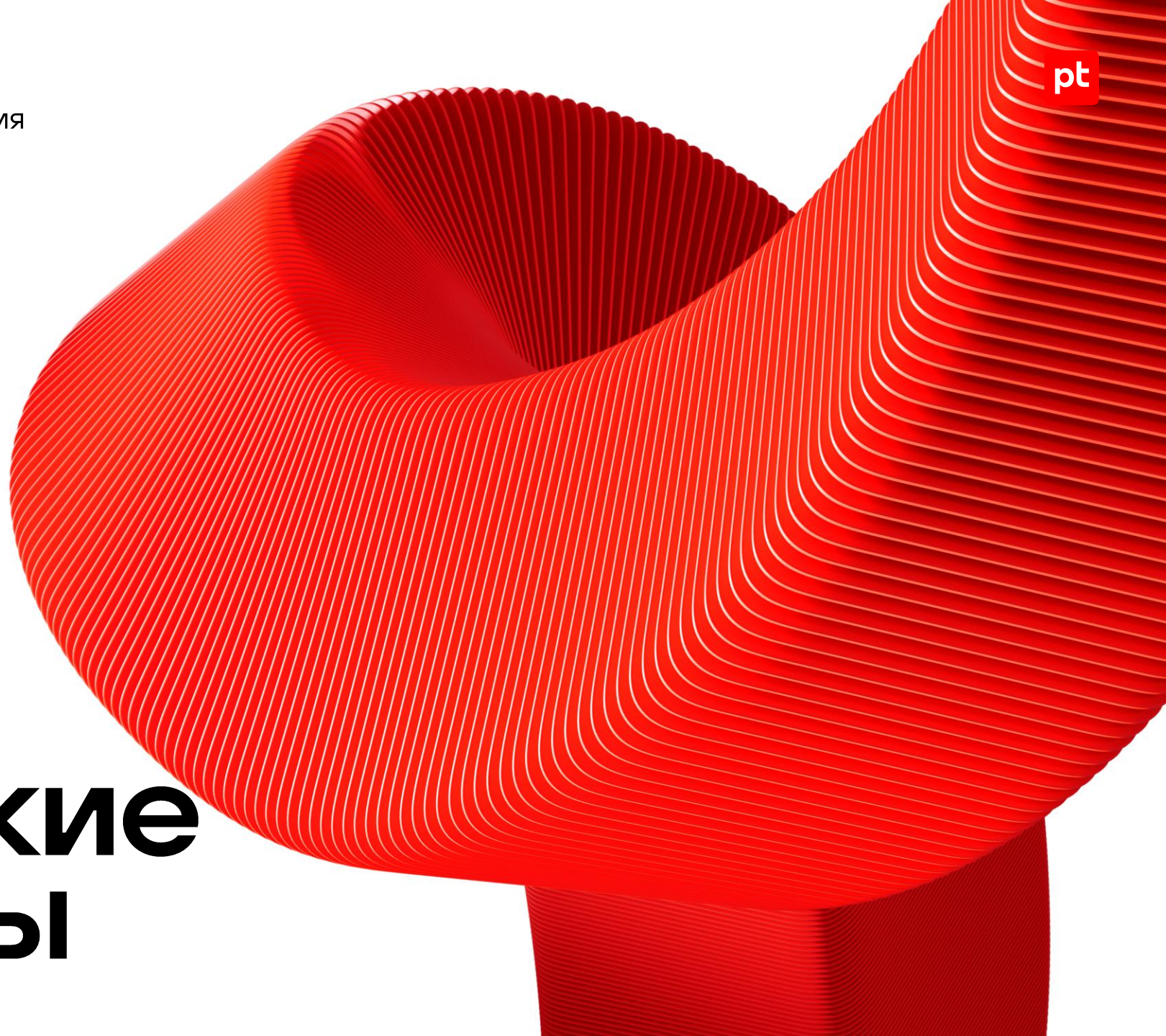
Денис Масленников

Заместитель руководителя направления аналитических исследований Positive Technologies



(Не)детские проблемы

Как нас атакуют

Дети — мишень для злоумышленников

Дети и подростки являются одними из наиболее уязвимыми к мошенникам группами людей. Дети и подростки хорошо разбираются в современных технологиях, однако у них может быть недостаточно жизненного опыта и знаний (в том числе, в области кибербезопасности), чтобы выявить мошенника, который пытается убедить их совершить те или иные действия (например, перевести денежные средства родителей на мошеннический счет)

