

# Онлайн безопасность

---



Школа безопасности  
Сергея Киселева



## Сергей Киселёв

кандидат юридических наук

Основатель и главный тренер  
Школы безопасности  
[@safety\\_school](https://www.instagram.com/safety_school)

Сын, муж, отец

За безопасность необходимо платить, а за ее отсутствие —  
расплачиваться.

Уинстон Черчилль

Для современных детей онлайн пространство стало неотъемлемой частью их жизни. В интернете они играют, общаются, учатся, дружат и даже влюбляются.

Сегодня простой запрет гаджетов не поможет. Это их новая реальность, и в ней надо научиться безопасно себя вести: как одному дома, в городе, на игровой площадке или школе делать правильный выбор, принимать безопасные решения.

Но с современными детьми нравовучения не работают. Новое время требует новых форматов: надо уметь быть интересными, вовлекать, разговаривать с детьми на их языке, отслеживать тренды.

Я обожаю детей. На своих живых тренингах подмечаю их горящие глаза, желание узнавать новое, быть героями!

Главная цель, которую я определил для своего пути, — предупредить как можно больше родителей о проблемах, связанных с безопасностью.

Дорогие родители, спасибо за вашу осознанность! Вместе мы сможем защитить наших детей в сети. Этот гайд поможет нам сделать это интересно и позитивно.

## КОГДА И С ЧЕГО НАЧАТЬ?

Когда Вы приходите в автошколу, руль сразу не дают. В первую очередь:

- а) Рассказывают, как устроен автомобиль, и
- б) Объясняют правила дорожного движения.

Только через несколько уроков по теории вождения, Вы садитесь за руль. Инструктор обязательно рядом. И у него есть свои педали.

Представьте, что Вы — инструктор. А родительский контроль — это педали.

Безопасность движения детей по онлайн-пространству в Ваших руках:

- Будьте рядом, пока ребенок не научится пользоваться интернетом.
- Выберите язык общения: заботливый консультант, а не следящий за дисциплиной полицейский.

## ВЫ ВПЕРВЫЕ ПЛАНИРУЕТЕ ДАТЬ ГАДЖЕТ

**Расскажите** маленькому ребенку, что интернет — это огромный мир! В нем есть все, что можно представить на нашей планете и за ее пределами. Есть хорошие мультики, книги, игры. Но есть и опасные, которые могут навредить.

**СОВЕТ:** Объясните, что такое интернет, в сравнении с сахаром, лесом или космосом. Далее — примеры, как это сделать

## КАК ОБЪЯСНИТЬ РЕБЕНКУ, ЧТО ТАКОЕ ИНТЕРНЕТ?

### Интернет как сахар

Немного можно, но если питаться только тортами (не следить за своим экранным временем) — станет плохо. Можно вспомнить вместе семейный случай, когда ребенок становился раздраженным от «цифрового переедания» во время самоизоляции или в выходные у бабушки

### Интернет как лес

Может ли ребенок сам ходить в лес? Нет. Потеряется. Все ли грибы и ягоды можно есть в лесу (нажимать на все ссылки)? Нет, конечно. Можно отравиться (заразить планшет или телефон). В лесу есть дикие животные (незнакомцы и хейтеры в сети)

### Интернет как космос

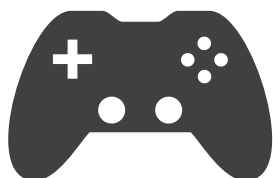
У Интернета даже значок в виде планеты. Но можно ли в космос выходить в футболке (ребенку без подготовки и специальных приложений в Интернет)? Нет. Нужен защитный скафандр (антивирусная программа, детский/родительский контроль)

**СОВЕТ:** Можно взять бумагу, карандаши и нарисовать объевшегося тортами ребенка, заблудившегося в лесу или вышедшего космонавта без скафандра

## ЕСЛИ РЕБЕНОК УЖЕ ЗНАКОМ С ИНТЕРНЕТОМ

**Спросите**, что для него значит Интернет?

«Игры», «Общение», «Мой любимый блогер», «Там прикольно», «Вся моя жизнь», «ТикТок».



Если Ваши дети отвечают так, они до конца не понимают, что такое Интернет.

Сделайте с ними упражнение «10 000 точек».





**РАСПЕЧАТАЙТЕ ЭТУ СТРАНИЦУ.  
УПРАЖНЕНИЕ «10 000 ТОЧЕК»**

A series of 30 horizontal dotted lines for writing.



## Цель упражнения «10 000 точек»

Продемонстрируйте ребёнку, что освоение интернета началось совсем недавно.

Люди еще учатся использовать его правильным образом. И очень важно уделять этому особое внимание.

## Техника выполнения

**Спросите:** «Как думаешь, что это?»

Внимательно выслушайте, а потом объясните, что это изображение истории человечества.

Каждая из точек — это поколение людей с тех пор, как наш вид возник 200 000 лет назад в Восточной Африке. Все это время постепенно развивались наше тело и мозг. Если взять одно поколение за 20 лет и разделить 200 000 на 20 лет, то получится 10 000 точек.



Как много из этих поколений жили с автомобилями, электричеством, водопроводом?

**Правильный ответ:** Около 150 лет, то есть почти 8 точек (пусть ребенок обведет их каким-нибудь цветом).



Сколько жили в мире с компьютерами и авиасообщением?

**Правильный ответ:** Около 50 лет, почти 3 точки (зарисуйте их еще одним цветом).



Как много поколений разобрались с гаджетами раньше, чем начали говорить?

**Правильный ответ:** Около 10 лет. Это половина точки. Но давай закрасим хотя бы 1 точку (возьмите самый яркий цвет).

**Скажите:** «Смотри, как много незакрашенных точек. И всего одна из них изображает время на Земле с интернетом. Пока люди еще учатся пользоваться интернетом, в сети появилось много вредителей и мошенников».





## ВАЖНО ОБЕЗОПАСИТЬ РЕБЕНКА. УСТАНОВИТЕ РОДИТЕЛЬСКИЙ КОНТРОЛЬ

### Как это сделать?

#### Для детей 5-6 лет

Установите программу перед тем, как впервые подарите малышу устройство.

Если разрешаете ребенку пользоваться Вашим гаджетом, создайте на этом устройстве отдельную учетную запись для ребенка.

В ней Вы сможете установить необходимые ограничения.

Помните, что зависимость формируется очень быстро.

Не давайте малышу телефон или планшет, когда он ест или для того, чтобы успокоить. Это может привести к тому, что малыш откажется есть без мультфильма, будет кричать или плакать, пока Вы не дадите ему телефон.

**Список программ родительского контроля Вы найдёте в приложении к гайду**

## Для детей 7-10 лет

Ребенку 7-10 лет компьютер понадобится для выполнения учебных задач, а телефон необходим для связи с родителями и друзьями, поэтому рекомендуется выделить ему отдельное устройство. Лучше всего установить программу родительского контроля перед тем, как дать ребенку его первый личный гаджет.

### **Скажите:**

«Я установил(а) специальную программу, чтобы защитить тебя. Она научит безопасно пользоваться интернетом, будет предупреждать о вредной информации и поможет найти телефон, если ты потеряешь его. Это твой скафандр в безграничном Интернете».

Рассказывать ребенку о всех возможностях программы нет необходимости. В отношениях с ребенком аккуратно используйте информацию, которую Вы получите с помощью родительского контроля. И пожалуйста, не следите за ребенком в сети.

Дети 7-10 лет большую часть свободного времени играют. Если ребенок проводит время за компьютерными играми, то у него может сформироваться игровая зависимость. Важно контролировать количество времени, которое ребенок проводит перед экраном.

Установите лимит на использование компьютера не более 2-х часов в день (4 порции по 30 минут). Экранное время будет контролировать сама программа.

## Для подростков 11- 13 лет

**Обсудите** установку и использование программы детского/родительского контроля. Это можно сделать обязательным условием покупки новой модели, которую подросток давно хотел.

**Программы лимита экранного времени Вы найдете в приложении к гайду**

**Скажите:** «Покупаем новый телефон (компьютер) с одним обязательным условием: на него будет установлен детский/родительский контроль. Эта программа защитит тебя от вредной информации на сайтах, предупредит меня о том, что незнакомый человек навязывает тебе свое общение, и подскажет мне, где ты сейчас находишься».

Если покупка нового устройства не входит в Ваши планы, расскажите подростку о своих опасениях и **предложите компромисс:**

«Сейчас много пишут об опасностях, которые подстерегают каждого из нас в реальной жизни и в интернете: похищения, ограбления, экстремизм, игры на деньги, виртуальные домогательства и шантаж. (Хорошо, если Вы приведете любой пример из жизни, известный подростку). Я очень волнуюсь за тебя, но понимаю, что ты растешь и хочешь большей свободы и самостоятельности. Давай договоримся: я перестану тебя расспрашивать о том, что ты делаешь, но мы установим программу, которая защитит тебя от вредной информации на сайтах, предупредит меня о том, что незнакомый человек навязывает тебе свое общение, и подскажет мне, где ты сейчас находишься».

