Детская кибербезопасность

Как уберечь своего ребенка в интернете?

Уважаемые педагоги и родители! Дорогие друзья!

Вы держите в руках брошюру, которая поможет уберечь Вашего ребенка от угроз в сети интернет. Эта проблема уже давно не виртуальна, а носит вполне реальный характер.

К сожалению, мы, взрослые, не всегда осознаем весь масштаб потенциальных вызовов в цифровом пространстве. Например, многие дети и подростки сталкиваются с кибертравлей – методичным и постоянным преследованием и унижением в сети, о которой родители могут даже не подозревать.

В сети неподготовленный юный пользователь может столкнуться с преступными группами, экстремизмом, финансовым мошенничеством, сексуальными домогательствами и другими опасностями. Брошюра ответит на вопросы о видах цифровых угроз, которые зачастую выходят за рамки сети. Вы узнаете, как различить преступные умыслы мошенников, что ими движет и какими уловками они попробуют обмануть ребенка.

Самое главное, что нужно понимать, – преступник попытается разорвать нить доверия между родителями и их детьми. Помните: тотальным запретом делу не помочь! Сделайте все возможное, чтобы сохранить Вашу связь с ребенком, – это поможет его защитить!

Уже несколько лет «Единая Россия» повышает цифровую осведомленность граждан. Также мы планомерно совершенствуем законодательство по защите детства. Теперь за преступления против половой неприкосновенности детей, которые, кстати, нередко зарождаются в сетевом общении с незнакомцами, – преступники могут получить пожизненное лишение свободы.

На ряду с этим партия сотрудничает с правительством Санкт-Петербурга в продвижении проекта «Защита будущего». Он помогает выявлять среди пользователей интернета подростков и молодежь, находящихся в кризисных состояниях, и оперативно передать сигнал об этом психологам, а в экстренных случаях – службе спасения.

В этой небольшой книге – опыт сотен людей, труд серьезных аналитиков, которые профессионально и давно занимаются вопросами детской кибербезопасности. Уверен, брошюра будет полезной и ответит на многие вопросы.

Сергей БОЯРСКИЙ,

первый заместитель председателя комитета Госдумы по информационной политике, информационным технологиям и связи, Секретарь Санкт-Петербургского регионального отделения «Единой России»

Оглавление

Деструктивное поведение и вредоносный контент

С развитием информационных технологий определить вредоносный контент иногда сложно даже взрослым. Существуют различные механизмы поэтапного внедрения в общество абсолютно любых убеждений посредством различных манипуляций. В соцсетях для этого используются «воронки вовлечения», которые вводят в норму ранее недопустимые для ребенка вещи.
В результате любой ребенок может стать жертвой в сети интернет.

Основные виды противоправных действий, совершаемых в цифровой среде в отношении несовершеннолетних

- Сексуальное домогательство
- Организация массовых расстрелов в школах (скулшуттинг)
- Вовлечение в опасные группы и движения (секты)
- Травля в интернете (кибербуллинг)
- Рассылка материалов, предназначенных для аудитории 18+
- Обман ребенка с помощью фишинга, чтобы получить его личные данные
- Вовлечение в употребление и продажу наркотиков
- Склонения к совершению самоубийства

Агрессия и травля в сети. Что такое кибербуллинг?

Кибербуллинг – это методичное и постоянное преследование и унижение человека в сети интернет

Важно помнить!

- Агрессия и травля в сети также опасны, как и их проявления в реальной жизни (в школе или на улице).
- Отсутствие возможности защититься у неподготовленного человека может привести не только к психологическим, но и к физическим травмам.
- Чрезмерная строгость без объяснений не помогут. Запрет общаться со сверстниками или отключение интернета могут заставить ребенка замкнуться в себе.

Ключевые характеристики кибербуллинга

Умышленность
Травля в сети не носит спонтанный характер. Она всегда умышленна.

Неравенство сил
Как правило, группа агрессоров более многочисленна, чем группа жертв.

Групповой процесс
В травлю всегда втягивается широкий круг участников.

