

**Как в интернете  
не попасться  
в преступные сети?**

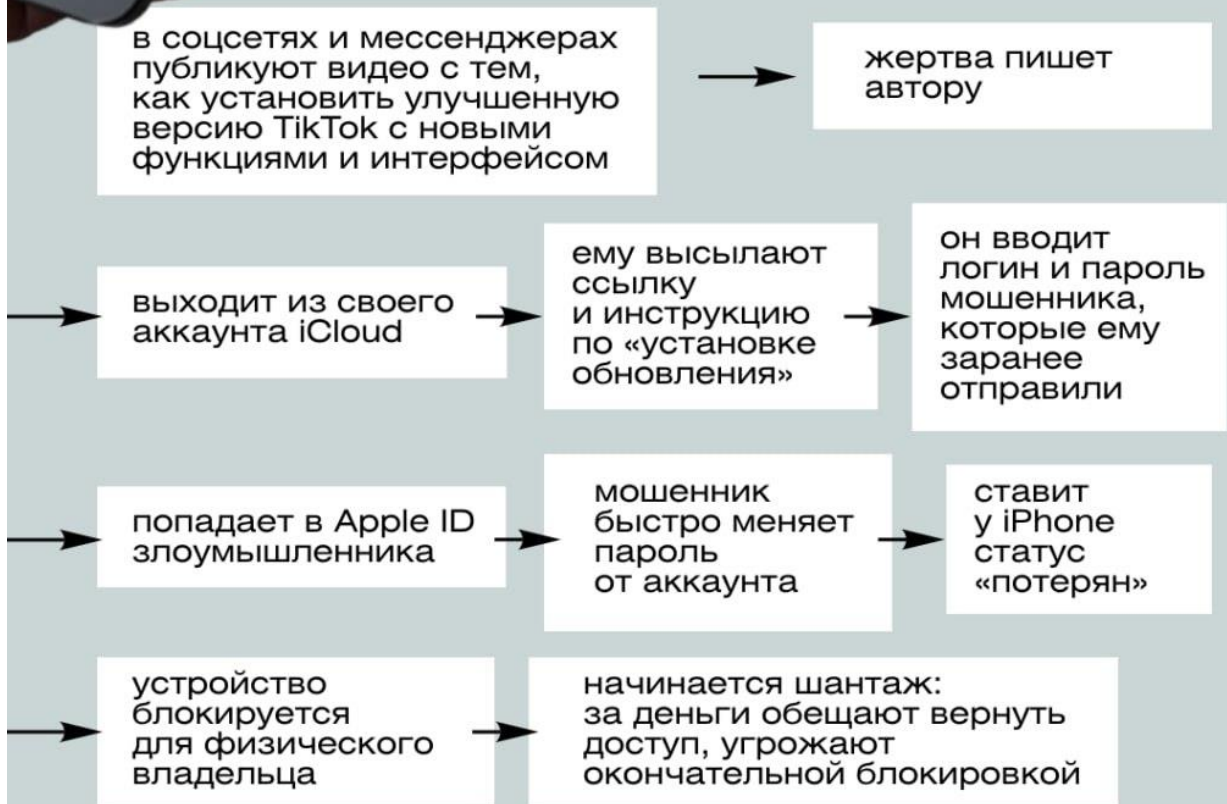
@NA\_STRAGE

О ВАШЕЙ БЕЗОПАСНОСТИ



# Схема обмана

**Злоумышленники пытаются заполучить доступ к Apple ID через установку «обновлённой версии» TikTok, бесплатного Minecraft и внутренней валюты в играх...**



В интернет-пространстве нужно быть предельно бдительными! Вступая в онлайн-диалог с незнакомыми пользователями, руководствуйтесь главным правилом:  
«Никогда не доверяй, проверяй!»