## РЕКОМЕНДАЦИИ. КОНТРОЛЬ МЕСТОПОЛОЖЕНИЯ

**Не скрывайте от ребенка,** что Вы будете видеть информацию о его местоположении.

**Скажите:** «Ты становишься взрослее и хочешь быть более самостоятельным. Я рад(а) этому, но волнуюсь, что не смогу помочь тебе, если вдруг понадобится. Ты можешь спокойно проводить время с друзьями, но не уходи далеко. Я должен(а) всегда знать, где ты. Мы можем вместе обсудить территорию, по которой ты свободно гуляешь. Эта программа будет сообщать мне, если ты выйдешь за границы. Если тебе надо куда-то уйти, позвони и предупреди меня».



**Предупредите подростка**, что программа позволит Вам читать его сообщения в социальных сетях и предупреждать вас о контактах с подозрительными людьми:

«Я смогу так же, как и все остальные, просматривать твою страницу, но только то, что ты опубликовал в общем доступе. Не волнуйся, в закрытую переписку я заглядывать не смогу, это твое личное пространство, которое я уважаю. Но если к тебе в друзья будет проситься подозрительный человек, например, незнакомый взрослый, программа сообщит мне об этом».



## РЕКОМЕНДАЦИИ. ВРЕМЯ В СОЦСЕТЯХ

**Для подростка 11-13 лет** особую значимость приобретает статус в группе сверстников. Интернет используется как средство общения и социализации.

**Дружите** со своим подростком в соцсетях и **объясните** ребенку, что необходимо делать перерывы в использовании социальных сетей.

**Предложите** семейные условия:

«Зависимость от социальных сетей стала проблемой для многих людей не только в подростковом возрасте. Психиатры признали эту зависимость хронической болезнью, требующей лечения. Самый простой способ профилактики зависимости — установление временных границ использования. Я готов(а) разрешить тебе общаться в социальных сетях на двух условиях: мы всегда будем друзьями в соцсетях, и мы не находимся в соцсетях ночью и в выходные».

**▶ В общении с ребенком этого возраста излишний контроль может навредить вашим отношениям. А контакт с ребенком — главный инструмент безопасности в сети. Помните, что программа родительского контроля — это скафандр ребенка в сети, а не инструмент слежки родителей.**

## КОНТАКТ С РЕБЕНКОМ В СЕТИ — ГЛАВНЫЙ ИНСТРУМЕНТ ОНЛАЙН БЕЗОПАСНОСТИ. КАК ПОНЯТЬ, ЧТО ОН ЕСТЬ?

Проведите **простой тест**.

**Ответьте** сначала сами, а потом **задайте** эти же вопросы ребенку.

1. Любимая игра ребенка и персонаж

---

2. Любимый мультфильм (серия или сюжет из него)

---

3. Любимый исполнитель и трек

---

4. Любимый блогер и выпуск

---

5. Лучшие друзья в онлайн

---

### Проверка результата

Если хотя бы 3 ответа совпали, Вы достаточно хорошо знаете интересы ребенка в сети. Если меньше, общайтесь с ребенком про интернет больше. Поговорите, интересуйтесь, а не допрашивая. Как будто Вы разговариваете с новым интересным для Вас человеком.



## ЭКРАННОЕ ВРЕМЯ. КАК ОГРАНИЧИТЬ БЕЗ ССОР?

### **ШАГ 1. Объясните ребенку, что интернет — это возможности.**

Расскажите, что кроме блогеров и игр, в сети есть:

- Интересные мультики про дружбу, путешествия, мечты, свершения.
- Обучение, книги и лекции на любую тему.
- Захватывающие экскурсии и театральные постановки лучших сцен мира.
- Конкурсы и соревнования в спорте, искусстве, моделировании и других увлечениях.
- Общение, обмен новыми идеями с иностранными ребятами.
- Обучение в иностранных школах.

### **ШАГ 2. Сделайте время после гаджета — активным совместным занятием.**

Чтобы научить ребенка самостоятельно регулировать свое экранное время, будьте самодисциплинированы и последовательны.

**Введите** неизменяемую схему пользования гаджетом.

## СХЕМА ПОЛЬЗОВАНИЯ ГАДЖЕТОМ

1

### Чем бы ты хотел заняться после пользования гаджетом?

Давай договоримся о совместном занятии/игре, которая нам с тобой будет интересна

2

### Заведи свой будильник на 30 минут

Это поможет тебе понять, что время с телефоном/планшетом закончилось

3

### Когда будильник прозвенит, мы с тобой поиграем в игру (что-то, что любит Ваш ребенок)

Иди играй/смотри, я тебя очень жду

Обязательно **выполняйте** все правила игры и свое обещание!

Совместным временем после гаджета Вы фиксируете положительный эффект переключения из виртуальной жизни в реальную.

Так гаджет и экранное время не станет чем-то особенным и не будет поводом для ссор.

## **ШАГ 3. Наглядно продемонстрируйте и объясните вред для здоровья от гаджетов.**

### **ОСАНКА**

Попросите ребенка встать к стене спиной, прижав пятки и затылок к стене — это правильное положение осанки. А теперь попросите ребенка взять гаджет и что-нибудь сделать в нем, не отстраняя затылка от стены.

Скажите, что это правильное положение пользования гаджетом. Но мало кто так делает. И поэтому у многих детей и взрослых болит шея и голова.

### **ГЛАЗА**

Поиграйте с ребенком в гляделки на время. Кто из Вас первый моргнет, тот проиграл. Не пройдет и 15-20 секунд, как Вам и ребенку захочется моргнуть.

После этого, проведите эксперимент с морганием у экрана. Попросите ребенка поиграть в игру или посмотреть мультфильм на устройстве (3-5 минут будет достаточно). Запишите лицо смотрящего ребенка. Покажите запись. Замечает ли он что-нибудь необычное? Оказывается, за 3 минуты ни разу не моргнул. Свет экрана завораживает. Но человеку необходимо моргать, чтобы глаза не уставали и не болели. Поэтому очень важно соблюдать время, проведенное в гаджете.

### **РУКИ**

Попросите ребенка взять телефон или планшет в руки. Уберите гаджет, сохранив положение рук и кистей. Попросите его так походить 10-15 минут, периодически подходя к зеркалу. Обратите внимание ребенка, когда он будет опускать руки вниз. Объясните, что руки затекают в положение гаджета. Это нездорово для скелета. Поэтому долго держать телефон в руках — вредно.

## ШАГ 4. Установите в семье правила диджитал-детокса.

Журналист The New York Times Ник Билтон во время одного интервью задал Джобсу вопрос: «Видимо, Ваши дети без ума от айпада?» И получил такой ответ: «Они не пользуются им. Дома мы ограничиваем время, которые дети проводят за экранами айпадов».

**Расскажите** ребенку, для чего нужен отдых от гаджетов и как его проводить.

▶ **Чтобы улучшить наше самочувствие.** Когда мы много играем/смотрим/поглощаем информацию, мозг перегружается и наше настроение может быть плохим, сил и энергии становится мало. Надо помочь организму восстановиться.

▶ **Чтобы лучше сделать уроки/проект/работу, связанную с хобби.** Гаджеты нас отвлекают. Быстрая информация и яркая картинка завоевывают наше внимание. Это специально сделали очень умные люди. Ты знаешь, что Стив Джобс, который придумал айфоны и айпады, ограничивал время, которое дети проводили с гаджетами? Давай прочитаем об этом в интернете.

▶ **Чтобы самому придумать что-то новое!** Чтобы стать изобретателем, музыкантом или решить сложную задачу. Только в бездействии мозг начинает работать по-новому. Это называется гибкость мышления. Когда перестает поступать много информации из экрана, мы начинаем придумывать что-то сами, творчески самовыражаться. Замечал когда-нибудь, что, когда ты отдыхаешь, тебе приходит свежая идея? Или появляется решение сложной задачи, которую ты раньше не мог решить?

## КАК ПОДГОТОВИТЬСЯ И КАК ПРОВОДИТЬ ДИДЖИТАЛ-ДЕТОКС?

В семье Джобса существовал запрет на использование гаджетов по ночам и в выходные.

- ▶ Обсудите со всеми членами семьи необходимость диджитал-детокса.
- ▶ Подберите комфортный для всех график и вводите его постепенно. Первый день диджитал-детокса сделайте пробным – на полдня.
- ▶ Определите место нахождения гаджетов на выходные. Это может быть коробка или корзина. Гаджеты всей семьи находятся там. Строгого запрета на использование устройств нет, их просто нет на глазах.
- ▶ Составьте план на время детокса. Так будет проще забыть о манящем телефоне. А выезд в интересное место всей семьей еще и укрепит отношения.
- ▶ Предупредите близких, что будете онлайн в понедельник.

Наслаждайтесь!)

- Напишите список мест и времени, свободных от гаджетов в Вашей семье.
- Разместите его на холодильнике.

1. Один час после пробуждения

2. Один час перед сном

3. В туалете и ванной

4. Во время еды

5. \_\_\_\_\_

6. \_\_\_\_\_

7. \_\_\_\_\_

8. \_\_\_\_\_

9. \_\_\_\_\_

10. \_\_\_\_\_

**Соблюдать необходимо всем членам семьи.** Иначе не сработает.

Если Вам нужен гаджет для работы, объясните это ребенку.

Но **не обманывайте его**, если перед сном Вы играете в стрелялку, листаете инстаграм или смотрите видео про рыбалку.

