10 СОВЕТОВ ДЛЯ ДЕТЕЙ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

СКОЛЬКО ВРЕМЕНИ СТОИТ ПРОВОДИТЬ В ИНТЕРНЕТЕ?

1. **Для развлечения и общения с настоящими друзьями Интернет не нужен, нужна реальная жизнь**. Сокращай время пользования Интернетом! Отводи для общения в виртуальном мире не более 1 часа в день. Не позволяй социальным сетям отбирать у тебя здоровье и перспективы!

2. **Анонимность в сети - миф. Всё, что мы выкладываем в Интернете, остаётся там навсегда.**

3. **Проводи больше времени в реальной жизни:** общайся с друзьями, родителями, найди себе действительно интересное увлечение, читай, занимайся спортом, придумывай и реализуй полезные социальные проекты, помогай людям, включайся в общественную деятельность, смелее используй свои таланты.

4. **Будь бдителен! В Интернете много мошенников, которые охотятся за твоими деньгами и данными.** Есть и такие преступники, целью которых является испортить как можно больше детей или загубить их жизнь. Некоторые делают это за большие деньги, продавая снимаемые детьми видео и фотографии, а некоторые потому, что психически больны. Однако понять это, общаясь в Интернете, невозможно. Просто не подпускай к себе незнакомых людей и не позволяй им сделать из тебя свою жертву.

5. **Не выкладывай свои персональные данные в Интернет!** Помни, что отправлять их не стоит даже друзьям.

6. **Закрой свои страницы в соцсетях от посторонних!** Будь осторожен с незнакомцами в Интернете, а если кто-то из них задает тебе странные вопросы, навязывает общение или ведет себя агрессивно – блокируй такого человека и не продолжай общение.

7. **Не бойся рассказать родителям о своих проблемах!** Если кто-то решит тебя обижать, травить, угрожать тебе, даже если ты попадешься на удочку мошенников, родители смогут помочь тебе и подскажут, как надо поступить.

8. **Помни, что из Интернета ничего не удаляется!** Если ты не хочешь, чтобы какие-то твои фото или посты увидели все друзья и знакомые – лучше вообще их не выкладывай.

9. **Не верь всему, что написано в Интернете!** В сети много вранья, многие заголовки пишутся просто для того, чтобы привлечь внимание. Если есть сомнения по поводу новости – лучше проверь, скорее всего это фейк.

10. **Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни.** Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

НЕ СЛЕДУЙ МОДЕ!

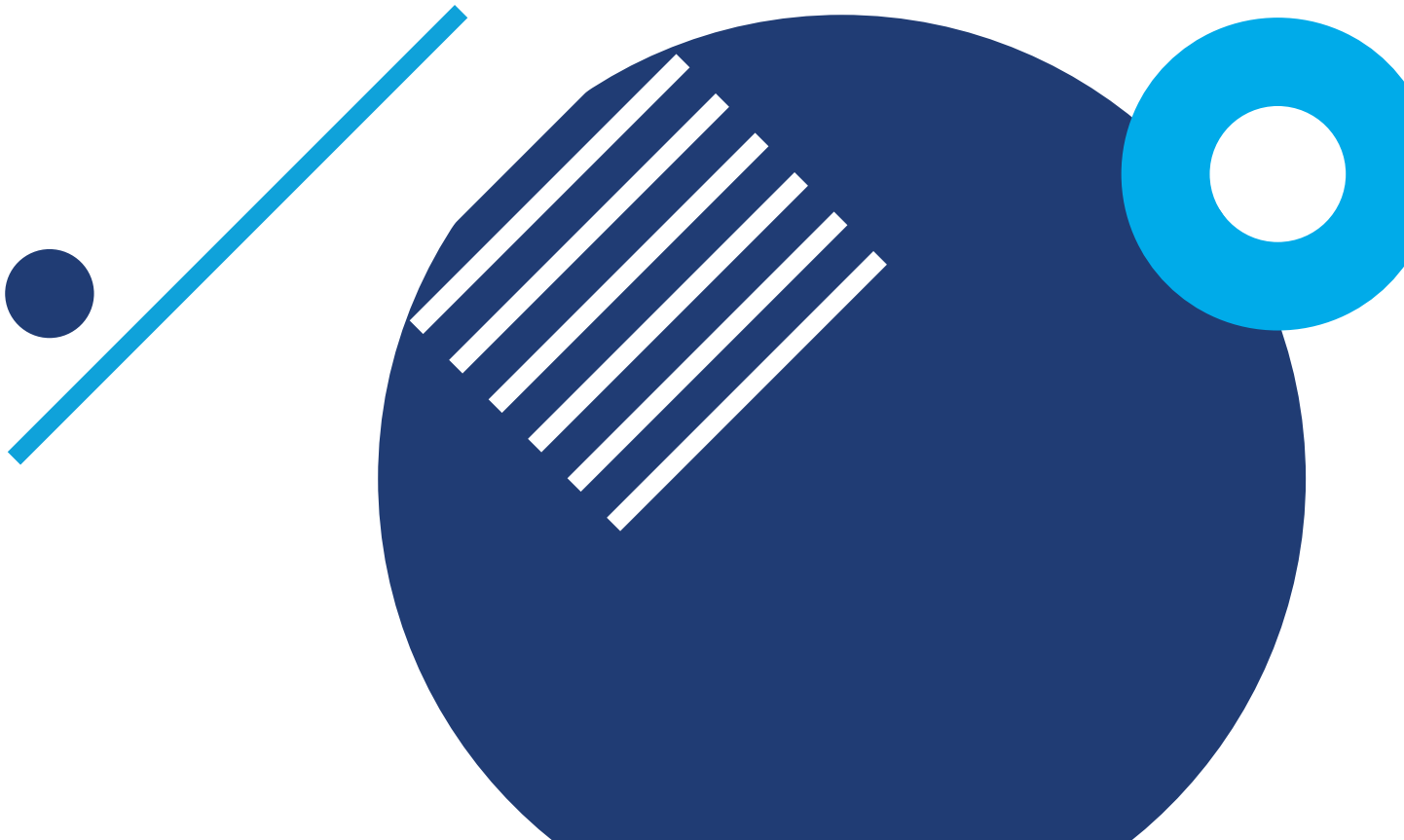
Социальные сети – самый верный способ «убить время». Сетевые развлечения поглощают его без остатка. Но с головой погружаясь в виртуальный мир, мы забываем про друзей, близких, учебу, работу, активный отдых и развитие.

Тебе может показаться, что не иметь профиля в социальной сети – это странно, но на самом деле все вовсе не так. Если у тебя нет профиля в соцсети – поздравляем! Ты уже победил! Ведь теперь у тебя будет гораздо больше времени на полезные вещи: учебу, спорт, настоящую, не сетевую дружбу!

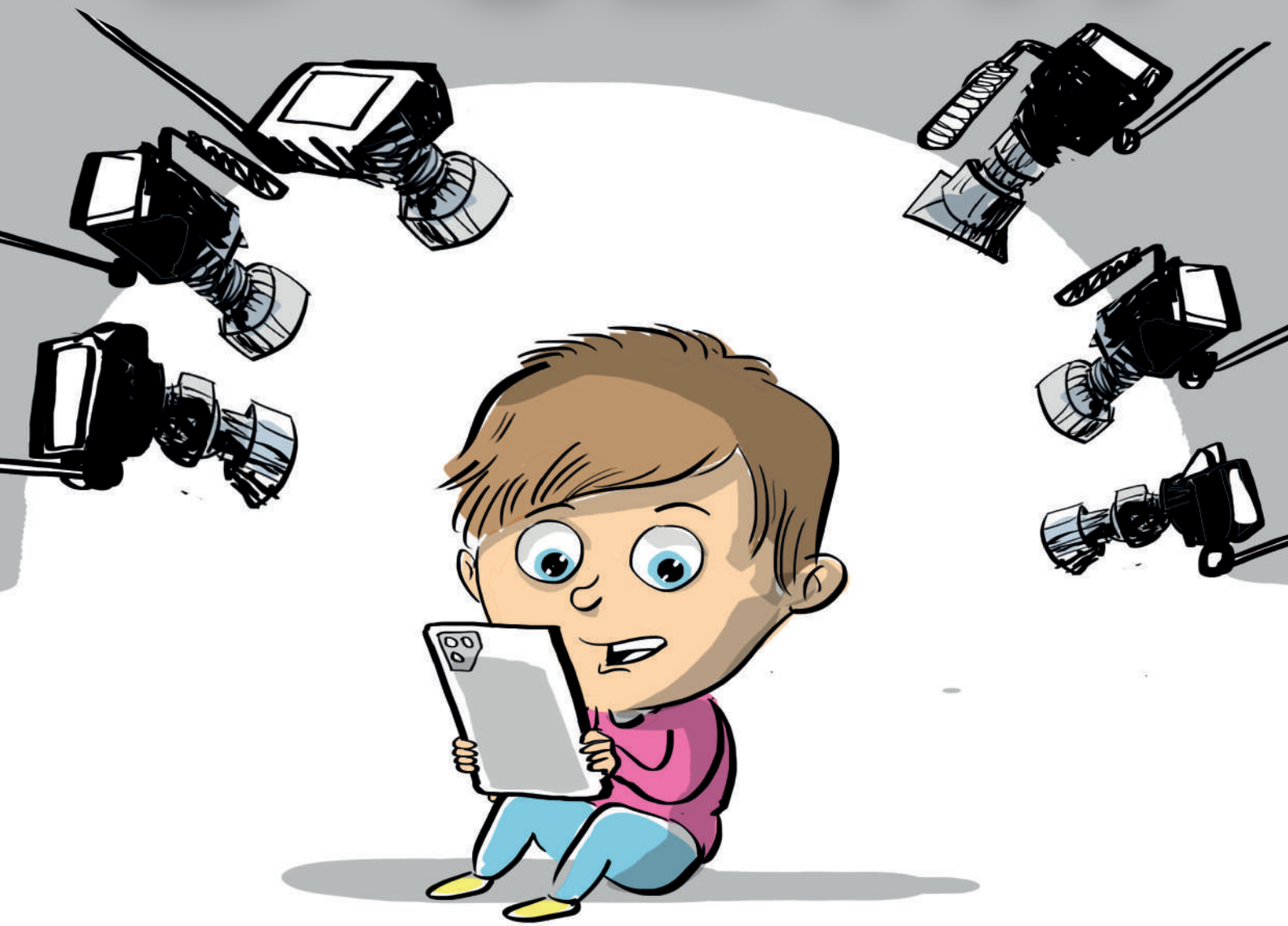
Все больше россиян признаются, что соцсети приносят им больше негативных эмоций: печаль, обиду, зависть. Отказ от соцсетей поможет стать по-настоящему счастливым.

Современные соцсети созданы не для общения. Они созданы для рекламы, для продажи товаров и услуг, навязывания чужого мнения. А если у тебя нет соцсетей – ты мыслишь и думаешь самостоятельно!

НЕ ПОГРУЖАЙСЯ В ИНТЕРНЕТ С ГОЛОВОЙ! ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!



АНОНИМНОСТЬ В СЕТИ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

Возможна ли анонимность в сети? Многим до сих пор не дает покоя этот вопрос, но на него есть однозначный ответ.

АНОНИМНОСТЬ В СЕТИ – МИФ!

Многим людям до сих пор кажется, что Интернет – безопасное и абсолютно анонимное место, где каждый может писать и делать все, что ему вздумается. Но это не так. Поэтому тебе следует помнить две важных истины:

1. **Всё, что однажды попало в Интернет, остаётся там навсегда.**
2. **В Интернете можно найти кого-угодно, даже если пользователь попытался скрыть о себе всю информацию.**

Многие пытаются скрыть свою личность в Интернете. Например, простые пользователи делают это, чтобы друзья или близкие не узнали о каких-то их увлечениях. Но гораздо чаще это делают хулиганы или преступники, которым важно, чтобы их действия остались в тайне. Они боятся проблем с законом и пользуются различными способами: создают фейковые профили в соцсетях, используют специальные программы-анонимайзеры.

Однако следует помнить, что каждое твое действие в Интернете содержит информацию о том устройстве, с которого ты это делал – например о телефоне или компьютере. А твой Интернет-провайдер видит все, что ты делаешь в Интернете несмотря на любую программу. Следовательно, эта информация может быть доступна кому угодно: от сотрудника полиции до преступника.

> **Важно помнить, что Интернет – это такое же публичное пространство, как улица, парк или школа. Там действуют те же правила – общайся прилично, соблюдай правила вежливого поведения и относись к другим людям так же, как хочешь, чтобы относились к тебе.**

Ведь каждое действие или грубость в Интернете может иметь последствия. **Клевета и оскорбление являются противоправными деяниями, за совершение которых предусмотрена ответственность.** Уважай других людей, относись с пониманием и состраданием к чужой беде. Научись ставить себя на место другого человека. А также больше времени проводи в реальном мире, общаясь с друзьями по-настоящему, а не в сети.

АНОНИМНОСТЬ В СЕТИ – МИФ!

5. **Соблюдай режим отдыха и сна.** Детям рекомендовано спать 9-10 часов. Только в таком режиме твой мозг сможет полностью отдохнуть, а организм восстановить силы. Отсутствие правильного режима сна негативно влияет на умственные способности, нервную систему, настроение, провоцирует возникновение ряда заболеваний. Днем старайся несколько часов проводить на свежем воздухе, включая в это время активную физическую нагрузку (быструю ходьбу, спортивные игры, занятия на тренажерах, пробежки, катание на велосипеде, роликах, коньках, танцы, фитнесс и пр.).

6. **Старайся воспринимать жизнь позитивно.** Трудности и неприятности возникают у всех людей без исключения, поэтому и тебе предстоит научиться их преодолевать. Знай, что не существует нерешаемых проблем, просто ты пока не нашел нужного решения. Люби свою жизнь, она у тебя одна.

ОБЩАЙСЯ С ДРУЗЬЯМИ В РЕАЛЬНОЙ ЖИЗНИ, А НЕ В ОНЛАЙНЕ!

ЭКРАННОЕ ВРЕМЯ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

СКОЛЬКО ВРЕМЕНИ СТОИТ ПРОВОДИТЬ В ИНТЕРНЕТЕ?

Знаешь ли ты, кто такой Билл Гейтс? Это один из создателей операционной сети Windows, которая, скорее всего, стоит и на твоем компьютере. Можно сказать, что именно этот человек создал для нас те компьютеры, которыми мы пользуемся. Как ты думаешь, сколько времени в день он разрешал своим детям проводить за компьютером?

Ответ тебя удивит: 45 минут в будни и 1 час 45 минут в выходные. При этом он не разрешал детям пользоваться компьютером вечером перед сном, а до 14 лет и вовсе не давал им в руки гаджетов.

Другой известный человек, исполнительный директор 3D Robotics Крис Андерсон ввёл родительский контроль и лимитировал время на все электронные устройства в доме. Он на своем примере убедился, к чему приводит слишком тесное взаимодействие с электронными гаджетами. По мнению Андерсона, опасность новых технологий заключается во вредном контенте и появляющейся зависимости от электронных новинок.

Почему так? Да потому что эти люди больше других знают об опасности, которую несет Интернет-зависимость для здоровья и психики пользователей.

Такие развлечения легко вызывают самую настоящую зависимость. Будь внимателен и сам старайся следить за собой. Бей тревогу, если заметил у себя следующие признаки:

1. Не ложишься спать, предварительно не посидев в смартфоне.
2. Каждый день ешь за компьютером или со смартфоном в руке.
3. Почти все выходные проводишь в Интернете, никуда не выходя.
4. Злишься или раздражаешься, когда приходится отложить смартфон или оторваться от Интернета.
5. Играешь в компьютерные игры два и более раз в неделю.
6. Сидишь в социальных сетях или «болталках» в ночное время.
7. Не высыпаешься, часто испытываешь головные боли или неприятные ощущения в глазах.

Если ты хочешь избежать Интернет-зависимости, то старайся придерживаться следующих правил:

1. **Сократи время использования гаджетов и компьютера.**
2. **Не бери в руки телефон хотя бы за час до того, как планируешь лечь спать.** Интернет, соцсети или игры могут вызвать яркие эмоции, которые помешают уснуть.
3. **Не ешь за компьютером и не используй телефон во время еды.** Отвлекись от них ненадолго, лучше вместо этого пообщайся с родственниками или друзьями.
4. **Старайся на выходных использовать компьютер и гаджеты как можно меньше.** В Интернете или в играх очень легко «зависнуть» и весь день пролетит незамеченным, а ты потом будешь сожалеть о потерянном свободном времени.

10 СОВЕТОВ РОДИТЕЛЯМ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

1. **Стройте открытые и доверительные отношения с ребенком.** Обсуждайте устройства и проводимое время в Интернете спокойно, чтобы ребенок всегда чувствовал и знал, что он может к вам обратиться, если попадет в неприятную ситуацию.

2. **Больше времени проводите вместе с ребенком в реальной жизни.** Отвлекайте его от Интернета и отвлекайтесь сами. Играйте с ребенком в активные игры, читайте, смотрите фильмы и общайтесь.

3. **Закладывайте полезные привычки** и помогайте ребенку развивать социальные и эмоциональные навыки, такие как уважение к другим, сопереживание, критическое мышление и ответственное поведение.

4. **Используйте устройства в хорошо просматриваемом месте в доме.** Это поможет следить за тем, с кем общается ваш ребенок в сети, когда пользуется телефоном, планшетом, телевизором, игровой приставкой и другими подключенными к Интернету устройствами.

5. **Установите ограничения**, чтобы время, проводимое перед экраном электронного устройства, было в балансе со временем в реальном мире. Грамотно сформировать ожидания по части того, где и когда допустимо пользоваться электронными устройствами, можно с помощью распорядка «электронного дня» всей семьи. Введите запрет на использование ребенком компьютера, планшета и смартфонов в ночное время. Учите ребенка, подавая пример. Чтобы привить ребенку правила цифровой безопасности, их следует понимать и соблюдать самим. Не лишним будет заключить семейное соглашение об использовании устройств и Интернета.

6. **Будьте в курсе того, какие приложения, игры и социальные сети использует ребенок. Убедитесь, что они соответствуют его возрасту.** Выставляйте в приложениях и играх ограничения на функции обмена сообщениями или чата в Интернете и передачи геолокации, так как это делает ребенка уязвимым для нежелательных контактов и раскрывает его местоположение.

7. **Проверьте настройки конфиденциальности** в играх и приложениях, которые использует ваш ребенок. Убедитесь, что в них выставлены наиболее строгие критерии. Ограничьте список лиц, которые могут посылать ребенку сообщения и попросите его советоваться с вами, прежде чем принимать приглашения в друзья от других пользователей.

8. **Используйте функции родительского контроля.** Это позволяет фильтровать опасные материалы, следить за тем, как ребенок использует подключенные к Интернету электронные устройства, ограничивать или блокировать на них доступ к сети и другие функции, например, камеру или покупки в приложениях.

9. **Обращайте внимание на настроение и поведение ребенка.** Смена привычек может свидетельствовать о том, что он попал в неприятную ситуацию. Важно, чтобы ребенок знал, что в любой ситуации, ему следует довериться и рассказать об этом вам.

10. **Обеспечьте безопасность персональной информации своей семьи.** Следите за тем, чтобы ребенок не размещал в Интернете информацию о себе и своей семье: личные или семейные фотографии, свою фамилию, данные о месте жительства, пребывания, учебы, работы родителей, маршрутах своего передвижения, реальных имен своих друзей или людей из круга общения родителей, данные свидетельства о рождении, паспорта или иных документов, номера телефонов, банковских карт, логины, пароли и тому подобную информацию. 50% детей указывают в Интернете свой настоящий возраст и делятся настоящими фотографиями, 10% пишут свой мобильный номер, а 9% указывают геолокацию (по данным Лаборатории Касперского).

