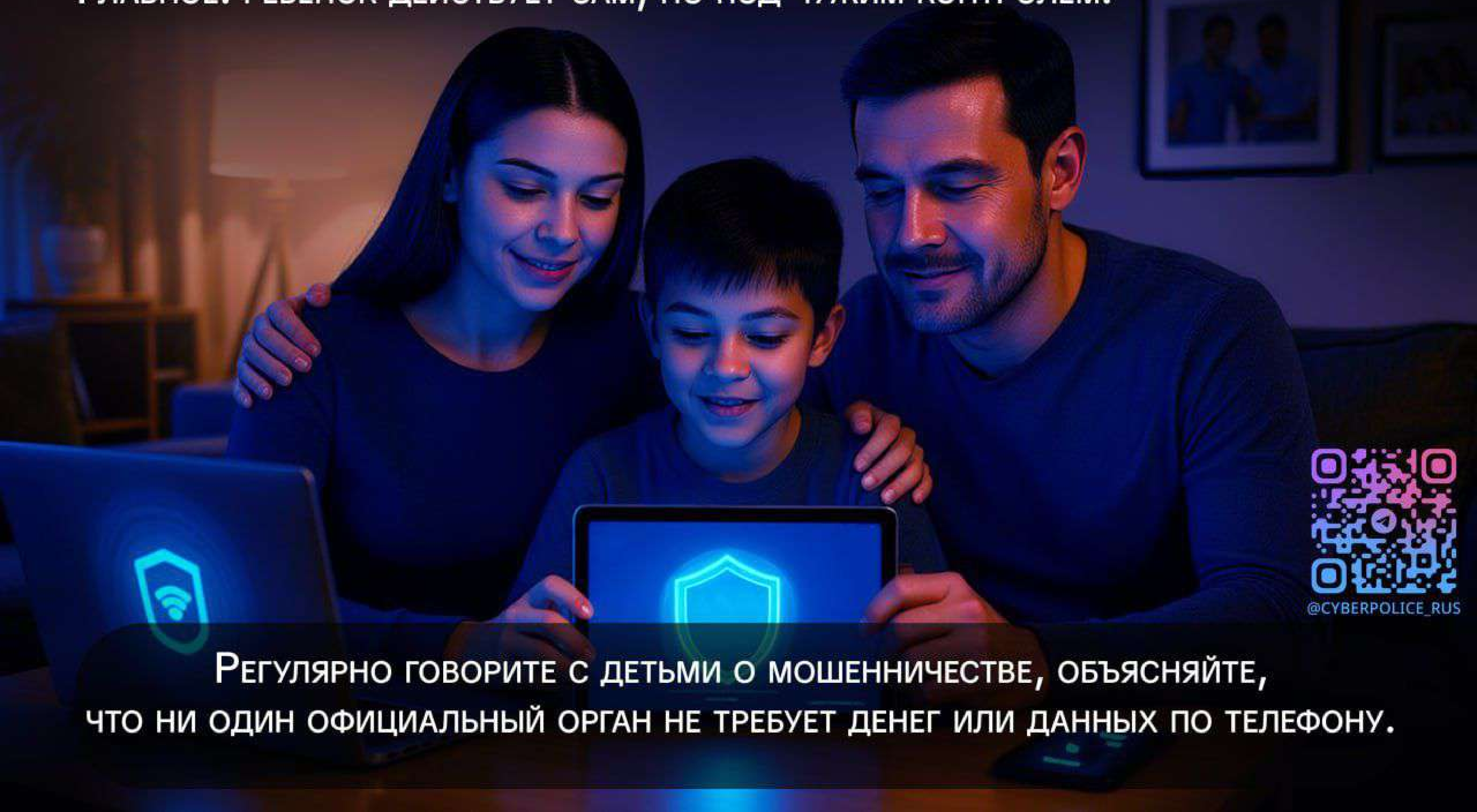


После получения денег мошенники моментально исчезают — блокируют жертву во всех мессенджерах и соцсетях, оставляя ребёнка одного с последствиями.

КАК МОШЕННИКИ БЕРУТ КОНТРОЛЬ



Дети легко поддаются манипуляциям — у них нет «социального иммунитета», они верят угрозам и паникуют. Мессенджеры дают преступникам прямой и анонимный доступ к жертве. Деньги забирают разными способами — от переводов до криптовалют и курьеров. Главное: ребёнок действует сам, но под чужим контролем.



Регулярно говорите с детьми о мошенничестве, объясняйте, что ни один официальный орган не требует денег или данных по телефону.