## СОСТАВЬТЕ ЧЕК-ЛИСТ ИГР И ИНТЕРЕСОВ

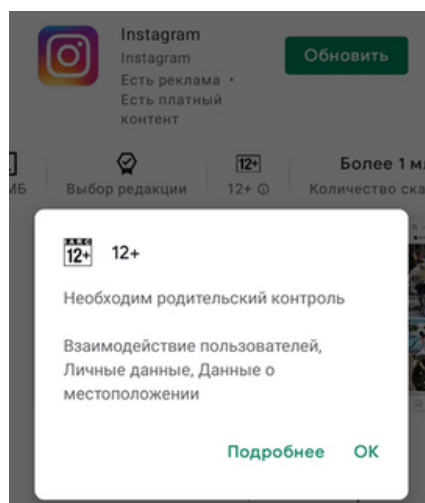
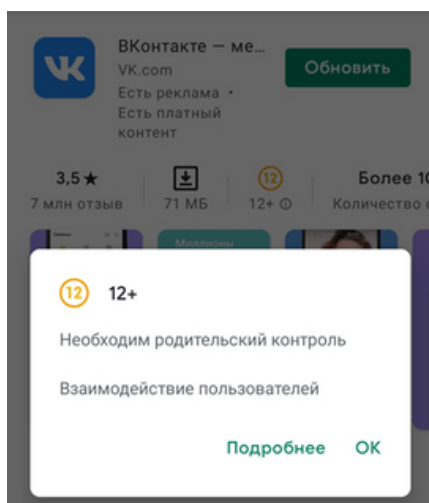
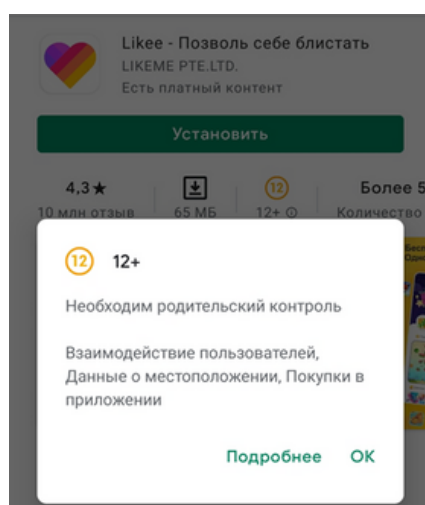
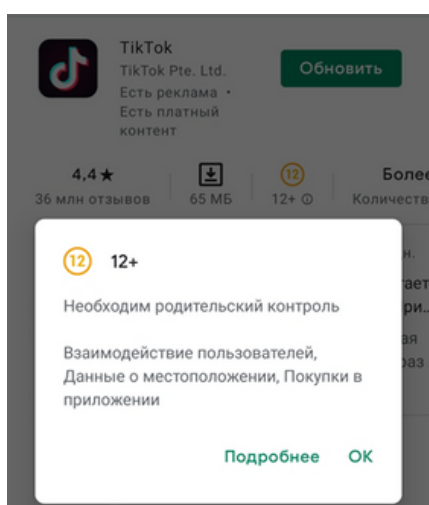
- Сделайте его совместно со своим ребенком.
- Повесьте распечатанный чек-лист на видное место.
- Используйте как подсказку для выбора совместных занятий на выходные.

1. Театр теней
2. Диафильмы
3. Настольные игры
4. Бокс/хоккей/футбол/ танцы
5. \_\_\_\_\_
6. \_\_\_\_\_
7. \_\_\_\_\_
8. \_\_\_\_\_
9. \_\_\_\_\_
10. \_\_\_\_\_



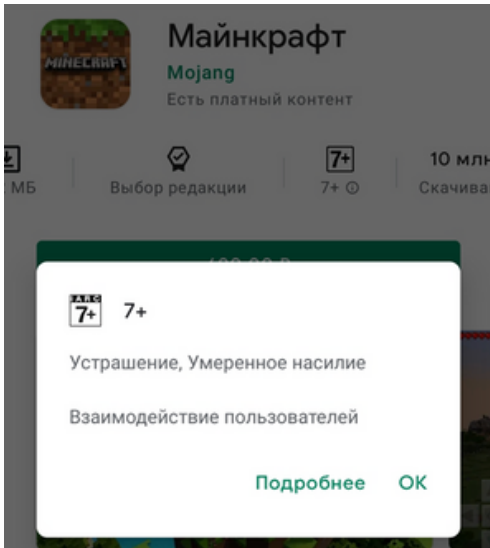
## ПРАВИЛА БЕЗОПАСНОСТИ В СОЦСЕТЯХ, МЕССЕНДЖЕРАХ И С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

Для начала запомните и расскажите детям, что в соцсетях установлено **ВОЗРАСТНОЕ ОГРАНИЧЕНИЕ**: строго с 12 лет





## СОБЛЮДАЙТЕ ВОЗРАСТНЫЕ ОГРАНИЧЕНИЯ В ИГРАХ



**Standoff 2 16+**

**Among Us 7+**

**Brawl Stars 7+**

**! Не привязывайте свои банковские карты к устройствам, на которых играет ребенок.**

Если у Вас списали деньги за донаты, игры, музыку, купленные Вашим ребенком, средства можно вернуть. Главное, сделать это быстро.

Сразу же **обратитесь в поддержку Apple или Google.**

Инструкции, как это сделать, находятся **здесь**:

[«Запрос возмещения за покупку в магазинах Apple»](#)

[«Возврат средств за покупки в Google Play»](#)

А потом отвяжите карты.

## ПОЧЕМУ В СОЦСЕТЯХ ТОЛЬКО С 12 ЛЕТ?

▶ **Попросите** ребенка обхватить Вашу голову своими руками.

Перенесите этот объем головы взрослого человека на его голову. Между ладонями и головой ребенка окажется зазор примерно в 2 сантиметра. Также можно измерить сантиметровой лентой.

▶ **Объясните**, что голова ребенка значительно меньше головы взрослого, потому что еще не все зоны мозга сформировались. Расскажите, что существует такая часть, которая называется префронтальная кора головного мозга. Она отвечает за сложные взаимодействия с незнакомыми людьми, объективную оценку оскорбительных комментариев, полноценный критический анализ контента.

**Например, если девочка в 9 лет попадает в ТикТок и ей под видео пишут, что она толстая, то она будет делать все, чтобы похудеть. Если мальчика 10 лет Вконтакте просят отправить взаимное интимное фото, то он сделает это и не сообразит, какие могут быть последствия. А это может послужить поводом для травли или вымогательства.**

**Скажите:** Чтобы ты не попал в беду, даже создатели соцсетей запрещают регистрироваться раньше 12 лет.

## ТОП 10 ПРАВИЛ БЕЗОПАСНОСТИ В СОЦСЕТЯХ. НАУЧИТЕ ЭТОМУ СВОЕГО РЕБЕНКА

- 1** Не указывай своих контактных данных: телефон, адрес дома, адрес и номер школы, не отмечай членов семьи. Твои одноклассники и друзья и так знают твои контакты, а посторонние обойдутся без конкретных подробностей.
- 2** Не рассказывай в постах и статусах о своих перемещениях, когда выходишь из дома, когда возвращаешься. Игнорируй вопросы об адресах и своих маршрутах от малознакомых людей.
- 3** Как бы ты ни доверял человеку, или как бы ты ни любил его, никогда не присылай ему твои полуобнаженные или обнаженные фотографии. Они вполне могут стать предметом шантажа, или оказаться в общем доступе. Ни-ког-да! То же самое относится к общению по скайпу. Сделать скрин — дело секунды.

**4** Первая реальная встреча с виртуальным другом должна проходить только в присутствии родителей. Если тебе совершенно ни к чему мое присутствие, то попроси контакты родителей нового друга. Мы должны связаться и договориться о вашей первой встрече. Такого быть не должно, но если ты по какой-то причине не сможешь поставить меня в известность, то подстрахуйся, рассказав о встрече хорошему другу. Пусть кто то из тех, кому ты доверяешь, всегда знает, куда ты идешь и с кем встречаешься. Это вовсе не так глупо, как может показаться. На первую реальную встречу лучше пойти вдвоем с надежным другом. Даже если у вас намечается романтическое свидание, и вы не хотите о нем никому рассказывать, назначь встречу в людном месте и ни в коем случае не соглашайся пойти в гости. Многие истории похищений и изнасилований начинались с предложений «встретиться у меня дома» или «зайти на минуту по пути к моей подруге что-то забрать».

**5** Любая попытка виртуального собеседника, с которым ты не знаком в реальности, поговорить на сексуальные темы, показать порно, эротическое видео или фото, кинуть ссылку на сайт с откровенным содержанием, просьбы поделиться интимной информацией должна быть оценена как грозящая опасность. С таким человеком общение лучше прекратить. Если тебе пишет незнакомый человек, начиная общение с «привет», или присылают ссылку на неизвестный сайт — игнорируй человека, не переходи по ссылке. Если тебе регулярно и навязчиво первым пишет посторонний, пытается завязать разговор — также игнорируй, а лучше отправь в бан/заблокируй его.

**6** Следи за тем, что пишешь в личных сообщениях, какую информацию доверяешь другому человеку. Лучше не писать о том, что ты боишься увидеть в открытом доступе. Выбери для откровенных разговоров телефон или личную встречу. Скриншоты твоих откровений могут быть показаны тем, кому их видеть не стоило бы.

**7** Помни, что на любом сайте есть техническая поддержка, в любой группе есть модерация. Если видишь человека с агрессивным и подозрительным поведением — всегда можно и нужно об этом сообщить, нажав кнопку «Пожаловаться».