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт
ligainternet.ru

ОБЩЕНИЕ С НЕЗНАКОМЦАМИ ОНЛАЙН: ПОЧЕМУ ЭТО ОПАСНО

Агрессоры в цифровом мире

Одна из самых больших опасностей в сети – люди, которые по разным причинам могут представлять угрозу для здоровья или психики ребенка. Такие люди зачастую угрожают не только детям, но и взрослым.

Кто представляет в Интернете наибольшую угрозу

- **Тролли и агрессоры.** Интернет-травля иногда носит организованный характер, когда группа обидчиков координирует свои действия и может даже иметь единый «центр управления».
- **Шантажисты.** Если информация или материалы личного характера попадают в руки к злоумышленникам, они могут использовать их для шантажа своей жертвы.
- **Вербовщики.** Эти люди ищут среди пользователей сети тех, кого смогут приобщить к каким-то определенным идеям, группам или движениям, зачастую носящим криминальный или экстремистский характер.
- **Манипуляторы.** Воздействуют на эмоции и психику широкой группы пользователей с целью вызвать у них агрессивное поведение или спровоцировать на какие-то действия.
- **Мошенники.** Стремятся похитить у пользователя его персональные данные или финансовые средства. С этой целью используют методы социальной инженерии, манипулируют эмоциями жертвы, а также прибегают к техническим средствам, подделывая сайты, профили и даже номера телефонов.
- **Педофилы.** Входят в доверие к ребенку, иногда маскируясь в Интернете под другого ребенка. Обманом навязывают ему встречу или заставляют его присылать материалы интимного характера.

Ключевой вопрос

Что такое «Нежелательный контакт»?

Внимание!

Нежелательным контактом называется любое общение в Интернете, беспокоящее вашего ребенка, создающее конфликтную ситуацию или обстоятельства, при которых ему может быть причинен вред. Также в сети ребенок может столкнуться с опасными или неуместными материалами, способными расстроить, напугать или обидеть его. 82% детей получают запросы на дружбу в социальных сетях от незнакомых людей, а 29% - от незнакомых взрослых (по данным Лаборатории Касперского)

Ребенку следует остерегаться незнакомцев в Интернете, которые:

- Задают много вопросов о его личной жизни.
- Просят об одолжениях в обмен на что-либо.
- Просят никому о них не рассказывать.
- Пытаются контактировать с ребенком множеством различных способов – смс, соцсети, онлайн-чаты и т.п.
- Задают ребенку вопросы о том, кто еще имеет доступ к его телефону, компьютеру или аккаунту.
- Лестно отзываются о внешнем виде ребенка.
- Задают вопросы или делают комментарии личного или интимного характера. 10% детей отмечали, что им приходили странные сообщения от взрослых пользователей.
- Настаивают на личной встрече. 37% детей встречаются с теми, с кем познакомились онлайн.
- Заставляют ребенка чувствовать себя виноватым или угрожают ему.

Полезные советы

- Расскажите детям, что делать, если им пишет кто-то, с кем они не хотят общаться.
- Уберите учетные записи детей из публичного доступа.
- Настоятельно посоветуйте ребенку удалить контакты людей, с которыми он не знаком лично.
- Договоритесь с детьми, какие данные они могут публиковать в Интернете, а какие нет. Например, фотографии, место жительства, учебы и т.д.
- Ребенку постарше предложите сделать страницы в соцсетях закрытыми для посторонних и подробно изучить настройки конфиденциальности, чтобы он мог контролировать, кто именно будет видеть его фотографии и записи.
- Лучший способ избежать опасного общения в сети – заблокировать человека, который пытается контактировать с ребенком и пожаловаться на его аккаунт администрации соцсети.
- Если вы поймете, что преследование ребенка со стороны незнакомых лиц, его травля или вовлечение в депрессивно-суицидальный контент не прекращаются, а все возможные меры помощи исчерпаны, следует сменить аккаунт ребенка, мобильное устройство и номер его телефона. Желательно на какое-то время полностью исключить ребенка из Интернета, например, пойти в поход с ребенком на несколько дней куда-нибудь, где не будет зоны покрытия сети.

Это надо знать!

Очень важно объяснить ребенку, что «виртуальные друзья» должны оставаться виртуальными, но если ребенок хочет встретиться с кем-либо из них, то вы хотели бы, чтобы он делал это с вашего разрешения. Безопаснее всего встречаться днем, в общественном месте и в сопровождении родителей или кого-либо из взрослых, кому ребенок доверяет.

Объясните ребенку, что он должен как минимум ставить кого-нибудь из родителей в известность о том, куда он направляется и с кем собирается встретиться.

Что делать, если ребенок попал в опасную ситуацию?

- Сохраняйте спокойствие и заверьте ребенка, что его никто не собирается ругать.
- Объясните ему, что даже взрослых иногда обманом заставляют делать то, о чем они потом жалеют.
- Дайте ребенку понять, что он всегда сможет обсудить с вами любой вопрос, не боясь наказания или критики.
- Не лишайте ребенка доступа в Интернет. Это может быть воспринято как наказание, и в дальнейшем ребенок не захочет рассказывать вам о своих проблемах.
- **Если вы считаете, что жизни или здоровью ребенка угрожают, сообщите об этом в полицию по номеру 102.**
- Прежде чем блокировать кого-либо или удалять записи, обязательно заснимите и сохраните доказательства – фото или скриншоты переписок, даты и время записей, ссылки на публикации или аккаунты.
- **Если эти материалы включают в себя интимные изображения детей младше 18 лет, имейте в виду, что хранение и распространение таких изображений является преступлением. Обязательно обратитесь в полицию.**

Личный пример

Обсудите с детьми, как они могут реагировать на различные раздражающие ситуации. Они должны понять, что в любой момент могут поговорить с вами, довериться, получить помощь!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru

РОДИТЕЛЬСКИЙ КОНТРОЛЬ

Полезный контроль

Родительский контроль – функция цифровых устройств и гаджетов, обладающая набором полезных свойств, позволяющих контролировать и отслеживать время, проводимое ребенком в Интернете, а также сайты, которые он посещает, просматриваемый контент и многое другое. Родительский контроль является самым популярным методом защиты ребенка от опасностей в Интернете. 41% опрошенных родителей использует приложения родительского контроля. А вот 19% родителей вообще не предпринимают никаких мер по защите ребенка в Интернете (по данным ВЦИОМ).

В условиях современного интернета, когда любой ребенок может получить доступ практически к любой информации вне зависимости от наличия возрастных ограничений, родительский контроль является крайне полезной функцией, которая поможет уберечь ребенка от деструктивного контента, помочь освоить финансовую грамотность и регулировать траты, а также уберечь ребенка от нежелательных знакомств, опасных людей в Интернете и преступников.

Ключевой вопрос

Как настроить родительский контроль?

Внимание!

Основные функции родительского контроля:

1. Контроль и нормирование экранного времени;
2. Возможность настраивать распорядок дня – в какое время ребенок может или не может пользоваться устройством;
3. Контроль посещаемых сайтов, вплоть до запрета или ограничения на открытие конкретных сайтов;
4. Контроль за открытием определенных приложений на смартфоне или программ на компьютере;
5. Возможность четко разграничить учебу и досуг ребенка путем настройки распорядка электронного дня;
6. Контроль за расходами ребенка и многое другое;
7. Контроль времени, проведенного в онлайн-играх.

Каким бывает родительский контроль:

1. Родительский контроль на смартфонах – современные смартфоны смартфоны на Android и iOS обладают встроенными функциями родительского контроля, которые подключаются непосредственно в настройках телефона.
2. Родительский контроль в браузерах – некоторые браузеры обладают встроенными функциями родительского контроля. В таком случае их функционал ограничивается использованием браузера и не распространяется на весь компьютер.
3. Родительский контроль на игровых приставках – приставки Xbox и PlayStation также обладают функциями родительского контроля, которые позволяют ограничить то, в какие игры ребенок может играть, как он может использовать приставку, и контролировать его расходы в магазинах игр для этих приставок.
4. Специализированные приложения и программы для родительского контроля. Такие приложения можно найти как в официальных магазинах приложений для смартфонов, так и просто в Интернете на сайтах разработчиков. Эти приложения и программы обладают самым широким функционалом, который позволяет контролировать действия ребенка как на компьютере, так и в телефоне, отслеживать его активность в соцсетях, телефонную книгу, финансовые траты, время использования устройства, игры и многое другое.

Личный пример

Объясните ребенку, что родительский контроль – это база его безопасности. Заключите соглашение о его установке.

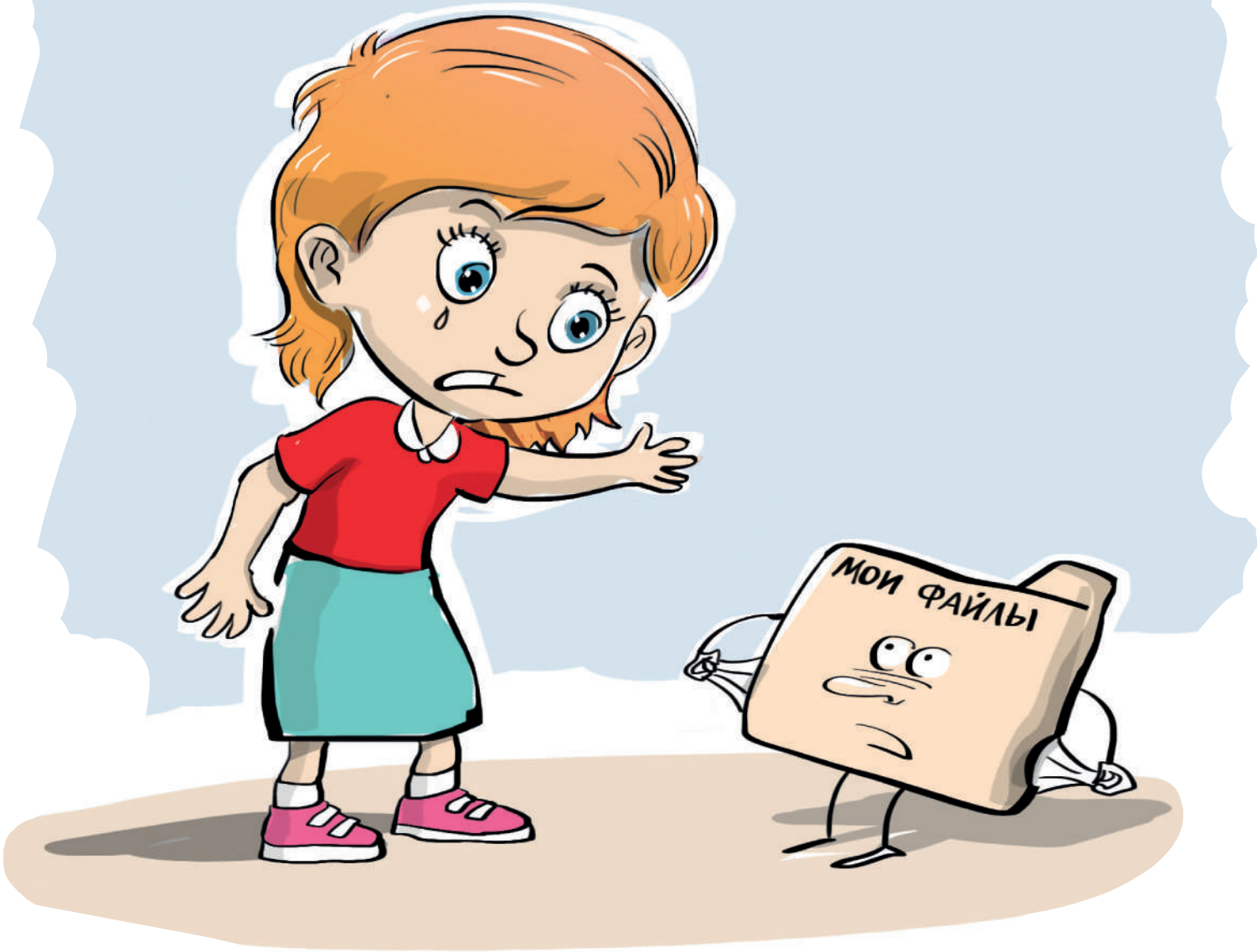
Более подробную инструкцию о том, как настроить родительский контроль на разных устройствах можно в инструкции по настройке родительского контроля Лиги безопасного Интернета https://ligainternet.ru/.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

Персональные данные – это все ключевые и важные сведения о человеке. Их следует тщательно беречь и не раскрывать в Интернете без необходимости. Раскрытие персональных данных в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже аккаунтов, мошенническим действиям, вымогательству денег у тебя или твоих близких, угрозах совершения компрометирующих тебя действий, краже денег и документов. В некоторых случаях это даже может привести преступника на порог твоего дома.

Что относится к персональным данным?

1. **Фамилия, имя, отчество;**
2. **Все твои документы** (паспорт, свидетельство о рождении, аттестат и др.);
3. **Банковские данные** (номер счета, карты, пин-код, CVV-код);
4. **Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы);
5. **Фотографии и видеозаписи с твоим изображением;**
6. **Данные о твоих родственниках;**
7. **Твои логины и пароли.**

Чаще всего пользователи сети сами выкладывают информацию о себе в Интернет. Мошенники охотятся за этими данными. Большинство информации о жертвах преступники находят в открытом доступе в соцсетях и в Интернете.

Как защитить свои персональные данные?

1. **Придумывай и используй разные сложные пароли для почтовых ящиков, соцсетей и других сайтов.** Пароль восстановить проще, чем вернуть украденные деньги.
2. **Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.**
3. **Не отмечай местоположение** своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.
4. **Не ставь в браузере «разрешить» всплывающим окнам.** Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ и соглашаться на какое-либо действие.
5. **Проверь, чтобы твои аккаунты не были доступны с чужих устройств.** В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.
6. **Закрой доступ к своим страницам в социальных сетях.** Включи настройки конфиденциальности.

МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!

ЦИФРОВАЯ ЗАВИСИМОСТЬ ДЕТЕЙ

Дети – цифровые аборигены

Наши дети в современном мире много времени проводят в Интернет. Все, что они смотрят, пишут и размещают в сети сохраняется навсегда, поисковики найдут сказанное или выложенное ими через годы. По прошествии лет ребенок станет совсем другим человеком, у него будут новые друзья, знакомые, новая работа и, возможно другие взгляды. И ему может стать неудобно, стыдно или невыгодно иметь такие цитаты, такие фотографии и такие связи. Сетевое поведение может аукнуться ребенку при поступлении в ВУЗ или на работу, при получении в визы или при интересных знакомствах.

Поисковики помнят всё. Кнопки «Удалить» из Интернета не существует.

Но помнит он только то, что мы сами ему о себе сообщили.

Ключевой вопрос:

Сколько времени, для чего и с кем наши дети в сети?

Внимание!

Не только дети, но и взрослые могут проводить в Интернете целый день. Видео, соцсети, игры - на это можно тратить очень много времени. Как показали независимые исследования в 76% случаев дети используют Интернет для игр, в 70% для просмотра видео, в 67% для общения с друзьями и в 53% для подготовки к урокам. 80% опрошенных школьников не могут обойтись без смартфона*. Среднее время, которое подростки проводят в Интернете, составило почти 6 часов в день*. Эта пугающая тенденция приводит к подмене реальных ценностей виртуальными.

Ключевые фигуры IT-отрасли, которые сами занимались разработкой устройств и программ, такие как Билл Гейтс или Стив Джобс, строго ограничивали время использования Интернета и гаджетов в своей семье. До определенного возраста они вообще не разрешали детям пользоваться смартфонами.

Признаки «беды»

1. Ребенок теряет интерес к нахождению на улице, встречам с друзьями или спортивным играм.
2. Ребенок плохо учится в школе, постоянно даже там «сидит» в смартфоне.
3. Ребенок утомляется, плохо спит, жалуется на головные боли и зрительное утомление.
4. У ребенка меняются привычки в еде.
5. Ребенок начинает плохо следить за личной гигиеной.
6. Ребенок зацикливается на конкретном сайте или игре.
7. Ребенок крайне агрессивно реагирует на просьбы отвлечься от его виртуальных занятий.
8. Находясь не за компьютером, ребенок ведет себя нервно или раздражительно.
9. Ребенок отдаляется от родителей, перестает разговаривать с ними на личные, волнующие его темы.
10. Ребенок отдаляется от одноклассников и друзей в реальном мире, отдавая предпочтение «виртуальному общению, находит себе лучшего друга «родную душу» в социальных сетях.
11. Ребенок проводит ночное время или часть времени, предназначенного для сна, в социальных сетях или за компьютерными играми.
12. Ребенок резко меняет свое отношение к вопросам, касающимся традиционных духовно-нравственных основ жизни, в частности: патриотизма, милосердия, сострадания, начинает защищать права на нетрадиционные сексуальные отношения, смену пола, гендерную идентичность, идеологию феминизма, чайлдфри и пр.
13. Ребенок проявляет беспричинную агрессию, замкнутость, депрессию, частую смену настроения.
14. На теле ребенка регулярно появляются ссадины, порезы или иные повреждения.

Полезные советы

1. Установите ограничения на то, когда и сколько времени может проводить ваш ребенок в Интернете во внеучебное время.
2. Введите запрет на использование ребенком телефонов, компьютеров и планшетов в ночное время. Общение ребенка через социальные сети и личную переписку в ночное время часто используется преступниками как методика доведения их до самоубийства, вовлечения в опасные квесты, нанесения вреда собственному телу, склонения к разговорам на сексуальные темы и иные виды деструктивного поведения.

---

* Всероссийский центр изучения общественного мнения

3. Используйте доступные вам технологии – функции родительского контроля! Инструменты для отслеживания времени, проведенного в сети, помогут вам установить рамки допустимого пользования электронными устройствами или Интернетом. Будьте честны с ребёнком и объясните, ради чего вы собираетесь использовать эти технологии. Родитель должен знать, чем ребенок занимается в сети! Более подробную пошаговую инструкцию о том, как настроить родительский контроль на разных устройствах можно найти на портале Лиги безопасного Интернета https://ligainternet.ru/

4. Отключите уведомления в приложениях социальных сетей, чтобы свести к минимуму отвлекающие факторы.

5. В зависимости от возраста вашего ребенка вы можете составить ежедневный распорядок использования гаджетов для всей семьи, в котором определено время на реальный мир (общение с друзьями и в семье без гаджетов), и время на виртуальный мир. Не противопоставляйте эти два мира, чтобы живое общение не было наказанием! Пусть расписание будет естественно чередовать различные полезные виды деятельности.

6. Не используйте смартфон как средство для освобождения ребенка от вас. Если ребенок слишком рано выйдет в Интернет, это может привести к «цифровой наркомании» и проблемам со здоровьем.

7. Разнообразьте список ваших домашних дел «оффлайновыми» занятиями – например совместными физическими упражнениями, чтением книг или настольными играми.

8. Обсудите возможность запрета использования электронных устройств во время занятий с классным руководителем вашего ребенка, вынесите данный вопрос на рассмотрение родительского собрания для распространения ограничения на всех учеников класса.

Личный пример

Вы можете подать хороший пример независимого поведения ребёнку и сами, сократив свой досуг перед экраном ноутбука или смартфона.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

ОПАСНЫЕ СООБЩЕСТВА ЦИФРОВОГО МИРА: КАК ИЗБЕЖАТЬ СЕТЕВОЙ МАНИПУЛЯЦИИ

Деструктивные сообщества в сети – проблема реального мира

В Интернете существует большое количество опасных групп, сообществ, которые распространяют опасные для жизни, здоровья, нравственности человека идеологию, увлечения, движения, в том числе, вовлекают в экстремистскую деятельность и совершение иных преступлений. К таким группам относятся:

Суицидальные сообщества – группы, в которых публикуется контент, связанный, с тематикой самоубийств. Сообщества суицидальной направленности часто маскируются, тем не менее, их можно выявить по таким признакам: романтизация смерти и идей самоубийства; героизация людей, совершивших самоубийство и подражание им; практика «селфхарма» (причинения вреда самому себе); распространение деструктивно-суицидальной информации разного вида разнообразными способами. Например, часто пропагандируется такой контент через аниме, идеи анорексии идеологию ЛГБТ сообществ и др. 46% россиян убеждены, что Интернет значительно увеличил число самоубийств (по данным ВЦИОМ).