Не заканчивается сама по себе
Зачастую травлю приходится прерывать извне. Внутри себя процесс непрерывен.

Регулярность
Человек, который подвергся травле, испытывает ее постоянно и регулярно.

Страдают все
Несмотря на разделение участников на агрессоров и жертву, от негативных психологических проявлений травли страдают все участники процесса.

Виды кибербуллинга

1. Исключение

Эта форма кибербуллинга аналогична бойкоту:
жертву намеренно исключают из отношений и коммуникации.

2. Домогательство

Постоянная и умышленная травля при помощи оскорбительных или угрожающих сообщений, отправленных Вашему ребенку лично или как части какой-либо группы.

3. Аутинг

Преднамеренная публикация личной информации ребенка с целью его унизить, при этом произведенная без его согласия.

4. Киберсталкинг

Преследование в сети, которое перерастает в реальную угрозу для безопасности и благополучия Вашего ребенка.
Этим термином могут называться попытки взрослых связаться с детьми, с целью личной встречи и дальнейшей сексуальной эксплуатации.

5. Фреипинг

Форма травли, в которой обидчик каким-либо образом получает контроль над учетной записью Вашего ребенка в социальных сетях и публикует нежелательный контент от его имени.

6. Диссинг

Передача или публикация порочащей информации о жертве онлайн.
Это делается с целью испортить репутацию жертвы или навредить ее отношениям с другими людьми.

7. Кетфишинг

Форма буллига, в которой киберхулиган с целью обмана воссоздает профили жертвы в социальных сетях на основе украденных фотографий и других личных данных.

Преступления против половой неприкосновенности детей

Преступления против половой неприкосновенности детей, зачастую начинаются в цифровом пространстве – с попыток незнакомого человека втереться в доверие к ребенку для дальнейшей сексуальной эксплуатации.

Преступники могут пытаться вывести ребенка на личную встречу, или получить от него интимные снимки и видео. Для получения такого материала злоумышленники прибегают к самым разным уловкам, чаще всего представляются сотрудниками модельных агентств.

Таким лжеагентам, к сожалению, готовы отправить «красивые фотографии» девочки самого нежного возраста – известны случаи, когда это делали девятилетние школьницы. Получив от ребенка такие снимки, злоумышленник начинает шантажировать его, угрожая отправить их родителям или в школу. Целью шантажа являются новые снимки и видео.

Как обезопасить ребенка от этой угрозы?

1. Объясните ребенку, что с незнакомцами нельзя говорить не только на улице, но и в сети.

2. Лучше заранее обсудить с ребенком возможные угрозы и опасности, которые влекут за собой встречи и онлайн-общение с незнакомцами, договориться о том, как он будет вести себя в той или иной ситуации.

3. Ребенок должен знать: никому нельзя отправлять свои фотографии, даже своим знакомым. Аккаунт друга может быть взломан и использован другим человеком. Сравнение с реальной жизнью в данной ситуации более чем уместно: ребенок должен понимать, что такие поступки сродни обнажению перед совершенно незнакомым человеком в реальной жизни.

4. Родители должны добавить своего ребенка в друзья во всех социальных сетях, где он общается, чтобы иметь возможность видеть, с кем он дружит.

5. Помните: чем раньше Вы установите эти правила для ребенка, тем лучше он их воспримет.

Основные отличия кибербуллинга от травли в реальной жизни

Анонимность
Агрессор чувствует себя безнаказанным, менее уязвимым и ответственным, может находиться далеко от жертвы (в другом регионе).

Не делает исключений
Жертвой травли в сети может стать любой человек вне зависимости от статуса в реальной жизни. Финансовое положение, уровень и качество образования не являются защитой от агрессоров.

Незаметность для взрослых
Кибербуллинг не оставляет физических следов, но оседает глубоко внутри человека. Его проявления нелегко распознать. Часто без инициативы ребенка травля в интернете остается незамеченной.

Психологический страх
В большинстве случаев жертва скрывает от посторонних факт травли в интернете.

Нельзя справится в одиночку
Кибербуллингу невозможно противостоять в одиночку.