**8** Приглашение в группу с суицидальным содержанием (или с любым другим, призывающим к асоциальному поведению) говорит о том, что собеседник не слишком адекватный. Даже имея мрачные взгляды на мир, друг никогда не будет призывать к самоубийству. И звать на кровавые разборки. Или покататься на крыше электрички в метро. И брать на слабо. И предлагать быстро заработать в интернете. Или сделать ставку. Ты уже чувствуешь разницу между обменом музыкой, картинками или текстами на тему «всё — тлен» и втягиванием в саморазрушение на практике?

**9** Старайся не вступать в разговоры и споры с троллями. Убедить в своей правоте, переспорить ты их не сможешь, зато они добьются своей цели – спровоцируют тебя на конфликт. Бан, бан, и бан, без выяснений.

**10** Если ты сделал что то, за что теперь очень стыдно, или с кем-то поссорился, или тебя отфрендили, или удалили из любимой игры, — это не катастрофа. Даже если тебя шантажируют. Можно на время покинуть игру/сайт/группу/сеть вообще, переехать в офлайн на какое то время. Приходи ко мне посоветоваться, я постараюсь тебе помочь. Надеюсь, такого не случится, но если ты не захочешь прийти ко мне, поговори с кем то из старших, чтобы решить проблему, если у тебя возникли настоящие трудности.

## ПОЧЕМУ НЕЛЬЗЯ ПИСАТЬ ВСЕ, ЧТО ЗАХОЧЕТСЯ. ПРАВИЛО ПЕРМАНЕНТНОГО МАРКЕРА

### Предупредите.

**Все, что пишется в сети, остается там навсегда.**

Как надпись перманентным (нестирающимся) маркером на белой доске или листе.

Не пиши, если не уверен, что хотел бы это оставить в Интернете навсегда.

Знай, что любое твое личное сообщение может стать видно абсолютно всем. Даже если ты его удалил.

**Во-первых**, могут успеть сделать скрин твоего сообщения, до того, как ты его удалил.

**Во-вторых**, есть специальные приложения, которые читают удаленную переписку. Но я, как тренер по безопасности, не рекомендую их использовать.

Вы разрешите стороннему приложению читать Ваши личные сообщения. Это небезопасно!

### **ВЫПОЛНИТЕ УПРАЖНЕНИЕ**

Попросите ребенка написать Вам сообщение в WhatsApp. Сделайте скрин экрана и предложите нажать кнопку удалить у всех.

Покажите переписку с удаленными сообщениями и сохранившийся снимок.

**Скажите:** видишь, теперь я могу показать всем фото твоего сообщения.

**ПОЧЕМУ НЕЛЬЗЯ ОТПРАВЛЯТЬ ФОТО/ВИДЕО,  
КОТОРЫЕ ТЫ НЕ ХОЧЕШЬ, ЧТОБ УВИДЕЛИ ВСЕ.  
ПРАВИЛО БАННЕРА**

Не выкладывай в сеть фото и видео, которые не хотел бы видеть на баннере перед домом или школой.

Даже самые близкие друзья могут показать эти фото в шутку или со злости.

- ▶ **ВЫПОЛНИТЕ УПРАЖНЕНИЕ** такое же, как и с удалением переписки.





## СКРИН ЭКРАНА ЗА 3 СЕКУНДЫ

### **ОБЯЗАТЕЛЬНО**

**Научите** ребенка делать скрин экрана на телефоне и планшете за 3 секунды.

Это первое, что должен будет сделать ребенок, когда ему напишут или пришлют что-то странное в сети.

Второе, что нужно будет сделать — показать скрин Вам.

А что вам нужно будет сделать? Правильно! Не «взорваться» критикой и нравоучениями. Почему? Потому, что ребенок больше никогда к Вам не подойдет с проблемным вопросом из сети.

**Успокойте** ребенка и **помогите** разрешить ситуацию.

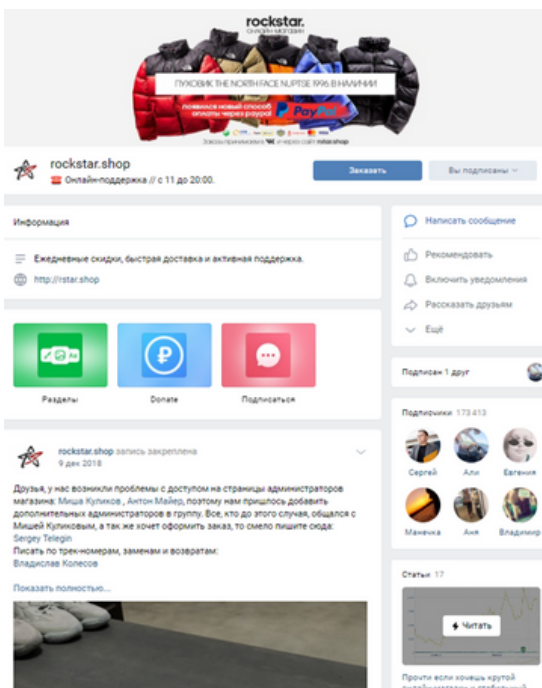
При необходимости обратитесь за помощью к нам.

## ПОДДЕЛЬНЫЕ СТРАНИЦЫ, ГРУППЫ, БОТЫ И МАГАЗИНЫ МОШЕННИКОВ В СОЦСЕТЯХ

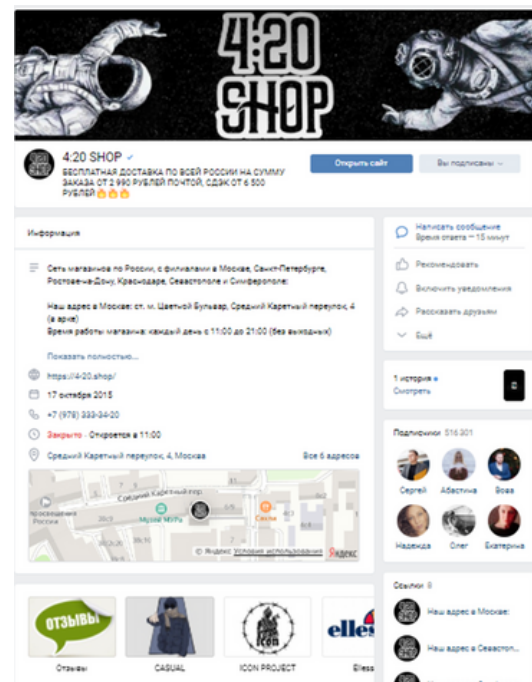
Как определить, настоящая страница или Вас обманывают?

### ► СДЕЛАЙТЕ УПРАЖНЕНИЕ.

Покажите ребенку два интернет-магазина.



**ROCKSTAR.SHOP**



**4:20.SHOP**

## ЗАДАЙТЕ ВОПРОСЫ

Где мошенники?

RockStar.Shop или 4:20 SHOP?

Почему ты так думаешь?

По каким признакам это понял?

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_

### **Правильный ответ: RockStar.Shop**

Расскажите, почему. Попросите ребенка это запомнить и обращать внимание в интернете.

- 
1. Живые контакты (указан телефон) и физический адрес сообщества
2. Актуальные сторис + лента сообщений со свежими публикациями
3. Живое и оперативное взаимодействие с другими участниками группы в ленте
4. Значок верификации сообщества (синяя галочка)

#### Верифицированное сообщество

Это официальное сообщество известной персоны или организации.

[Узнайте больше о новой верификации](#)

4:20 SHOP ✓

5. Отсутствие донатов

Давайте вместе создадим кроссовки мирового масштаба!

Для попадания на обложку сумма доната должна быть не менее 10 Р

Отправить донат

## ПОЧЕМУ НУЖНЫ НАДЕЖНЫЕ ПАРОЛИ

### Объясните ребенку

Надежные пароли — основа интернет-безопасности. За паролями спрятаны твои очень личные данные, переписки, банковские данные.

### Запомни:

#### **НЕЛЬЗЯ** включать в пароль

- даты рождений
- имена и фамилии
- названия сайтов

#### **Надёжный пароль:**

- длинный, не короче 15 символов
- состоит из цифр, Прописных и строчных букв, специальных символов
- не связан с данными о тебе

## НО РАЗВЕ МОЖНО ЗАПОМНИТЬ СЛОЖНЫЙ ПАРОЛЬ?

Да. И это не потребует особых усилий.

Понадобится **стихотворение**. Не выбирайте банальное. Возьмите редкое, которое мало кто знает, еще лучше - придумайте собственное.

Возьмём для примера самое простое четверостишие:

В траве сидел кузнечик,  
В траве сидел кузнечик,  
Совсем как огуречик,  
Зелененький он был.

**Переключим** раскладку клавиатуры на латиницу и снова запишем эти четыре строки (без знаков препинания), сохраняя прописные и строчные буквы. Теперь возьмем у каждого слова только первый символ. У нас получится: DncrDncrCrjPj,

Осталось **добавить цифры**. Откуда их взять? Из того же четверостишья. Запишите количество букв в каждом слове первой строки: в(1) траве(5) сидел(5) кузнечик(8). Добавьте цифры в любое место пароля. Итоговый вариант: 1Dncr5Dncr5Crj8Pj,

А еще можно взять за основу известное выражение, записать его строчными и заглавными латинскими буквами, замените некоторые из них похожими цифрами или символами: l\_p0Mn | O\_4y9n0e Mg№vEn | E (Я помню чудное мгновенье).