Аутодеструктивные сообщества – группы, распространяющие идею и практики причинения самому себе физического или психологического вреда. Например, группы «селфхарм». Часто бывают подготовительным этапом для вовлечения детей в суицидальные группы.

Сообщества школьных расстрелов (скулшутинг) – движение, ставшее популярным в США. Эти сообщества романтизируют и продвигают идею массовых убийств и, в особенности, массовых убийств среди детей и подростков в школах. К таким относится, например, движение «Колумбайн», признанное террористическим на основании решения Верховного суда Российской Федерации. По данным исследователей, скулшутинг пропагандируется даже через «кровавое аниме».

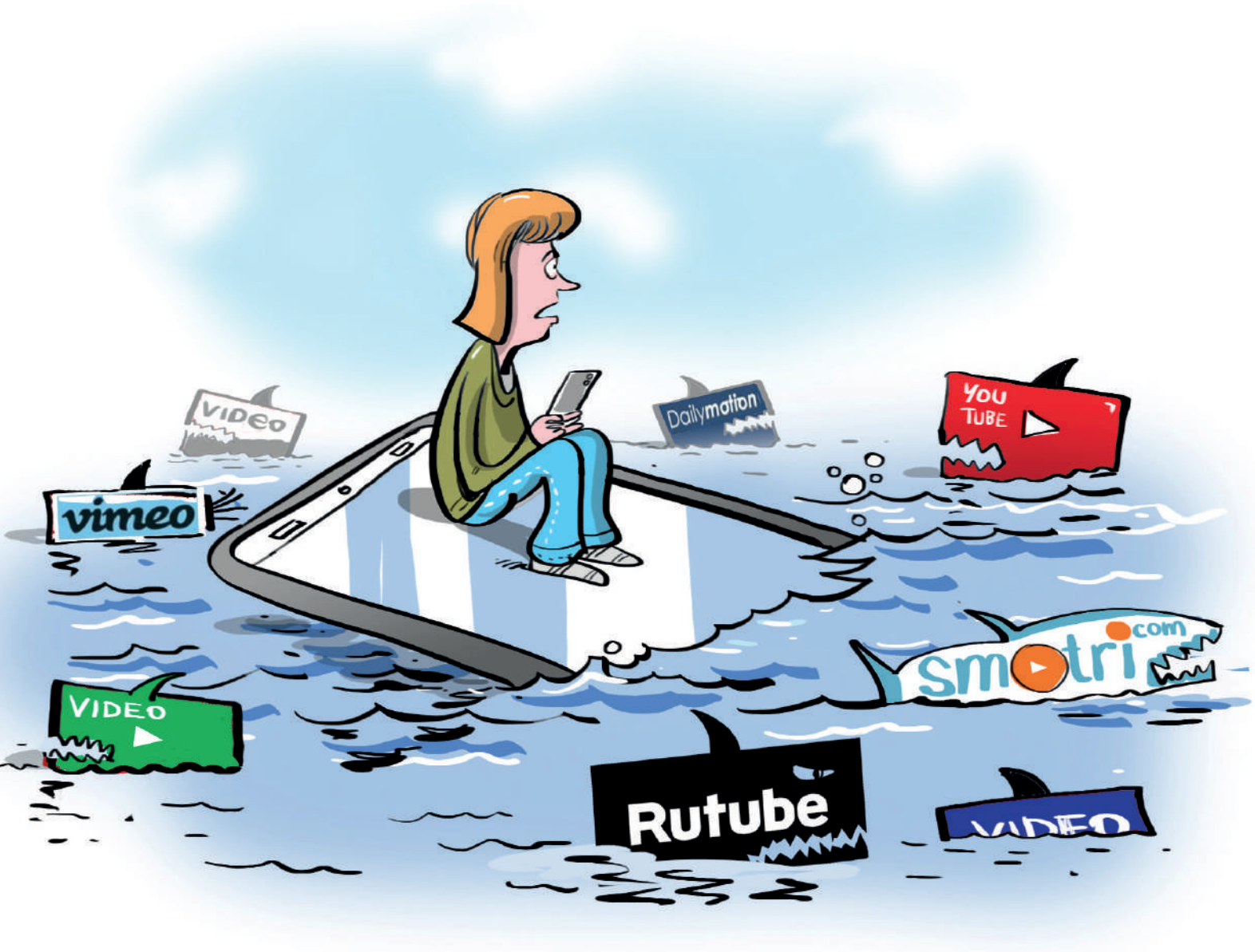
Сообщества по криминальной идеологии – продвигают идеалы из криминальной среды среди подростков. Наиболее известным примером является движение АУЕ (признано экстремистским и запрещено на территории Российской Федерации). В таких сообществах романтизируется не только криминальный, но и тюремный образ жизни и быт, а также криминальные герои книг, фильмов и сериалов.

Сообщества по пропаганде наркотиков – данные сообщества пропагандируют не только употребление наркотиков, романтизируя наркопотребление и образ жизни наркоманов, но и вовлекают своих членов в распространение наркотиков. Для этого пользователям массово рассылаются предложения о «подработке», где обещают высокую заработную плату. Бывают случаи и втягивания в эту деятельность детей и подростков. При этом несовершеннолетние, решившие подработать курьером, как правило, устанавливаются правоохранительными органами (в отличие от их работодателей-преступников) и получают реальные сроки лишения свободы.

Экстремистские сообщества – сообщества, занимающиеся публикацией и распространением экстремистского контента, пропагандирующие экстремистские идеи, а также привлекающие своих подписчиков к совершению преступлений на почве политики, расовой, национальной или религиозной ненависти.

Ключевой вопрос

Как помочь ребёнку не попасть в деструктивное сообщество?



Внимание!

На что обратить внимание...

- Наличие в сообществах, которые посещает ребенок, или в ленте новостей его аккаунта, фотографий увечий: порезы, ссадины, кровь, травмы и т.п.
- Наличие фотографий в мрачных тонах, с депрессивным содержанием.
- Наличие в ленте цитат, обесценивающих жизнь или традиционные духовно-нравственные, в том числе, семейные ценности; содержащих пренебрежительные/неуважительные высказывания по отношению к родителям, деторождению, служению Отечеству, исторической памяти народа России, ценности жизни человека, руководству страны и принимаемым решениям.
- Наличие в подписках у подростка или в ленте новостей его аккаунта сообществ, посвященных скулшутингу, а также лицам, которые совершали эти преступления.
- Интерес к «аниме» у ребенка или его друзей.
- Ребенок стал часто проводить время вне дома, скрывать информацию о том, где и с кем проводит время, при этом вы не знаете телефонов его друзей и их родителей, его успеваемость в школе упала.
- У ребенка появились денежные средства или дорогие вещи, происхождение которых вы не знаете или он пользуется вещами, которые ему, якобы, дал временно поносить товарищ.

Последствия вовлечения в деструктивные движения

- **Снижение способности самостоятельно думать и принимать решения.**
- **Отказ от личной ответственности.**
- **Отрицание авторитетов, в том числе родителей, учителей и знакомых.**
- **Обесценивание норм морали и общечеловеческих ценностей.**
- **Выраженная симпатия к антигероям, антидвижениям.**
- **Выраженное стремление к разрушению и деструктиву.**
- **Снижение успеваемости в школе.**
- **Неуважение и травля учителей.**
- **Нарушение коммуникации и конфликты со сверстниками.**
- **Формирование школьных банд или радикальных группировок.**
- **Политизация детей и подростков.**
- **Рост преступлений среди детей и подростков.**
- **Рост наркомании среди подростков.**
- **Попытки самоубийства и причинения себе вреда.**

Как вовлекают в опасные сообщества?

Для вербовки и привлечения новых людей в движение вербовщики используют своеобразную «Воронку вовлечения».

Как это работает?

Чаще всего вербовка начинается с личного и очень навязчивого общения. Вербовщики пытаются завладеть всем вниманием и временем пользователя. Один из основных способов вербовки – маркетинговая «воронка вовлечения». Суть «воронки» заключается в том, что пользователь сначала привлекается в какую-либо группу по интересам, затем по активности в этих группах или комментариях, он отбирается и через личные сообщения приглашается в тематическое сообщество с более узкими интересами. После этого происходит отбор пользователя в закрытые группы и чаты, где уже происходит вовлечение в опасную и даже преступную деятельность сообществ. Особенностями таких групп может быть персональный доступ к ним только членам сообщества (особенно если общение происходит через мессенджеры). То есть родители или иное лицо не сможет попасть в группу, используя свои телефон или компьютер. После этого пользователи приступают к выполнению заданий в реальном мире.

Это надо знать!

1. **Постоянные флешмобы могут быть опасны** – это регулярные задачи, например: облейся холодной водой, напиши пост и поставь правильный хештег, опубликуй свои фото в конкретных условиях и т.п. Такие активности «дрессируют» пользователей на бездумные массовые действия.
2. **Массовые тесты, квесты, задания** – псевдотесты на IQ, творческие способности, тип личности и т.п. Они не несут никакой пользы и не могут определить ничего из вышеперечисленного, но подталкивают пользователей к ненужной им активности.
3. **Общественные и явно политические задания** могут выражаться в требовании у ребенка поставить на аватар радужный (ЛГБТ) флаг, опубликовать пост с поддержкой или осуждением какого-либо внутриполитического или мирового инцидента, распространить фейковую новость, сдать деньги на поддержку какой-либо организации.
4. **Максимальный перепост** служит формированию среди пользователей привычки делать репосты каких-либо публикаций к себе в ленту. Таким образом публикации, в том числе и фейки, могут распространяться лавинообразно, каждый раз захватывая все больше и больше пользователей, которые занимаются их репостом и распространением.
5. **Метод наводнения** – формирование постоянного и плотного информационного поля вокруг какого-либо вопроса. В результате у пользователей складывается ложная уверенность, что какая-либо позиция поддерживается разными независимыми источниками и обсуждается на разных уровнях, а значит эта позиция важна и правдива.
6. **Метод «от вас скрывают, а я расскажу правду»** – придает максимальную правдоподобность сообщению и создает у пользователей чувство избранности, ведь с ними поделились какой-то правдой, которую от всех остальных скрывают.
7. **Виртуальные рейтинги и награды** – в соцсетях, сетевых сообществах и массовых играх используются награды и рейтинги, призванные подстегнуть интерес пользователей, заставить их участвовать в активности не «просто так», а за какую-либо награду, даже если эта награда – символическая позиция в виртуальном рейтинге.

Личный пример

Обращаем внимание на молодёжный сленг и изучаем его! Для этого бывает достаточно посмотреть значение разных слов в Интернете. Так, например, слова «самовыпил» и «выход» могут означать самоубийство. Пора бить тревогу по всем фронтам!

Цифры:

58% **убеждены, что современные дети живут в более опасное время, чем они сами** *(по данным ВЦОМ).*

46% **опрошенных считают, что Интернет значительно увеличивает количество самоубийств** *(по данным ВЦОМ).*

60% **опрошенных взрослых уверены, что социальные сети и их контент оказывают вредное воздействие на детей** *(по данным ВЦОМ).*

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЦЕНИМ И УМЕЕМ СОХРАНЯТЬ!

Что надо знать о персональных данных

Персональные данные – все данные о человеке, своего рода «паспорт его личности». Их следует тщательно беречь и не раскрывать в Интернете без необходимости. В противном случае это может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям. Безопасность – это наша непререкаемая ценность для детей и взрослых!

Что относится к персональным данным?

1. Фамилия, имя, отчество;
2. Номера и реквизиты всех документов (паспорт, СНИЛС, ИНН, свидетельство о рождении, аттестат об образовании, медицинский полис и т.п.);
3. Банковские данные (номер счета, карты, пин-код, CVV-код и т.п.);
4. Ваша контактная информация (номера телефонов, адреса электронной почты, адреса жительства, работы или учебы);
5. Фотографии и видеозаписи с вашим изображением;
6. Данные о ваших родственниках;
7. Ваши логины и пароли.

Ключевой вопрос:

Насколько реально и как сохранить персональные данные вашей семьи?

Внимание!

Более трети россиян (37%) не знают, для чего и как могут быть использованы персональные данные (по данным ВЦИОМ)!

Соцсети, мессенджеры и видеохостинги ежедневно собирают о нас огромное количество данных. Делается это, в первую очередь, для заработка денег. Большинство крупных платформ – бесплатны, ведь их владельцы зарабатывают на своих пользователях. Точнее – на их персональных данных, при перепродаже или использовании в рекламе. Соцсети и мессенджеры берут эти данные не только из профиля пользователя, но и из его переписки. Обратите внимание: вся переписка постоянно хранится на серверах социальной сети или мессенджера, поэтому в результате утечки, кражи или хакерской атаки ваша частная жизнь может стать достоянием общественности.

Источники беды

Не стоит надеяться на «приватные» публикации, просматривать которые может только ограниченный круг лиц, которых настраивает сам пользователь. Ведь утечка может произойти через любого из этих людей. Иногда происходят крупные утечки, в результате чего данные тысяч пользователей попадают в открытый доступ. Но чаще всего пользователи сами выкладывают информацию о себе в Интернет. Защитите себя и свою семью! 80% информации о жертвах преступники находят в социальных сетях (по данным Роскомнадзора).

Кроме персональных данных о каждом человеке собираются также его фото- и видеоизображения. Современного человека ежедневно снимают сотни видеокамер, расположенных в публичных местах. Эта информация собирается, в первую очередь, государственными органами с целью обеспечения безопасности, раскрытия преступлений и т.п. Однако следует помнить, что такие видеозаписи могут попасть и в руки к шантажистам или иным злоумышленникам. Будьте осторожны! Не помогайте мошенникам, добровольно передавая им персональные данные.

В текущей ситуации большинство порталов органов власти и коммерческих компаний становятся объектами хакерских атак в ежедневном режиме.

Так, за последнее время в публичный доступ утекли базы данных пользователей компании «Яндекс.Еда» и клиентов медицинской лаборатории «Гемотест». Все это происходит из-за того, что в России до сих пор нет существенной административной и уголовной ответственности для операторов подобных баз. Так, «Яндекс.Еда» «отделалась» штрафом всего лишь в 60 тысяч рублей.

Важно помнить, что из-за халатности или экономии компании на хранении данных, которые мы оставляем, оформляя карточку в магазине, на заправке или любом другом месте могут стать достоянием общественности.

Надо помнить!

Активный пользователь Интернета оставляет цифровой след – иногда свой полный портрет: состояние здоровья, внешность и физические данные, привычки, места пребывания, уровень дохода, данные о личной и интимной жизни и многое другое. Приложения на телефоне могут получить доступ микрофону, камере, акселерометру (используется для измерения движений устройства) и следить за своим пользователем круглосуточно. Всё это может представлять интерес для преступников! Мошенничество, шантаж, травля – вот неполный список того, для чего злоумышленники могут использовать информацию о пользователях. Следите за культурой поведения в сети, сохраняйте свою частную жизнь и конфиденциальность!

В соответствии с действующим законодательством любой гражданин вправе отказаться от предоставления своих персональных данных. Согласие на обработку персональных данных может быть отозвано гражданином у организации в любой момент.

Если вас принуждают к подписанию согласия на обработку персональных данных и отказывают в предоставлении услуги, смело обращайтесь в прокуратуру.

Полезные советы

1. Посоветуйте своему ребенку при регистрации в социальных сетях использовать только имя или псевдоним (никнейм).
2. Следите за тем, чтобы ребенок не размещал в интернете лишнюю информацию: где он живет, где учится, какой дорогой ходит на уроки и т.п.
3. В настройках камеры на телефоне следует отключить геотеги (геолокацию, место съемки). Эта функция показывает, где именно делалась фотография. В таком случае любой желающий по фото может отследить пользователя.
4. Полезно будет настроить приватность в аккаунте своего ребенка. Таким образом его профиль смогут смотреть только его друзья.
5. Объясните ребенку, что нельзя выкладывать в Интернет фото или скан-копии его документов или банковских карт.
6. Расскажите ребёнку, что персональными данными стоит делиться только с ограниченным кругом лиц – самыми близкими. Не стоит передавать такие данные друзьям, а особенно незнакомым людям из соцсетей.
7. Ребёнку надо знать, что злоумышленники могут пытаться выведать информацию и персональные данные через личные сообщения в социальных сетях. Особенно внимательно стоит реагировать на ссылки, которые незнакомцы присылают ребёнку в личных сообщениях. Лучше по ним не переходить, а неизвестные файлы – не открывать.
8. Расскажите ребенку, что нельзя подключаться к первому попавшемуся бесплатному Wi-Fi в публичном месте. Через такую бесплатную сеть злоумышленники могут получать доступ к персональным данным пользователей.

Личный пример

Тщательно отбирайте фото и видео, которые вы сами выкладываете в Интернет!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

ЧТО ТАКОЕ «НЕЛЬЗЯ»: ОБМЕН ИНТИМНЫМИ ФОТОГРАФИЯМИ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

Незнакомцы в сети – всегда источник опасности

Наибольшую опасность для ребенка в Интернете представляют незнакомцы, которые могут начать общение с целью обмена интимными фотографиями или сексуального насилия.

Часто в сети несовершеннолетних обманом или уговорами заставляют совершать действия сексуального характера на веб-камеру или посылать интимные изображения. Они просят ребенка сохранять их отношения в тайне и стремятся физически и эмоционально разлучить его с близкими и друзьями.

Ранее Лигой безопасного Интернета был проведен эксперимент. В социальной сети был зарегистрирован аккаунт ребенка. В течение суток после регистрации аккаунта начали приходить сообщения и запросы на дружбу от незнакомых взрослых.

Ключевой вопрос

Как предостеречь ребёнка
от общения с незнакомцами в цифровой среде?

Внимание!

Излишне доверительное общение с незнакомцами в Интернете и рассылка своих фотографий или видео может привести к очень неприятным последствиям:

- **Травля** – фотографии и видео могут использовать тролли или агрессоры с целью травли жертвы, ее унижения и высмеивания;
- **Шантаж** – фото и видео интимного характера могут использовать для шантажа жертвы, вымогая деньги или склоняя к каким-либо действиям, в том числе интимного характера.
- **Вовлечение детей в изготовление детской порнографии и занятие проституцией -** фотографии и видео могут использовать преступники, с помощью шантажа или за плату вымогая фотографии ребёнка, либо принуждая его к занятию проституцией.

Каким образом незнакомцы входят в доверие к ребенку?

- Регулярно посещают популярные среди детей сайты, соцсети и сообщества, некоторые выдают себя за детей, чтобы обманом втянуть в разговоры и общение;
- Используют собранные о ребенке сведения, чтобы завязать с ним доверительные отношения, в ходе которых ребенок станет легче делиться с ними новой информацией о себе;
- Распространяют сексуально откровенные материалы и могут уговаривать ребенка делиться с ними его интимными фотографиями. Впоследствии преступники могут использовать фотографии ребенка для шантажа и угроз, чтобы встретиться лично или заставить ребенка присылать еще больше своих фотографий и видео;
- Фото и видео интимного характера у ребенка могут попросить и знакомые ему и его родителям люди.