## Лайфхак от МВД

Не нужно переходить по незнакомым ссылкам, открывать сообщения или принимать запросы от незнакомых пользователей: любой из них может оказаться преступником, а в его сообщении или запросе может скрываться вредоносная программа или другой опасный контент

@NA\_STRAGE

О ВАШЕЙ БЕЗОПАСНОСТИ





## Ребята!

Если в интернете в отношении вас совершают противоправные действия, сразу же сообщите об этом родителю, другому взрослому или в милицию **по телефону 102** или в **чат-бот МВД «Мы всегда рядом»**

@NA\_STRAGE

О ВАШЕЙ БЕЗОПАСНОСТИ

# Не защищал свой Apple ID?

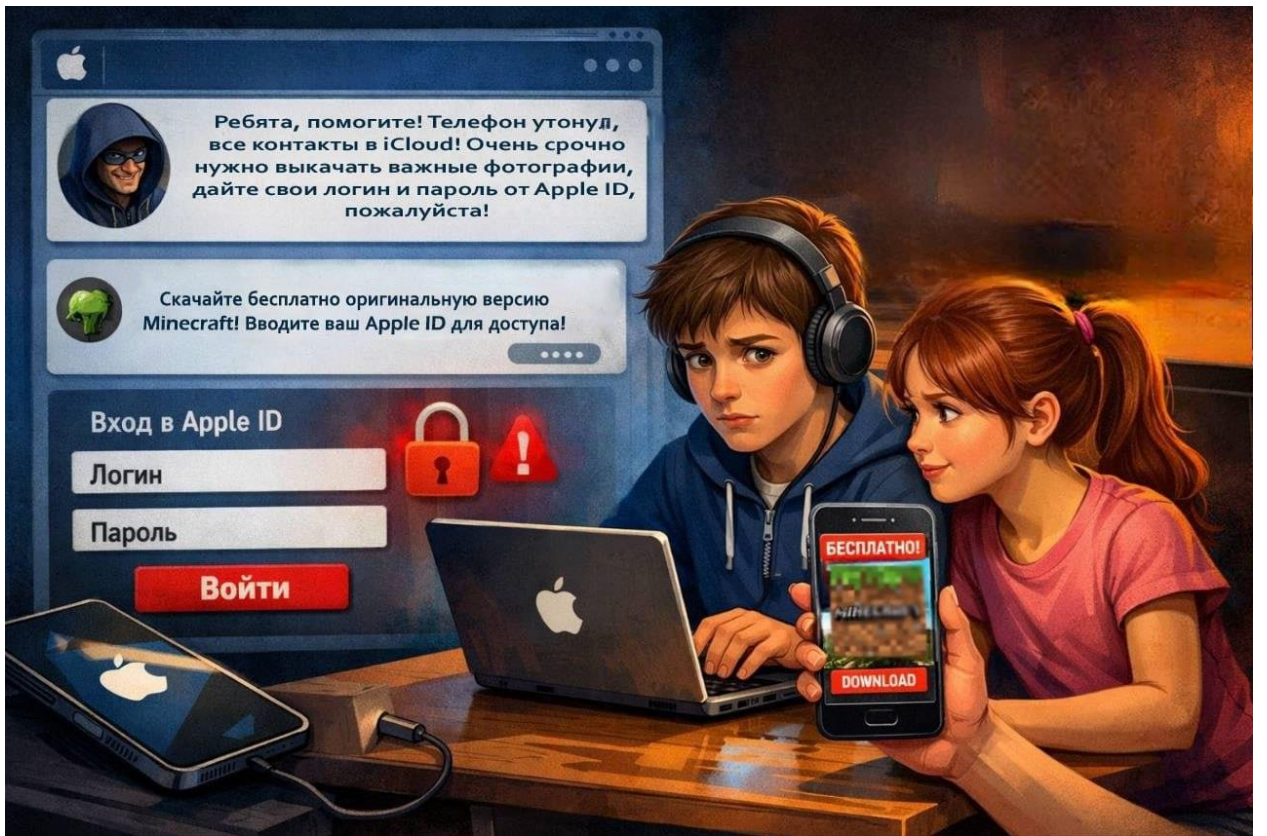
Вот что тебя ждёт!



Вся информация украдена  
iPhone превращён в кирпич  
Списаны деньги с карт



Будь бдителен! Защити свой Apple ID  
прежде чем станет слишком поздно!



# Защити свой Apple ID!

Не дай злоумышленникам завладеть твоими данными!



Используйте сложный пароль



Включите Двухфакторную аутентификацию



Остерегайтесь фишинга



Защищайте свой устройства



Не сообщайте свой пароль и коды из SMS никому!