Возрастные категории

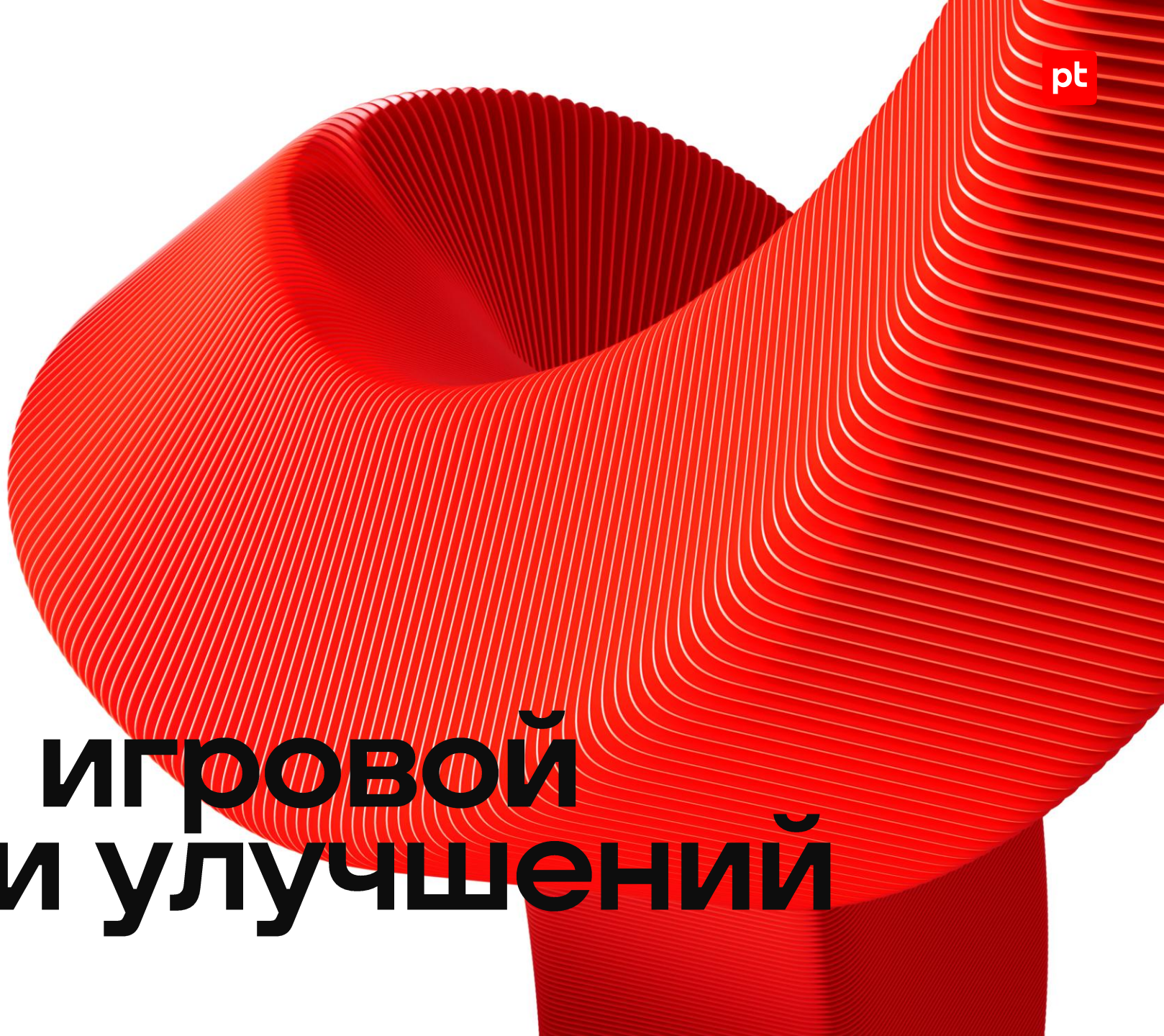
3-6 лет	Высокая доверчивость, ограниченное понимание
7-11 лет	Развивается критическое мышление, общение в сети увеличивается
12-15 лет	Активное использование соцсетей, самостоятельное общение
16-18 лет	Повышенная самостоятельность, может быть больше осведомлён о рисках