Полезные советы

Если вы обнаружили, что кто-то начинает с вашим ребенком опасное общение, то вы можете предпринять следующие шаги:

1. Помогите ребенку сделать страницы в соцсетях закрытыми и изменить настройки конфиденциальности. В случае с детьми помладше сделайте это самостоятельно.
2. Договоритесь с ребенком о том, какие публикации разрешено делать на своей странице.
3. Посоветуйте ребенку удалить из друзей и подписчиков тех, с кем он лично не знаком. Если ребенок не уверен в том, стоит ли добавлять того или иного пользователя в друзья, то лучше этого не делать.
4. Разговаривайте с ребенком о том, что в случае неприятной или неловкой ситуации он всегда может к вам обратиться, и вы вместе разрешите ситуацию. Особенно важно, чтобы ребенку было комфортно говорить о неудобных вещах, которые вызывают у него сожаление или стыд.
5. Объясните ребенку, что непристойные сообщения или просьбы от незнакомцев необходимо блокировать и направлять жалобы на них в администрацию сайта или сервиса, а также сообщать родителям.
6. В случае обнаружения нежелательных контактов в соцсетях ребенка и склонения к действиям сексуального характера необходимо сообщить в полицию, прикладывая все имеющиеся доказательства: ссылки на аккаунты незнакомцев, скриншоты переписки и т.д.

ЗА РАСПРОСТРАНЕНИЕ ДЕТСКОЙ ПОРНОГРАФИИ, А ТАКЖЕ ЗА ДЕЙСТВИЯ СЕКСУАЛЬНОГО ХАРАКТЕРА В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ, ПРЕДУСМОТРЕНА УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ.

Личный пример

Объясните ребенку, что личными данными, а также некоторыми фото и видео изображениями не стоит делиться и со знакомыми людьми, и даже с друзьями. Расскажите о возможных последствиях таких действий. Любые подобные фото и видео изображения могут быть размещены в публичном доступе и нанести психический и эмоциональный вред ребенку. Поясните, что все, что попадает в Интернет, остается там навсегда.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ: необходимые средства защиты

Процветающий бизнес на каждом из нас

Современные технические средства очень сильно изменили виды мошенничества, которые используются злоумышленниками. Они могут, например, подделывать сайты, создать страницу абсолютно идентичную странице Интернет-магазина с нужным вам товаром, но при оплате деньги отправятся напрямую к мошенникам.

Самым распространенным способом мошенничества в Интернете является «фишинг». С его помощью мошенники выуживают у пользователя данные и потом используют их в своих целях. В Интернете существует огромное множество фишинговых сайтов. Они могут копировать страницу, например, известной соцсети. При попытке войти в свой профиль на таком сайте мошенники получат полный доступ к вашему аккаунту.

Они с лёгкостью подделывают любой номер телефона и не только его цифры, но даже могут сделать так, что при звонке ребёнок увидит надпись, например, «полиция», «мама», «брат» и т.п. Более половины россиян регулярно получают звонки от мошенников (по данным ВЦИОМ). Страшно? Есть способы остановить злоумышленников!

Ключевой вопрос

Как противостоять преступным действиям мошенников?

Внимание!

Современные мошенники активно используют социальную инженерию – психологические приемы, вынуждающие жертву сделать именно то, что нужно мошеннику, например перейти по ссылке, скачать вредоносный файл или сообщить код из СМС. По данным ВЦИОМ, 9% россиян теряли деньги в результате действий Интернет-мошенников, а 6% заявляли о краже крупных сумм.

За чем же охотятся цифровые мошенники?

- **Деньги;**
- **Персональные данные;**
- **Логины и пароли.**

Надо запомнить!

1. Для современных мошенников персональные данные являются не менее ценными, чем денежные средства, а иногда они даже полезнее. Именно с помощью персональных данных преступники отнимают у жертвы денежные средства, входя к ней в доверие. Кроме того, персональные данные сами по себе имеют ценность, ведь мошенники могут продавать их другим преступникам.
2. Кроме онлайн-мошенников существует другая, не менее опасная группа – телефонные мошенники. Они могут представиться кем угодно: сотрудником банка, полиции, прислать СМС от имени родственника. Они также используют социальную инженерию, пытаясь украсть данные. Иногда мошенники специально охотятся за голосом человека, например, задавая навязчивые вопросы. Их интересует то, как абонент назовет свои ФИО, а также скажет: «Да». В дальнейшем мошенники могут использовать записи голоса для входа в банковский аккаунт жертвы, голосом подтверждая банковские операции.
3. Еще одна опасность в Интернете – скрытые платные подписки. Многие мошенники или недобросовестные организации провоцируют пользователей на оформление подписок таким образом, что пользователь узнает об этом только тогда, когда обнаружит регулярное списание денег со своего счета. Такую скрытую подписку можно случайно оформить при переходе на сайт с пиратским контентом, при скачивании файла или приложения или при оплате какой-либо услуги в Интернете. Так, например, однократно купив что-либо или пожертвовав деньги, можно не заметить галочку, которая подтверждает ваше согласие на подписку. Иногда создатели сайта специально делают эту галочку едва различимой или даже вовсе скрытой с экрана. Будьте бдительны!

Полезные советы

Как защитить ребенка от мошенничества в Интернете?

1. В первую очередь следует научить ребенка перепроверять информацию. В случае с сайтами следует обращать внимание на адресную строку – нет ли в адресе сайта каких-либо изменений или неточностей. Если адрес отличается от настоящего даже на один символ – это явный признак подделки. Если входящий звонок поступает от представителя банка или другой структуры, следует самостоятельно перезвонить в эту организацию и задать им вопрос, есть ли у них такой сотрудник и мог ли он вам сейчас звонить. Чаще всего банки не осуществляют операции по звонкам. Однако следует учитывать, что мошенники могут целиком скопировать даже настоящий номер и представиться настоящим именем сотрудника.
2. Объясните ребенку, что не следует принимать поспешных решений. Мошенники могут требовать от жертвы принять решение в текущий момент. Они рассчитывают на то, что в спешке, панике или страхе человек утратит бдительность и охотнее согласится на перевод денег. В таком случае можно ответить: «Сейчас я все проверю и перезвоню вам», или «перезвоните мне через 5-10 минут, мне нужно время, чтобы подумать». Обычно этого времени хватает человеку, чтобы распознать мошенников, проверить информацию и не допустить ошибки.

3. Ребенка следует приучить беречь свои персональные данные с раннего возраста. Ребенок должен знать, что именно относится к персональным данным и что их нельзя размещать в Интернете без необходимости. Опасность представляют как сами данные, так и фотографии документов. Даже простое размещение номера телефона в социальной сети может привести к нежелательным звонкам, спаму, угрозам или шантажу.
4. Если у ребенка уже есть банковская карта, не следует хранить на ней много денег. Лучше всего класть деньги на карту тогда, когда он собирается что-то потратить или хранить на ней небольшое количество денег, которое не страшно будет потерять.
5. Не привязывайте телефон ребенка к банковским картам, счетам, платежным системам. Все платежи за ребенка лучше проводить самостоятельно.
6. Ограничивайте установку приложений на телефон ребенка. Наличие на телефоне антивируса и родительского контроля позволит защитить телефон от спама и вредоносных программ.
7. Установите ограничения и контроль на мобильном счете ребенка. Лимит расходов, можно установить в личном кабинете мобильного оператора. Там же можно отключить возможность оформления платных подписок и изменения тарифа.
8. Научите ребенка опасаться звонков с незнакомых номеров и не перезванивать на них. К любому звонку с неизвестного номера следует относиться с осторожностью. Если перезвонить на такой номер, вас могут перевести на линию, где за каждую минуту разговора с вашего счета будут списываться огромные деньги.
9. Объясните ребенку, что нельзя переходить по ссылкам из СМС и загружать файлы, которые пришли с неизвестного номера. Такой файл или ссылка могут установить на устройство вирус или отправить все данные владельца телефона прямо в руки к мошенникам.
10. Подключите ребенку защиту от нежелательных звонков. Такая функция есть у смартфонов на системах Android и iOS. Она позволит отфильтровать спам, звонки с опасных и нежелательных номеров.
11. Если ребенок уже стал жертвой мошенников, следует немедленно обратиться в полицию. Не забудьте сохранить все доказательства мошеннической деятельности – скриншоты сайтов, переписок, квитанции онлайн-платежей.

Личный пример

Установите на смартфоне ребенка надежный пароль, который он должен знать наизусть и ни с кем не делиться. Это обезопасит устройство при попадании в руки чужих людей, в том числе других детей.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт
ligainternet.ru

КЛИПОВОЕ МЫШЛЕНИЕ: ЦЕНА ДЛЯ ЛИЧНОСТИ

Небезопасные клипы

Клиповое мышление – тип мышления, заключающийся во фрагментарном восприятии информации. Люди с преобладающим клиповым мышлением склонны к восприятию информации отрывочно и порционно, небольшими кусками, при этом значительно страдает глубина понимания материала, а также критический подход к информации.

У современных подростков такой тип мышления преобладает. Его формированию активно способствует формат подачи информации в соцсетях, особенно короткие видео (в TikTok, YouTube).

Особенности клипового мышления:

- Фрагментарность;
- Яркость;
- Кратковременность;
- Нелогичность;
- Отрывочность;
- Разрозненность;
- Поддержание общения одновременно с несколькими собеседниками.

Ключевой вопрос: Как бороться с клиповым мышлением?

Внимание!

Основной причиной развития клипового мышления у детей и подростков является особенность преподнесения информации в Интернете. Информация в сети подается отрывочно, в виде коротких статей или видео. Ярким примером является чтение новостей «по заголовкам». В таком случае человек менее склонен сомневаться в информации и перепроверять ее.

Считается, что клиповое мышление преобладает у тех, кто большую часть свободного времени проводит в Интернете ввиду специфики подачи информации. В среднем, современные подростки в возрасте от 12 до 17 лет тратят на Интернет почти 6 часов в день (по данным Mediascope).

У современной молодежи по данным экспертов зафиксированы проблемы, связанные с чтением. При попытке прочитать и усвоить сложный текст, (например, инструкцию), многие подростки начинают испытывать резь в глазах и головную боль.

Что способствует формированию клипового мышления:

- Музыкальные клипы;
- Реклама на ТВ;
- Электронные СМИ;
- Мобильные средства связи;
- Социальные сети и мессенджеры, такие как TikTok, YouTube.

Развитие клипового мышления проводит к следующим проблемам:

- Внушаемость;
- Плохая обучаемость;
- Гиперактивность;
- Дефицит внимания;
- Предпочтение визуальных символов логике и углублению в текст;
- Неспособность к восприятию однородной информации (в т.ч. книжного текста);
- Снижение уровня грамотности у подростков и студентов;
- Вместо логических связей выстраиваются эмоциональные;
- Ослабляется или нивелируется чувство сопереживания, а также ответственности.

Полезные советы

- Контролируйте экранное время ребенка.
- Воспользуйтесь приложениями для тренировки памяти и внимания.

Личный пример

Организуйте «время без гаджетов» - по вечерам или по выходным дням, когда не только ребенок, но и вся семья сможет максимально отвлечься от телефонов, компьютера и Интернета.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт
ligainternet.ru

ВЕРБОВКА И ОТБОР ДЕТЕЙ В ДЕСТРУКТИВНЫЕ СООБЩЕСТВА В СОЦИАЛЬНЫХ СЕТЯХ

Реальность опасности для детей в сети

Социальные сети являются самым эффективным и широким по охвату инструментом, с помощью которого злоумышленники могут вербовать пользователей в разные преступные организации.

К опасным сообществам в социальных сетях относятся:

- Группы, пропагандирующие экстремистскую и нацистскую идеологию: террористические группировки, (в том числе движение «Колумбайн», признанное террористическим движением на основании решения Верховного суда РФ), шутеры, нацистские, неонацистские движения и др.
- Группы и каналы, пропагандирующие опасные увлечения: зацепинг, опасные квесты, группы с пропагандой наркотиков, трэш-стримеры, шок-контент и др.
- Группы, пропагандирующие причинение вреда себе или окружающим: селфхарм (буквально переводится как «вред себе»), пиплхейт (движение, пропагандирующее ненависть к людям), депрессивно-суицидальные группы («синий кит» и аналогичные), анорексию и др.
- Группы, пропагандирующие нетрадиционные духовно-нравственные ценности: оккультизм, сатанизм, чайлдфри, феминизм, нетрадиционные сексуальные отношения, смену пола, гендерную идентичность, зоофилию и пр.
- Аниме-сообщества. В отличие от традиционной японской культуры аниме, современные аниме могут быть очень опасны, поскольку нередко пропагандируют насилие, сексуальные извращения, каннибализм, убийства и самоубийства. По данным исследователей через «кровавое аниме» популяризуется даже скулшутинг. Аниме-продукция также является лидером по депрессивно-суицидальному контенту. По данным опроса экспертов из числа сотрудников подразделений по делам несовершеннолетних органов внутренних дел, многие несовершеннолетние, имевшие опыт суицидального поведения, увлекались данной субкультурой.

Ключевой вопрос

Как гарантировать безопасность ребёнка в опасной среде?

Внимание!

Ребенок должен знать об опасностях общения с незнакомцами в Интернете, а также доверять своим родителям.

Важно, чтобы в случае опасности, появления странных друзей или попытки втянуть ребенка в сомнительную деятельность, он, в первую очередь, обращался за помощью к родителям.

82% детей получают заявки в друзья от незнакомых людей, 29% детей получают заявки от незнакомых взрослых (по данным Лаборатории Касперского)

Деструктивные сообщества могут:

1. **Нанести непоправимый вред психическому и физическому здоровью ребенка. Могут быть опасны для жизни ребенка.**
2. **Сформировать нетрадиционные духовно-нравственные ценности, опасные взгляды и убеждения, основанные на насилии и мизантропии.**
3. **Заставить ребенка причинить вред себе или окружающим.**

В Интернете действует большое количество преступников, чьей целью является вовлечение все новых и новых пользователей в деятельность таких опасных сообществ. Такие лица называются «вербовщиками».

Чаще всего вербовка начинается с личного и очень навязчивого общения. Вербовщики пытаются завладеть всем вниманием и временем пользователя. Один из основных способов вербовки – маркетинговая «воронка вовлечения». Суть «воронки» заключается в том, что пользователь сначала привлекается в какую-либо группу по интересам, затем по активности в этих группах или комментариях, он отбирается и через личные сообщения приглашается в тематическое сообщество с более узкими интересами. После этого происходит отбор пользователя в закрытые группы и чаты, где уже происходит вовлечение в опасную и даже преступную деятельность сообществ. Особенностями таких групп может быть персональный доступ к ним только членам сообщества (особенно если общение происходит через мессенджеры). То есть родители или иное лицо не сможет попасть в группу, используя свои телефон или компьютер. После этого пользователи приступают к выполнению заданий в реальном мире.

Полезные советы

1. Спрашивайте или аккуратно проверяйте, с кем ведёт переписку ребёнок в личных сообщениях.
2. Обращайте внимание на поведение и новые интересы ребёнка: аниме, депрессивная литература, специализированные книги об оружии и стрельбе.
3. Замечайте изменения круга общения ребёнка, спрашивайте о его новых друзьях.
4. Обращайте внимание, если ребенок в реальной жизни выполняет задания, полученные в Интернете, так называемые, челленджи. Они могут содержать опасные для здоровья действия, например: сделать фото в экстремальных условиях или пробраться на закрытую территорию. Такие челленджи начинаются с простых и безобидных действий, а заканчиваются потенциальной угрозой для здоровья и жизни ребенка.
5. В случае обнаружения нежелательных контактов в соцсетях ребенка и потенциальной угрозе, необходимо сообщать в полицию, прикладывая все имеющиеся доказательства: ссылки на группы и сообщества, скриншоты переписки, ссылки на аккаунты преступников и т.д.

6. По возможности обеспечьте регистрацию ребенка в социальных сетях со своего компьютера или номера телефона, что позволит отслеживать его действия в Интернете. Следует помнить, что ребенок, вовлеченный в деструктивные сообщества, заводит второй (третий) аккаунт в социальных сетях, который держит в тайне от родителей.
7. Не стесняйтесь читать сообщения и переписку своего ребенка. Это не является нарушением его прав, но есть непременное условие обеспечения его безопасности. Не забывайте регулярно проверять в компьютере несовершеннолетнего историю его запросов и поиска в Интернете. В настройках браузера находится вкладка «История» («Закладки», «Загрузки», «Журнал»), где можно найти страницы недавних посещений ребенка. Если вы обнаружили, что ребенок регулярно стирает историю поиска, то это может быть тревожным знаком, требующим особого внимания.
8. Необходимо помнить, что первым этапом вовлечения ребенка в деструктивные сообщества является его отдаление от родителей и близких людей, провоцирование конфликтов между ними, культивирование претензий, ненависти и агрессии к родным и друзьям. Поэтому не всегда вызывающее и агрессивное поведение ребенка по отношению родителям является искренним желанием и осознанным поведением несовершеннолетнего, а лишь результатом манипуляции его сознанием со стороны преступников. Поэтому очень важно не ссориться с ребенком и не конфликтовать, а пытаться всегда оставлять возможность для диалога, искать подлинную причину его поведения и устранить ее. Старайтесь постоянно поддерживать своего ребенка.
9. Постарайтесь сдерживать внешние проявления бурных реакций на агрессивное и неконструктивное поведение ребенка или содержимое его переписки. Пытайтесь говорить с ребенком спокойно, без негативных эмоций объяснить ему недопустимость его поведения или почему тот или иной контент может представлять угрозу. Ребенок должен знать об опасностях общения с незнакомцами в Интернете, а также доверять своим родителям. Важно, чтобы в случае опасности, появления странных друзей или попытки втянуть ребенка в сомнительную деятельность, он, в первую очередь, обращался за помощью к родителям.
10. Поддерживайте контакты с друзьями и одноклассниками ребенка, а также их родителям, информация от которых может быть весьма полезной для общего понимания интересов, сложностей и проблем ребенка, а также для принятия своевременных мер.

Личный пример

Интересуйтесь (с определенной регулярностью!), на какие группы и сообщества в соцсетях подписан ребёнок.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

РЕАЛЬНЫЕ ПОСЛЕДСТВИЯ ВИРТУАЛЬНОЙ ЖИЗНИ:

О ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЯХ ПРОТИВОПРАВНОЙ АКТИВНОСТИ ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ

При общении в сети Интернет несовершеннолетнему нужно понимать, что публичные высказывания, нарушающие требования закона, могут повлечь серьезные последствия, вплоть до привлечения его к административной и уголовной ответственности.

Публичное высказывание на форуме или в социальной сети, оставленный под публикацией комментарий или суждения, фотографии и видеоролики, размещенные на открытых интернет-ресурсах, могут быть квалифицированы правоохранительными органами как административное правонарушение или преступление, если они содержат информацию, запрещенную для распространения на территории Российской Федерации.

За правонарушения и преступления несовершеннолетнего в виртуальных сетях, ответственность, как правило, выше, чем за такие же правонарушения без использования Интернета.

Повторное совершение подростком административного правонарушения влечет более строгую административную и даже уголовную ответственность.

Каждый подросток должен знать положения Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) и Уголовного кодекса Российской Федерации (УК РФ) так как незнание закона не освобождает от ответственности.

Подростки, достигшие 16-летнего возраста, могут быть привлечены к административной и уголовной ответственности за совершение с использованием Интернета, следующих видов правонарушений и преступлений.

За противоправные действия в сети Интернет против чести, достоинства, жизни и здоровья и конституционных прав личности (включая кибербуллинг: троллинг, издевательство, кибертравля, киберпреследование, раскрытие личной информации):

- **оскорбление**, то есть унижение чести и достоинства другого лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме, – по статье 5.61 КоАП;
- **угрозу убийством или причинением тяжкого вреда здоровью** – по статье 119 УК РФ;
- **клевету** – распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, в том числе, – по части 2 статьи 128.1 УК РФ;
- **доведение лица до самоубийства или до покушения на самоубийство** путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего, – по части 2 статьи 110 УК РФ;
- **склонение к совершению самоубийства** путем уговоров, предложений, подкупа, обмана или иным способом при отсутствии признаков доведения до самоубийства – по части 3 статьи 110.1 УК РФ;
- **содействие совершению самоубийства** советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению или обещанием скрыть средства или орудия совершения самоубийства – по части 3 статьи 110.1 УК РФ;
- **организацию деятельности, направленной на побуждение к совершению самоубийства** путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, – по части 2 статьи 110.2 УК РФ*;
- публичные действия, выражающие явное неуважение к обществу и совершенные в целях **оскорбления религиозных чувств верующих**, – по статье 148 УК РФ;
- **незаконное распространение в сети персональных данных человека без его согласия –** действия, направленные на раскрытие личных данных другого человека неопределенному кругу лиц, в том числе информации о его фамилии, имени, отчестве, годе и месте рождения, месте жительства и месте учебы, почтовом и электронном адресе, номере телефона, состоянии здоровья:
- **сбор, запись, передачу, в том числе распространение, предоставление, доступ персональных данных без согласия лица** – по частям 1, 2 статьи 13.11 КоАП РФ;
    - **незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну,** без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации – по части 1 статьи 137 УК РФ**;

---

* Лицо, добровольно прекратившее такую преступную деятельность и активно способствовавшее раскрытию и пресечению преступлений, предусмотренных статьями 110, 110.1, 110.2 УК РФ, освобождается от уголовной ответственности, если оно не совершило другого преступления.