**Это надёжные пароли. Вы без труда вспомните их.**

## КАК ЧАСТО МЕНЯТЬ ПАРОЛЬ?

Мы рекомендуем менять пароль каждые 4 месяца, т. е. **3 раза в год.**

### ЗАЩИТА ПАРОЛЯ

- **Никому не сообщайте** и не отправляйте свои пароли.
- **Не оставляйте** в доступном месте пароли, записанные на бумаге.
- **Используйте менеджер паролей** или встроенное в браузер хранилище паролей.
- **Используйте разные пароли** для Ваших учетных записей. Если будете использовать одинаковые пароли, а злоумышленник узнает пароль от одной учетной записи, он сможет получить доступ ко всем остальным.
- Настройте на всех учетных записях **двухфакторную аутентификацию**. Это когда для подтверждения входа в аккаунт нужно ввести еще и пароль из СМС.

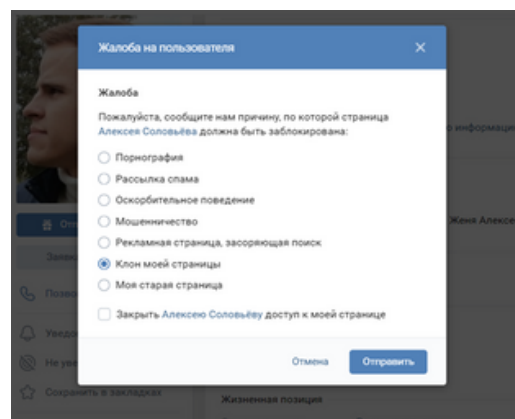
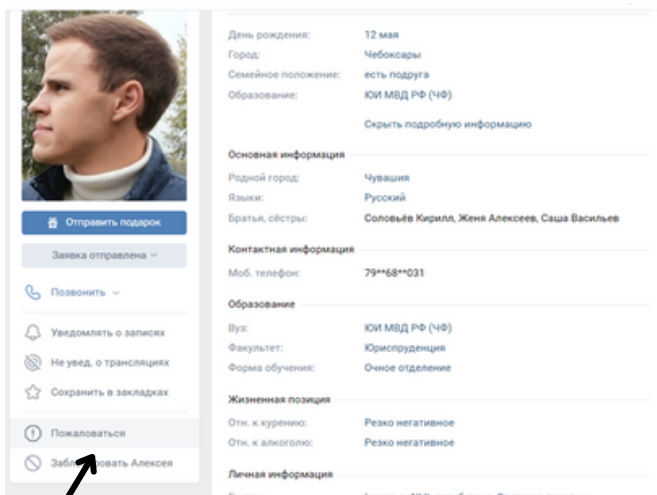
## КЛОНЫ В СОЦСЕТЯХ

**ПРОВЕРЯЙТЕ КЛОНЫ** на свои страницы и страницы ребенка в соцсетях 1 раз в 4 месяца.

- Установите программу FindClone из Apple store или Google play.
- Проверьте, есть ли странички с Вашими фото.



**При обнаружении клона, сообщите об этом модераторам соцсети.**





## ОПРЕДЕЛИТЕ УРОВЕНЬ БЕЗОПАСНОСТИ В СЕТИ

Вы уже многое обсудили с детьми. И теперь можно закрепить знания.

Пройдите вместе тест

1

Какие пароли из этих можно назвать надежными?

- 1.20122010
- 2.Qwerty
- 3.Lenalvanova2010
- 4.15DncrD58ncrCrjPj
- 5.Korob04k

2

Можно ли использовать один и тот же пароль для почты и всех социальных сетей?

- 1.Конечно, да.
- 2.Можно, если пароль сложный.
- 3.Ни в коем случае.

3

После регистрации соцсеть предлагает вам подключить двухфакторную аутентификацию. Это когда вы вводите логин и пароль, и на телефон приходит СМС с кодом, который нужно ввести для доступа к странице. Как поступите?

1. Конечно, подключу.
2. Зачем терять столько времени.
3. Мне такое не нужно, у меня и так крутой пароль.

4

Вы бесплатно скачали в соцсетях книгу «История Мира» в двух частях. В папке «Загрузка» появилось 2 файла: Mir\_1.pdf и Mir\_2.exe. Как поступите?

1. Первый файл похож на вирус, второй можно открывать.
2. Второй файл подозрительный, а первый безопасен.
3. А что не так? Открою оба.
4. Все это очень подозрительно, лучше купить книгу в официальном интернет-магазине.

5

Вам приходит сообщение от подруги: «У меня проблемы, можешь мне срочно денег прислать?» Как поступите?

1. Позвоню подруге и спрошу, она ли это написала
2. Задам хитрый вопрос, ответ на который знает только подруга.
3. Пришлю денег без вопросов. Может быть, помощь нужна срочно. Мало ли что случилось
4. Проигнорирую

6

Вам приходит письмо от неизвестного отправителя: «Здравствуйтесь, высылаю документы». Во вложении, судя по картинкам, действительно лежат документы. Как поступите?

1. Отвечу на письмо: «Похоже, вы ошиблись, я не жду никаких документов»
2. Посмотрю из любопытства, что там приложено. Ну-ка...
3. Удалю сообщения и пожалуюсь на спам. Это мошенники"

7

Вы завели почтовый ящик на Gmail. С адреса support@gmail.com получили письмо: «Уважаемый пользователь! Кто-то только что пытался войти в ваш аккаунт, используя ваш пароль. Вы заблокировали подозрительную попытку входа и настоятельно рекомендуем вам сменить пароль». Ниже видна синяя кнопка с надписью «Сменить пароль».

1. Удаляю письмо и пожалуюсь на спам. Это точно мошенники.
2. Нажму на синюю кнопку и сменю пароль. Не хочу, чтобы меня взломали.

8

Вы регистрируетесь в социальной сети. Какую реальную информацию о себе укажете на странице?

1. Вообще никакую. Сделаю фейковую страницу. Имя и фамилию придумаю
2. Только имя и фамилию
3. Имя, фамилию и дату рождения
4. Имя и фамилию, дату рождения, школу
5. Имя и фамилию, дату рождения, школу, район, лучших друзей, любимые цитаты — все, что захочу. Зачем скрываться? Это же социальная сеть и я там для общения

9

Какой-то незнакомец несколько дней подряд пишет Вам в социальной сети гадости и обзывает Вас. Вы догадываетесь, что это Ваш знакомый. Кто именно — непонятно... Как поступите?

1. Буду угрожать ему полицией.
2. Постараюсь выяснить, кто это, чтобы поговорить лично.
3. Попробую объяснить, что он заблуждается и я не такая уж плохая, как он считает
4. Ничего не сделаю, только расстроюсь и буду плакать
5. Забаню этого тролля — и дело с концом

10

Человек, в которого Вы влюблены, живет за две тысячи километров от Вас. Он просит, чтобы Вы прислали ему свое интимное фото. Как поступите?

1. Я же люблю его! Пришлю, конечно
2. Если он пообещает никому не показывать фото — тогда пришлю.
3. Пришлю, только вначале закрасю кое-что...
4. Не пришлю ни в коем случае

!**Итог теста (запишите Ваши ответы)**

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

7. \_\_\_\_\_

8. \_\_\_\_\_

9. \_\_\_\_\_

10. \_\_\_\_\_



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

1) Какие пароли из этих можно назвать надежными?  
Только пароль 15DncrD58ncrCrjPj

### Признаки ненадежного пароля:

- ▶ банальность и очевидность (qwerty, 123456); пользователи чаще всего выбирают, а злоумышленники взламывают именно такие пароли;
- ▶ одно слово (password), даже длинное и редкое (parallelepiped);
- ▶ слово на русском языке, набранное в латинской раскладке (gfhjkm – «пароль»);
- ▶ сочетание цифр и букв, из которого получается слово (kor0bo4ka);
- ▶ пароль содержит твои имя и фамилию и / или дату рождения (Lenalvanova12052004).

### Признаки надежного пароля:

- ▶ длинный, не короче 15 символов;
- ▶ в нем есть цифры, ПРОПИСНЫЕ и строчные буквы, специальные символы.



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

Ради чего столько времени на сложные пароли? Кого интересуют мои аккаунты?



**Вот несколько вариантов, что можно сделать после взлома почты или аккаунта:**

1. Притвориться Вами и вымогать деньги у близких
2. Изменить Ваши пароли на всех ресурсах, где Вы зарегистрированы
3. Разослать кучу спама от Вашего имени и испортить Вам репутацию
4. Вывести деньги с Ваших электронных кошельков
5. Распространить переписку (где могут быть Ваши секреты), фотографии (которые Вы не хотели бы показывать другим), сканы документов
6. Если Вы администрируете группы в соцсетях — испортить их, удалить все содержимое и загрузить туда от Вашего имени порнографические ролики
7. Залить на Вашу страницу контент, который нарушает закон (например, объявления о продаже наркотиков), а отвечать придется Вам, владельцу аккаунта. И доказать, что Вы ни причем, будет очень трудно.





## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

Но мало иметь отличный пароль.

В нем нет смысла, если Вы:

- Записываете пароль на бумажке или сохраняете в текстовом файле.

