

## ***Как защитить детей от интернет-мошенников***

Главное, что может во многом защитить ребенка от мошенников в интернете — это его осведомленность о схемах обмана и доверительные отношения с родителями. Важно рассказывать детям, как распознать обманщика и что делать, если в друзья набивается неизвестный человек из интернета. Рассказываем об основных схемах обмана детей и о том, как родители могут минимизировать риски лишиться денег или пострадать от утечек персональных данных.

### ***Что нужно мошенникам и как они обычно связываются с детьми***

Основные цели мошенников — кража персональных или платежных данных, паролей от аккаунтов, фото документов. Получив эту информацию, преступники могут обчистить счета родителей и ближайших родственников ребенка, взять на их имя [кредиты](#), получить доступ к личным фото или перепискам, чтобы шантажом вымогать деньги.

Дети из-за небольшого жизненного опыта доверчивы, и если их не научить, как распознавать мошенников, последствия могут быть катастрофическими для семейного бюджета.

### **Чаще всего мошенники связываются с детьми:**

**В играх.** Обманщики заводят дружбу с детьми в чатах мобильных или компьютерных игр. Нередко выдают себя за популярных игровых блогеров и просят выполнить «задания», чтобы получить подарки, редкие игровые артефакты, игровую валюту или скины. Задания обычно заключаются в том, чтобы прислать фото документов, личные фото, данные банковских карт родителей

**В мессенджерах и соцсетях.** Преступники могут выходить на детей в Telegram-чатах, в группах в популярных соцсетях. Намерения те же — выудить информацию, которую можно использовать для своего обогащения.

## ***Как мошенники обманывают детей***

Нужно как можно раньше рассказать ребенку о том, кто такие мошенники и как они действуют, научить с осторожностью относиться к любым заманчивым предложениям в сети. Как правило, киберворы используют следующие схемы:

**1. Просят перейти по ссылке, скачать файл или приложение.** Мошенник, установив контакт с ребенком, может отправить ему ссылку или файл и попросить открыть, чтобы «выполнить задание» и получить за это подарки. Часто ссылка имитирует страницу банковского сайта. Мошенники в качестве задания могут попросить ребенка ввести на этой странице данные банковских карт родителей. После этого деньги на карте списываются мошенниками.

Злоумышленники также могут предложить считать QR или сформировать QR в приложении и переслать его им. Могут попросить

подтвердить действие с телефона родителей или попросить сообщить код под предлогом авторизации, регистрации или участия в розыгрыше или опросе.

Еще одна распространенная схема — при переходе по ссылке на компьютер попадает вирус. Когда пользователь открывает свой онлайн-банк и вводит пароль, вирус считывает нажатия на клавиатуру. Так мошенники получают пароли от банковских аккаунтов.

## **2. Предлагают купить внутриигровую валюту, артефакты, скины**

Среди детей популярны мобильные игры, многие из них имеют собственные магазины, где продают внутриигровую валюту, скины, артефакты. Мошенники заводят дружбу с ребенком и предлагают купить у них цифровой контент дешевле, чем в магазине. Или приобрести аккаунт с кучей уже купленных артефактов. Ребенок переводит деньги, но никакого цифрового контента или аккаунта, естественно, не получает.

## **3. Обещают легкий заработок или призы в интернете**

Часто мошенники предлагают подросткам подработку в интернете и обещают легкий и быстрый заработок. Они могут присылать подобные предложения в мессенджер, в чаты, зазывать детей через короткие ролики на популярных видеосервисах, всплывающие рекламные баннеры и т.д. Работу предлагают действительно несложную — например, установить приложение, ежедневно посещать определенные сайты. Также предлагают зарабатывать на ставках или криптороторговле, обещая выигрыши и сверхдоходы.

Еще ребенку могут прислать сообщение, что он выиграл суперприз (например, популярную игрушку или ролики), но чтобы получить его, нужно заплатить.

## **4. Втягивают в дропперство**

**Дропперство** — это вывод денег с чужих банковских карт через подставных лиц. Работает это так: подростку предлагают оформить дебетовую карту (ее можно оформить с 14 лет) и за денежное вознаграждение отдать ее мошенникам. Затем злоумышленники переводят на нее украденные с чужих карт средства и снимают.

Подросткам также предлагают «привести друга», то есть вовлечь других детей в дроппинг, за каждого обещают заплатить пару тысяч рублей. Участвуя в подобных схемах, подросток может получить наказание за соучастие в мошенничестве. Для граждан от 16 лет и старше в России предусмотрена уголовная ответственность за подобные преступления.

Взламывают аккаунты друзей и с них просят о помощи

Мошенники, заполучившие доступ к аккаунту подростка, рассылают его друзьям сообщения с просьбой одолжить денег или перейти по ссылке, чтобы проголосовать за знакомого в онлайн-конкурсе.

## **5. Открыто угрожают и манипулируют**

Некоторые преступники предпочитают действовать более грубо и прямолинейно — шантажируют, манипулируют, угрожают. Например, могут написать, что родителям или кому-то из друзей угрожает опасность, и нужно срочно прислать деньги или данные банковских карт.

Часто киберворы, завоевав доверие ребенка, вытягивают из него личную информацию или фото, а потом шантажируют, угрожая разослать компрометирующие данные его друзьям и родственникам.

### **Как родители могут оградить ребенка от мошенников**

1. *Выстраивайте доверительные отношения с ребенком.* Для того, чтобы действительно быть в курсе происходящего в жизни ребенка, - с кем общается, чем увлекается, на что тратит свои карманные деньги — нужно планомерно выстраивать с ним доверительные отношения. Важно, чтобы он сам рассказывал родителям о новых знакомствах и событиях в своей жизни. При этом не стоит нарушать его личное интернет-пространство, мониторя все переписки и устанавливая жесткие ограничения. Это приведет к обратному результату — ребенок закроется, и рассчитывать на его доверие в этом случае будет уже бесполезно.

2. *Расскажите ребенку об основных схемах обмана.* Первым делом нужно объяснить ребенку, как распознать мошенника, какие уловки используют преступники, чтобы втереться в доверие, и почему ко всем знакомствам в интернет-пространстве нужно относиться критически. Следует рассказать про опасность перехода по ссылкам, про вирусы и коды подтверждения, про основы финансовой и компьютерной грамотности. Еще следует рассказать, что делать, если ребенок заподозрил преступника в своем новом знакомом — нужно сразу же сообщить об этом родителям.

3. *Защитите свою банковскую карту и карту ребенка.* Карты для детей до 14 лет привязывают ко счету одного из родителей. В этом случае стоит настроить на своем смартфоне уведомления о тратах ребенка. Если суммы увеличились или значительно выросла частота трат, имеет смысл аккуратно поинтересоваться у ребенка, в чем причина. Можно также ограничить сумму, доступную ребенку для ежедневных трат.

Банки предлагают партнерские сервисы для защиты средств, хранящихся на картах, от мошеннических схем. Например, у Газпромбанка есть страховка «Защита карты» от ПАО «Группа Ренессанс Страхование», которая покрывает самые распространенные виды мошенничества. При этом страховка распространяется на все карты, которые оформлены на физическое лицо в Газпромбанке.

4. *Подключить Родительский контроль.*

Включите функцию Родительского контроля в сервисах, которыми пользуется ребенок. Отключите отображение рекламы на компьютере, чтобы ребенку не попадались вредные баннеры. Функция Родительского контроля не гарантирует полной безопасности, а служит скорее дополнительной мерой защиты.

ООД УУП и ПДН УМВД России по Ивановской области

## Варианты вербовки дропперов:

рассказы о «планах по продажам»  
в банках:

«Оформи карту за вознаграждение»

- вовлечение в сетевой маркетинг:  
«Приведи друга с картой - получи  
деньги»

- предложение «трудоустройства»:  
«Стань администратором лотереи и  
отправляй выигрыш победителям»

- сообщение о якобы ошибочной  
операции:  
«По ошибке отправил Вам деньги -  
верните, но на другую карту или счёт»



### Что делает дроппер?

Передает чужие деньги от одного человека другому ;

Переводит деньги на незнакомые счета и карты по указанию мошенников;

Снимает или вносит чужие наличные в банкоматы;

Оформляет на себя банковские карты и отдает их мошенникам, либо дает доступ к своему онлайн-банку;

Мошенники предлагают вознаграждение, при этом сам «дроппер» становится соучастником мошеннической схемы.

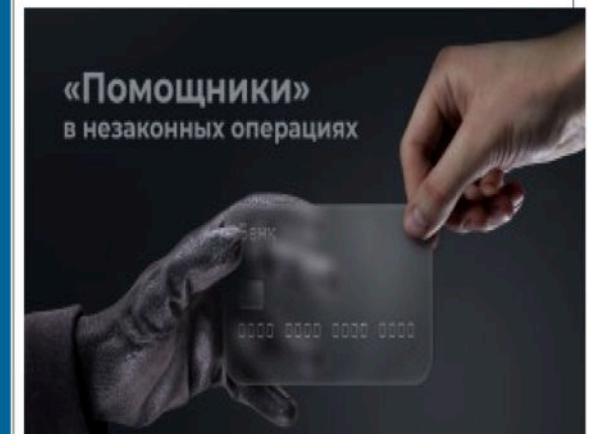
УМВД России  
по Ивановской области

ДЖ



*- люди, которых  
мошенники  
используют для  
обналичивания  
украденных денег*

«Помощники»  
в незаконных операциях



# Защити себя и своих близких от кибермошенничеств

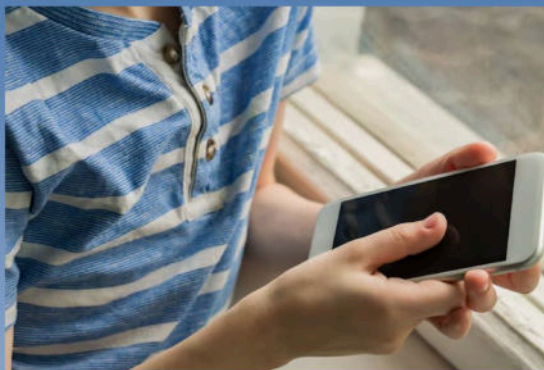
## Варианты вербовки дропперов:

рассказы «о планах по продажам» в банках: «оформи карту за вознаграждение».

вовлечение в сетевой маркетинг: «Приведи друга с картой—получи деньги»;

предложение «трудоустройства»: «Стань администратором лотереи и отправляй выигрши победителям».

сообщение якобы об ошибочной операции: «По ошибке отправил вам деньги—верните, но на другую карту или счет».



## Где мошенники ищут потенциальных дропперов?

В интернете;

В социальных сетях;

В мессенджерах;

По электронной почте.

Через знакомых рассказывают о возможности заработать «легкие» деньги.

В общественных местах расклеивают объявления о «легком» заработке.



С какими проблемами сталкиваются дропперы:

Банки ограничивают дропперам доступ к картам и онлайн-банку.

Сложности с получением банковских услуг у дропперов сохраняются вне зависимости от того, сколько времени прошло после участия в преступной схеме.

Потерпевшие обращаются в суд и родители подростков — дропперов выплачивают всю полученную преступным путем с



## Чтобы не попасться на уловки мошенников, необходимо:

объяснить детям, что нельзя выполнять требования незнакомцев, передавать данные карты или устанавливать приложения.

использовать родительский контроль: настроить ограничение доступа на мобильных устройствах ребенка, подключить уведомления в онлайн-банке, чтобы реагировать на подозрительные транзакции.

обучать ребенка, как поступать в случае подозрительных звонков, указать номера телефонов, по которым несовершеннолетний может связаться с родителями или другими близкими.

в случае угрозы со стороны незнакомых людей следует обязательно обратиться к родителям или родственникам.

уделять внимание не только собственной финансовой безопасности, но и обучению детей базовым правилам

цифровой гигиены.



### Одна из схем — запугивание через звонки.

Аферисты звонят ребенку, представляясь сотрудниками полиции, службы безопасности или других организаций, сообщают о «чрезвычайной ситуации с родителями».

Например, утверждают, что родителям угрожает опасность, и чтобы их спасти требуют срочно продиктовать номера банковских карт.

**Еще одна схема обмана связана с онлайн-играми. Мошенники создают поддельные акции или выигрыши**

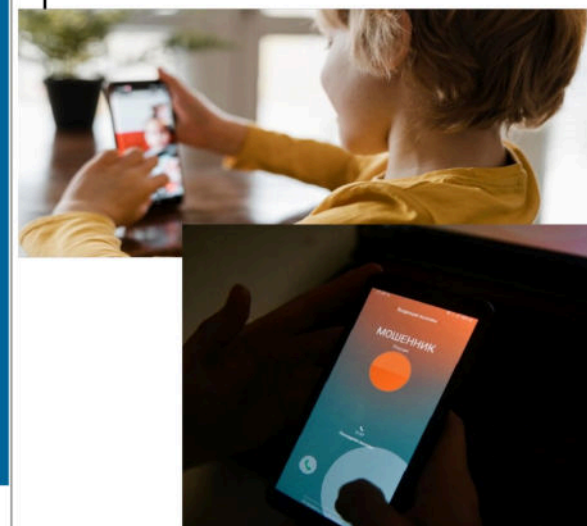
**в играх и просят ввести данные банковской карты для получения «приза» или предлагают приобрести игровую валюту, например, в Roblox. Несовершеннолетние берут деньги из дома и переводят мошенникам.**

УМВД России  
по Ивановской области

ДЖ

## ПРЕДУПРЕЖДАЕТ О НОВОМ ВИДЕ МОШЕННИЧЕСТВА -вовлечение

*Мошенники используют методы социальной инженерии, чтобы запугать несовершеннолетних, обманом заставить их передать доступ к средствам родителей*



# Защити себя и своих близких от кибермошенничеств

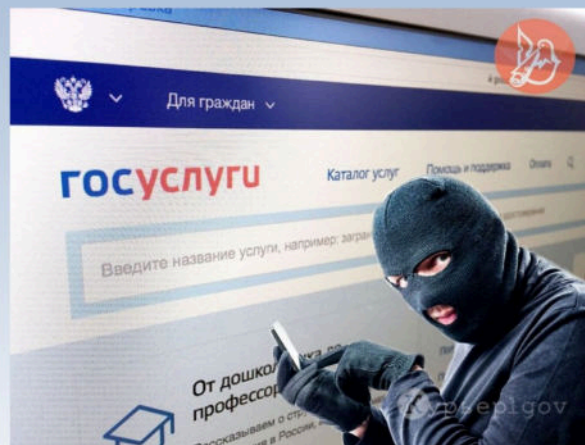
## Виды мошеннических схем

Мошенники под видом руководителей школ или учителей звонят родителям и говорят, что нужно обновить электронный журнал, список учащихся или профиль ученика в «Сферуме». Для этого злоумышленники используют данные работников школы, дипфейк технологии и подменные номера, сообщили в ведомстве. Они просят называть коды из СМС и получают через них доступ к «Госуслугам»

В «Сферуме» сообщили, что обновления на платформе происходят автоматически и исключительно на устройстве пользователя, без участия третьих лиц. «Для этого не используются коды из СМС, в том числе коды от «Госуслуг». Информация об обновлениях сервиса может приходиться исключительно от платформы в виде системного сообщения и носит только информационный характер», – говорится в сообщении сервиса, поступившем в РБК. Там указали, что «коммуникации по учебе



## Виды мошеннических схем



Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том. Стоит ли воспользоваться теми или иными услугами, предлагаемыми в интернете.

Не оставляйте в свободном доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.

Не отправляйте о себе слишком много при совершении покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то их запрашивает, будьте бдительны – скорее всего, это мошенники.

**Установите на свои компьютеры антивирусные программы и персональный браузер. Он поможет предотвратить кражу конфиденциальных данных или другие подобные действия.**