** Исключение составляют случаи собирания или распространения таких сведений: 1) в государственных, общественных или иных публичных интересах; 2) если сведения о частной жизни гражданина ранее стали общедоступными: 3) если сведения о частной жизни гражданина были преданы огласке самим гражданином по его воле.

- **незаконное распространение информации о несовершеннолетнем,** пострадавшем в результате противоправных действий (бездействия), если эти действия (бездействие) не содержат уголовно наказуемого деяния, - по части 3 статьи 13.15 КоАП РФ;

- незаконное **распространение в сетях информации, указывающей на личность несовершеннолетнего** потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, а также распространение информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда его здоровью, психическое расстройство или иные тяжкие последствия, - по части 3 статьи 137 УК РФ.

Уголовная ответственность установлена также за **жестокое обращение с животным** в целях причинения ему боли или страданий, а равно из хулиганских побуждений или из корыстных побуждений, повлекшее его гибель или увечье, **совершенное с публичной демонстрацией таких действий, а также их фото- и видеоизображений в сети Интернет,** – по части 2 статьи 245 УК РФ***.

За распространение в сети Интернет фейковых новостей – заведомо недостоверной или заведомо ложной информации о социально значимых событиях:

- распространение **заведомо недостоверной** общественно значимой информации под видом достоверных сообщений, создавшее угрозу причинения вреда жизни или здоровью граждан, имуществу, угрозу массового нарушения общественного порядка или общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи (если эти действия не содержат уголовно наказуемого деяния) – по частям 9, 10 статьи 13.15 КоАП РФ;

- публичное распространение **заведомо ложной информации** об обстоятельствах, представляющих угрозу жизни и безопасности граждан, или о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств – по статье 207.1 УК РФ;

- публичное распространение под видом достоверных сообщений **заведомо ложной общественно значимой информации**, повлекшее по неосторожности причинение вреда здоровью человека, смерть человека или иные тяжкие последствия, - по частям 1, 2 статьи 207.2 УК РФ;

- публичное распространение под видом достоверных сообщений **заведомо ложной информации**, содержащей данные об использовании Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, а равно содержащей данные об исполнении государственными органами Российской Федерации своих полномочий за пределами территории Российской Федерации в указанных целях, - по статье 207.3 УК РФ.

***В настоящее время подготовлен законопроект, предусматривающий административную и уголовную ответственность за так называемые «треш-стримы» и иные общественно опасные действия по распространению в информационно-телекоммуникационных сетях, в том числе в сети Интернет, фото- или видеоматериалов с изображением деяний, совершенных с особой жестокостью либо издевательствами, в том числе с использованием фото- или видеоматериалов с участием несовершеннолетних.

За незаконное распространение в сети Интернет информации о потенциально опасных предметах и веществах:

- распространение сведений, содержащих **инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств**, незаконному изготовлению или переделке оружия, основных частей огнестрельного оружия, если эти действия не содержат признаков уголовно наказуемого деяния, - по части 5 ст. 13.15 КоАП РФ;

- распространение информации, содержащей **предложения о розничной продаже дистанционным способом алкогольной продукции**, спиртосодержащей пищевой продукции, этилового спирта, или спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции, - по части 8.ст. 13.15 КоАП РФ;

- **пропаганду наркотических средств, психотропных веществ или их прекурсоров**, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ – по части 1.1 статьи 6.13 КоАП РФ;

- **пропаганду закиси азота** – по статье 13.1 КоАП РФ;

- **склонение к потреблению наркотических средств, психотропных веществ или их аналогов –** по п. «д» части 2, частям 3, 4 статьи 230 УК РФ.

За преступления в сфере компьютерной информации:

- **неправомерный доступ к охраняемой законом компьютерной информации,** если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи - по статье 272 УК РФ;

- **создание, распространение или использование компьютерных программ либо иной компьютерной информации**, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - по статье 273 УК РФ.

За преступления против общественной нравственности с использованием сети Интернет (включая «секстинг» – склонение несовершеннолетних к пересылке личных фотографий, сообщений интимного содержания):

- **распространение, публичная демонстрация или рекламирование порнографических материалов или предметов** – по п. «б» части 3 статьи 242 УК РФ;

- **распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних,** – по п. «г» части 2 статьи 242.1 УК РФ.

За противоправные действия террористического и экстремистского характера, совершенные с использованием сети Интернет:

- **публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма** (то есть публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании) или **пропаганда терроризма** (то есть деятельность по распространению материалов или информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности) – по части 2 статьи 205.2 УК РФ;

- **заведомо ложное сообщение об акте терроризма**, то есть о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, совершенное из хулиганских побуждений либо в целях дестабилизации деятельности органов власти, - по статье 207.1 УК РФ;

- **массовое распространение экстремистских материалов,** включенных в опубликованный федеральный список экстремистских материалов******,** а равно их производство либо хранение в целях массового распространения, - по статье 20.29 КоАП РФ;

- действия, направленные на **возбуждение ненависти либо вражды**, а также на **унижение достоинства человека либо группы лиц** по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием СМИ либо информационно-телекоммуникационных сетей, включая сеть «Интернет», если эти действия не содержат уголовно наказуемого деяния - по статье 20.3.1. КоАП РФ;

- **повторное совершение указанных действий** после привлечения лица к административной ответственности за аналогичное деяние в течение одного года влечет уголовную ответственность - по ст. 282 УК РФ;

- **публичные призывы к осуществлению экстремисткой деятельности** – по части 2 статьи 280 УК РФ;

- **публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации,** - по части 2 статьи 280.1 УК РФ;

- **публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации** в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях, - по части 1 статьи 20.3.3 КоАП РФ;

******** См.: Экстремистские материалы: Министерство юстиции Российской Федерации (minjust.gov.ru) - https://minjust.gov.ru/ru/extremist-materials/

- те же действия, **совершенные лицом повторно** после привлечения к административной ответственности за аналогичное деяние в течение 1 года, либо повлекшие смерть по неосторожности или причинение вреда здоровью граждан, имуществу, массовые нарушения общественного порядка или общественной безопасности либо иные тяжкие последствия, - по частям 1, 2 статьи 280.3 УК РФ;

- **публичные призывы к осуществлению деятельности, направленной против безопасности Российской Федерации**, либо к воспрепятствованию исполнения органами власти и их должностными лицами своих полномочий по обеспечению безопасности Российской Федерации – по п «в» части 2 статьи 280.4 УК РФ;

- **пропаганда либо публичное демонстрирование нацистской атрибутики или символики,** либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами, если эти действия не содержат признаков уголовно наказуемого деяния, - по части 1 статьи 20.3 КоАП РФ;

- те же действия, **совершенные неоднократно** лицом, подвергнутым административному наказанию за указанное правонарушение, - по статье 282.4 УК РФ;

- **создание экстремистского сообщества, склонение, вербовка или иное вовлечение лица в деятельность экстремистского сообщества, в том числе с использованием сети Интернет, и участие в нем** – по статье 282.1 УК РФ*****;

- **организация деятельности общественного или религиозного объединения либо иной организации,** в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремисткой деятельности******, склонение, вербовка или иное вовлечение лица в деятельность экстремистской организации, **а также участие в деятельности такой организации** – по статье 282.2 УК РФ;

- **публичные призывы к развязыванию агрессивной войны** – по частям 1, 2 статьи 354 УК РФ;

- **реабилитация нацизма,** то есть отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, одобрение преступлений, установленных указанным приговором, а равно распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, совершенные публично, – по п. «в» части 2 статьи 354.1 УК РФ;

- **распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России,** связанных с защитой Отечества, а равно осквернение символов воинской славы России, оскорбление памяти защитников Отечества либо унижение чести и достоинства ветерана Великой Отечественной войны, совершенные публично, - по части 4 статьи 354.1 УК РФ.

***** Лицо, впервые совершившее преступления, предусмотренные статьями 282.1, 282.2 УК РФ, и добровольно прекратившее участие в деятельности экстремистского сообщества, освобождается от уголовной ответственности, если в его действиях не содержится иного состава преступления.

****** Международное молодежное движение «Колумбайн» и международное общественное движение АУЕ внесены по решению Верховного Суда РФ в национальную часть перечня террористических и экстремистских организаций. - См.: Перечень общественных объединений и религиозных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» :: Министерство юстиции Российской Федерации (minjust.gov.ru), https://minjust.gov.ru/ru/documents/7822/

КАЖДЫЙ ПОДРОСТОК ДОЛЖЕН ЗНАТЬ ПОЛОЖЕНИЯ КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ (КОАП РФ) И УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ (УК РФ) ТАК КАК

НЕЗНАНИЕ ЗАКОНА НЕ ОСВОБОЖДАЕТ ОТ ОТВЕТСТВЕННОСТИ.

НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига
безопасного
интернета

Сайт
ligainternet.ru

СЕМЕЙНОЕ СОГЛАШЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ГАДЖЕТОВ

Договариваемся о ценностях

Смартфон и ребенок: почему думающие родители составляют семейное соглашение об использовании цифровых устройств?

Каждый родитель должен помнить, что Интернет является потенциально опасной средой для ребенка. Доступ в сеть для несовершеннолетних сегодня никак не ограничивается. Отсутствуют возрастные ограничения, а те, что есть – легко обойти, отсутствует лимит на время использования Интернета или гаджетов. По данным исследования, проведенного Лабораторией Касперского, половина детей в России проводит в гаджетах до четырех часов в день, а 26% детей тратят на них все свободное время.

Ключевой вопрос:

Что можно включить в семейное соглашение об использовании гаджетов?

Неконтролируемый доступ к Интернету несет для детей и подростков большую опасность:

- Формируется цифровая зависимость.
- Возникают новые потребности: делать селфи, публиковать в Интернете все события из своей жизни, получать одобрение (в виде лайков или комментариев) от других пользователей.
- Ухудшается память и познавательные способности.
- Ухудшается социализация и навыки общения.
- Происходит задержка речевого развития.
- Сокращается общение с родителями и сверстниками, учащаются конфликты. По данным Лаборатории Касперского, 39% родителей признают, что из-за цифрового образа жизни детей в семье нередко случаются конфликты.
- Формирование доверия к цифровой среде приучает к добровольному предоставлению доступа к своим личным данным.

Как с этим бороться?

Несмотря на бурный рост цифровых технологий и их глубокое проникновение в жизнь человека, по мнению ученых, ребенку школьного возраста необходимо строго лимитировать время пользования гаджетами, а ребенку дошкольного возраста лучше и не пользоваться устройствами в развлекательных целях.

Ребенок может утверждать, что все его одноклассники или друзья активно пользуются гаджетами и используют их для игр или развлечений. Несмотря на это, ему следует объяснить правила безопасности в Интернете и заключить с ним семейное соглашение на использование гаджетов.

Семейное соглашение – это набор правил о том, как, когда и в каком количестве члены семьи могут использовать разнообразные цифровые устройства: смартфоны, планшеты, компьютеры, ноутбуки, телевизоры или игровые приставки.

Соглашение должно всесторонне охватывать все спорные моменты использования гаджетов и Интернета, как дома, так и в школе.

Полезные советы

Многие известные личности в цифровой среде сами ограничивают использование устройств и Интернета в своих семьях. Например Билл Гейтс, основатель Microsoft и создатель операционной системы Windows, ограничивал своим детям использование компьютера до 45 минут в будни и 1 часа 45 минут по выходным, а до 14 лет вообще запрещал им пользоваться устройствами.

Стив Джобс, основатель Apple, запрещал детям пользоваться гаджетами по ночам и в выходные дни, а также во время еды. То же относится и ко многим другим известным разработчикам и цифровым магнатам. Причина этого проста – эти люди, как никто другой, знают и понимают опасность цифровизации жизни, Интернет-зависимости и гаджетов, поэтому своих собственных детей они постарались оградить от этого.

Это важно!

- **В современных условиях семейное соглашение может помочь уберечь (оградить) ребенка от вредного воздействия Интернета.**
- **Соглашение должно соответствовать возрасту и потребностям ваших детей.**
- **Написание и подробное разъяснение такого соглашения поможет ребенку развить навыки критического мышления и самодисциплины.**
- **Со временем пункты соглашения можно пересмотреть и переписать.**

Примеры семейного соглашения:

СЕМЕЙНОЕ СОГЛАШЕНИЕ
об использовании устройств и Интернета.

Я, _____, согласен (-сна) со следующими правилами:

1. Я буду спрашивать у родителей разрешение перед тем, как взять телефон/планшет или поиграть в игру.
2. Я буду использовать телефон/планшет только в этих комнатах: _____ (например, кухня или гостиная).
3. Я не буду использовать гаджеты и выходить в Интернет во время еды.
4. В Интернете я буду общаться только с теми людьми, с которыми знаком лично.
5. В Интернете я буду общаться вежливо и использовать только приличные слова.
6. Я буду спрашивать разрешение у родителей перед тем, как опубликовать в Интернете фото или видео.
7. В школе я не буду доставать телефон и заходить в Интернет во время уроков.
8. Если что-то в Интернете меня напугает, разозлит или расстроит, я расскажу об этом родителям.
9. Когда закончится время для использования устройств, я перестану ими пользоваться и открывать социальные сети или игры.
10. Я не буду использовать устройства и выходить в сеть после _____ : _____

_____ ФИО _____ Подпись

СЕМЕЙНОЕ СОГЛАШЕНИЕ
об использовании устройств и Интернета.

1. Все члены семьи могут использовать смартфоны (за исключением телефонных разговоров) не более _____ часов в будние и не более _____ по выходным.
2. Все члены семьи не могут использовать гаджеты в этих комнатах: _____ _____ (например, спальня, кухня)
3. Все члены семьи не могут использовать гаджеты во время приема пищи.
4. Все члены семьи не могут использовать гаджеты во время совместного отдыха (просмотр фильма, прогулка, игра в настольные игры и т.п.).
5. Все члены семьи могут использовать устройства и Интернет только с _____ : _____ до _____ : _____.

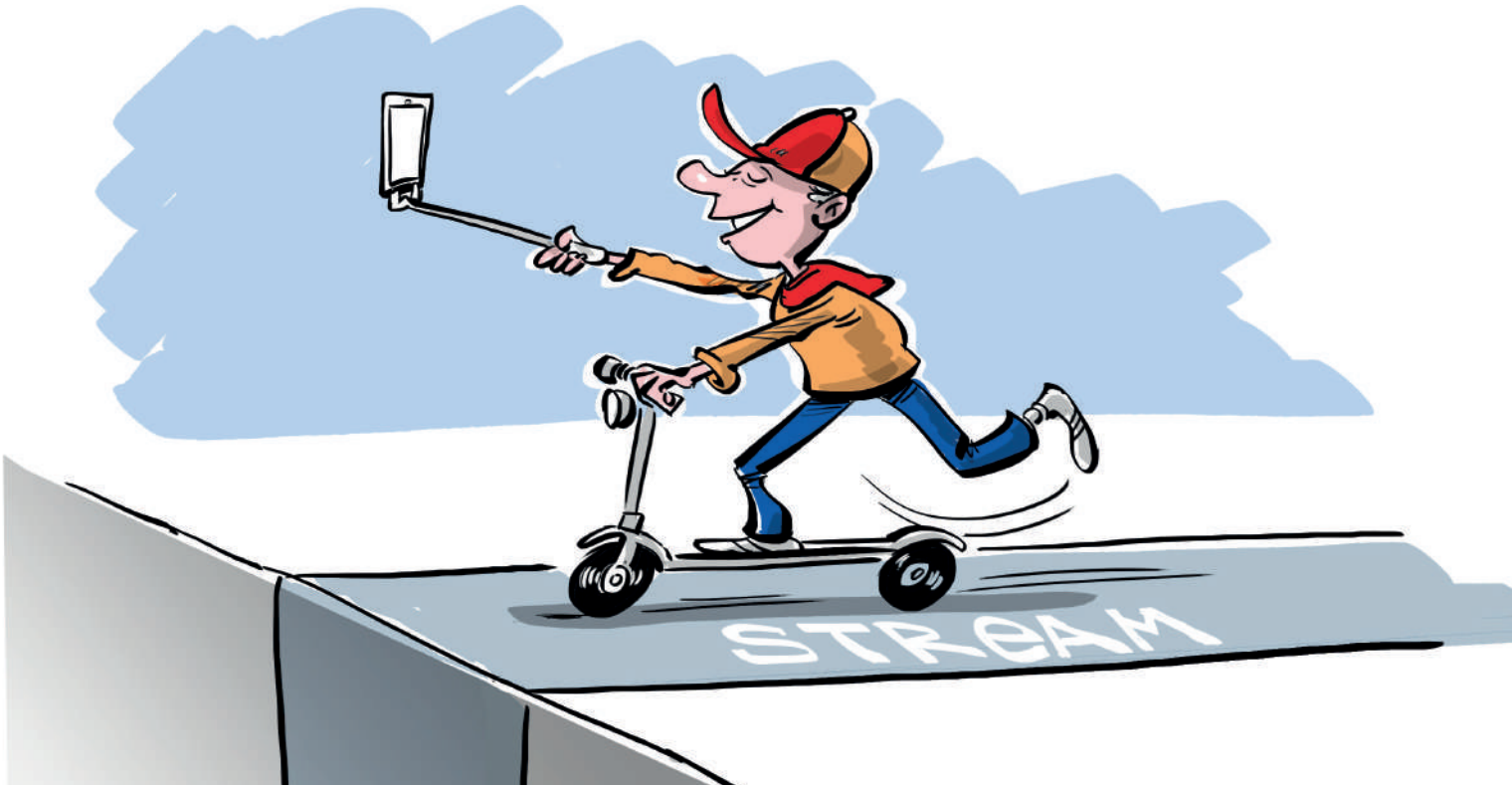
_____ ФИО _____ Подпись
_____ ФИО _____ Подпись
_____ ФИО _____ Подпись

ПРЯМЫЕ ТРАНСЛЯЦИИ

Прямые трансляции позволяют пользователям Интернета, в том числе детям и подросткам, снимать видео и транслировать его в режиме реального времени на широкую аудиторию. Функция прямых трансляций доступна во многих приложениях, социальных сетях, видеохостингах и даже на площадках для онлайн-игр. Трансляции дают возможность пользователям делиться своим творчеством с другими. Но важно помнить, что дети и подростки, транслируя видео онлайн, делятся им не только с друзьями.