**В чем дело:** любой, кто увидит пароль, может им воспользоваться.

- Сохраняете пароль в браузере и не заботитесь об антивирусной защите.

**В чем дело:** есть вирусы, которые воруют пароли из браузера.

- Подключаетесь к публичному Wi-Fi и вводите пароль.

**В чем дело:** злоумышленники могут перехватить трафик и узнать пароль.

- Не разлогиниваетесь и пускаете за свой компьютер / ноутбук / планшет посторонних.

**В чем дело:** им даже не понадобится пароль, чтобы войти в Ваши аккаунты.

**Качественный пароль не защитит Вас, если Вы беспечны.**

Причина большинства так называемых взломов — человеческий фактор.

Не угадывание простого пароля 12345, а «я дала смартфон знакомому, он прочитал мою переписку, перекинул себе мои фотографии и выложил их в Интернет».

**Берегите свои устройства.**



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

**2) Можно ли использовать один и тот же пароль для почты и всех социальных сетей?**

**Конечно, нет.**

Но как запомнить десятки сложных паролей?

Если Вам совсем сложно держать их в голове, поможет менеджер паролей — программа, которая хранит все пароли.

Для доступа к ним надо помнить один единственный мастер-пароль. Если не знаете, какой менеджер выбрать, установите KeePass или LastPass.

**3) После регистрации соцсеть предлагает Вам подключить двухфакторную аутентификацию. Это когда Вы вводите логин и пароль, и на телефон приходит СМС с кодом, который нужно ввести для доступа к странице. Как поступите?**

**Конечно, подключу.**

Человек, который узнал пароль, не получит доступа к Вашему аккаунту, если Вы подключили двухфакторную аутентификацию.



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

**4) Вы бесплатно скачали в соцсетях книгу «История Мира» в двух частях. В папке «Загрузка» появилось 2 файла: Mir\_1.pdf и Mir\_2.exe. Как поступите?**

Расширение pdf принадлежит файлу, который открывается в Adobe редакторе. Расширение exe означает, что это исполняемый файл. Когда Вы его откроете, запустится программа. Какая? Вряд ли полезная.

Купить книгу в интернет-магазине означает убить двух зайцев сразу. Заяц первый — это безопасно, вам не подсунут вредоносную программу. Заяц второй — это честно: автор получит деньги за работу. Не хотите платить, опасаясь, что книга не понравится? Обычно магазины разрешают прочитать ознакомительный фрагмент: от 10 до 25 % текста. Этого достаточно, чтобы понять, нравится книга или нет.



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

**5) Вам приходит сообщение от подруги: «У меня проблемы, можешь мне срочно денег прислать?» Как поступите?**

Похоже, кто-то взломал страницу подруги. Самый быстрый способ проверить, с кем Вы переписываетесь, — позвонить ей и спросить, что случилось.

**6) Вам приходит письмо от неизвестного отправителя: «Здравствуйте, высылаю документы». Во вложении, судя по картинкам, действительно лежат документы. Как поступите?**

Удалю и пожалуюсь!

Что случится, если вы кликнете на картинку? Там не документы, а скрытая гиперссылка. Она приведет Вас на сайт, замаскированный под сайт электронной почты. Вы увидите окно для ввода логина или пароля и подумаете, что случайно выкинуло из почты. Заново введете пароль — и вуаля, он достанется злоумышленникам.



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

Это называется **ФИШИНГ**. Ловля виртуальной рыбки. Вместо рыбака — мошенники, вместо рыбки — Вы, Ваши логины и пароли. Неважно, насколько пароль длинный и надежный, если Вы добровольно его отдаете.

### Как обезопаситься от фишинга?

- ▶ Любые письма без личной информации подозрительны. «Добрый день, посмотрите документы», «Я прислал Вам реквизиты во вложении», «Вот мой отчет». Если бы Вы на самом деле ждали документы или отчет, Вы могли бы легко попасться на удочку. Но секундочку: а где Ваше имя, где обращение? Его нет? Значит, письмо не Вам.э
- ▶ Письма, которые требуют немедленно что-то сделать, — подозрительны. Фишинговые письма любят пугать. Например, так: «Внимание!!! Банк предупреждает, что на Ваше имя взят кредит, по процентам Вы задолжали уже 60 тысяч рублей. Перейдите по ссылке, чтобы прочитать подробности». «Объем почтового ящика заканчивается, пополните его сейчас же» «Вас только что пытались взломать, срочно меняйте пароль!»...



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

- ▶ Если Вы случайно перешли по странной ссылке из письма и открылось окно, предлагающее Вам ввести логин и пароль, — посмотрите на адресную строку. К примеру, Вы пользуетесь почтой Gmail. Если вместо привычного адреса mail.google.com Вы видите любую другую надпись, которая отличается хотя бы одной буквой (google.mail.com.ru, d-google.com), — это сайт-мошенник.

**7) Вы завели почтовый ящик на Gmail. С адреса suport@gmail.com вы получили письмо: «Уважаемый пользователь! Кто-то только что пытался войти в ваш аккаунт, используя ваш пароль. Мы заблокировали подозрительную попытку входа и настоятельно рекомендуем вам сменить пароль». Ниже видна синяя кнопка с надписью «Сменить пароль». Как поступите? Удалю письмо и пожалуюсь на спам. Это мошенники.**

Если это письмо от администрации почтового сервиса, от банка, от платежной системы — проверьте, с какого адреса оно пришло. Что не так с почтой suport@gmail.com?



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

Как пишется слово support, то есть «поддержка»? С двумя буквами "р". Настоящий адрес техподдержки — support@gmail.com. Если адрес кажется странным и Вы сомневаетесь, не мошенники ли это, — введите его в поисковик или загляните на официальный сайт почтового сервиса, банка, платежной системы, магазина. Там указан настоящий адрес.

### 8) Вы регистрируетесь в социальной сети. Какую реальную информацию о себе укажете на странице?

**Максимум имя и фамилия.** Но к чему такая секретность? Любая информация, которой Вы публично делитесь, **доступна всему миру.** И может быть использована как угодно.

Например, ребенок указал на своей странице, что ее зовут Катя, маму — Ольга Сергеевна, а любимую собаку — Рекс.

Выходит ребенок из школы после уроков, к нему подъезжает машина, из нее высовывается неизвестный парень и кричит: «Катя, с Рексом беда! Он еле живой! Ольга Сергеевна попросила, чтоб я тебя подвез. Быстрее, садись!»



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

Ребенок ужаснется и сядет в машину. Или нет? Может, задумается: «Стоп! Почему мама послала за мной незнакомца, а не позвонила? Где телефон? Сейчас все выясню».

Звонит маме. Та изумляется: О чем ты говоришь? Рекс жив и здоров, а я на работе. Незнакомца тем временем и след простыл.

### Обсудите с ребенком:

«Зачем он это сделал? Вряд ли с добрыми намерениями. Но как ему чуть не удалось обмануть эту девочку? Он просто зашел на страницу в соцсети. Увидел фотографию, нашел ссылку на страницу мамы, по номеру школы отыскал ее адрес, по дате рождения понял, в каком девочка классе, узнал, когда кончаются уроки, по записям на стене выяснил, как зовут собаку...»

Если Ваша дочь говорит: «Я не настолько глупая, чтобы попасться на такую очевидную удочку!», **скажите**: дело не в этом. Если ты публикуешь в соцсетях много личной информации – ты не удержишь всю ее в уме. Никому это не под силу. В неожиданной ситуации вроде «С Рексом беда, мама зовет, поехали!» ты не успеешь подумать «Что за...», как полетишь спасать Рекса.





## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

**Взрослые постоянно прокалываются на приватности.** Одни публикуют фотографии «Я танцую пьяный на столе» и анекдоты о преступниках, а потом удивляются, почему их не взяли работать в банк.

Другие выкладывают вид из окна квартиры, по которому ясно, где она находится. Потом пишут, что купили дорогой телевизор и кучу драгоценностей. Затем — что улетают в Турцию на две недели.

Ты уже понимаешь, к чему я? Верно: они серьезно рискуют вернуться домой и обнаружить вскрытую квартиру без телевизора и драгоценностей.

«Так что же теперь, — возмутится Ваш ребенок, — ничего о себе не рассказывать? Не делиться фотографиями, не называть имен? Что тогда можно? Молчать? Какая-то асоциальная сеть получается!».

**Скажите** ребенку:

«Ты сама (сам) решишь, что делать со страницей. Просто помни: все, чем ты публично делишься, доступно всему миру. Некоторые вещи лучше оставлять личными и не доверять социальным сетям и Интернету. И помни о правилах перманентного маркера и баннера».



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

9) Какой-то незнакомец несколько дней подряд пишет Вам в социальной сети гадости и обзывает Вас. Вы догадываетесь, что это Ваш знакомый. Кто именно — непонятно... Как поступите?

Не расстраивайтесь из-за анонимов, которые присылают гадости. Даже если подозреваете в них знакомых. Эти смельчаки ни за что бы не сказали гадости в лицо. Потому и пишут в соцсетях. Они трусы. Что делать с докучливым собеседником? **Черный список — наше все.** Забанить и забыть.

Чтобы не тревожили интернет-тролли, задаваки, приставалы и прочие малоприятные личности, установите удобные настройки приватности. Ограничьте круг людей, которые могут писать личные сообщения, только друзьями или друзьями друзей. Оставьте возможность писать на своей стене (в своей хронике) только себе. Закройте страницу.