Основные темы, с которых начинается травля в сети

- Хобби и увлечения
- Религиозные убеждения
- Внешность
- Особенности характера
- Материальное положение

Часто основная причина травли заключается в отличиях жертвы от агрессоров. Это может быть внешность, уникальные увлечения (хобби и секции), религиозная принадлежность.

Нередко причиной для травли могут стать особенности характера – вспыльчивость, реакция ребенка на провокацию. Главная задача агрессора – заставить жертву проявлять неконтролируемые эмоции.

Почему агрессор начинает травлю?

- Показывает свою силу и превосходство
- Выплескивает накопившийся негатив
- Добивается своей цели, получив деньги
- Причиняет реальный вред другому
- Выражает свое отношение
- Просто развлекается

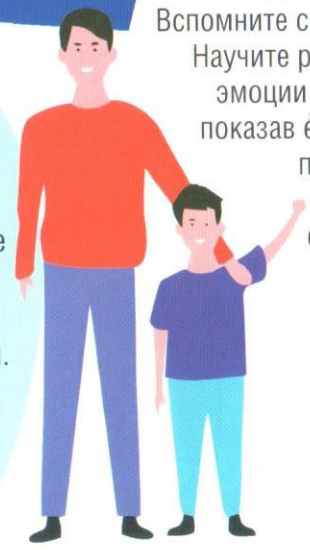
Часто агрессор сам является жертвой травли со стороны более сильного. Иногда это проявляется в семье.

Часто травля носит вполне корыстный характер. Агрессор хочет что-то получить от жертвы (деньги, цифровую материальную ценность).

Травля зачастую возникает из мелкой шутки. Для отдельных людей травля – распространенный вид развлечений.

Как предотвратить травлю?

Наблюдайте, но не контролируйте!
Дайте ребенку ощущение свободы, безопасности и комфорта. Не злитесь на него и не ограничивайте его общение со сверстниками. Задавайте вопросы, интересуйтесь увлечениями и пользуйтесь интернетом вместе с ним. Если это возможно, играйте в игры, которые ему нравятся, станьте его другом в интернете. Так Вы сможете вовремя распознать угрозы.



Главное правило – станьте другом своему ребенку!
Вспомните свою молодость. Научите ребенка держать эмоции под контролем, показав ему правильный пример. Если Вы станете другом своему ребенку, он станет чаще советоваться с Вами, и это поможет ему справиться с агрессией в интернете.

Что делать, если ребенок столкнулся с травлей или с преследованием в сети?

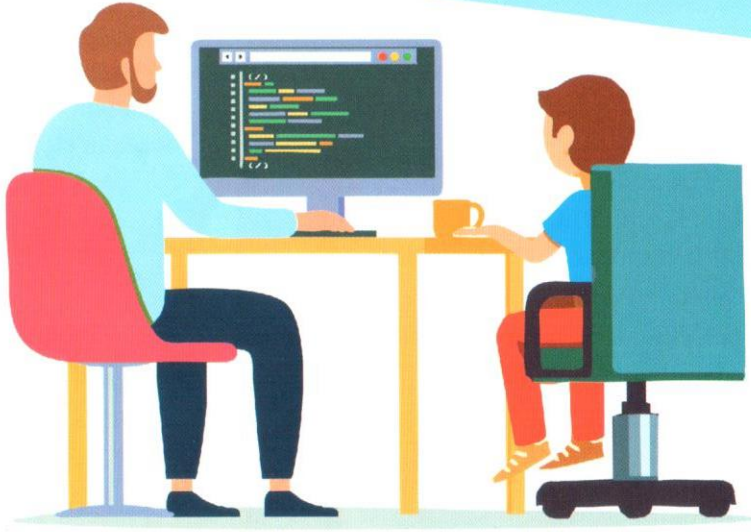
Обязательно сообщите в правоохранительные органы, в первую очередь – в следственный комитет!
Не проходите мимо и не откладывайте на потом!
Если Вы видите, что ситуация зашла далеко, аккуратно подведите ребенка к нужному разговору:

«Может быть тебе нужна моя помощь?»