© Влада безпечності

Как защитить  
***iPhone***  
**ребёнка**  
ОТ МОШЕННИКОВ



@MIA\_STRASC

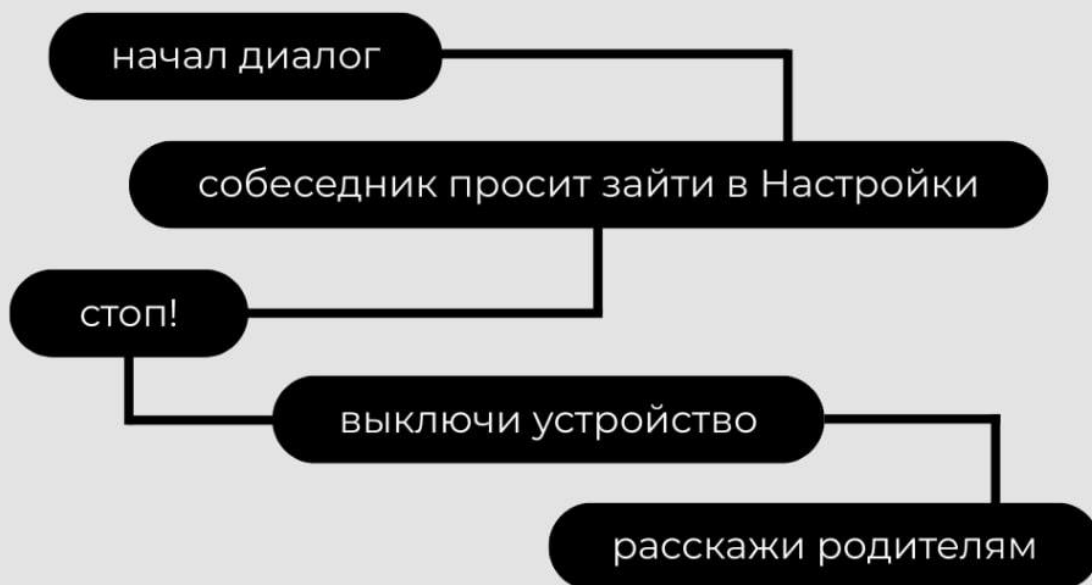


# Чужой *Apple ID* не вводи! Никогда!

Даже если просит друг

Настройки iPhone – это не для игр. Нельзя выполнять в настройках телефона (раздел iCloud/Apple ID) то, что советует незнакомый человек из интернета.

«Бонусы» и «читы» – это обман. Настоящие моды и призы не устанавливаются через настройки самого телефона



# Что должны сделать родители

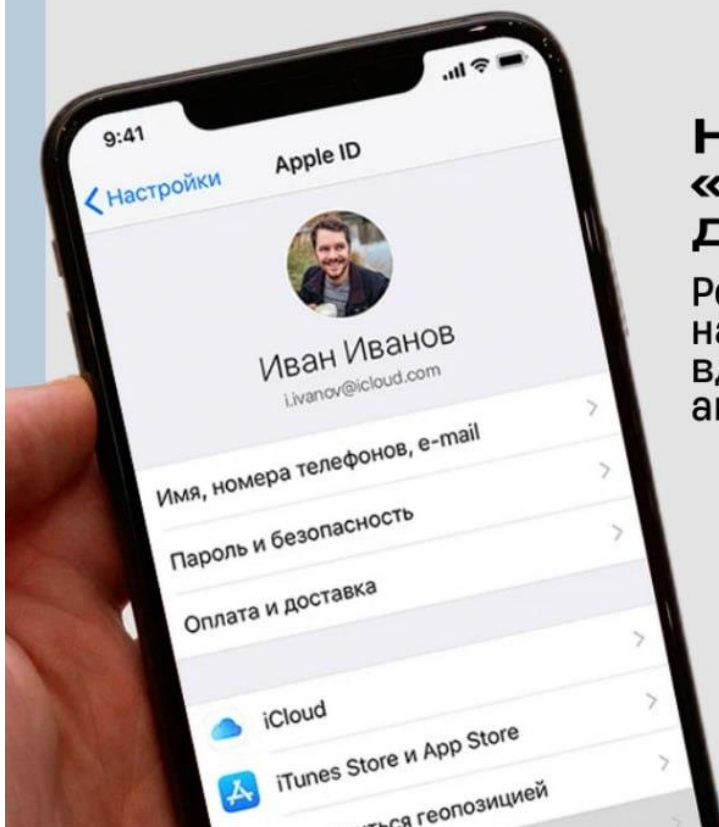
возьмите iPhone

откройте «Настройки»