Большая и важная таблица

Угроза / Возрастная группа	3–6 лет	7–12 лет	13–15 лет	16–18 лет
Покупка игровой валюты и улучшений	Вероятность: средняя Критичность: средняя	Вероятность: высокая Критичность: средняя	Вероятность: высокая Критичность: средняя	Вероятность: средняя Критичность: средняя
Нелегальный заработок и принуждение к ПД	Вероятность: очень низкая Критичность: средняя	Вероятность: низкая Критичность: высокая	Вероятность: средняя Критичность: высокая	Вероятность: высокая Критичность: очень высокая
Мошенничество (шантаж, обман)	Вероятность: низкая Критичность: средняя	Вероятность: средняя Критичность: высокая	Вероятность: высокая Критичность: очень высокая	Вероятность: высокая Критичность: очень высокая
Социальная инженерия	Вероятность: низкая Критичность: средняя	Вероятность: средняя Критичность: высокая	Вероятность: высокая Критичность: высокая	Вероятность: высокая Критичность: очень высокая
Кибербуллинг	Вероятность: низкая Критичность: средняя	Вероятность: средняя Критичность: средняя	Вероятность: высокая Критичность: высокая	Вероятность: высокая Критичность: высокая

Методы атак на детей

Покупка игровой валюты и улучшений



Общая статистика

Средний возраст

9-10 лет

Последствия

Прямые финансовые потери

Средний ущерб

300 000 рублей

Чем заманивают

- Реклама с бесплатными промокодами
- Реклама от лиц известных людей
- Вредоносные QR-коды

Схемы с играми

Покупка игровой валюты

Школьник перевёл мошенникам 900 тысяч рублей с маминой карты. Он хотел купить валюту в игре Roblox. Злоумышленник выманил деньги у подростка, притворившись известным блогером

Использование темы для других схем

Для получения бесплатного промокода для игры надо было взять телефон мамы или папы и сделать скрин рабочего стола. Когда школьник отправил фото, с ним связались злоумышленники и сообщили, что телефон мамы заражен опасными вирусами, из-за которых у нее спишут 70 тысяч. Чтобы этого не произошло неизвестные попросили школьника сообщить все пароли от банковских приложений

Как это происходит

Размещает рекламу с бесплатными промокодами/игровой валютой с большими скидками

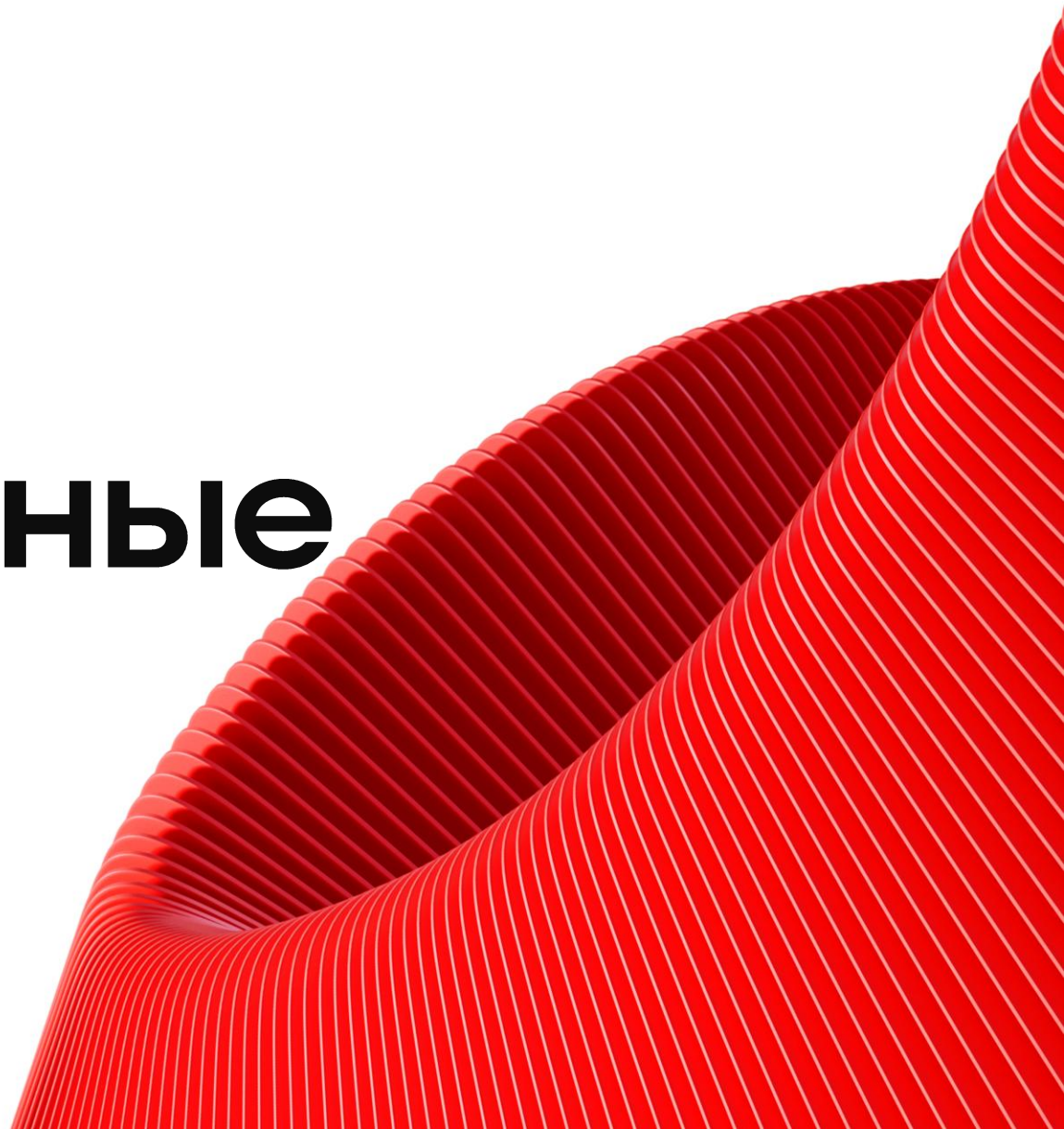
Ребенок списывается с мошенником

Ребенок оплачивает покупку мошенникам

Мошенник дает ребенку различные задания, например, сделать скриншот телефона родителей

Зачастую действуют от имени известных людей

Противоправные действия и нелегальный заработок



Общая статистика

Средний возраст

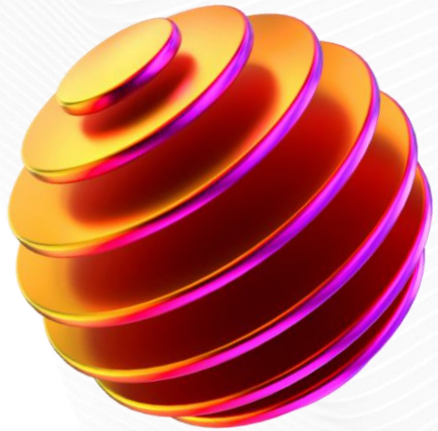
14 лет

Последствия

Ответственность перед законом, прямые финансовые потери, вред здоровью

Что за заработок

- Поджоги и причинение иного вреда *(иногда с последующим шантажом родителей)*
- Сваттеры
- Дропперы



Легкий заработок – уголовная ответственность

Дроп

Человек, который обналичивает деньги, украденные мошенниками с банковских счетов третьих лиц. Дропперами становятся люди, которые верят, что могут быстро и легко заработать. Зачастую они остро нуждаются в деньгах, поэтому соглашаются на любую работу

Заливщик

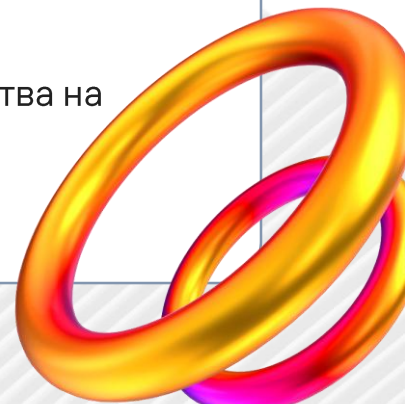
Получает наличные деньги, вносит их на свой счет и переводит другим дропам

Обнальщик

Снимает в банкомате поступившие деньги и передает их третьему лицу

Транзитник

Перечисляет денежные средства на другую банковскую карту или электронный кошелек



Как вербуют?

- Под видом органов государственной безопасности
- Под видом сотрудников банка
- Под видом легитимного работодателя
- Под видом человека, который ошибся

Люди, откликнувшиеся на подобные объявления, часто становятся участниками мошеннических схем

Вывод денег через сим-карты

На счет мобильного телефона внезапно поступают денежные средства

Для возврата денег злоумышленник предоставляет номер карты или кошелька

Возвращая денежные средства, можно стать **дропом-транзитником**

Мошенник сообщает, что ошибочно перевел деньги на неверный номер телефона

Не только дропами едины

С подростком связался неизвестный и предложил сумму денег, если тот подпалит входную дверь в одной из квартир. Молодой человек согласился. Ему через тайник выслали телефон и попросили заснять на камеру свой поджог.

Статья 7.17. КоАП РФ

Двое студентов и школьник подожгли кабину поезда в Краснодаре, По информации СМИ, за это неизвестные пообещали им полторы тысячи долларов. За поджог локомотива им грозит до 15 лет заключения.

Статья 205 УК РФ

Шантаж

Общая статистика

Средний возраст

14 лет

Последствия

Прямые финансовые потери, причинение вреда здоровью

Ущерб

∞

С чего может начаться

- Знакомства в телеграме
- Взломанный аккаунт Госуслуг
- Коды из пункта выдачи
- Звонок от «правоохранительных» органов

Популярная схема №1

Мошенник под видом учителя/завуча/директора

Могут представиться кем угодно

Подтвердить доступ на образовательный портал и прислать код из смс

Код от госуслуг для дальнейшего шантажа

Пройти тестирование перед экзаменами на некотором сайте

Утечка персональных данных

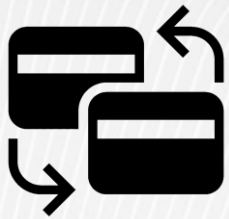
Родители попали в беду

Кража денежных средств

Популярная схема №2

Мошенник под видом сотрудника правоохранительных органов

Перевод средств террористическим организациям



Родителям грозит тюрьма

Банковские счета родителей взломаны

Мошенник просит ребенка заснять дома на видео, где хранятся деньги, драгоценности и тд

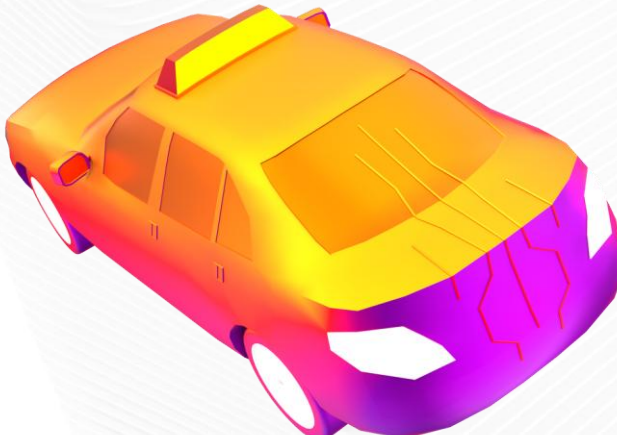
Заставляет ребенка самостоятельно передать «курьеру» найденные ценности для «декларирования»

Слайд с примерами

Школьник из Москвы отдал мошенникам более 5 млн рублей. В Москве аферисты убедили 12-летнего ребёнка передать им более 5 миллионов рублей, 7 тысяч долларов и 2,7 тысячи евро. Они запугали ребёнка, заявив, что его родителей посадят в тюрьму, если он не отдаст деньги

12-летнего школьника вынудили отдать мошенникам 750 тыс.рублей. Злоумышленники нашли подростка на сайте знакомств, представившись школьницей. После флирта выманили геопозицию и начали угрожать ударом беспилотника и обвинением в терроризме

Мошенники дозвонились школьнику и убедили подростка, что его аккаунт взломан и теперь на его имя оформляются микрозаймы. Также они сообщили, что для решения проблемы ему необходимо взять украшения его мамы и передать курьеру для «декларации». Ущерб от действий аферистов составил 900 тыс. рублей



Дипфейки в помощь злоумышленникам

Инструменты искусственного интеллекта используют как специалисты по информационной безопасности, так и хакеры для подготовки и реализации фишинговых атак

