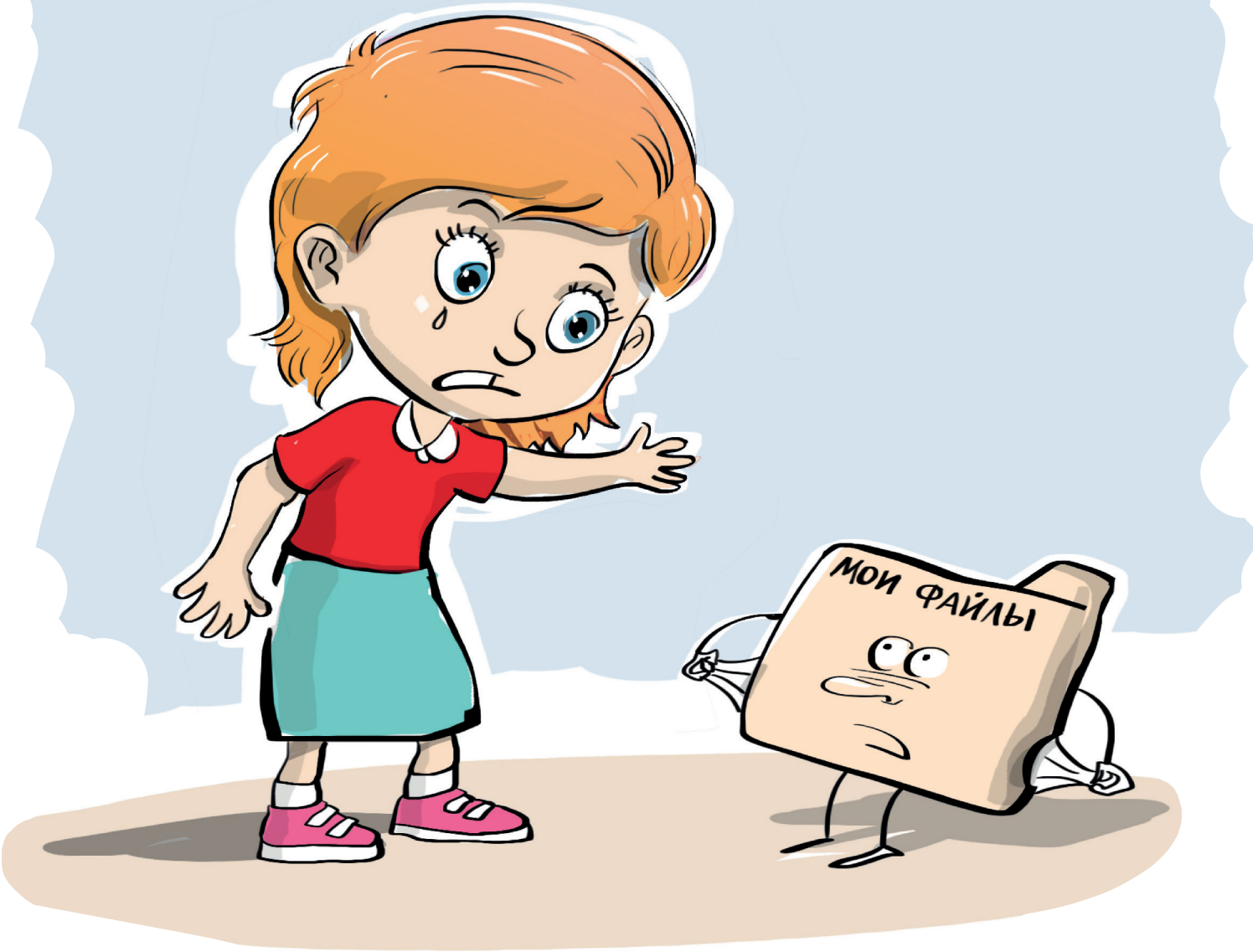
ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ



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.**

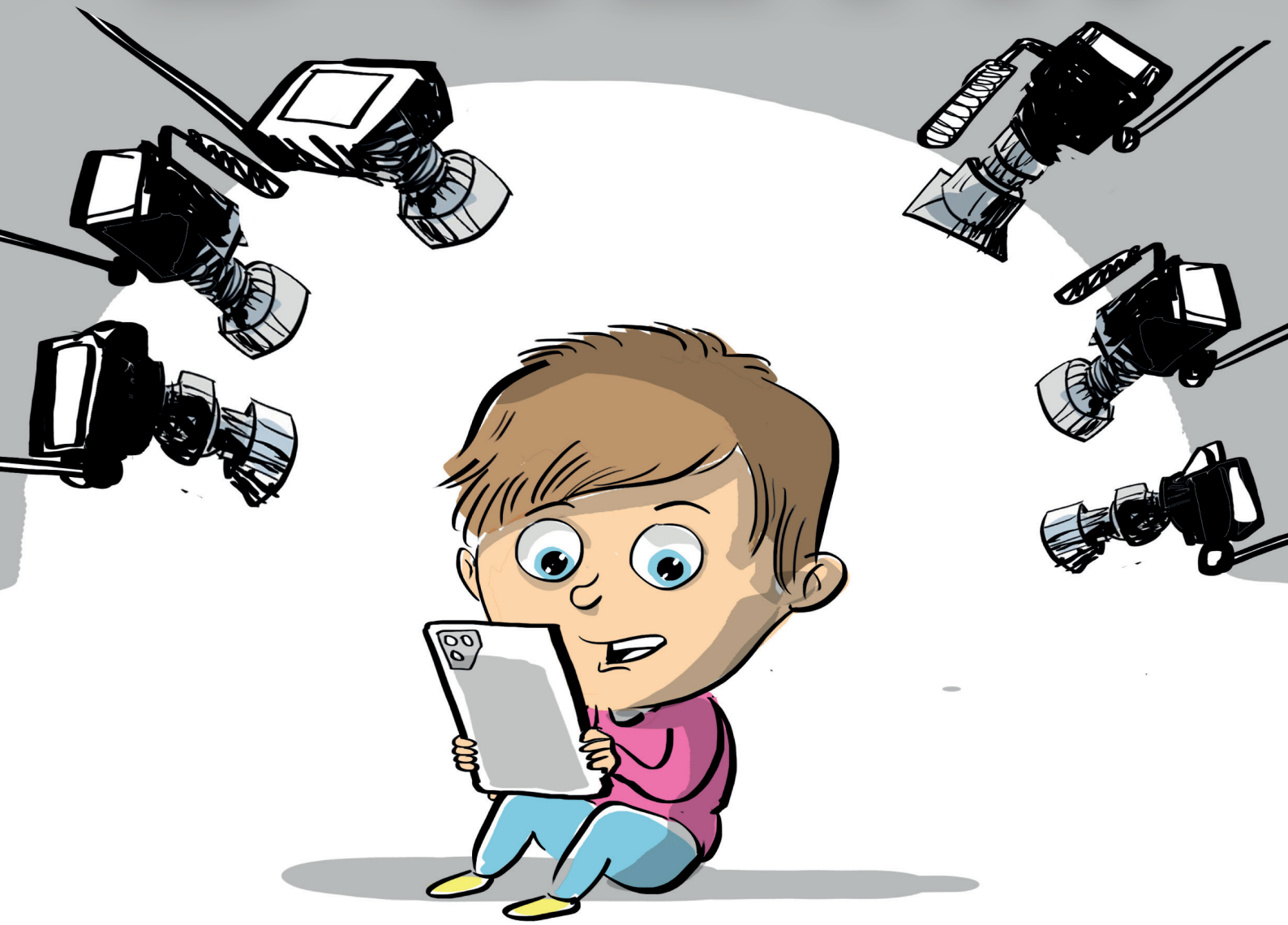
Чаще всего пользователи сети сами выкладывают информацию о себе в Интернет. Мошенники охотятся за этими данными. Большинство информации о жертвах преступники находят в открытом доступе в соцсетях и в Интернете.

