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

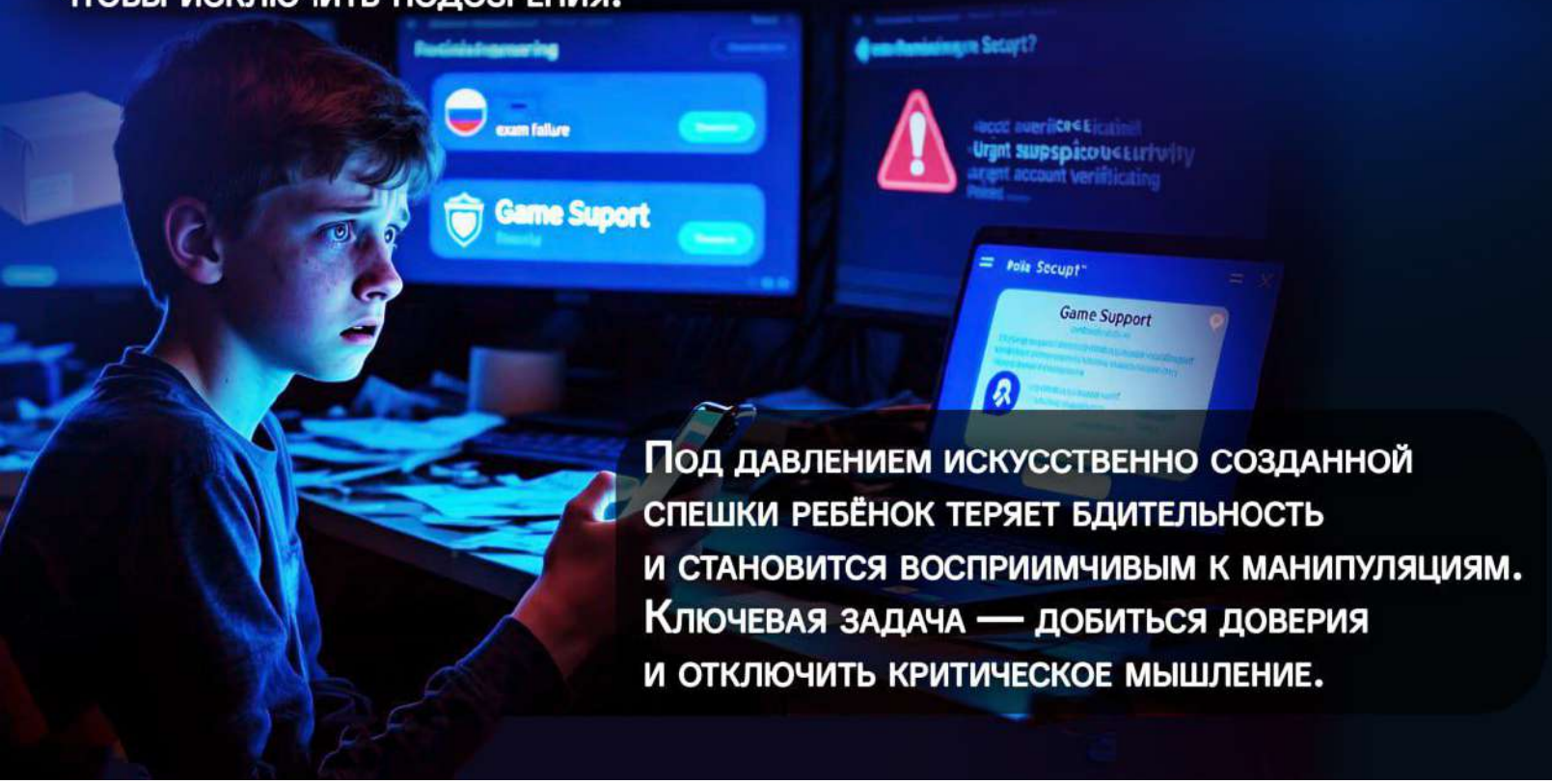
Мошенники сознательно выбирают те онлайн-платформы, где чаще всего общаются дети и подростки.
Они активно действуют в социальных сетях, мессенджерах, а также в чатах игровых сервисов и на сайтах с объявлениями.
Эти места удобны для контакта с молодыми пользователями, где злоумышленники могут выдать себя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