Чем опасны прямые трансляции

- **В ходе просмотра любого видео, в том числе, трансляций, можно сделать скриншот**, а само видео можно записать и сохранить с помощью отдельных программ.
- **В зависимости от настроек конфиденциальности на конкретных платформах дети и подростки могут не знать кто в данный момент смотрит видео.** В итоге за детьми могут наблюдать другие взрослые.
- **Иллюзия приватности** (закрытости) онлайн-трансляции приводит к тому, что подростки показывают слишком большое количество личной информации. Даже если автор видео не называет своего настоящего имени, он может выдать свою личность или место жительства другими способами.
- **Во время трансляций, которые проводят дети и подростки, зрители могут оставлять комментарии,** в том числе, оскорбительного содержания, которые в дальнейшем могут привести к травле, преследованию, неуместным вопросам, разжиганию ненависти.
- **Лайки и комментарии к публикации или видеоролику существенно увеличивают охват публикации,** привлекают новых зрителей, и таким образом, видеоролик попадает в рекомендации видеохостинга или социальной сети. Зачастую, именно с целью получения популярности подростки снимают различные провокационные видеоролики.
- **Контент прямых трансляций практически не модерируется платформами.** Дети и подростки, которые смотрят такие трансляции либо записи этих прямых эфиров, могут столкнуться с любым непотребным контентом, с нецензурной лексикой, жестокостью, сценами насилия, откровенными сценами и иной деструктивной информацией.



Что должны сделать родители, чтобы обезопасить своих детей?

Узнайте больше о приложениях, сайтах, платформах и соцсетях, которыми пользуется ваш ребенок. К таким приложениям относятся: YouTube, Вконтакте, TikTok, Twitch, Discord. Просмотрите настройки конфиденциальности на этих ресурсах, проверьте наличие функции родительского контроля, обратите внимание на способы направления жалоб в службу поддержки на неприемлемый контент или поведение других пользователей.

Помогите ребенку настроить параметры конфиденциальности. Например, если сделать учетную запись закрытой, то ребенок сможет сам одобрять или отклонять подписчиков, ограничивать круг лиц, которые могут просматривать его контент и ограничивать входящие сообщения.

Объясните ребенку, что ему следует ограничить число подписчиков только теми, с кем он знаком в реальной жизни.

Нередко подростки могут проводить прямые трансляции в тайне от родителей. Например, ночью, в своей комнате, когда родители спят. Чтобы избежать этого, стоит подумать об ограничении использования Wi-Fi в ночное время.

О чем родители должны поговорить со своими детьми?

- **Расскажите детям о негативных последствиях,** к которым может привести неосторожное проведение прямых трансляций. В последствии удалить из Интернета какую-либо информацию о себе невозможно.
- **Объясните, что скриншоты и записи трансляций,** которые могут сделать другие пользователи, в будущем **могут быть использованы для шантажа, травли, оскорблений.**
- **Поддержите открытое общение со своим ребенком.** Важно, чтобы он знал и понимал, что всегда сможет прийти к вам за помощью.

Трэш-стримы

Особо опасной категорией онлайн-трансляций являются трэш-стримы. Трэш-стримы содержат контент, включающий в себя насилие, избиения, унижения, пытки, истязательства над людьми или животными.

Несмотря на очевидный аморальный и противоправный характер таких трансляций, до сих пор трэш-стримы присутствуют на многих платформах. Из-за преступной халатности и отсутствия модерации на площадках Twitch и YouTube, трэш-стримы не блокируют. Итогом этого становятся смерти участников в прямом эфире, первая из которых произошла в 2020 году во время трансляции на YouTube.

Ежедневно трэш-стримы смотрят более миллиона детей по всей России. Опасность таких трансляций, особенно для детей и подростков, заключается в следующем:

- **Трэш-стримы продвигают аморальное поведение,** ненависть к другим людям, в том числе среди детей и подростков;
- **Трэш-стримы пропагандируют жестокость и насилие;**
- **Трэш-стримы могут напугать и причинить необратимый вред психике ребенка;**
- **Могут привить ребенку ценности, основанные на насилии и жестокости;**
- **Ребенок может попытаться повторить увиденное в трансляции,** в том числе, опасное или насильственное действие. В результате может быть нанесен вред его здоровью или здоровью окружающих.

Если вы наткнулись в сети на подобный контент, необходимо отправить жалобу в МВД РФ или Прокуратуру РФ.

ПОИСКОВЫЕ СИСТЕМЫ

Поисковые системы, также известные как «поисковики» — это сайты и алгоритмы, предоставляющие пользователю быстрый доступ к необходимой информации при помощи поиска по обширной коллекции данных. С помощью поисковиков по запросу из ключевых слов пользователи находят нужные им сайты или контент.

С помощью поисковиков дети могут свободно находить интересные видео и игры. У них под рукой находится огромное количество веселого, информативного и образовательного контента. Однако нельзя забывать, что поисковая выдача содержит много неприемлемого, жестокого, аморального и недопустимого для просмотра материала.

Алгоритмы поисковых систем определяют, какие результаты каждый пользователь получает по своему запросу. **Отображение тех или иных сайтов зависит от множества факторов:** их популярности у других пользователей, индексации (включения в базу данных поисковика), местонахождения человека, данных с его устройства. **Первые позиции результатов по запросу занимают рекламируемые или продвигаемые сайты, либо информация.**

Именно дети часто с помощью «поисковиков» сталкиваются с различным непристойным и противоправным контентом: порнографическими материалами, сайтами по продаже наркотиков и иной информацией подобного характера. Несмотря на то, что по закону поисковые системы должны удалять такой контент и такие ресурсы из поисковой выдачи, зачастую этого не происходит, и поэтому дети сталкиваются с этим практически ежедневно при использовании сети Интернет.

Поисковые системы обладают собственной системой модерации, которая не всегда справляется с большим количество деструктивного контента, содержащегося на разных сайтах. По этой причине пользователи часто не получают по своему запросу необходимый результат, либо попадают на сайты, содержащие противоправный контент.

Отдельное внимание стоит уделить поисковым подсказкам. Когда пользователь вводит запрос в поисковике, он может увидеть похожие запросы, которые популярны у других пользователей. Эти подсказки также могут вести на сайты, содержащие деструктивный контент, а в некоторых случаях они и сами распространяют такой контент или дезинформацию.

Что могут сделать родители, чтобы защитить детей от опасного контента?

- **Используйте настройки фильтрации.** Они доступны во многих поисковых системах. Так вы сможете ограничить материалы, которые ваш ребенок найдет в Интернете. Данный способ не является надежным на все 100%, но он поможет вашему ребенку избежать взрослого контента или насилия.
- **Сами помогите ребенку найти в Интернете те материалы, которые ему интересны.** Старайтесь контролировать онлайн-активность ребенка.
- **Установите ограничения на количество времени, которое ваш ребенок проводит в сети.** В этом могут помочь различные приложения с функцией родительского контроля.

Что родители должны рассказать детям?

- **Объясните ребенку, что Интернет является публичным местом.** Среди миллиардов пользователей Интернета есть и те, кто выкладывает неприличный, опасный и даже противозаконный контент, который может навредить психике, а иногда повлечь и вред для здоровья. Объясните ребенку, что далеко не все, что опубликовано в Интернете, является достоверным и точным.
- **Объясните ребенку, что если он столкнется в сети с контентом, из-за которого почувствует себя некомфортно и неприятно, то он может абсолютно спокойно рассказать об этом вам, не опасаясь порицания и наказания.**

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

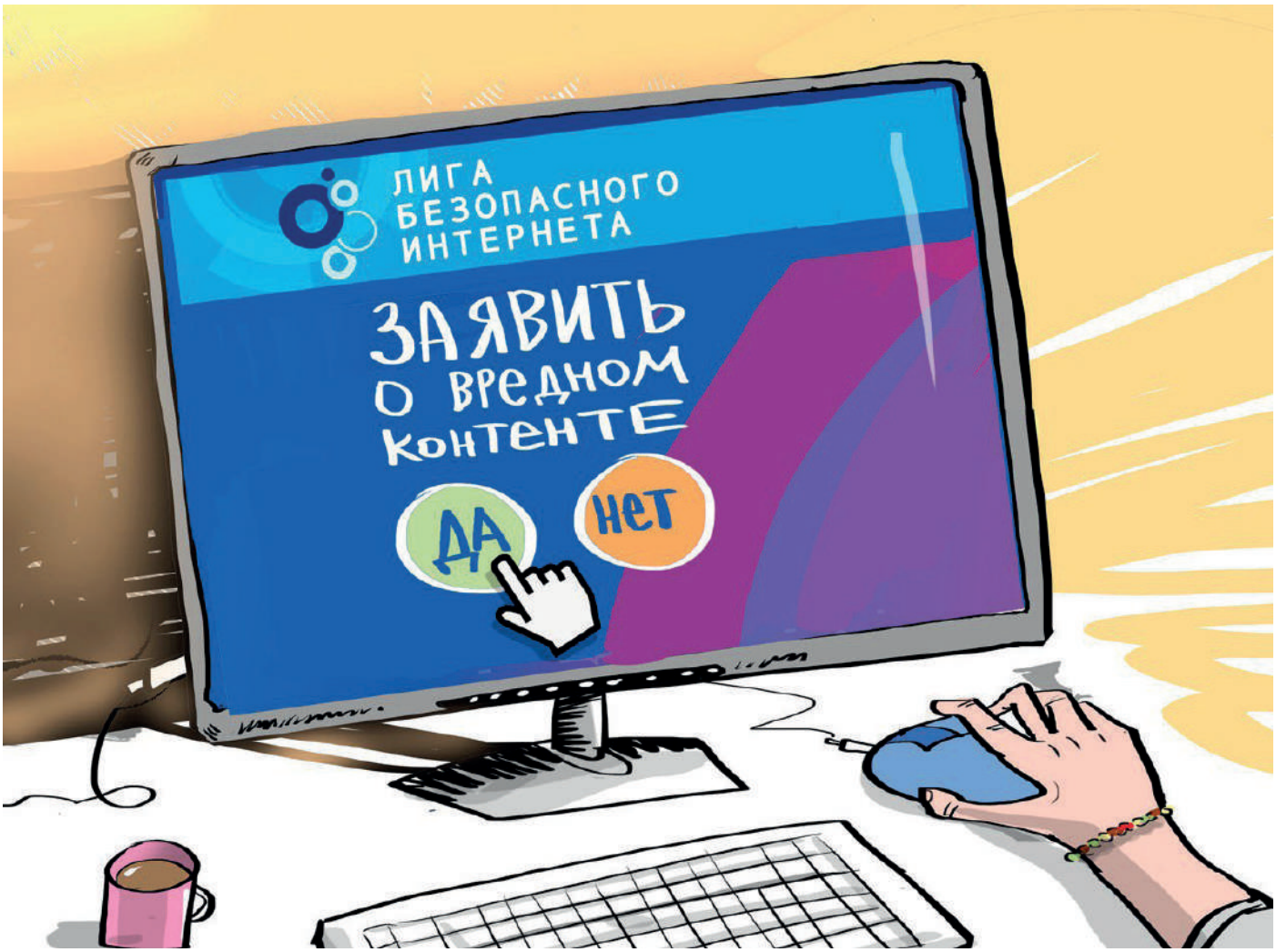
ОПАСНЫЕ ПУБЛИКАЦИИ В СОЦИАЛЬНОЙ СЕТИ: ПОЧЕМУ НЕЛЬЗЯ ПРОМОЛЧАТЬ!

Ваше право повлиять на Интернет

Многие из вас сталкиваются с опасным контентом в соцсетях. Такой контент может принимать самые разные формы. В опросе, проведенном ВЦИОМ, 32% опрошенных заявили о вреде, который Интернет приносит обществу, 35% согласились, что контент в Интернете может нести угрозу семейным ценностям, а 46% отметили, что Интернет значительно увеличивает число самоубийств.

> Здесь дана подробная инструкция по обращению в органы власти в связи с распространением деструктивного контента. Инструкция универсальна и применима ко всем социальным сетям. Направление обращений в органы власти — это ваше право по закону. **Никто не может вас в этом ограничить.**

В обращении указывается конкретная ссылка на аккаунт, группу, сообщество, чат или список таких ссылок. Желательно также прикладывать скриншоты самих публикаций, так как часто они бывают удалены/заблокированы/скрыты к моменту рассмотрения письма.



Ключевой вопрос:

Куда и к кому обращаться по поводу опасной информации в сети?

Внимание!

Вы установили факты распространения детской порнографии, призывов к суициду, рекламы азартных игр (онлайн-казино), склонения несовершеннолетних к противоправным действиям. По всем этим темам нужно обращаться в Роскомнадзор.

Сделать это можно двумя способами:

- **Первый:** если у вас есть аккаунт на госуслугах, то проще направить через приложение Роскомнадзора. Вы можете скачать его в магазине приложений как для Android, так и для Apple:

https://play.google.com/store/apps/details?id=org.rkn.ermp
https://apps.apple.com/us/app/ркн/id1511970611

В приложении необходимо приложить ссылку и скриншот опасной публикации. Здесь очень быстро можно отследить результат обращения, проверить был ли заблокирован тот или иной ресурс.

- **Второй:** если нет учетной записи на госуслугах, то можно направить через форму на официальном сайте Единого реестра запрещённых сайтов:

https://eais.rkn.gov.ru/feedback/

Здесь необходимо выбрать тему обращения, прикрепить ссылку и скриншот опасной публикации.

Надо знать!

Наркотики, экстремизм:

Если кто-то в видео или публикации пропагандирует наркотики, говорит об эффектах от их употребления или демонстрирует употребление, то нужно обращаться в Министерство внутренних дел Российской Федерации. Для этого на сайте МВД России необходимо выбрать Главное управление по контролю за оборотом наркотиков.

Также в МВД России необходимо обращаться, если вы столкнулись с информацией экстремистского характера, в том числе с контентом, посвященным скулшутингу (массовые расстрелы в школах). Для этого на сайте МВД России необходимо выбрать Главное управление по противодействию экстремизму.

Чаще всего это довольно агрессивные публикации с использованием нецензурной брани, где содержатся призывы убивать, громить, крушить, истреблять, использовать оружие, физическую силу, выходить на улицы для применения насилия, нападать на группы людей или социальные учреждения.

Форму для подачи заявления вы можете найти на официальном сайте МВД России:

https://мвд.рф/request_main

На сайте необходимо заполнить данные и вставить текст письма. В тексте необходимо добавить ссылку на публикацию и указать название соцсети и прикрепить скриншот.

ЛГБТ-пропаганда, видеоролики с насилием, жестокостью, истязанием людей или животных, пропаганда проституции и аморального образа жизни, информация, вызывающая у детей страх, ужас или панику, видео ненасильственных смертей и катастроф:

Подача заявления по такому контенту осуществляется на официальном сайте Генеральной Прокуратуры Российской Федерации:

https://epp.genproc.gov.ru/web/gprf/internet-reception

Введите текст обращения и прикрепите скриншот опасной публикации. Необходимо также добавить ссылку на публикацию и указать название социальной сети.

Также, обращения о фактах нарушения Российского законодательства в Интернете можно присылать Лиги безопасного Интернета: info@ligainternet.ru или передавать по горячей линии: 8 (800) 700-56-76. Лига безопасного Интернета перенаправляет все входящие обращения в соответствующее ведомство.

Не опускайте руки!

ВОПРОС: «Я направил/а обращение и получил/а ответ, в котором содержится отказ в рассмотрении или опасная информация не была обнаружена».

ОТВЕТ: Любой ответ, содержащий отказ в рассмотрении обращения, либо отказ в удалении противоправной информации, вы можете обжаловать в прокуратуре. Инструкция по обращению в прокуратуру дана выше. К письму необходимо приложить сканы/копии ответов с отказом.

Также вы можете такие ответы присылать нам, в Лигу безопасного интернета. В дальнейшем мы перенаправим их в Роскомнадзор, МВД или Генеральную прокуратуру и будем добиваться удаления информации.

Ответы вы можете присылать на почту info@ligainternet.ru с пометкой «Отказ». Если вы хотите публиковать ответы в комментариях, то не забывайте закрывать на скриншотах ваши персональные (личные) данные!

Личный пример

Чем больше обращений будет подано, тем быстрее социальные сети будут очищены от противоправного контента.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

КАК ГАРАНТИРОВАТЬ СВОЮ БЕЗОПАСНОСТЬ В СЕТИ

Сложное слово, простые правила

Кибербезопасность (компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Ваш цифровой след хорошо виден! О каждом пользователе Интернета ежедневно собирается и хранится огромное количество информации. В основном ее собирают социальные сети и мессенджеры. Делается это для того, чтобы как можно точнее идентифицировать каждого пользователя и показывать ему наиболее актуальную рекламу. Чем точнее реклама попадает в интересы и увлечения пользователя, тем больше шансов, что он поддастся на нее, купит товар или приобретет услугу. Однако вся эта информация может попасть в руки к мошенникам. По данным ВЦИОМ, 57% получают звонки от телефонных мошенников, 19% получают от них сообщения, а 9% россиян потеряли деньги в результате действий мошенников.

Ключевой вопрос: Как обеспечить кибербезопасность?

Внимание!

Мошенники могут испо льзовать ваши данные самыми разными способами:

- Продать их другим мошенникам;
- Втереться в доверие и использовать для вымогательства денег;
- Использовать для шантажа;
- Использовать для травли.

Полезные советы

1. **Следите за галочками** (разрешениями), которые ставите (даёте сайтам и приложениям). Иногда кнопка «Ок», появившаяся на экране, означает полный доступ к вашему микрофону, камере или телефонной книге. Таким же образом, вы можете неосторожно оформить подписку на ненужную вам услугу или установить ненужные, а иногда и опасные программы на компьютер. Будьте бдительны!
2. **Старайтесь не пользоваться бесплатными сервисами.** Большинство бесплатных сервисов и приложений, включая мессенджеры и VPN-плагины, могут предоставлять свои услуги на бесплатной основе. Если программа доступна бесплатно, следует задуматься, чем же зарабатывают ее разработчики. Как правило – это персональные данные пользователей программы, которые она ежедневно записывает и передает разработчикам. Те же, в свою очередь, продают их сторонним организациям.
3. **Помните,** что все ваши публикации в Интернете не только публичны, но и хранятся вечно. Помните! Любая приватность может быть нарушена, публикации могут стать доступны в случае утечки.
4. **Не публикуйте и не отправляйте материалы интимного характера.** Любая информация, которую вы выкладываете в Интернет, может стать поводом для шантажа, провокации, а в будущем может даже принести проблемы в карьере. Материалы интимного характера, даже в переписках, не удаляются из Интернета и могут быть использованы преступниками для изготовления порнографических материалов с целью последующей продажи или фальсификации компромата. Никогда не отправляйте фото и видео интимного характера даже самым близким людям, поскольку всегда существует вероятность утечки информации из-за неосторожности, взлома почты или аккаунта.
5. **На незнакомые сайты лучше даже не заходить.** Некоторые сайты способны самостоятельно устанавливать вредоносные программы и вирусы. Для этого даже не нужно ничего скачивать, достаточно просто зайти на сайт. То же относится к письмам и сообщениям, которые приходят из незнакомых источников.
6. **Ненадежные и сомнительные письма лучше не открывать** и уж тем более нельзя скачивать файлы, пришедшие от неизвестного отправителя в письмах или мессенджерах. Это относится даже к текстовым файлам. Например, файлы формата .pdf, в котором распространяется большинство документов, вполне способны распространять вирусы среди скачавших пользователей.