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!

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.

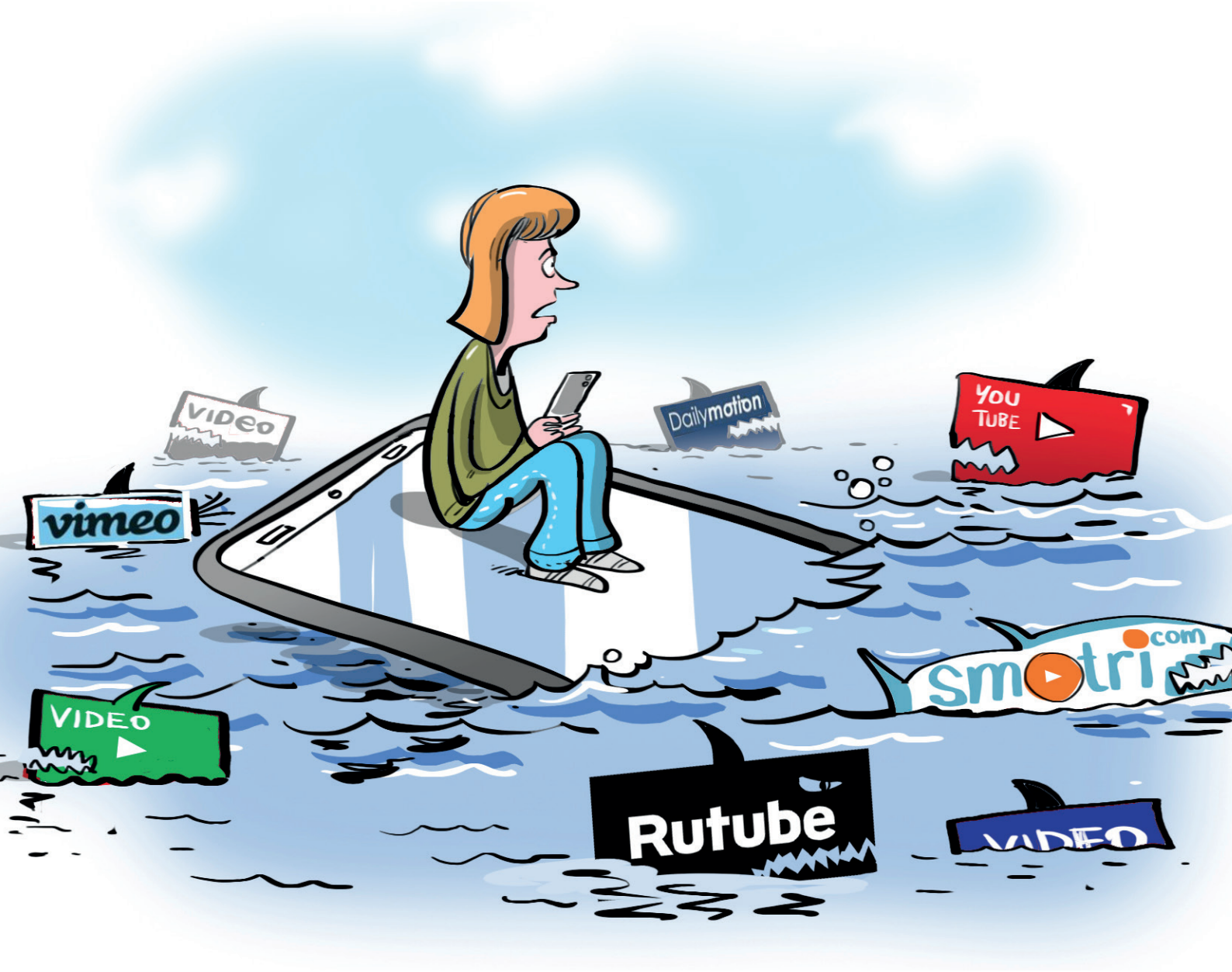
Если ты хочешь избежать Интернет-зависимости, то старайся придерживаться следующих правил:

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.