- Помогите заблокировать обидчика
- Обеспечьте настройки приватности страницы
- Помогите сделать скриншоты
- Помогите написать в службу поддержки

Помните главное правило:

Ваш ребенок должен держать себя в руках: если жертва проявит эмоции, её затянут в воронку травли и будут подливать «масло в огонь».

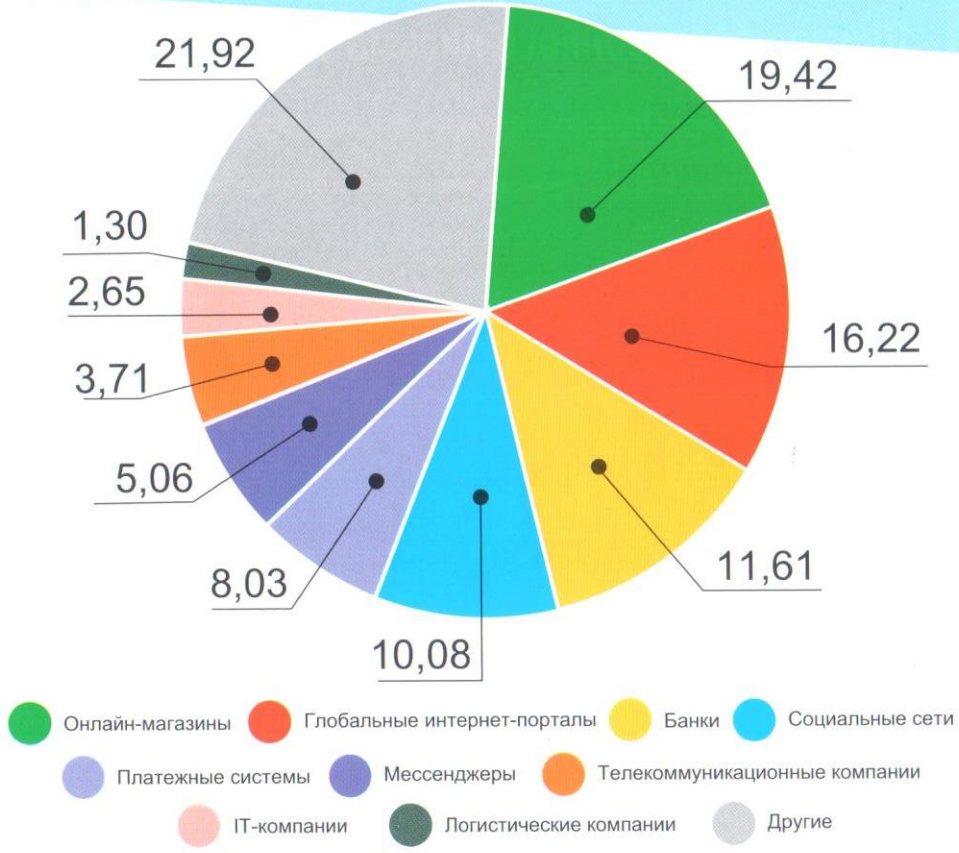


Финансовое мошенничество в сети – реальность

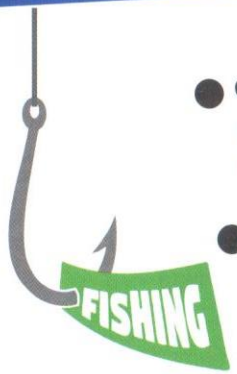
В 2021 году преступники похитили у клиентов российских банков 13,5 млрд руб.

Больше всего мошеннических операций было произведено при совершении покупок в интернете (фишинг).

Все чаще мошенники интересуются электронными счетами детей и подростков. С каждым годом количество несовершеннолетних владельцев электронных счетов растет. У детей появляются свои банковские карты, они расплачиваются с помощью смартфонов, осуществляют покупки в интернет-магазинах.