Личный пример

Не публикуйте в соцсетях лишнюю информацию о себе. Абсолютно вся информация, включая ваши фото, адреса, увлечения, имена домашних животных и многое другое, могут быть использованы мошенниками для установления личности, создания подробной картины о вас, как о пользователе, и подбора персональных мошеннических схем.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

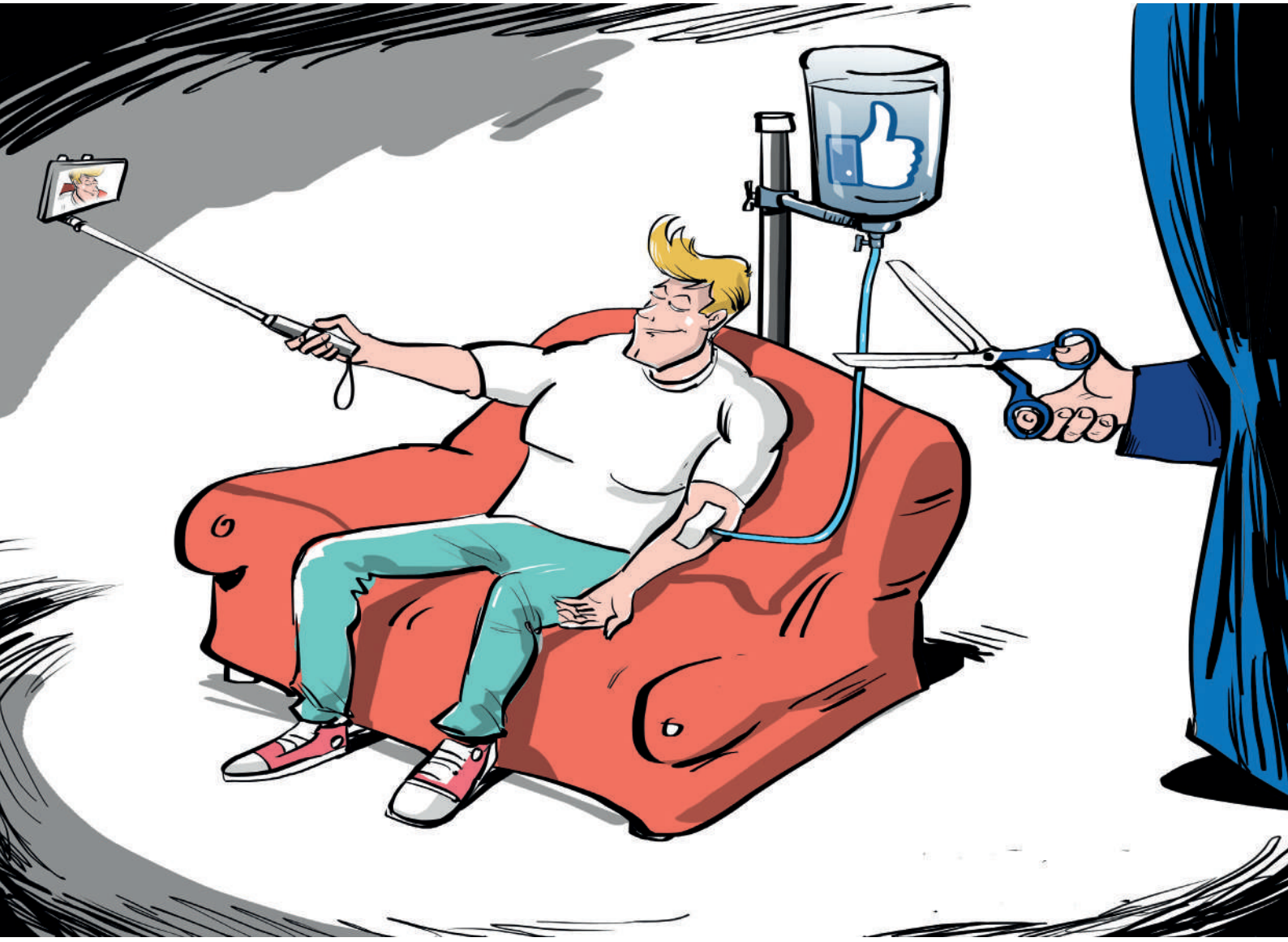
Лига безопасного интернета

Сайт ligainternet.ru

ВОЗДЕЙСТВИЕ ВИРТУАЛЬНОЙ ЖИЗНИ: ИЛЛЮЗИИ СОЦСЕТЕЙ

«Мультиреальность» как ценность и проблема

Современные дети и взрослые существуют одновременно в двух реальностях – реальной и виртуальной. Перенос частной жизни в виртуальное пространство приводит к тому, что цифровой мир не просто дополняет реальную жизнь, а становится ее полноценной частью. Это называют «мультиреальностью».



Ключевой вопрос

Какие существуют проблемы в «мультиреальности», как их минимизировать?

Внимание!

Виртуальная жизнь может целиком заменить реальную, люди пытаются переносить шаблоны и модели подведения из виртуального мира в реальный.

Признаки чрезмерного погружения человека в виртуальный мир:

- Если во время разговора или дискуссии в реальной жизни человек не может отстоять свою точку зрения, он попытается «забанить» (заблокировать) собеседника так, как сделал бы это в соцсети – уйти от разговора, перестать отвечать, игнорировать собеседника.

- Многие дети сегодня учатся пользоваться смартфонами и Интернетом еще до того, как научатся писать и читать. С самого раннего возраста они начинают поглощать огромное количество не самого качественного развлекательного контента. Каждый четвертый ребенок в возрасте от 0 до 12 месяцев использует Интернет. Более половины детей в возрасте до 3 лет используют Интернет каждый день. Это приводит к изменению умственного развития, ухудшению памяти и социальных навыков.

- Происходящее в социальных сетях представляет для детей больший интерес, чем собственные впечатлений в реальной жизни. Всё интересное, что происходит в жизни, необходимо фотографировать и выкладывать в соцсети. Например, достопримечательность на отдыхе необходимо сфотографировать и «запостить» в соцсети. Публикация для пользователя гораздо важнее, чем сама достопримечательность.

Преодолевайте иллюзии! Соцсети постоянно создают иллюзии, которым подвержено большинство пользователей. Эти иллюзии часто переносятся и в реальный мир:

Иллюзия недолговечности – большинство пользователей уверено, что все, что они выложили в сеть, будет жить несколько часов или дней. Но старые публикации никуда не пропадают, даже если их удалить. Они хранятся и формируют обширный цифровой след об авторе, их можно восстановить и использовать для шантажа или компромата. По данным Лаборатории Касперского, 22% детей выкладывали в Интернет информацию, о размещении которой в последствии жалели.

Иллюзия доброжелательности – авторы публикаций в социальных сетях ожидают видеть похвалу и одобрение в свой адрес. Несогласных или возмущенных людей можно просто «забанить», так они не смогут комментировать и даже просматривать публикации пользователя. Чем больше пользователь находится в плену этой иллюзии, тем меньше он готов к нападениям недоброжелателей и «троллей» в соцсети и тем сильнее будет травмирован в случае травли или агрессии. 30% детей, по данным Лаборатории Касперского, близко знакомы с травлей в социальных сетях – они либо сами были ей подвержены, либо становились очевидцами подобного.

Иллюзия ценности – многие пользователи уверены, что все, что они пишут и публикуют – нужно и полезно для остальных пользователей. В какой-то степени, это действительно так. Только вся эта информация нужна и полезна не для других пользователей, а для самой соцсети и ее разработчиков. Ведь чем больше информации о себе вы опубликуете, тем более точный портрет смогут собрать о вас алгоритмы соцсетей и тем более дорогую рекламу смогут вам показывать.

Полезные советы:

- **Не переносите поведение из социальных сетей в реальный мир!** Общение с собеседником лично совершенно не похоже на общение в чате.
- **Внимательно относитесь к тому, что публикуете!** Если вы не готовы столкнуться с критикой – лучше не публиковать. В Интернете много недоброжелателей.
- **Помните,** что любая информация в Интернете, фото, видео или сообщения могут быть восстановлены даже спустя много лет после удаления.
- **Общайтесь с людьми в реальности,** а не в социальных сетях. Чем меньше вы пользуетесь смартфоном, тем лучше!

Личный пример

Отключайте смартфон хотя бы на несколько часов в день. Цените время, которое вы проводите вместе с семьей, не тратьте его на социальные сети и приложения.

По данным исследования ВЦИОМ *(Всероссийский центр изучения общественного мнения)* **почти каждый третий (29%) пользователь соцсетей и мессенджеров в России тратит на них более 3 часов в день, а среди молодежи 18-24 лет эта цифра достигает 72%.**

По данным Лаборатории Касперского:

22% детей жалели
о том, что выкладывали в Интернет.

30% детей сталкивались с травлей в соцсетях –
подвергались ей либо видели травлю в отношении других.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

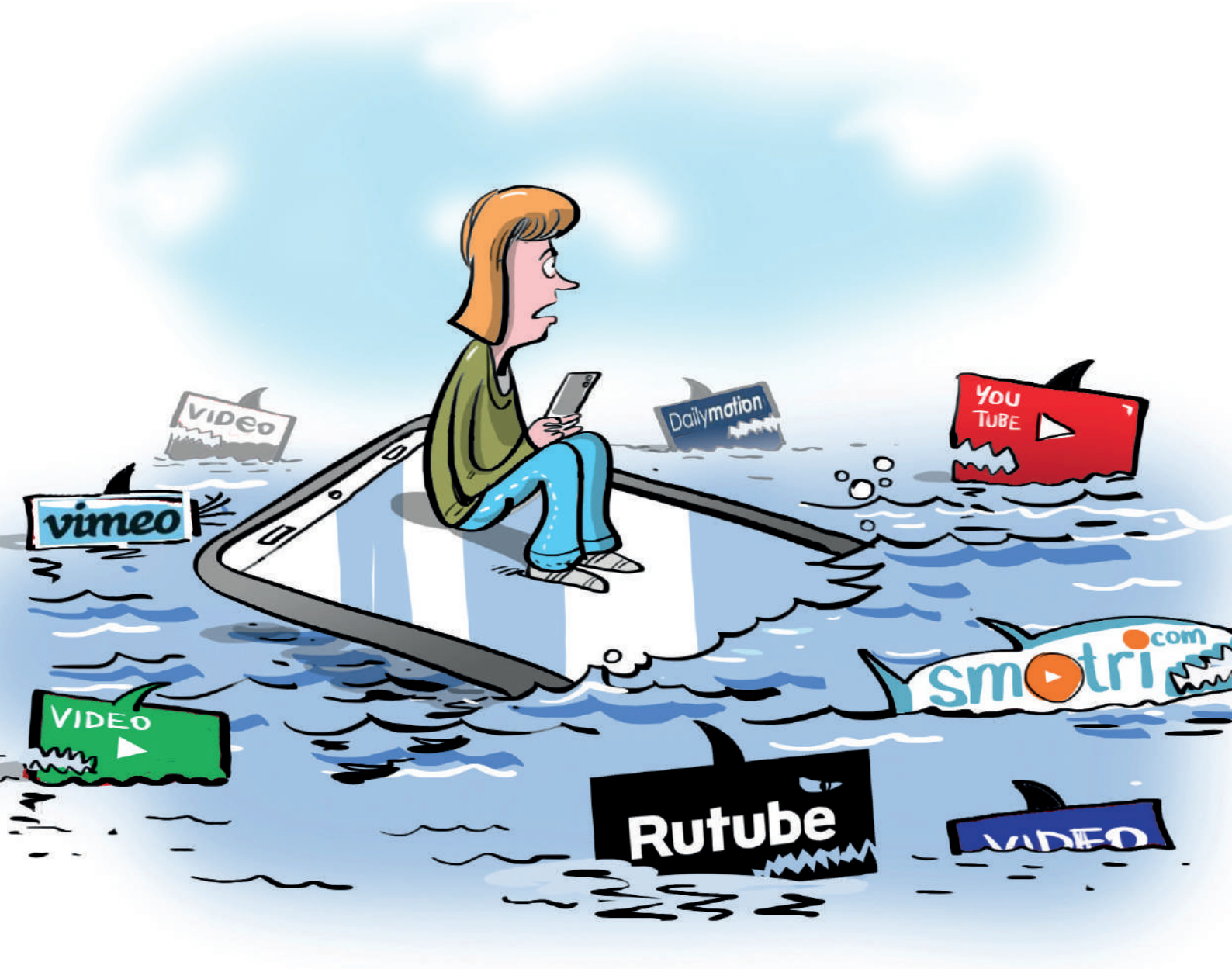
лига безопасного интернета

Сайт
ligainternet.ru

ВИДЕОХОСТИНГИ

Видеохостинги – специальные сайты, где пользователи могут загружать и просматривать видео, делиться ими со своими друзьями. С помощью видеохостингов любой пользователь, в том числе ребенок или подросток, получает доступ к огромному количеству разнообразного контента. Создатели видео учитывают интересы детей и размещают такие вирусные видео, которые дети будут смотреть снова и снова. Это формирует у детей и подростков настоящую зависимость.

Среди миллионов видео, которые ежедневно загружаются на видеохостинги, присутствует большое количество опасного, деструктивного и неприемлемого для детей и подростков контента. Зачастую дети получают к этому контенту доступ, несмотря на возрастные ограничения и опасное содержание таких видео.



Чем опасны видеохостинги?

- На многих сайтах обмена видео **нет возможности ограничить круг лиц**, которые могут смотреть видео, загруженные пользователем.

- Как и в случае с онлайн-трансляциями, в записанных видео **подростки могут случайно выдать личную информацию**. Например, названия школы может хватить, чтобы злоумышленники могли вычислить место жительства ребенка.

- Функция комментирования видео дает пользователям **возможность писать неуместные и оскорбительные сообщения**.

- Модерация некоторых видеохостингов (**YouTube, Twitch) не удаляет видеозаписи противоправного, деструктивного или экстремистского характера**: пропаганду наркотиков, ЛГБТ, экстремизма, опасных для жизни увлечений и т.п.

- Рекомендательные алгоритмы видеохостингов **показывают пользователю деструктивные и противоправные видео**, даже если пользователь не интересуется этой тематикой.

- Опасные видеоматериалы **делают детей агрессивными** и повышают риск возникновения психических расстройств.

- Видеохостинги **формируют зависимость от просмотра видео**, «затягивают» настолько сильно, что ребенок теряет счет времени и не может отличить реальную жизнь от виртуальной.

Самый популярный видеохостинг в России и в мире – «YouTube». Именно он представляет наибольшую опасность для жизни, здоровья и психики детей. **Опасный контент на YouTube не удаляется и намеренно продвигается среди детей и подростов в России.**

В 2021 году американские исследователи обнаружили, что рекомендательные алгоритмы YouTube предлагают пользователям видеоролики, которые нарушают собственные правила онлайн-площадки. Согласно данным эксперимента, подобные материалы составили 71% от общего количества просмотренных участниками исследования видео.

На YouTube неоднократно были случаи, когда после просмотра мультиков и подростковых программ про спорт и разные увлечения, рекомендательный алгоритм выдавал детям контент откровенно фейкового и антироссийского содержания со сценами насилия и жестокости. Об этом многие родители детей сообщали в Лигу безопасного Интернета.

Видеохостинг является одним из мест, где кибербуллинг происходит чаще всего – о таких случаях заявили 79% детей, пользующихся YouTube. В России данная статистика сочетается с крайне высокой уверенностью родителей в том, что их дети не подвергаются кибербуллингу.

При просмотре некоторых роликов на YouTube дети имеют все шансы столкнуться с опасными материалами, стать агрессивными, поддаться суицидальным мыслям, оказаться завербованными в экстремистские организации или попасть под «зомбирование западной пропаганды».

Что должны сделать родители, чтобы обезопасить своего ребенка?

- **Будьте в курсе**, на кого подписан ваш ребенок в видеохостингах.
- **Знайте, какую информацию содержат видео**, которыми ваш ребенок обменивается со своими сверстниками.
- **Проверяйте любимые видео вашего ребенка** и каналы, на которые он подписан. Так вы сможете понять, какие видео ваш ребенок смотрит на портале.
- **Проверяйте, можно ли на этом видеохостинге отправлять жалобы** на неуместный, оскорбительный и опасный контент.
- **Узнайте, как работает раздел комментариев** на этом сервисе. Так вы сможете понять, можно ли ограничить комментарии – проверять их перед публикацией или вовсе отключить.

Что родители должны обсудить со своими детьми?

- **Обязательно объясните ребенку,** какую информацию ему можно, а какую нельзя рассказывать и показывать в своих видео. Объясните, почему некоторые вещи нельзя публиковать на всеобщее обозрение.
- **Расскажите ребенку о необходимости настройки** и защиты конфиденциальности его аккаунта. Личные видео, не предназначенные для чужих глаз, лучше вовсе не публиковать.
- **Расскажите ребенку, что абсолютно всё,** что он публикует, в том числе и видео, так или иначе **попадает в публичный доступ,** где его могут увидеть не только друзья, но и вся школа, все родственники, друзья родственников, и даже родители одноклассников. Если ребенок сомневается, хочет ли он, чтобы все эти люди увидели его видео, то лучше его не публиковать.
- **Покажите и объясните ребенку, как на данном видеохостинге отправить жалобу в службу поддержки** на неприемлемые видео и оскорбительные комментарии.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

МАНИПУЛЯЦИИ В ИНТЕРНЕТЕ: ФЕЙКИ, ЛОЖЬ, НЕДОСТОВЕРНАЯ ИНФОРМАЦИЯ

Что такое «фейк»?

Проблема верифицированных источников информации сейчас стоит очень остро не только в России, но и во всем мире. Фейк – целенаправленно распространяемая ложная информация под видом достоверной. Может выражаться в самых разных формах, таких как: текстовые материалы, новостные статьи, аудио- и видеозаписи, передачи, а иногда и целые фильмы, снятые в документальном или псевдодокументальном жанре.

Ключевой вопрос:
Жизнь в век дезинформации.
Фейки и ложь в сети

Основным местом концентрации фейков является Интернет. Подобные материалы чаще всего распространяются через интернет-мессенджеры, а уже оттуда попадают в социальные сети или «желтые» средства массовой информации.

Фейки могут распространяться с самыми разными целями:

1. Ради шутки или создания повышенного внимания какому-либо событию.
2. Для увеличения посещаемости сайта («накручивания счетчика просмотров»). Создаются «громкие» заголовки-приманки, кликнув на который пользователи переходят на сайт и таким образом увеличивают трафик этого сайта.
3. С целью дезинформации читателей о реальной ситуации: изменения настроения в обществе, отношения людей к какому-либо вопросу, создания паники или волнения среди людей.

Внимание!

Самый распространенный формат фейков, с которым сталкивался практически каждый – **фейковые новости.** Миллионы людей, подвергаясь регулярному воздействию фейков, начинают верить ложной информации, что в перспективе приводит к негативным последствиям. Лишь 49% россиян, согласно опросу, проведенному ВЦИОМ, уверены, что смогут отличить фейк от настоящей новости.

С фейками в интернете сталкиваются не только взрослые, но и дети. Ребенок может увидеть заголовок на сайте, содержащий ложную информацию. Фейки могут целенаправленно рассылаться пользователям в мессенджерах или соцсетях. Кроме того, иногда происходят взломы официальных сайтов или страниц известных организаций. В таком случае злоумышленники могут рассылать ложную информацию от их лица.

Как правило, в информационном пространстве **фейки живут относительно недолго – 3-4 дня.** Для искусственного поддержания интереса к подобному материалу совершаются «вбросы» – ложная информация поступает в Интернет через специальные каналы, откуда распространяется в настоящие СМИ, либо же расходится по пользователям и распространяется с помощью пересылки друг другу.

Кроме фейков существуют и самые настоящие «ментальные вирусы». Ментальные вирусы – это какие-либо тексты, статьи или новости, а иногда аудио- или видеозаписи, содержащие в себе определенную идею. Как и настоящие вирусы, они способны заражать сознание людей и целого общества, внедряя вредную, опасную и разрушительную идею.

Источники опасности:

- **У каждого фейка есть конкретная цель** – могут провоцировать людей на совершение опрометчивых поступков.
- **С учетом специфики Интернета - очень большой охват аудитории, скорость распространения.**
- **Могут представлять угрозу жизни и здоровью людей.**
- **Инструмент манипуляции.** Создатели фейка могут управлять подвергнувшимся воздействию как организованной структурой.

Как распознать фейк?

1. Сообщение быстро распространяется в соцсетях или мессенджерах.
2. Сообщение очень эмоциональное, вместе с тем не содержит факты, которые возможно перепроверить.
3. Передаются сведения об угрозе жизни и здоровья большого числа людей, а также о наличии многочисленных жертв.
4. Присутствует указание на то, что власти скрывают информацию во избежание паники или волнений. Именно поэтому вы не найдете ничего в СМИ. Подчеркивается, что значимая для общества информация специально утаивается.
5. Присутствует просьба о максимальном распространении информации, либо о сокрытии (ведь автор сообщил ее вам «по секрету»).
6. Присутствует указание на лицо, сообщившее новость (врач больницы, водитель скорой, учитель школы, знакомый знакомого), либо информация о месте, где что-то произошло (номер больницы, название города, адрес школы).
7. Источник информации сложно установить.