раздел [Имя]

покажите ребёнку, как выглядит экран входа в Apple ID

объясните: «Эту область трогать без меня нельзя»



## Настройте «Семейный доступ»

Родители увидят, если на устройстве ребёнка вдруг появился новый аккаунт



ФУА\_АТКЛБЕ

О ВАШЕЙ БЕЗОПАСНОСТИ

# Важно!

Для детского аккаунта в настройках «Семейного доступа» установите «Запрос на покупки». Это добавит ещё один барьер.

## Ограничьте возможность установки программ

В «Экранном времени» → «Контент и конфиденциальность» можно запретить установку и удаление приложений без пароля. Это снизит риск, если обман связан со скачиванием приложения



# Что делать, если ребёнок уже вошёл в чужой iCloud и телефон заблокирован?

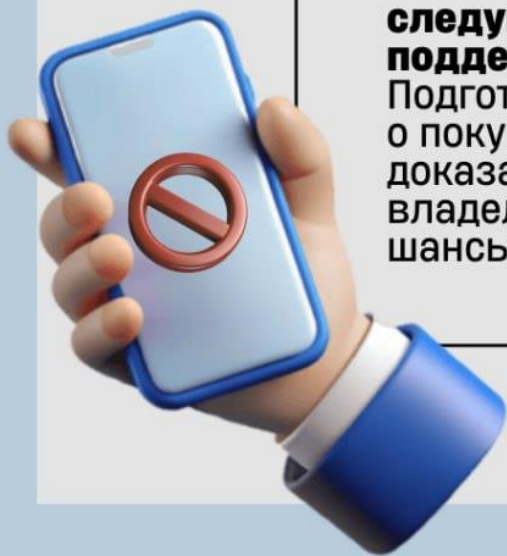
**Не платите!**

Выплата не гарантирует разблокировку.

// Вы потеряете деньги, и мошенник может потребовать ещё.

**Если блокировка уже случилась, следуйте инструкциям службы поддержки Apple.**

Подготовьте чек/документ о покупке iPhone. Это главное доказательство того, что вы – владелец устройства. Без чека шансы на помощь резко падают



КАК  
МОШЕННИКИ  
*используют детей*  
ЧТОБЫ УКРАСТЬ  
ДЕНЬГИ  
РОДИТЕЛЕЙ



ВАЖНО  
ЗНАТЬ



МИЛИЦИЯ МОГИЛЕВЩИНЫ



# ЧТО ПРОИСХОДИТ?



Лже-психологи из школы звонят подросткам, предлагая тесты и "проверку данных". Присылают фишинговые ссылки и пугают

**"УТЕЧКОЙ"  
ЛИЧНЫХ ДАННЫХ  
И УГОЛОВНЫМ  
ПРЕСЛЕДОВАНИЕМ**



МИЛИЦИЯ МОГИЛЕВЩИНЫ





# ПОСЛЕ ЭТОГО:



Потом «психологи» передают звонок  
лжесотрудникам  
правоохранительных органов — в  
форме, с поддельными  
удостоверениями, которые требуют  
молчать

**И НЕ  
РАССКАЗЫВАТЬ  
РОДИТЕЛЯМ**



МИЛИЦИЯ МОГИЛЕВЩИНЫ



# МОШЕННИКИ ЗАСТАВЛЯЮТ ПОДРОСТКОВ/ ДЕТЕЙ:



- Тайно снимать и переводить крупные суммы со счетов родителей
- Оформлять кредиты на себя или родителей (если это студенты и тд)
- Передавать наличные курьерам под разными предложениями