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

**10) Человек, в которого Вы влюблены, живет за две тысячи километров от Вас. Он просит, чтобы Вы прислали ему свое интимное фото. Как поступите?**

### **Не отправлю!**

У Вас была любовь, и Вы высылали интимные фото. Представьте, что чувства прошли. А снимки-то остались. Если Вы поссорились – возможно, обиженный человек захочет отомстить. Будет шантажировать: «Пришли мне денег или больше таких фоток, и я не отправлю их твоей маме». Или выложит снимки в группу «Ужасные девушки нашего города». Или разошлет их Вашим друзьям. Это и до травли может довести.

Предположим, Вы полностью доверяете человеку и думаете, что он никогда не поделится с кем-то снимками. А если его страницу взломают? Он настолько же хорош в интернет-безопасности, как и Вы, или беспечно говорит: «Да у меня все под контролем»? Тогда он напоминает водителей, которые при попытке пассажира пристегнуть ремень безопасности возмущаются: «Ты что, не доверяешь мне? Я за рулем с рождения!». Даже если это правда — на дороге полно других автомобилей, и от лихачей и пьяных никто не застрахован.



## ПРАВИЛЬНЫЕ ОТВЕТЫ. ЗАКРЕПЛЯЕМ МАТЕРИАЛ

В интернет-отношениях есть еще одна опасность. И дело не только в фото. Если Вы ни разу не видели этого человека, не говорили с ним по видеосвязи — Вы не можете быть полностью уверены, что переписываетесь со сверстником, а не с дядечкой пятидесяти лет или девочкой двенадцати лет, которым захотелось поразвлечься. Убедитесь, что собеседник — действительно тот, за кого себя выдает, чтобы ненароком не влюбиться в персонажа, которого кто-то выдумал для развлечения.

## ЗАДАЙТЕ ДЕТЯМ НЕСКОЛЬКО ВОПРОСОВ

На этот раз постарайтесь найти правильные ответы самостоятельно вместе с ребенком. Я приведу краткие ответы, чтоб Вам было легче искать и размышлять.

?

Ты хочешь рассказать подруге (другу) секрет, и тебя просто распирает от нетерпения. Как поступишь: напишешь ей (ему) в соцсети, в мессенджере, позвонишь или поговоришь лично? Почему?

!

Только лично. Иначе этот секрет могут увидеть другие.

?

Можно ли давать кому-нибудь пароль от своего аккаунта? Почему?

!

Пароль никому не даем! Пароль, который узнал хотя бы 1 человек, Вам больше не принадлежит. Даже знакомый может использовать твои фото, видео, записи, контакты и личную информацию.

?

Можно ли сохранять пароли в браузере? Почему?

!

В браузере нежелательно. Лучше в специальных приложениях или хранилище антивирусной программы. Иначе вирус может похитить пароли из браузера.

?

Как ты определишь, добавлять ли человека в друзья в соцсети или лучше не стоит?

!

Добавлять в друзья можно только тех, кого знаешь лично.

?

Как проверить, настоящая ли фотография у человека на аватарке, или он позаимствовал ее у другого пользователя?

!

С помощью приложения FindClone или через поиск по фото в Google и Yandex.

?

Что ты посоветуешь подруге (другу), которая отправила интернет-знакомому свою интимную фотографию и столкнулась с шантажом и вымогательством денег?

!

Сделать скрины переписки и срочно обратиться к родителям.

?

Если злоумышленник украдет твой смартфон или планшет, какую важную информацию он получит? Какой ущерб вор может тебе нанести? Как обезопаситься от этого прямо сейчас?

!

Он получит ответ ко всей моей жизни...

Надо настроить отпечаток пальца, Face ID и пароль на экране блокировки, а не графический ключ.

## ТРАВЛЯ В СЕТИ (КИБЕРБУЛЛИНГ)

**Кибербуллинг** — это насилие в цифровом пространстве.

- Когда в интернете травят, то делают следующие вещи:
- Оскорбляют в открытых комментариях
- Ведут поддельные страницы в соцсетях от имени жертвы
- Размещают фото, личную информацию, чтобы шантажировать или издеваться над жертвой
- Угрожают
- Преследуют
- Исключают из разных сообществ и чатов.

Каждый второй подросток (учащийся 7-11 классов) становился жертвой травли в Интернете (кибербуллинга). До 72% школьников в той или иной форме являются участниками кибербуллинга. Основная площадка для травли — **соцсети**.

Родителям трудно поверить, но признать проблему — первый шаг к её решению.



## ТРАВЛЯ В СЕТИ

.....

60% пользователей рунета,  
сталкиваясь с агрессией  
в адрес других людей,  
занимают  
наблюдательную позицию

.....



**13%**

Боятся, что агрессия перекинется на них

В том числе по этой причине наблюдатели не вступаются за жертву

**65%**

Считают поддержку жертвы бессмысленной

Большая часть пользователей считает, что их публичная поддержка ни на что не повлияет

**20%**

Чувствуют бессилие при виде травли

Агрессия в сети влияет и на наблюдателя тоже

## ПОПЫТКА ЗАЩИТИТЬ ЖЕРТВУ МОЖЕТ ОБОБРАТИТЬСЯ ТРАВЛЕЙ

Пользователи рунета замечают, что в стремлении защитить жертву наблюдатель может превратиться в агрессора. Поддержка путём унижения другой стороны иногда оборачивается травлей.

«Когда ругают за дело, это не травля, но повод для травли. Я наблюдаю такое постоянно. Это не значит, что нельзя высказываться. Но когда хочешь кого-то обвинить, ты должен в десять раз все взвесить».



«Я считаю, что если человек не призывает людей к дальнейшим действиям, то это не буллинг. Дальше – это уже не моя сфера ответственности, а их».



«Если человек подготовлен, у него есть аргументы, это не буллинг. Но в комментариях он может начаться. Я видела кейсы, когда про человека писали, например, «Он меня обокрал». И после этого этому человеку на стене пишут «Сдохни». Пост был не буллингом, а призывом к справедливости. Но дальше уже начался буллинг».



## ВЫ СТАЛИ СВИДЕТЕЛЕМ КИБЕРБУЛЛИНГА



Да

Зацепила ли вас  
эта ситуация?

Нет

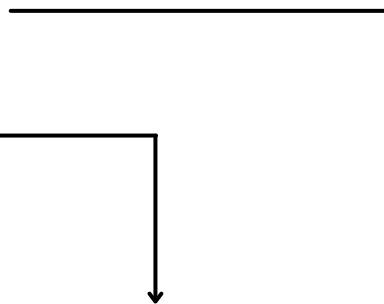


Оцените свое состояние:  
можете ли вы выдержать  
агрессию буллера, если она  
перейдет на вас? В  
стабильном ли состоянии  
вы находитесь? Есть ли у вас  
внутренние точки опоры?

Вы имеете полное право  
никак не реагировать на  
происходящее и не  
испытывать по этому  
поводу никаких чувств

Да

Нет



Вы можете написать в  
комментариях и  
переключить внимание  
буллера на него  
самого. Сохраняйте  
нейтральность и  
помните: агрессия  
может быть  
перенаправлена  
на вас

Вы можете написать  
в личные  
сообщения  
буллеру, но будьте  
готовы к тому, что  
агрессия может  
быть  
перенаправлена на  
вас

Вы можете  
написать  
пострадавшему  
в личку со  
словами  
поддержки

Вы можете  
написать в  
поддержку  
социальной  
сети, в которой  
происходит  
буллинг,  
приложив  
скриншоты

Вы можете  
оставить  
нейтральный  
поддерживаю  
щий  
комментарий  
тому, кого  
травят

## ЧТО ДЕЛАТЬ, ЕСЛИ ВАШ РЕБЕНОК ПОДВЕРГСЯ ТРАВЛЕ В СЕТИ

1. Отнеситесь к ребенку серьезно.
2. Не игнорируйте его проблемы и переживания словами «Не обращай внимание на этих троллей!»
3. Сразу включайтесь — не ждите пока разберутся сами, тем более, что за никами агрессоров в сети могут скрываться взрослые люди.
4. Успокойте и поддержите ребенка: «Хорошо, что ты мне сказал. Ты правильно сделал. Ты в этом не виноват. Ты не один попал в такую ситуацию».
5. Задавайте правильные вопросы, отвечайте на вопросы и постарайтесь помочь преодолеть тревоги.
6. Не провоцируйте агрессию словами: «Ты что им ответить не мог?!»
7. Придумайте и проиграйте несколько работающих сценариев при травле в сети, отработайте помещение в черный список, блокировку и бан.
8. Расскажите ребенку про юридическую ответственность за травлю.
9. Устройте себе и ребенку цифровой детокс на несколько дней.
10. Обратитесь с жалобой в администрацию соцсети, правоохранительные органы.

**Но часто дети не рассказывают про свою проблему.  
Как распознать травлю?**

## МАРКЕРЫ КИБЕРБУЛЛИНГА. ПО КАКИМ ПРИЗНАКАМ МОЖНО ПОНЯТЬ, ЧТО ВАШ РЕБЕНОК ПОДВЕРГАЕТСЯ ТРАВЛЕ В СЕТИ?

Кибербуллинг часто является продолжением травли в жизни (в школе, во дворе, в сообществах по интересу). И наоборот, нередко конфликты в интернете переходят реальность.