Виды фишинга



- **Фишинг через поисковые системы – создание копии оригинального сайта с целью получить Ваши личные данные (логины и пароли).**
- **Фишинг через электронную почту – спам-рассылка писем на электронную почту жертв с вредоносной ссылкой.**
- **Смишинг – фишинговая атака с использованием СМС, а также фишинг в мессенджерах. В сообщении присутствует ссылка на вредоносный сайт.**

Пример электронного письма от мошенников

Письмо-уловка (фишинг)

У Вас не погашен кредит

Заголовок письма вызывает тревогу, побуждает к немедленному действию

От кого: **Aleksey** <Aleksey@e04ech.asia>
Кому:
Сегодня, 7.30

Странный адрес для коллекторского агентства

СУПЕРБАНК

СУПЕРБАНК РОССИИ

Текст письма тоже побуждает к рефлекторным действиям – немедленно открыть файлы

Уважаемый (-ая) Иванов Иван Иванович,
меня зовут Арсенов Алексей Дмитриевич, я представитель коллекторской группы Супербанка России.
На ваше имя 17.08.2021 был оформлен потребительский кредит через наш онлайн банкинг на сумму 427 998 рублей.
На данный момент задолженность не погашена. На 17.08.2022 ваш долг составляет 663 773 рублей с учетом пени (0,5% в сутки).
В связи с этим, на ваше имя Супербанком России был составлен судебный иск.

Ознакомьтесь с документами:

Договор займа.zip
Судебный иск.zip

Письмо содержит какие-то документы, которые надо открыть

С уважением,
Супербанк России

Подпись, как правило, не содержит контактных данных

Меры предосторожности

- Обращайте внимание на предупреждения от Ваших поисковых систем (Google, Yandex и др.)
- Сообщайте своему банку о факте возможного мошенничества и перепроверяйте любую информацию напрямую
- Не вводите свой пароль на страницах, открывшихся по ссылкам из писем
- Будьте осторожны со «срочными запросами» и подозрительно выгодными предложениями магазинов
- Не спешите!

Не бойтесь попросить о помощи!

Опасные онлайн-игры (не путать с развлекательными играми)

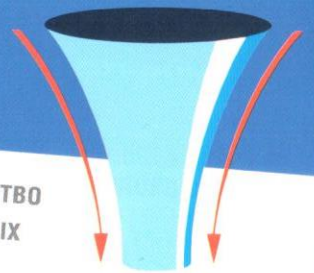
Помните! Дети и подростки играют во множество компьютерных игр. Большинство из них не несут никаких негативных последствий для ребенка. Даже если в игре присутствуют элементы насилия и другие деструктивные проявления, зачастую Вы можете оградить от них своего ребенка просто внимательно ознакомившись с рейтингом, указанным на игре. Правильно выставляйте возрастные настройки в игровых приложениях. Это автоматически исключит возможность покупки игры с неподходящим возрастным рейтингом.

8+ 14+ 12+

Играйте вместе с ребенком или наблюдайте за его игрой

Вы сможете понять, является ли игра вредоносной, просто ознакомившись с ее сюжетом и правилами.

Как ребенка втягивают в опасные онлайн-игры



Воронка вовлечения – это поэтапное внедрение в общество абсолютно любых убеждений посредством определенных манипуляций. На каждом этапе этой воронки ранее недопустимые для ребенка вещи начинают казаться ему допустимыми.

Как это происходит в жизни?

Например, подросток просматривает новостную ленту юмористического паблика, где каждый третий-четвертый пост публикуется не с простым юмором, а с юмором, пропагандирующим какое-то деструктивное направление.

Поначалу подросток может не принимать деструктивный юмор. Но, из-за множества лайков к картинкам и одобрения такого «юмора» в комментариях, он неизбежно со временем примет эти идеи как норму. Дальше ребенок попадает в одну или несколько деструктивных групп.

Общедоступные группы

Начинается все с массовых групп широкого охвата, которые не имеют каких-то определенных тем или направлений. Как правило, это юмористические паблики или околошкольные группы со специфическим юмором.

1. Эти сообщества знакомят несовершеннолетнего сразу со всеми видами деструктивных направлений
2. Пропаганда наркотиков, суицида или школьных расстрелов всегда подается с юмором
3. Со временем несовершеннолетний начинает интересоваться чем-то определенным, подписывается на узкотематические группы

Закрытые группы

Как только ребенок проникнется деструктивными идеями, кураторы групп его заметят и пригласят в закрытые сообщества «для своих», где некоторое время будут наблюдать за ним. Потом кураторы перейдут с подростком на личное общение, дадут ему ложное чувство важности и избранности. Далее ребенка начнут использовать уже в реальных действиях в офлайне.

КРАШ-ФЕТИШ
Удовольствие от убийства мелких и средних животных

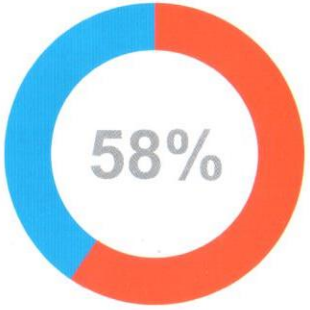
ФУРРИ
Люди, испытывающие нездоровое влечение к антропоморфным животным

ГРУППЫ СМЕРТИ
Планомерное доведение до самоубийства

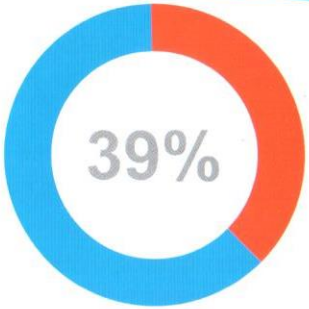
АУЕ
Пропаганда насилия, романтизация криминала

Накрученный таким контентом ребенок, запутавшись в том, кто же он есть, попадает в депрессивные группы, а оттуда – в суицидальные

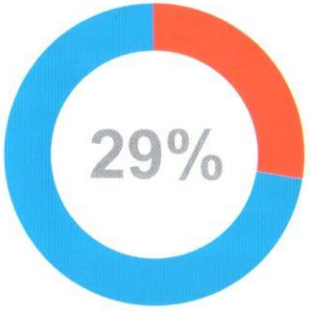
Распространенные ошибки, которые подростки совершают в интернете



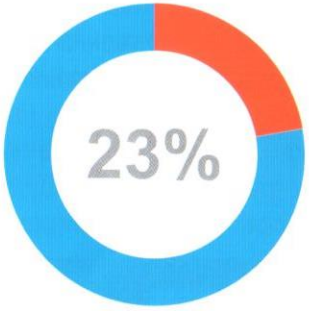
Указывают свой домашний адрес и мобильный телефон



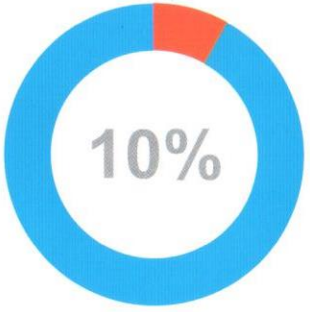
Указывают номер школы



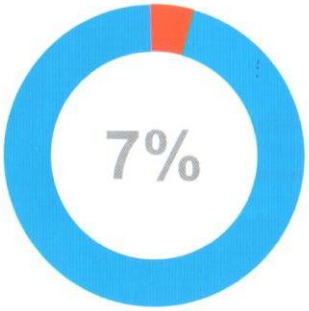
Выкладывают фото, на которых видна обстановка в квартире