**\*СТУДЕНТКУ СОСЕДНЕЙ СТРАНЫ  
ОБМАНОМ ЗАСТАВИЛИ СНЯТЬ И  
ПЕРЕВЕСТИ СВЫШЕ 1 МЛН  
РУБЛЕЙ СО СЧЕТА ОТЦА И  
ОФОРМИТЬ КРЕДИТ.**



**МИЛИЦИЯ МОГИЛЕВЩИНЫ**





# ЧТО ДЕЛАТЬ?



Поговорите с детьми о безопасности  
в интернете и объясните, что

**СВЕДЕНИЯ О  
БАНКОВСКИХ КАРТАХ И  
СЧЕТАХ – ЭТО СТРОГО  
КОНФИДЕНЦИАЛЬНАЯ  
ИНФОРМАЦИЯ**



Старайтесь установить доверительные  
отношения с дочкой или сыном,  
независимо от того, сколько ему/ей лет



МИЛИЦИЯ МОГИЛЕВЩИНЫ

# БУДЬТЕ ОСТОРОЖНЫ!



Берегите себя и тех, кто рядом с вами. Помните: вы всегда можете обратиться за помощью в милицию по телефону 102



МИЛИЦИЯ МОГИЛЕВЩИНЫ



КАК

НЕ

СТАТЬ

ЖЕРТВОЙ

ТОП 5  
ТОП 5  
ТОП 5

кибермошенников

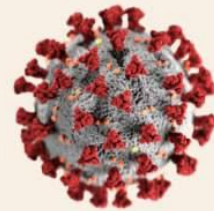


# Основные риски пользователей в цифровом пространстве



## ФИШИНГ

Атака происходит через письма или сообщения от лица доверенных сервисов (банк/почта)



## ВИРУСЫ

Вредоносные программы, способные повредить или заблокировать ваше устройство, а также украсть ваши данные.

## RANSOMWARE

Тип вредоносного ПО, блокирующего доступ к системе или файлам и требующего выкуп за восстановление.





## КАК СЕБЯ ОБЕЗОПАСИТЬ?

№1: Используйте надёжные пароли и двухэтапную аутентификацию



№2: Не устанавливайте приложения по просьбе посторонних



№3: Будьте осторожны с подозрительными сообщениями и ссылками



№4: Регулярно обновляйте ПО и используйте антивирус



полезные  
советы





**ПРОВЕДИТЕ ВРЕМЯ В ИНТЕРНЕТЕ  
КАК СУПЕРГЕРОЙ — БЕЗОПАСНО  
И С УЛЫБКОЙ!**



*Соблюдение простых правил  
безопасности позволит вам сохранить  
свои сбережения!*

**Okay!**



*Милиция Минска*

КИБЕРПРОСТРАНСТВО

**ОПАСНАЯ**  
ИГРОВАЯ

**ДЕТСКАЯ** **СРЕДА**  
ПЛОЩАДКА



**ЗАЩИТИ**  
**СВОЕГО РЕБЕНКА**  
**ОТ УГРОЗЫ!**



УВД БРЕСТСКОГО ОБЛИСПОЛКОМА

# ОТКУДА ЖДАТЬ БЕДЫ?

НЕЖЕЛАТЕЛЬНЫЙ КОНТЕНТ

ПРОПАГАНДА НАРКОТИКОВ

ЭКСТРЕМИЗМ

НАСИЛИЕ

ПОРНОГРАФИЯ

СУИЦИДАЛЬНЫЕ ГРУППЫ



**ОПАСНАЯ ИГРА**  
ПРИСОЕДИНЯЙСЯ К НАМ!

КИБЕРБУЛЛИНГ

ЛОЖНАЯ ИНФОРМАЦИЯ

КОМПРОМЕТИРУЮЩИЕ ФОТО

НЕПРИСТОЙНЫЕ СООБЩЕНИЯ  
ОТ ИМЕНИ ЖЕРТВЫ ЕЕ ЗНАКОМЫМ

УГРОЗЫ

ОБИДНЫЕ  
СООБЩЕНИЯ



УВД БРЕСТСКОГО ОБЛИСПОЛКОМА

# ОТКУДА ЖДАТЬ БЕДЫ?

ОБЩЕНИЕ  
С НЕЗНАКОМЦАМИ

ОНЛАЙН-ХИЩНИКИ,  
КОТОРЫЕ МОГУТ  
МАНИПУЛИРОВАТЬ,  
ШАНТАЖИРОВАТЬ,  
ВОЗЛЕКАТЬ  
В НЕЗАКОННУЮ  
ДЕЯТЕЛЬНОСТЬ  
ИЛИ ДОМОГАТЬСЯ