При проверке информации есть ряд маркеров, на которые очень важно обратить внимание:

1. **Оригинал всегда лучше любого пересказа,** поэтому всегда важно искать оригинальный источник информации и задумываться на сколько этому источнику информации можно доверять. Не является ли, например, источником новости желтое СМИ или какая-то из «тизерных» сеток, которые занимаются привлечением трафика пользователей с помощью «кликбейтных», то есть громких заголовков.
2. **При работе с оригинальными источниками важно смотреть взаимосвязь между этими источниками информации.** Если информация опубликована в разных источниках, то как они сами между собой связаны. Не является ли это партнерской сетью ресурсов или единой сетью распространения информации.
3. **Чаще всего разнообразие фейковых сообщений очень низкое,** постоянно публикуется фактически одно и то же сообщение. Практически все фейки являются перепостами.
4. **При сравнении оригинальной настоящей новости и фейка, у настоящей новости всегда очень много свидетелей,** очень много участников, они по-разному рассказывают своими словами о том, что произошло. Настоящая новость имеет очень много серьезных верифицированных источников информации. Сейчас ни одна заслуживающая внимания новость не проходит мимо ведущих средств массовой информации.
5. **Очень важно обратить внимание на контекст новости** и проверять полную суть любой цитаты, которая используется в том или ином сообщении. Не стоит доверять ссылкам на громкие и авторитетные имена. Проверять нужно как цитаты, так и факты, кому бы они не принадлежали, какая бы известная фамилия ни была озвучена.
6. **Очень важно обращать внимание на суть, смысл самого материала,** а не на мелкие детали, которых очень много в фейках. Они, таким образом, отвлекают внимание от содержания, придавая некую достоверность материалу.
7. **В новой информационной реальности важно научиться доверять серьезным средствам массовой информации, официальным источникам,** которые дорожат своей репутацией и ответственно относятся к распространению новых сведений и данных.

Полезные советы

Если вы получили или обнаружили недостоверную информацию, есть простые шаги, с помощью которых можно защитить себя, своих друзей и родственников от массового распространения этого сообщения:

1. **Стоит дождаться официального подтверждения или опровержения** громкой новости, прежде чем пересылать что-то друзьям и знакомым.
2. **Обратитесь в службу поддержки** и направьте туда все имеющиеся у вас ссылки, скриншоты и т.д.
3. **Обратитесь в полицию, Роскомнадзор** и прикрепите ссылки и скриншоты страниц, содержащих недостоверную информацию.
4. **Если вы считаете, что сообщение или публикация является общественно опасной, вы можете прислать скриншот и ссылку в Лигу безопасного Интернета по адресу: info@ligainternet.ru или в сообщениях VK: vk.com/liga.**

Внимание!

В случае обнаружения фейковой информации не стесняйтесь и пользуйтесь кнопкой «Пожаловаться» (в случае с социальными сетями или мессенджерами). Мессенджеры и соцсети должны оперативно блокировать такие сообщения и публикации.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

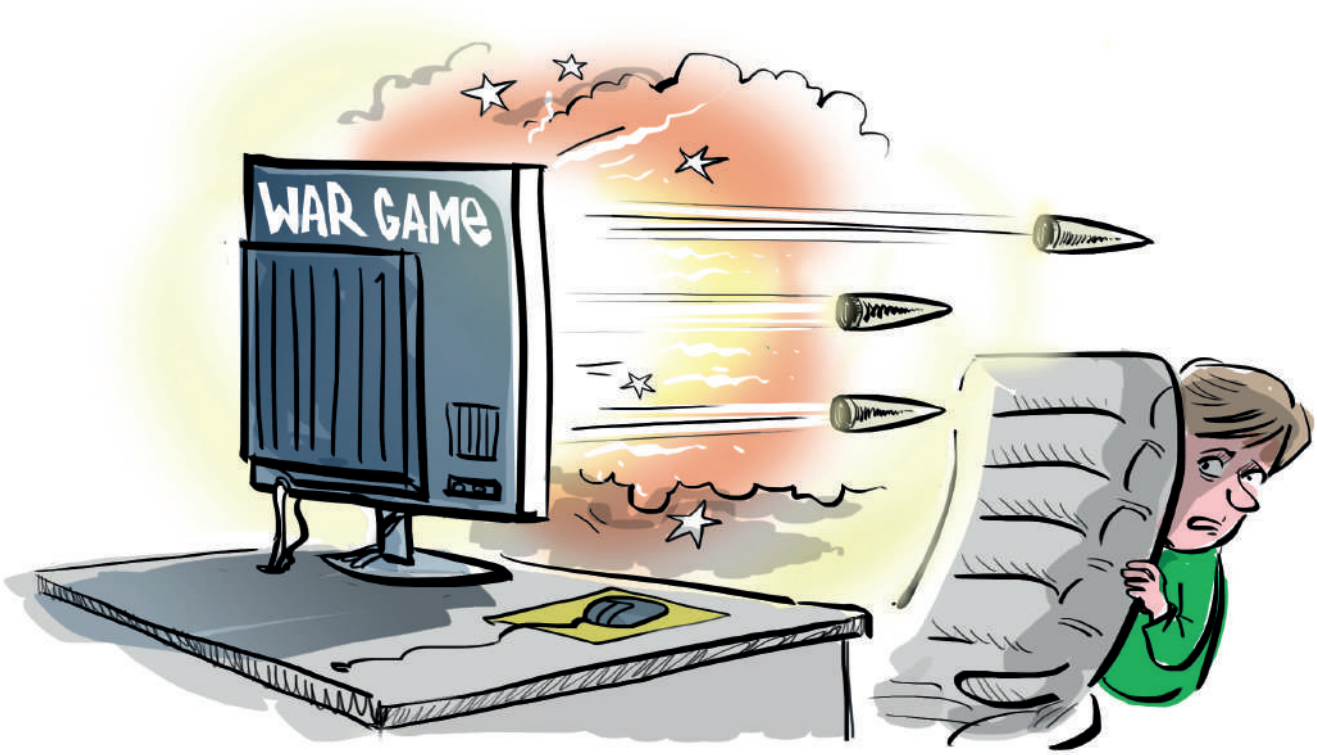
Сайт ligainternet.ru

ОНЛАЙН-ИГРЫ

Онлайн-игра – компьютерная игра, главной особенностью которой является необходимость постоянного подключения к сети Интернет. Число игроков в самых популярных онлайн-играх может достигать сотен тысяч пользователей.

Для достижения высокого результата в игре пользователям необходимо взаимодействовать между собой. Для этого используются: внутриигровой форум, чат, голосовое общение. Эта особенность онлайн-игр делает их очень популярными среди детей и подростков, но далеко не каждая игра может подойти ребенку по возрасту.

Многие родители не задумываются в какие игры играют их дети, и не контролируют соблюдение возрастных ограничений, не проверяют с кем они общаются в играх, сутками проводя время за компьютером.



Какие опасности есть в онлайн-играх?

Жестокие сюжеты – некоторые компьютерные игры, особенно в жанре «стрелялки от первого лица», пропагандируют жестокость и насилие. Видеоигры указанного жанра, изначально разработанные для тренировки сотрудников служб специального назначения для выработки оптимального поведения в экстремальной ситуации, вызывают повышенный интерес у детей и нередко случается, что ребенок хочет повторить сценарий такой игры в реальности. Многие эксперты отмечают, что подростки, планировавшие вооруженные нападения на образовательные учреждения, почти все свое свободное время проводили в онлайн-играх подобного жанра.

Дети и подростки во внутриигровых чатах, в специализированных приложениях, а также в чатах стриминговых платформ, где обсуждаются онлайн игры (таких как Twitch, Discord) общаются с совершенно незнакомыми людьми и могут стать жертвой агрессии, травли и неприемлемого общения со стороны незнакомых взрослых игроков.

Во внутриигровых чатах незнакомые взрослые могут отправить ребенку ссылки на мошеннические ресурсы, частные сервера или закрытые группы в соцсетях.

Общение в игровых чатах практически невозможно отследить и контролировать. Этим пользуются провокаторы и преступники, которые ищут в игровых сообществах детей и подростков, поддающихся внушению, и заманивают их в свои преступные схемы.

Многие современные онлайн-игры позволяют создать свой собственный «сервер», в котором можно реализовать любую идею: воссоздать любую точку на земном шаре, либо создать симуляцию боевых действий, причем такой хостинг может находиться в любой точки земного шара. Управляется такой сервер только администратором (модератором), доступ предоставляется исключительно по рассылаемым пользователям ссылкам-приглашениям (инвайтам).

Администратор такой закрытой платформы, обладая полными правами, распределяет роли, придумывает названия и символику, вводит систему рангов. Для достижения нового ранга может устанавливать условия в виде специальных квестов: «убить определенное количество персонажей другой фракции, похитить их ценности на определенную сумму и т.д.». При выборе названий, с учетом закрытости платформы, администратор может использовать в качестве названий наименования запрещенных в Российской Федерации террористических группировок: «ИГИЛ», «Аль-Каида», «Боко Храм» и другие.

Все действия вроде бы совершаются в игровой манере, но параллельно они отпечатываются в сознании ребенка. Подросток радуется тому, что достиг нового ранга в игре, а на самом деле он даже не догадывается, что может быть вовлечен в серьезное преступное сообщество.

Некоторые игры используют GPS и постоянно собирают информацию о местоположении игрока. А это значит, что и другие участники игрового сообщества могут узнать, где находится ребенок в данный момент.

Что должны сделать родители, чтобы обезопасить детей?

1. **Изучите онлайн-игры, в которые играет ваш ребенок.** Поищите в Интернете информацию об игре, найдите ее официальный сайт, ознакомьтесь со скриншотами и видео из игры. Обратите внимание, подходит ли игра по возрасту для вашего ребенка. **Обязательно обратите внимание на следующее:**
   - Есть ли в игре модерация? Модераторы – это пользователи, которые следят за тем, чтобы игроки не нарушали установленных правил, будь то правил для общения между игроками или правил самой игры.
   - Содержит ли игра материалы откровенно сексуального или насильственного характера?
   - Есть ли в игре чат с другими игроками? Можно ли его отключить?
   - Существуют ли дополнительные настройки, которые можно отключить или включить для большей безопасности ребенка в игре?
2. **Ознакомьтесь с правилами поведения в игре, а также внутриигровых чатов.** Можете ли вы сообщить о каких-либо неуместных действиях, пожаловаться на оскорбительное поведение других игроков?
3. **Помогите ребенку создать логин и пароль.** Родителям следует внимательно следить и контролировать действия детей в сети.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

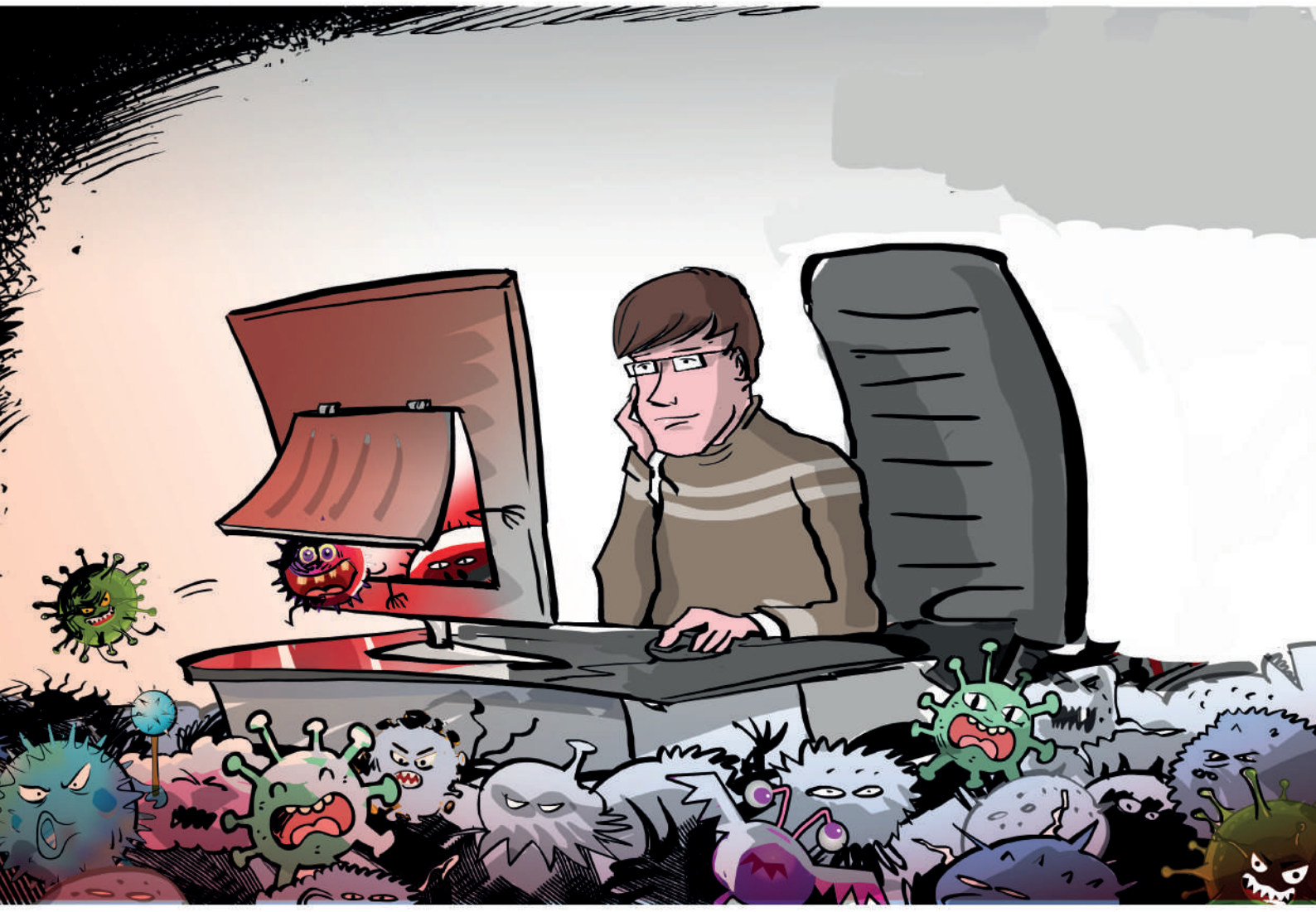
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

КИБЕРУГРОЗЫ: ЗНАНИЕ О ФАКТОРАХ ОПАСНОСТИ – ВАША БЕЗОПАСНОСТЬ!

Ключ в виртуальный мир

Современный смартфон – полноценный персональный компьютер. Он обладает всеми теми же функциями, что и домашний компьютер или ноутбук, а в чем-то даже их превосходит. В отличие от домашнего компьютера смартфон имеет постоянный доступ в Интернет, он работает 24 часа в сутки, имеет продвинутую камеру и микрофон, а также датчики движений, что позволяет ему круглосуточно записывать всю информацию о своем пользователе. Так, смартфон является нашим ключом в виртуальную реальность.



Ключевой вопрос

Как сделать свой смартфон безопасным?

Источники проблемы

- **Огромное количество навязчивой рекламы** – сайты, приложения, соцсети и игры – все это содержит огромное количество рекламы, на которой зарабатывают их разработчики. По данным Всероссийского центра изучения общественного мнения 29% россиян получают спам ежедневно.
- **Информационный шум** – в цифровом мире множество неконтролируемых уведомлений, которые приходят на телефон практически ежеминутно. Большинство пользователей не хотят тратить время на их отключение и удаление. А они содержат часто совсем ненужные рекламные предложения, приманки и являются способом вымогательства денег пользователя.
- **Установка нежелательного и вредоносного программного обеспечения** – при переходе по новой ссылке, скачивании файлов, установке приложений (даже из проверенных источников!) существует вероятность установки вирусов, шпионских или рекламных программ. Опасность могут представлять даже приложения, скачанные из официальных магазинов смартфонов. По данным ВЦИОМ, лишь 16% родителей устанавливают на устройство их ребенка антивирус.
- **Утечка персональных данных владельца** – все, что содержится в смартфоне, начиная от логинов и паролей, заканчивая фотографиями, банковскими реквизитами и даже перепиской, может не только попасть в руки к мошенникам, но и стать достоянием общественности.

Внимание!

Чем активнее используется устройство, тем больше данных о своем владельце оно накапливает. К таким данным относятся не только ваши фото, видео, переписки, но и такие данные, как:

- история установки и использования приложений;
- история энергопотребления, то есть циклов и времени зарядки, интенсивности работы;
- история уведомлений и действий;
- история магазина приложений;
- история браузера;
- история перемещений по городу и многое другое.

Надо знать!

Вредоносные приложения на смартфонах пытаются заработать на пользователе – вытянуть деньги, внимание пользователя, показывая ему рекламу или перенаправляя на сайты, украсть персональные данные или профиль пользователя, передать мошенникам доступ к самому устройству.

Вредоносные приложения бывают разными:

- **Фальшивые приложения** – копия настоящих приложений, как правило, банковских или приложений мобильных операторов. Их задача – полностью замаскировавшись под настоящее приложение, украсть у пользователя данные от личного кабинета и получить доступ к мобильному или банковскому счету.
- **Приложения-вымогатели** – блокируют устройство и требуют перечисление денег за разблокировку.
- **Денежные «пиявки»** – программы со скрытой подпиской. Однажды купив подобную программу или совершив покупку с её помощью, можно обнаружить, что она оформила «полноценную» подписку и деньги теперь списываются регулярно. Как правило, всегда можно отказаться от «денежной пиявки» и отменить такую подписку. Следите за своими расходами в сети.

Информация к размышлению

Вредоносные программы можно разделить на две большие категории:

- **Вирусы** – вредоносные программы, которые напрямую вредят устройству, установленным программам. Распространяются по Интернету и заражают устройства.
- **Трояны** – маскируются под настоящие программы, а иногда даже могут выполнять некоторые полезные функции. Похищают данные пользователя, рассылают спам, создают трафик на сайты.

Как вирусы попадают на устройство?

- **Из зараженного электронного письма** или файла, приложенного к письму – нельзя открывать письма, пришедшие из неизвестных источников, а особенно скачивать и запускать файлы, прикрепленные к этим письмам. Вирусы могут распространяться даже через текстовые файлы, например в формате .pdf.
- **Через зараженный сайт** – многие сайты способны самостоятельно устанавливать на компьютеры вирусы. Для этого бывает достаточно просто открыть страницу. Это особенно актуально для нелегальных сайтов, например, с пиратским контентом.
- **Через установку неизвестных приложений** с неизвестного сайта – если вы скачиваете что-либо из Интернета, убедитесь, что источник надежен. Программы лучше скачивать с официальных сайтов разработчиков этих программ.

Как защитить себя от киберугроз:

- **Не открывайте письма и сообщения от незнакомых отправителей;**
- **Не скачивайте пиратский контент;**
- **Внимательно проверяйте адреса веб-сайтов**, которые вы посещаете;
- **Не устанавливайте на телефон или компьютер, приложение из непроверенного источника;**
- **Не давайте приложениям разрешения, которые не нужны им для работы** – приложению «калькулятор» не нужен доступ к микрофону смартфона;
- **Следите за своими расходами в сети** и за тем, какие подписки оформляют приложения;
- **В настройках телефона отключите уведомления** от приложений, которые вы не хотите получать;
- **Установите на компьютер и телефон антивирус;**
- **Храните на телефоне как можно меньше информации о себе.** Так вы защититесь от утечки данных;
- **Подключите на телефоне функцию защиты от спама**. На некоторых устройствах она доступна в настройках или ее можно подключить у мобильного оператора.

Личный пример

Не открывайте MMS и сообщения, присланные с незнакомых номеров!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru