

Федор Чунжеков

Руководитель исследовательской группы
Positive Technologies Cyber Analytics



Технические угрозы: вредоносы, фишинг и защита данных

Дети — мишень для злоумышленников

Дети и подростки — одна из групп, наиболее уязвимых для мошенников.

Дети 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 чужой счет).



Почему летом опаснее

- ▶ Больше свободного времени – больше экранного времени у детей.
- ▶ Меньше контроля – больше развлечений.
- ▶ Большее количество потребляемого контента – больше векторов компрометации.



Как атакуют частных лиц

Доля методов в атаках на частных лиц, 2024 год



Распространенные типы вредоносного ПО

Типы вредоносного ПО в атаках на частных лиц, 2024 год



Загрузка вредоносного ПО на устройство дает атакующим практически полный контроль над скомпрометированным устройством и доступ к конфиденциальным данным, хранящимся на устройстве.

Как распространяются вредоносы

- Сообщения в мессенджерах
- Фишинговые сайты
- Взломанные версии приложений, игр, пиратские версии фильмов
- Вредоносные QR-коды и вредоносная реклама

Фишинг: как ловят детей

Фишинг — это цифровое мошенничество, когда ребёнку подсовывают поддельную ссылку или приложение, чтобы украсть логины, фото, пароли, доступ к телефону.

Дети не проверяют ссылки, переходят, вводят данные — и теряют доступ или заражают устройство.

Типичные приманки:

- ▶ «Подпишись или скачай модуль и получи бесплатно...»
- ▶ «Вы выиграли подарок...»
- ▶ Секретные функции в играх и приложениях
- ▶ «Получи игровой предмет бесплатно»

Как это происходит

Размещает рекламу
с бесплатными
промокодами или
игровой валютой
с большими скидками



Ребенок списывается
с мошенником



Зачастую действуют от имени
известных людей



Ребенок оплачивает
покупку мошенникам



Мошенник дает ребенку
различные задания,
например сделать скриншот
телефона родителей

Приемы фишеров

>	Ответы на экзамены	<i>«Продаются ответы на государственный экзамен»</i>
>	Ложная помощь и защита	<i>«Я вижу, что тебя обижают в чате. Отправь мне пароль, я все исправлю»</i>
>	Обещание награды и подарков	<i>«Купон на бесплатные игровые предметы: пройди простой опрос и введи свой логин и пароль»</i>
>	Авторитетный знакомый	<i>«Я учитель (тренер), пришли мне домашку (личные данные) для проверки»</i>
>	Социальное одобрение	<i>«Ваша фотография набрала 1000 лайков — перейдите по ссылке, чтобы увидеть статистику»</i>
>	Страх упущенной выгоды	<i>«Осталось 5 мест на эксклюзивный ивент (розыгрыш)»</i>

Популярная схема № 1



Популярная схема № 2

Мошенник под видом
сотрудника
правоохранительных органов



Перевод средств
террористическим
организациям



Родителям грозит
тюрьма



Банковские счета
родителей взломаны



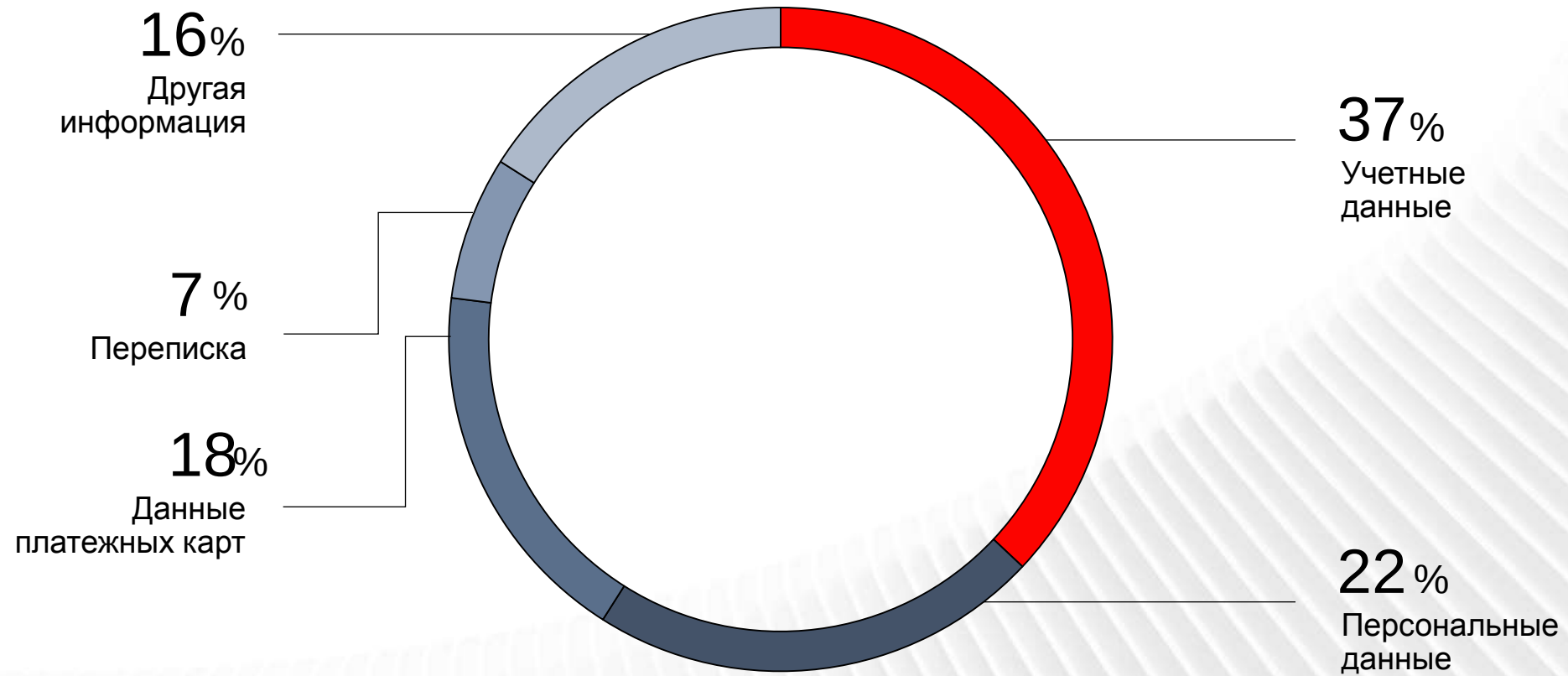
Мошенник просит ребенка заснять дома на видео, где
хранятся деньги, драгоценности и т. п.



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

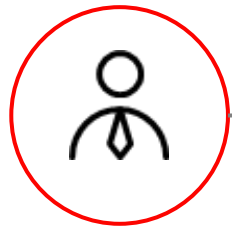
Утечки конфиденциальной информации

Типы украденных данных в успешных атаках на частных лиц, 2024 год

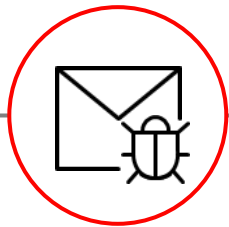


Дипфейки в помощь злоумышленникам

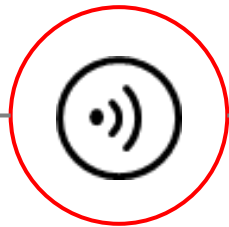
Инструменты искусственного интеллекта используют как специалисты по ИБ, так и хакеры для подготовки и реализации фишинговых атак



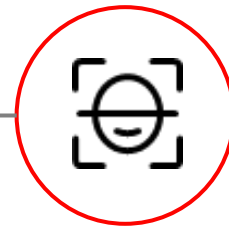
поддерживают
диалог с жертвой



генерируют
фишинговые
сообщения



создают
дипфейки
голосов



создают
дипфейки
изображений



создают
дипфейки видео

Что делать?

Базовые принципы безопасности

Принцип нулевого доверия



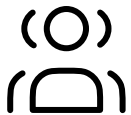
Не публикуйте
в открытом доступе
слишком много



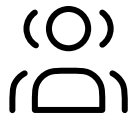
Загружайте приложения
только из официальных
источников



Используйте надежные
пароли — и разные для
разных ресурсов



Следите за настройками
конфиденциальности



Не открывайте
подозрительные письма,
ссылки и сообщения



Регулярно обновляйте
приложения,
установленные на ваших
устройствах



Не используйте
публичные сети Wi-Fi
для работы на важных
сайтах



Где возможно, используйте
многофакторную
аутентификацию



Не верьте бесплатным
призам, розыгрышам и
тому подобному

Какие важные мысли надо донести до детей

- ✧ Проблемы взрослых должны решаться взрослыми — дети их решить не смогут
- ✧ Не стоит бездумно переходить по ссылкам, скачивать и запускать файлы из недоверенных источников
- ✧ Если на вас начали давить — сразу прекращайте коммуникацию
- ✧ Бесплатный сыр бывает только в мышеловке

Взрослым на заметку

Чего делать не стоит



Устраивать проверки и допросы



Запрещать использование социальных сетей и гаджетов



Ругаться на ребенка и кричать на него



Давить на подростка



Сравнивать с другими (особенно в вопросах успеваемости, достижений и т. п.)



Пугать неизвестностью

Что может помочь



Поговорить о возможных угрозах и рассказать о рисках



Создать возможность обратиться за помощью



Не оставлять ребенка один на один с его проблемами



Знать ценности ребенка и его увлечения



Проговаривать свои чувства и страхи



Уметь просить прощения, если неправы

Важно на своем примере
показывать детям, что значит «быть
на чеку»

Полезные ссылки



Positive Research



Карточки по детской
безопасности

Спасибо!