@CYBERPOLICE_RUS

Установление контакта и формирование легенды

@CYBERPOLICE_RUS

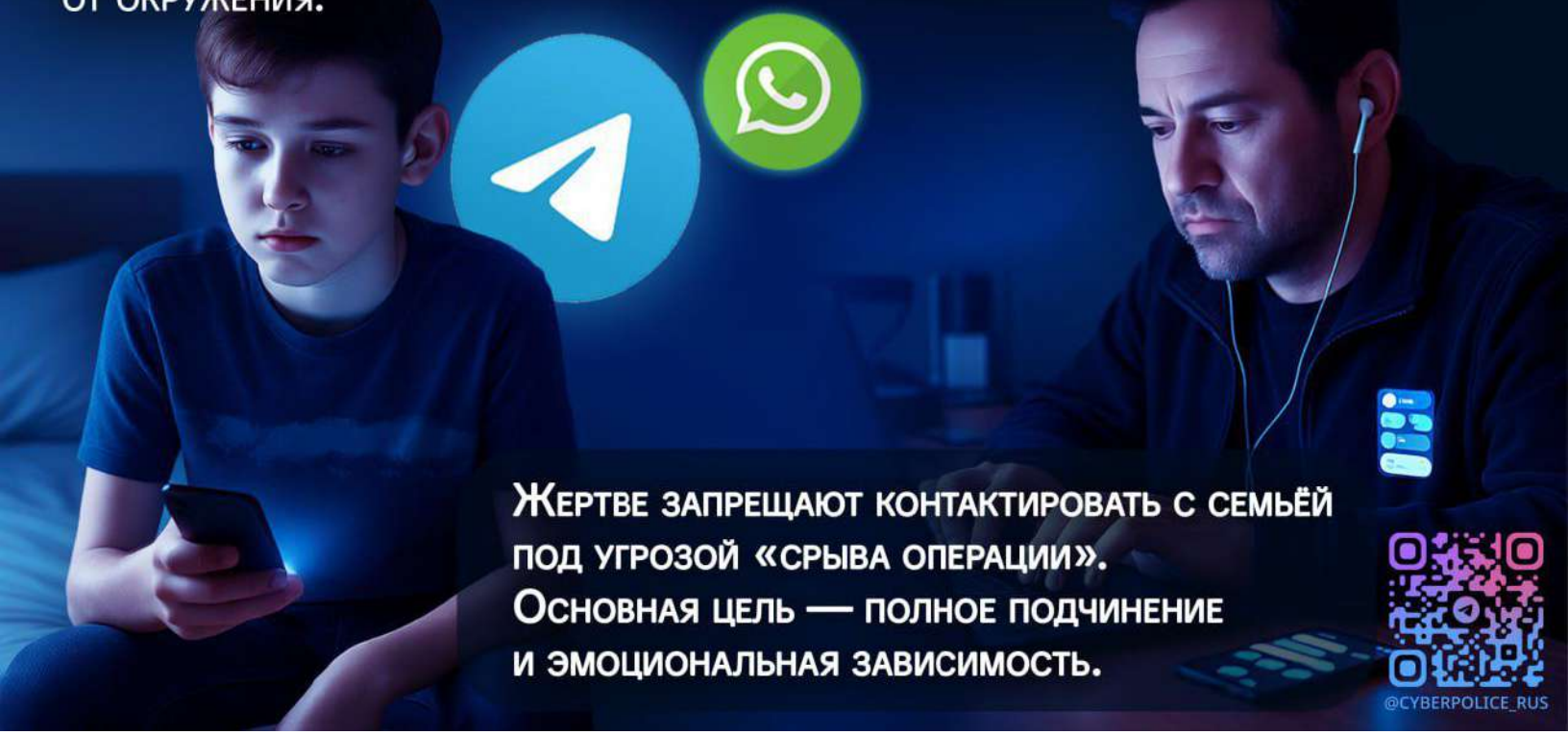
Мошенник инициирует общение, представляясь доверенным лицом (сотрудником школы, курьером, техподдержкой). Он создаёт иллюзию срочной проблемы: угроза блокировки аккаунта, ошибка в доставке, регистрация в учебном сервисе. Легенда строится на повседневных ситуациях, чтобы исключить подозрения.