поддерживают диалог с жертвой

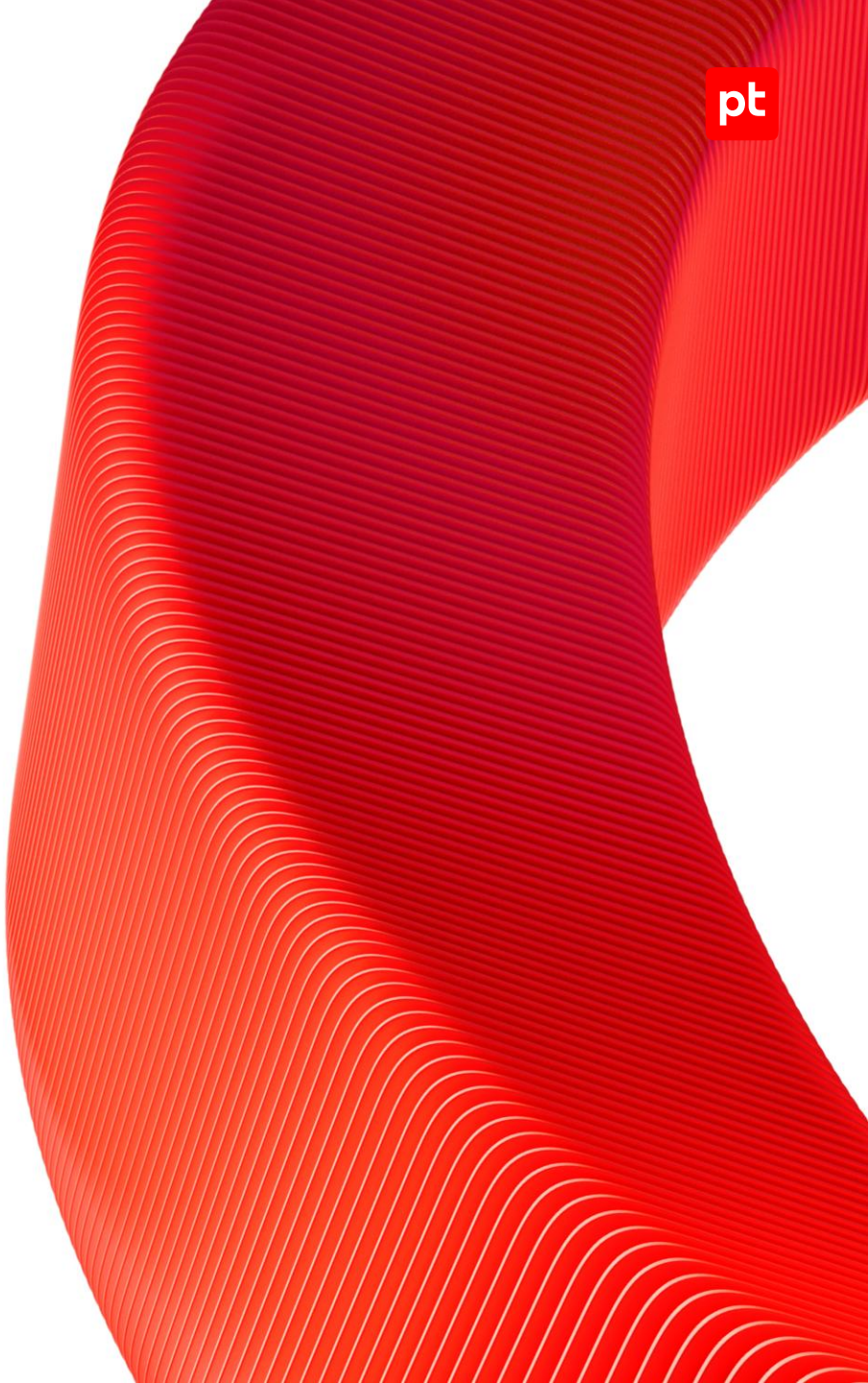
генерируют фишинговые сообщения

создают дипфейки голосов

создают дипфейки изображений

создают дипфейки видео

Что еще?

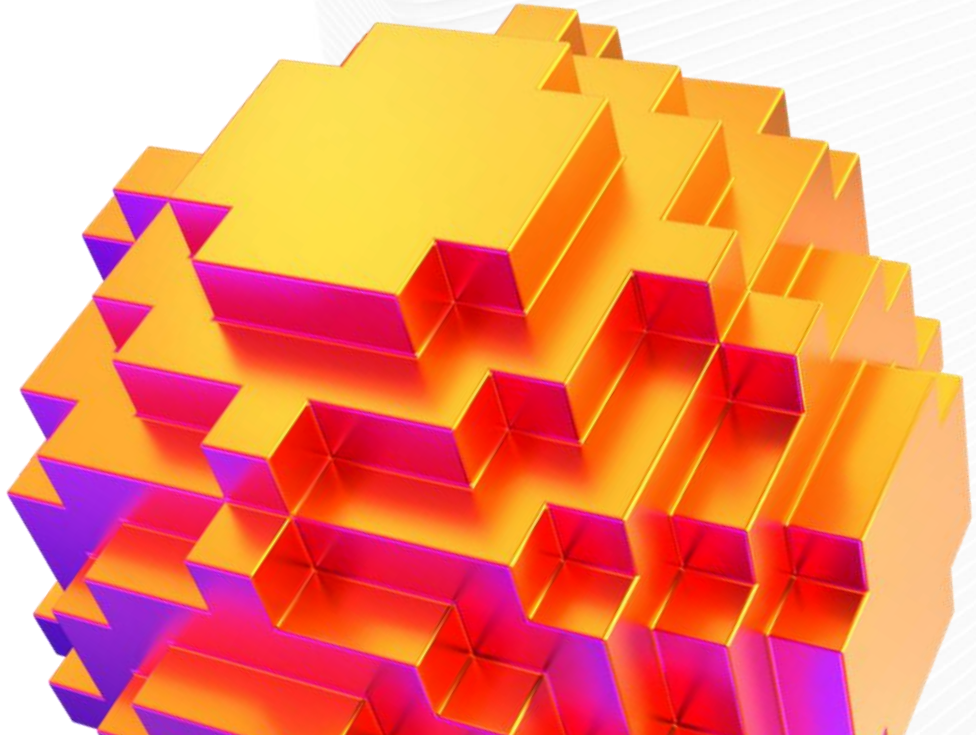


Социальная инженерия

Ответы на экзамен	*«Продаются ответы на государственный экзамен»*
Ложная помощь и защита	*«Я вижу, что тебя обижают в чате. Отправь мне пароль, я всё исправлю»*
Обещание награды и подарков	*«Купон на бесплатные кристаллы/скины/валюту в игре — пройди простой опрос и введи свой логин и пароль»*
Притворство авторитетом	*«Я учитель/тренер, пришли мне домашку/личные данные для проверки»*
Социальное одобрение	*«Ваша фотография набрала 1000 лайков — перейдите по ссылке, чтобы увидеть статистику»*
Манипуляция страхом упущенной выгоды	*«Осталось 5 мест на эксклюзивный ивент/розыгрыш»*

Маркетплейсы

Схема: В электронном письме, которое получает жертва, указывается, что ей отправлен подарок. Письмо написано якобы от лица известного онлайн-магазина, активным покупателем которого является пользователь. Чтобы получить подарок, ему необходимо перейти по ссылке. Далее жертва попадает на поддельный сайт маркетплейса, где ей предлагается ввести данные своей банковской карты. За это действие мошенники обещают промокод на скидку, бесплатный товар или иное вознаграждение.



Случаи из жизни

Мошенник позвонил ребёнку и сказал, что случайно перевёл её маме 1 миллион рублей, и потребовал вернуть деньги. Запугав девочку, он заставил её зайти в банковское приложение с телефона матери и перевести ему крупную сумму