МОШЕННИЧЕСТВО



ФИНАНСОВЫЕ  
УЛОВКИ,  
ПЛАТНЫЕ  
ПОДПИСКИ,  
КРАЖА ЛИЧНЫХ  
ДАННЫХ,  
"БЕСПЛАТНЫЕ  
ПОДАРКИ"



УВД БРЕСТСКОГО ОБЛИСПОЛКОМА

# ОТКУДА ЖДАТЬ БЕДЫ?

ЗАВИСИМОСТЬ



ЧРЕЗМЕРНОЕ ВРЕМЯ  
В СЕТИ,

РАЗРУШАЮЩЕЕ  
РЕАЛЬНЫЕ  
КОММУНИКАТИВНЫЕ  
НАВЫКИ  
И ПСИХИКУ

ВРЕДНОСНОЕ ПО

ВИРУСЫ,  
ТРОЯНСКИЕ КОНИ,  
ШПИОНСКИЕ ПРОГРАММЫ,  
ЗАРАЖАЮЩИЕ  
УСТРОЙСТВА  
И КРАДУЩИЕ  
ИНФОРМАЦИЮ



# КАК ЗАЩИТИТЬ РЕБЕНКА?

НАСТРОЙТЕ РОДИТЕЛЬСКИЙ КОНТРОЛЬ: ИСПОЛЬЗУЙТЕ ФУНКЦИИ НА УСТРОЙСТВАХ И У ОПЕРАТОРОВ

ОБУЧАЙТЕ ОСНОВАМ БЕЗОПАСНОСТИ: ОБЪЯСНИТЕ, ЧТО НЕЛЬЗЯ ДЕЛИТЬСЯ ЛИЧНЫМИ ДАННЫМИ, ПЕРЕХОДИТЬ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ, ВСТРЕЧАТЬСЯ С НЕЗНАКОМЦАМИ ИЗ СЕТИ.



ПООЩРЯЙТЕ ДОВЕРИЕ: РЕБЕНОК ДОЛЖЕН ЗНАТЬ, ЧТО МОЖЕТ ОБРАТИТЬСЯ К ВАМ, ЕСЛИ СТОЛКНЕТСЯ С ПРОБЛЕМОЙ

КОНТРОЛИРУЙТЕ АКТИВНОСТЬ: ИНТЕРЕСУЙТЕСЬ, ГДЕ РЕБЕНОК ПРОВОДИТ ВРЕМЯ ОНЛАЙН, В КАКИЕ ИГРЫ ИГРАЕТ, С КЕМ ОБЩАЕТСЯ.

УСТАНОВИТЕ ПРАВИЛА: ОБСУДИТЕ, СКОЛЬКО ВРЕМЕНИ МОЖНО ПРОВОДИТЬ В ИНТЕРНЕТЕ, КАКИЕ САЙТЫ ПОСЕЩАТЬ.

УВД БРЕСТСКОГО ОБЛИСПОЛКОМА



# ВНИМАНИЕ И УЧАСТИЕ РОДИТЕЛЕЙ



= БЕЗОПАСНОСТЬ  
РЕБЕНКА В КИБЕРСРЕДЕ



УВД БРЕСТСКОГО ОБЛИСПОЛКОМА



**ВАЖНО!**

расскажите своим детям

Мошенники **блокируют**  
**телефоны** через "бесплатный  
доступ" к популярной игре

# Какой предлог?

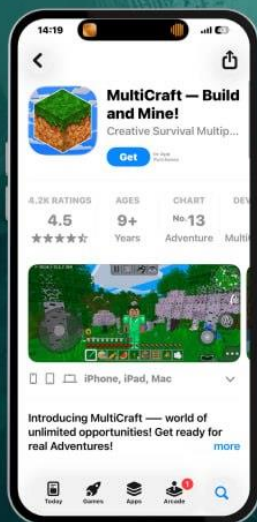


Аферисты предлагают детям бесплатный **MINECRAFT**, моды, скины или специальные версии игры.

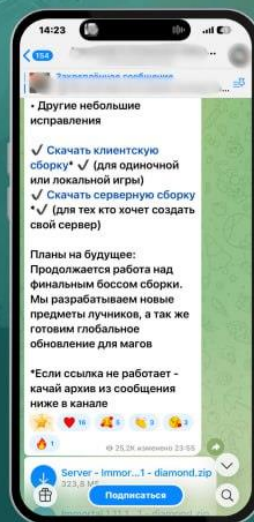
А для этого **переводят ребёнка в мессенджер** и убеждают выполнить несколько “простых действий”. На самом деле цель одна — получить доступ к телефону или аккаунтам.

## ПОМНИТЕ!

Бесплатные версии популярных игр в соцсетях почти всегда **являются уловкой**, за которой следует обман и вымогательство денег.

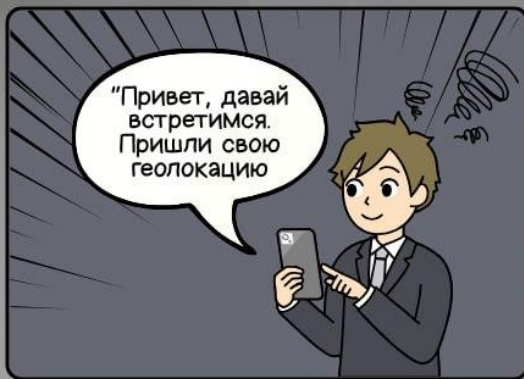


App Store



Неизвестный канал в мессенджере

# МОШЕННИКИ ЗВОНЯТ ДЕТЯМ!



**НЕ ПОДДАВАЙТЕСЬ НА ПРОВОКАЦИИ!**

Мошенники стали использовать детей в схемах кражи денег у их родителей.



Они действуют под видом «друзей из интернета» или «официальных представителей служб», чтобы вызвать доверие и управлять страхом.

## Сначала всё выглядит достаточно безобидно:



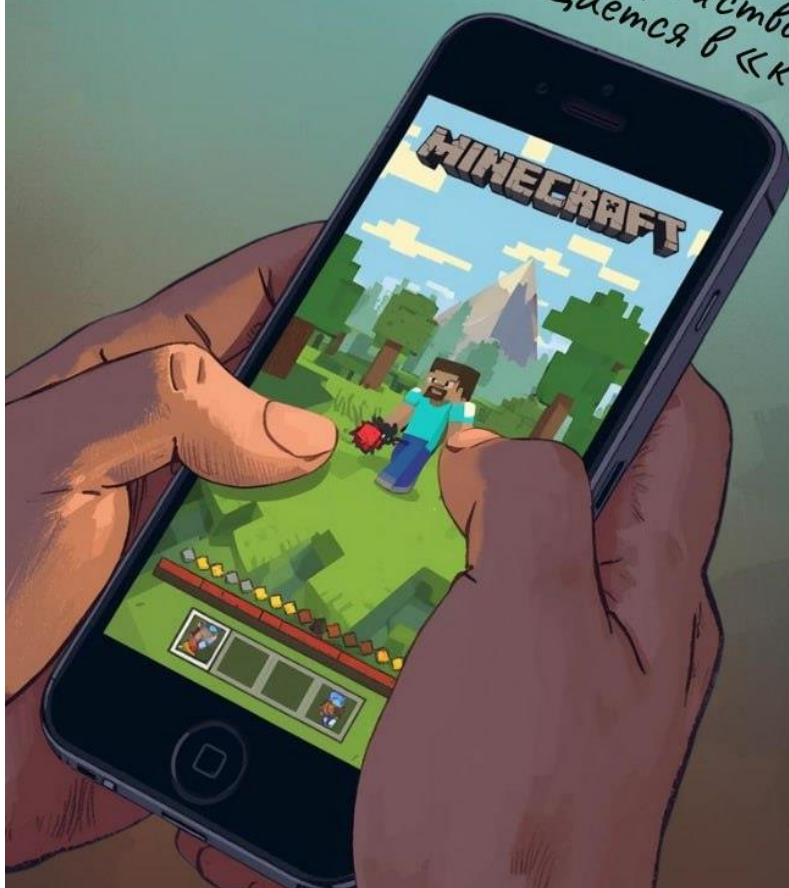
Общение кажется обычным — пока не появляются тревожные детали и давление.

## Как ребёнка лишают доступа к телефону?

Под предлогом установки игры мошенники просят ввести чужой Apple ID, отключить защиту и установить неизвестное приложение.

После этого аферисты **переводят смартфон в режим потери.**

*Если говорить просто,  
устройство  
превращается в «кирпич».*



**За возврат  
доступа  
аферисты  
вымогают  
деньги.**

## Как защитить ребёнка от онлайн-мошенников?



Родителям важно объяснять детям, что **бесплатного в интернете почти не бывает**, следить за тем, **какие приложения устанавливают дети**, и сразу **реагировать**, если кто-то пытается вымогать деньги.

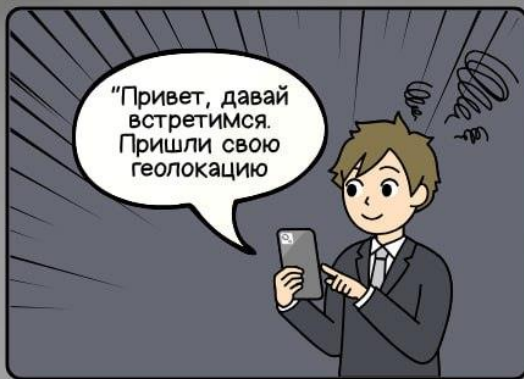
**Помните:** если ребёнок стал жертвой мошенников, **нельзя переводить средства**. Необходимо сразу обратиться в милицию!



Например, можно воспользоваться нашим чат-ботом в Telegram



# МОШЕННИКИ ЗВОНЯТ ДЕТЯМ!



**НЕ ПОДДАВАЙТЕСЬ НА ПРОВОКАЦИИ!**

Мошенники стали использовать детей в схемах кражи денег у их родителей.



Они действуют под видом «друзей из интернета» или «официальных представителей служб», чтобы вызвать доверие и управлять страхом.

## Сначала всё выглядит достаточно безобидно:



Общение кажется обычным — пока не появляются тревожные детали и давление.

Когда контакт установлен, мошенники включают сценарий страха.

## Они могут!

обвинить в «передаче секретной информации»



заявить о «рассрочке, оформленной на твое имя»




пригрозить «обыском» или «ответственностью родителей»




Далее подростку предлагают «спасти семью» или «сохранить деньги».


Просят положить наличные в безопасное место, передать курьеру или «задекларировать» их, чтобы деньги не изъяли во время проверки.



Твои данные попали к «аферистам». Сбережения твоих родителей в опасности!



Что я могу сделать, чтобы спасти свою семью?



Да, деньги есть в сейфе. Сейчас я его открою.



Возьми дома все наличные и сложи их в сумку. За ними придет сотрудник банка!

## ЧТО ВАЖНО ПОМНИТЬ РОДИТЕЛЯМ?

- 1 Разговаривайте с детьми о схемах, которые используют мошенники, регулярно
- 2 Объясните: настоящие сотрудники банков и милиции никогда не общаются через мессенджеры и не просят деньги.
- 3 Поддерживайте доверие, чтобы ребёнок не боялся рассказать о подозрительном звонке или сообщении.

A cartoon illustration of a woman with grey hair, wearing a grey t-shirt, standing with her hands clasped. A speech bubble above her contains text. The background is a solid orange color.

Если кто-то требует деньги, просит молчать или пугает «обыском» — это обман

# НАПОМИНАЕМ:

правоохранители,

операторы сотовой связи,

НЕ

сотрудники банка

ЗВОНЯТ

в мессенджерах, не просят помочь в поимке злоумышленников, продлить договор на оказание услуг или взять кредит.

Если вам поступил подобный звонок – немедленно прекратите разговор и сообщите о произошедшем в милицию.



наш чат-бот