Это очень важная тема, поэтому я выйду за рамки сети. Расскажу признаки и травли, и кибербуллинга.

### Как понять, что Ваш ребенок подвергся травле?

- ▶ Давно не был «онлайн» во Вконтакте, не хочет ходить в школу, подключаться к занятиям в Zoom или гулять во дворе, хотя раньше делал это с удовольствием.
- ▶ Перестает отвечать на уроках, получает плохие оценки, хотя всегда учился хорошо.
- ▶ Симмулирует болезни, чтобы не идти в школу, не выходить в Zoom или гулять: голова болит, живот скрутило и др.
- ▶ Чаше «портит» или «теряет» свои вещи: обувь, одежду, рюкзак, учебники, игрушки, гаджеты, деньги. Начинает просить больше денег, но нового ничего не появляется. Приходит из школы голодным. Странно объясняет потребность в них.

## МАРКЕРЫ КИБЕРБУЛЛИНГА. ПО КАКИМ ПРИЗНАКАМ МОЖНО ПОНЯТЬ, ЧТО ВАШ РЕБЕНОК ПОДВЕРГАЕТСЯ ТРАВЛЕ В СЕТИ?

### Как понять, что Ваш ребенок подвергся травле?

- ▶ Отказывается от любимых занятий, которым раньше уделял часы и дни: резко перестает сидеть в телефоне и планшете, собирать Лего, играть на гитаре, читать, тренироваться, рисовать и др.
- ▶ Плохо спит.
- ▶ Сокращает общения с друзьями и родными, со сверстниками в сети. Не хочет ни с кем разговаривать, особенно про школу или отношения со сверстниками.
- ▶ Часто злится и тревожится перед новым днем, даже если это выходной.
- ▶ Чаще получает синяки и ссадины, происхождение которых объясняет неохотно или невнятно.
- ▶ Меняет пищевое поведение, плохо и нерегулярно ест.

## МАРКЕРЫ КИБЕРБУЛЛИНГА. ПО КАКИМ ПРИЗНАКАМ МОЖНО ПОНЯТЬ, ЧТО ВАШ РЕБЕНОК ПОДВЕРГАЕТСЯ ТРАВЛЕ В СЕТИ?

Приведенные маркеры очень похожи на общие изменения в поведении подростка с 12 до 17 лет, но в отличие от подростковых изменений при буллинге приведенные признаки появляются **стремительно**.

Важно заметить в эти 2-3 дня и далее, что практически все не как обычно.

Но не спрашивайте: «Что случилось?», «Тебя обижают?», «Ты что, наркоманишь?» и прочие бесполезные вопросы, на которые можно ответить: «Ничего», «Нет», «Нормально», «Мам, пап вы что?!».

Расскажите историю из своего детства, когда Вы также переживали и менялись, как он(она) сейчас, поделитесь секретом. И по правилу социального обмена Вы получите историю в ответ.



## КАК ПОСТУПАТЬ ПРИ КИБЕРБУЛЛИНГЕ РЕБЕНКУ?

### Расскажите это ребенку:

- Сделай скриншот всех оскорбительных сообщений. Не удаляй их. Они нужны, чтобы наказать обидчика.
- Не отвечай кибербуллеру. Единственная его цель — обидеть тебя и увидеть, как ты переживаешь. Как бы ни было страшно, неприятно, обидно, не отвечай!
- Заблокируй кибербуллера. Он может создать новую страницу и писать с другого аккаунта. Заблокируй каждую его страницу. Подумай, нормальный человек тратил бы время на то, чтобы создавать несколько страниц ради оскорблений другого?
- Измени настройки в аккаунте. Сделай так, чтоб тебе могли писать только друзья.

## КАК ПОСТУПАТЬ ПРИ КИБЕРБУЛЛИНГЕ РЕБЕНКУ?

### Расскажите это ребенку:

- Если ты знаком с обидчиком в реальной жизни, при встрече или по телефону скажи, чтоб он это прекратил. Обидчик может думать, что ты побоишься или постесняешься говорить об этом за пределами сети. Если боишься, постарайся набраться сил и через страх сделать это.
- Обратись к учителю, директору школы, тренеру, в полицию.
- Удали из друзей всех, кого ты не знаешь в реальной жизни и кто тебя недавно обижал.
- Напиши администраторам/модераторам соцсети/ группы, что тебе пишут оскорбления и угрозы. Они должны предотвращать такие случаи.
- Поделись со мной своей проблемой. Во-первых, одному справиться крайне тяжело. Во-вторых, я могу помочь решить твою проблему.

## КАК ОБРАТИТЬСЯ С ЖАЛОБОЙ?

1.Соберите доказательства оскорблений. Сделайте скриншоты, видео и аудиозаписи сообщений, информации, которую распространяют о Вас.

2.Сделайте скриншоты групп, в которых состоит кибербуллер. Как общается в открытом доступе.

3.Подайте жалобу администрации соцсети с приложением всех скринов.

4.Если кибербуллер знаком в реальной жизни, пишите родителям с предоставлением всех скринов. У обидчика могут быть адекватные родители, которые даже представить не могли, что их ребенок делает ужасные вещи.

## КАК ОБРАТИТЬСЯ С ЖАЛОБОЙ?

5.Если эти действия не помогают, отправляйте жалобу в комиссию по делам несовершеннолетних управы/администрации района или инспектору по делам несовершеннолетних.

6.Если нет результата, пишите жалобы о бездействии представителей госучреждений в Департамент образования, в прокуратуру, уполномоченному по правам человека в городе.

7.Если это не помогло или кибербуллер не знаком, подавайте в суд. Прикрепите все чеки о расходах: на юриста, на психолога, на занятия с тренером по безопасности.

### **Знайте!**

**Ответственность за травлю в сети предусмотрена законом.**

## ОТВЕТСТВЕННОСТЬ ЗА ТРАВЛЮ В СЕТИ

**Вы и ребенок должны знать, что наказание предусмотрено строгое!**

- **Сплетни про жертву и клевета**
  - ст. 152 ГК РФ
  - ст. 152.2 ГК РФ
  - ст. 128.1 УК РФ
- **Фотожабы**
  - ст. 152.1 ГК РФ
- **Оскорбления**
  - ст. 5.61 КоАП РФ
- **Угроза убийством**
  - ст. 119 УК РФ
- **Описание способов самоубийств**
  - ч. 3 ст. 110.1 УК РФ
- **Религиозные шутки**
  - ст. 148 УК РФ
- **Издевательства на национальной почве**
  - ст. 282 УК РФ
  - ст. 20.3.1 КоАП РФ

## СПАСИБО ЗА ВНИМАТЕЛЬНОЕ ИЗУЧЕНИЕ ГАЙДА!

### Теперь Вы знаете:

---


- что такое интернет и зачем нужен родительский контроль
- как регулировать экранное время без ссор
- как безопасно вести социальные сети
- что делать если Вас или ваших детей травят в сети
- как безопасно играть в онлайн игры и совершать покупки в сети

Рад, что теперь у вас есть инструменты онлайн безопасности. Держите гайд под рукой и обращайтесь к нему каждый раз, когда будете волноваться за себя и ребенка в сети. Станет намного легче.

## ПОЛЕЗНЫЕ МАТЕРИАЛЫ И ПРИЛОЖЕНИЯ


### КНИГИ

---

- "На цифровой игле" Андерс Хансен
  - «Гаджетомания: как не потерять ребенка в виртуальном мире» Элизабет Килби
- 

### МУЛЬТФИЛЬМЫ

---

- Полезные мультфильмы по онлайн безопасности 0+
  - Полезные мультфильмы для подростков про безопасность в играх
- 

## ПРОГРАММЫ ДЕТСКОГО/РОДИТЕЛЬСКОГО КОНТРОЛЯ

Мы проанализировали родительский контроль для iOS и Android по следующим критериям:

- Защита настроек родительского контроля паролем
- Соккрытие браузера и приложений
- Запрет на установку и удаление приложений
- Запрет на совершение встроенных покупок и запрос на разрешение покупок
- Фильтрация контента онлайн-магазинов по возрастному цензу
- Фильтрация веб-сайтов по принципу «разрешено/запрещено все, кроме»
- Ограничение на громкость воспроизводимой музыки



## ПРОГРАММЫ ДЕТСКОГО/РОДИТЕЛЬСКОГО КОНТРОЛЯ

- Ограничение на использование мобильных данных
- Ограничение по времени использования устройства и блокировка устройства в определенный временной интервал, а также возможность удаленной блокировки
- Отслеживание местоположения ребенка
- Кнопка паники (в случае чрезвычайной ситуации позволяет ребенку нажать на тревожную кнопку, и информация об этом будет срочно отправлена на родительское устройство вместе с координатами ребенка)
- Мониторинг истории звонков, SMS-трекер
- Статистика использования устройства

**Считаем лучшими:**

**Для Android: Kaspersky SafeKids, Kidslox**

**Для iOS: Kaspersky SafeKids, Kidslox и встроенный родительский контроль iOS**



## Школа безопасности Сергея Киселева

Обращайтесь с любыми вопросами

**ЗАПИСАТЬСЯ НА КОНСУЛЬТАЦИЮ**

**И помните, что мы с вами не просто  
учимся безопасности, мы ее создаем!**

Увидимся на нашем  
Телеграмм-канале

<https://t.me/safetyschool>