Ущерб: 780 000 рублей

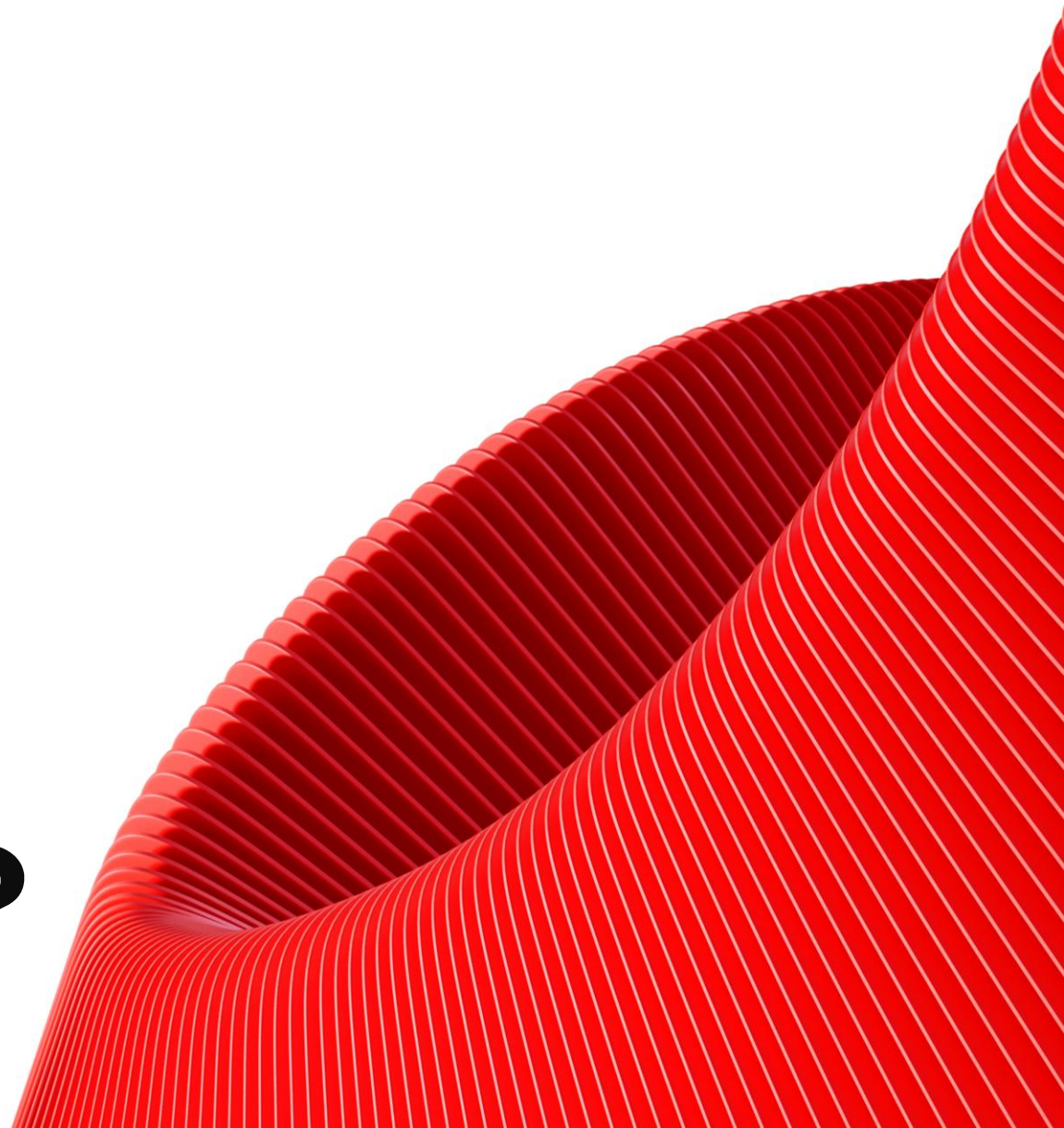
14-летний подросток получил сообщение в мессенджере, предлагающее удвоить прибыль с помощью выгодных инвестиций. Увлеченный заманчивой перспективой, подросток перевел сумму в 287 тыс. рублей из личных накоплений матери без ее ведома на указанный в сообщении расчетный счет

Ущерб: 287 000 рублей

Девочка увидела в интернете рекламу, где рассказывали как увеличить количество просмотров в аккаунте. Школьница перешла по ссылке и с ней сразу же связались мошенники. По их указке она сначала опустошила банковский счёт матери, далее сменила пароль в банковском приложении, а потом оформила кредит в размере

Ущерб: больше 500 000 рублей

А что делать?



Это база

Принцип нулевого доверия

- Не публикуйте в открытом доступе слишком много
- Загружайте приложения только из официальных источников
- Используйте надежные пароли – и разные для разных ресурсов
- Следите за настройками конфиденциальности
- Не открывайте подозрительные письма и сообщения
- Регулярно обновляйте приложения, установленные на ваших устройствах
- Не используйте публичные сети Wi-fi для критичных ресурсов
- Где возможно, используйте многофакторную аутентификацию
- Не верьте бесплатным призам, розыгрышам и так далее

И это база

Positive Research

Карточки по детской безопасности

Спасибо!