Размещают информацию о родителях и родственниках



Указывают на странице свой реальный возраст

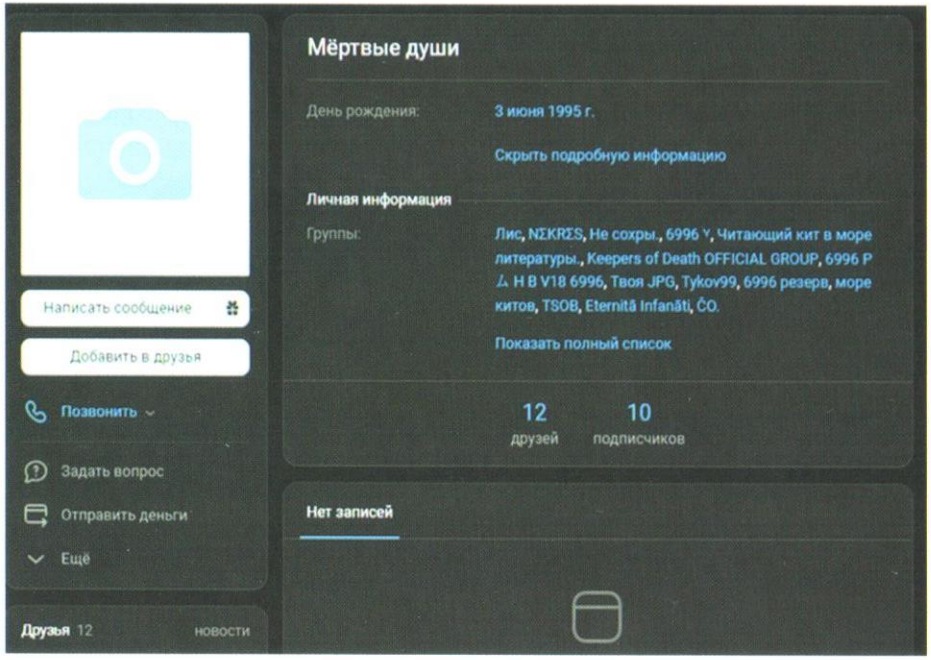


Публикуют свою геолокацию

Каждая из этих ошибок может послужить причиной для проявления противоправных действий в сети

Как определить подозрительных друзей в социальных сетях?

- Отсутствие фото в профиле и на аватаре, все изображения на странице либо абстрактны, либо содержат странные образы или символы.
- Страницы друзей – депрессивные, агрессивные или пошлые. Имеют нецензурные статусы. В ленте и на «стене» присутствуют мемы в большом количестве.
- Огромное количество друзей (если это не блогер) или, наоборот, небольшое их количество без фото.
- Отсутствие личных фотографий: семьи, родителей, знакомых и вообще какой-либо хроники жизни.
- Они подписаны на большое количество групп с опасным, странным и сомнительным названием, где явно предлагают что-то негативное.
- На странице присутствует большое количество нецензурной лексики, агрессивных высказываний и постов, а также радикальные призывы.
- Размещают изображения сатанистских символов и знаков – кресты, «звезды», а также знак с использованием слов «оно» и «ад»; названия, включающие слово «суицид» (англ. «suicide»), в том числе написанные с ошибками («suecid», «suicid» и т.д.), а также названия с использованием иероглифов, иврита, арабской вязи, санскрита, экзотических шрифтов (примеры: «УЖСГЗХ», «3RR0R») и т.п.



Как понять, что Ваш ребенок столкнулся с опасной онлайн-игрой?

Не высыпается, даже если рано ложится спать

Систематический недосып – один из способов введения человека в состояние эмоциональной нестабильности. Отсутствие сна приводит к подавлению защиты ребенка.

Регулярно смотрит «страшные» видеоролики

Просмотр страшных роликов приводит к снижению чувствительности к неприятным действиям и образам, что, в свою очередь, снимает барьеры восприятия.

Совершает символичные действия

Стоит на краю крыши, сидит на карнизе, высовывается в окно. Данные действия могут быть заданиями от «кураторов», призванными манипулировать смыслами и тренировать подчинение ребенка воле кураторов.

Немотивированные травмы, порезы, ушибы

Ушибы и порезы можно получить на улице или в спортивной секции. Но, если они появляются у ребенка регулярно и причина их появления не ясна, необходимо вмешаться.

Часто слушает присланную музыку

Ребенок регулярно слушает в наушниках присланную музыку и раздражается, если ему запрещают это делать.

Рисует страшные, непонятные символы

Рисует плывущих вверх китов, бабочек, единорогов, неправильные религиозные символы. Спросите ребенка незаискивающим тоном, что это означает, и внимательно выслушайте ответ.