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 «обостряется». 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 семьёй под угрозой «срыва операции». Основная цель — полное подчинение и эмоциональная зависимость.

@CYBERPOLICE_RUS

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 предлогов:

- «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».

@CYBERPOLICE_RUS

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.

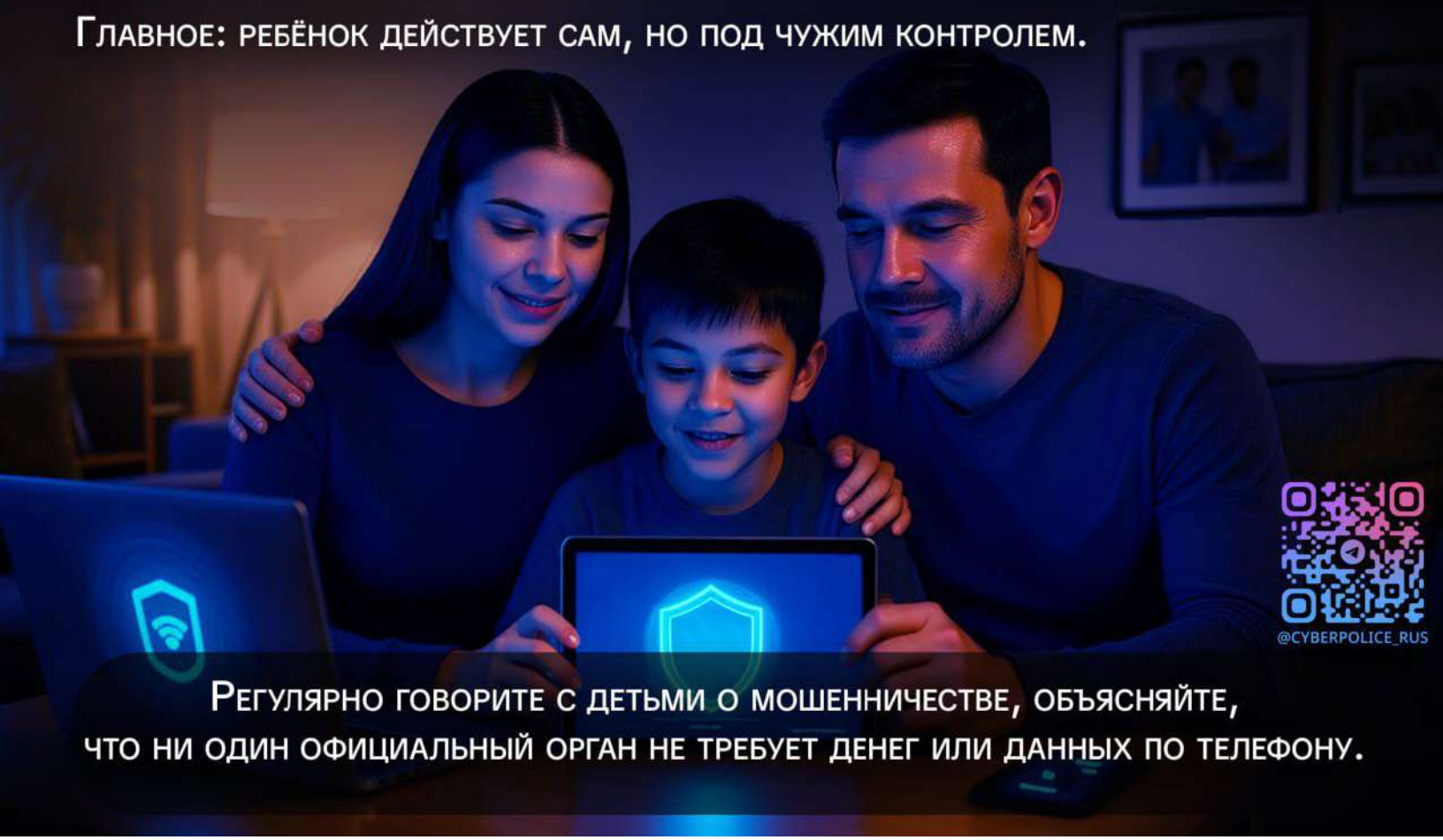
@CYBERPOLICE_RUS

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.



@CYBERPOLICE_RUS

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