Каждый из этих примеров в отдельности может быть безобиден. Некоторые из них – элементы естественного поведения подростка. Но, если Вы замечаете проявления в поведении ребенка, которые описаны в нескольких пунктах или сразу во всех, обратите на это пристальное внимание. Установите с ребенком позитивный контакт.

Что делать, если ребенка втянули в опасную онлайн-игру?

Если Вы заметили, что ребенок встает в нестандартное время, часто врет, замыкается в себе, на его теле появились порезы, изменились его поведенческие реакции, наблюдается заторможенность и смена интересов...

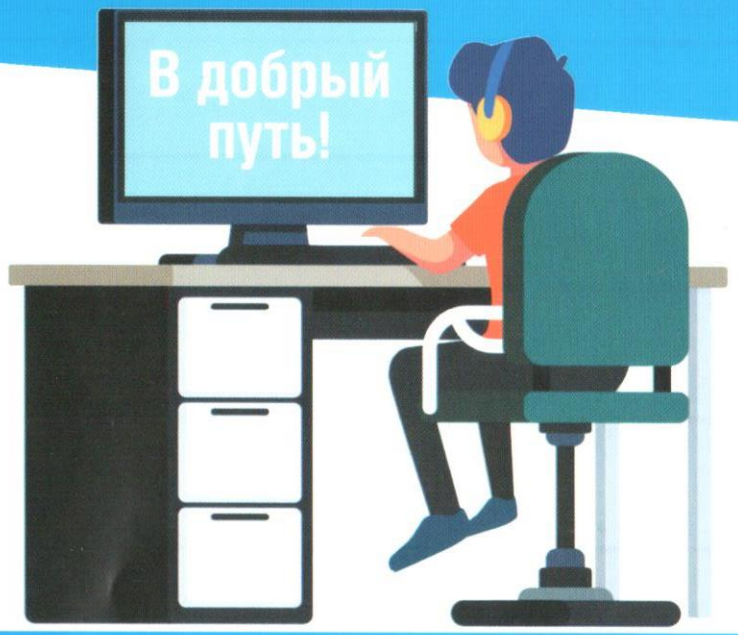
Полностью ограничьте его доступ к интернету! Отключите компьютер и заберите смартфон.

Восстановите его привычный распорядок дня.
Помогите ребенку вернуться в устойчивое эмоциональное состояние. Ребенок должен высыпаться, хорошо питаться и понять, что его окружают близкие, любящие люди.
Все время проводите с ребенком, говорите с ним, задавайте вопросы, узнайте, с кем он общается.

Немедленно обратитесь за помощью к специалистам. Позвоните в службу доверия:

+7 (800) 200-01-22

Общие рекомендации



1. Расскажите ребенку об основах кибербезопасности. Ваше внимание – главный метод его защиты!
2. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, с кем он дружит в интернете так же, как интересуетесь его реальными друзьями.

3. Если Ваш ребенок имеет аккаунты в соцсетях, внимательно изучите, какую информацию размещают его участники в своих профилях.
4. Приучите детей никогда не выдавать личную информацию по электронной почте, в чатах и мессенджерах.
5. Настаивайте, чтобы дети никогда не соглашались на личные встречи с теми, с кем познакомились в интернете.

Полезные телефоны и контакты

Общественная приемная «Единой России» в Санкт-Петербурге:

+7 (812) 571-97-38

Группа правовой помощи гражданам в цифровой среде:

+7 (812) 318-24-62

Анонимные телефоны доверия в Санкт-Петербурге:

+7 (800) 200-01-22 — телефон доверия для детей и родителей

004 — телефон Городского мониторингового центра (помощь для взрослых и детей)

+7 (812) 635-55-77 — горячая линия Комитета по здравоохранению Санкт-Петербурга

+7 (812) 344-08-06 — телефон доверия экстренной психологической помощи семьям в трудных жизненных ситуациях

+7 (812) 576-10-10 — кризисная психологическая помощь для детей и подростков