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

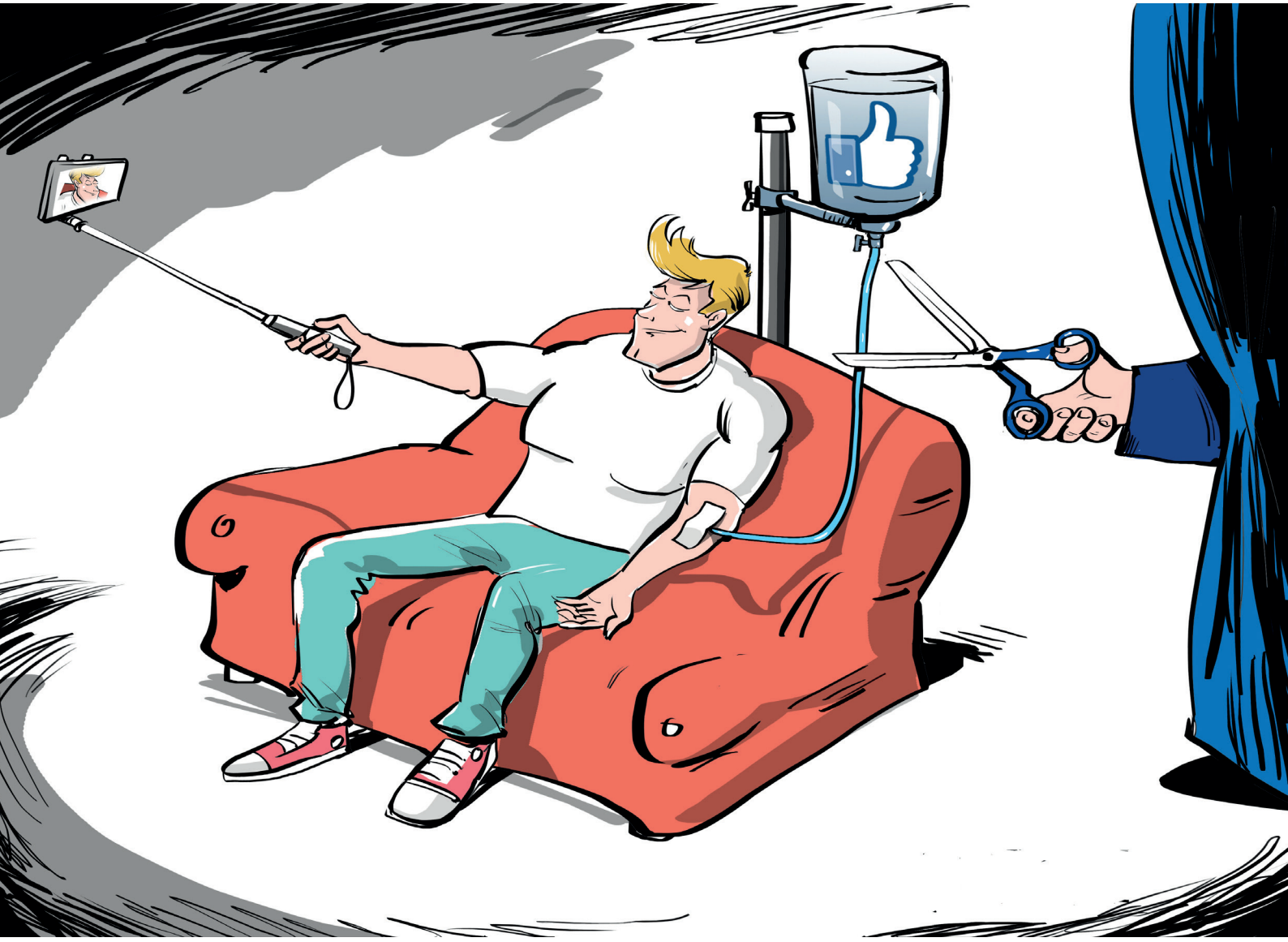
лига безопасного интернета

Сайт
ligainternet.ru

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

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

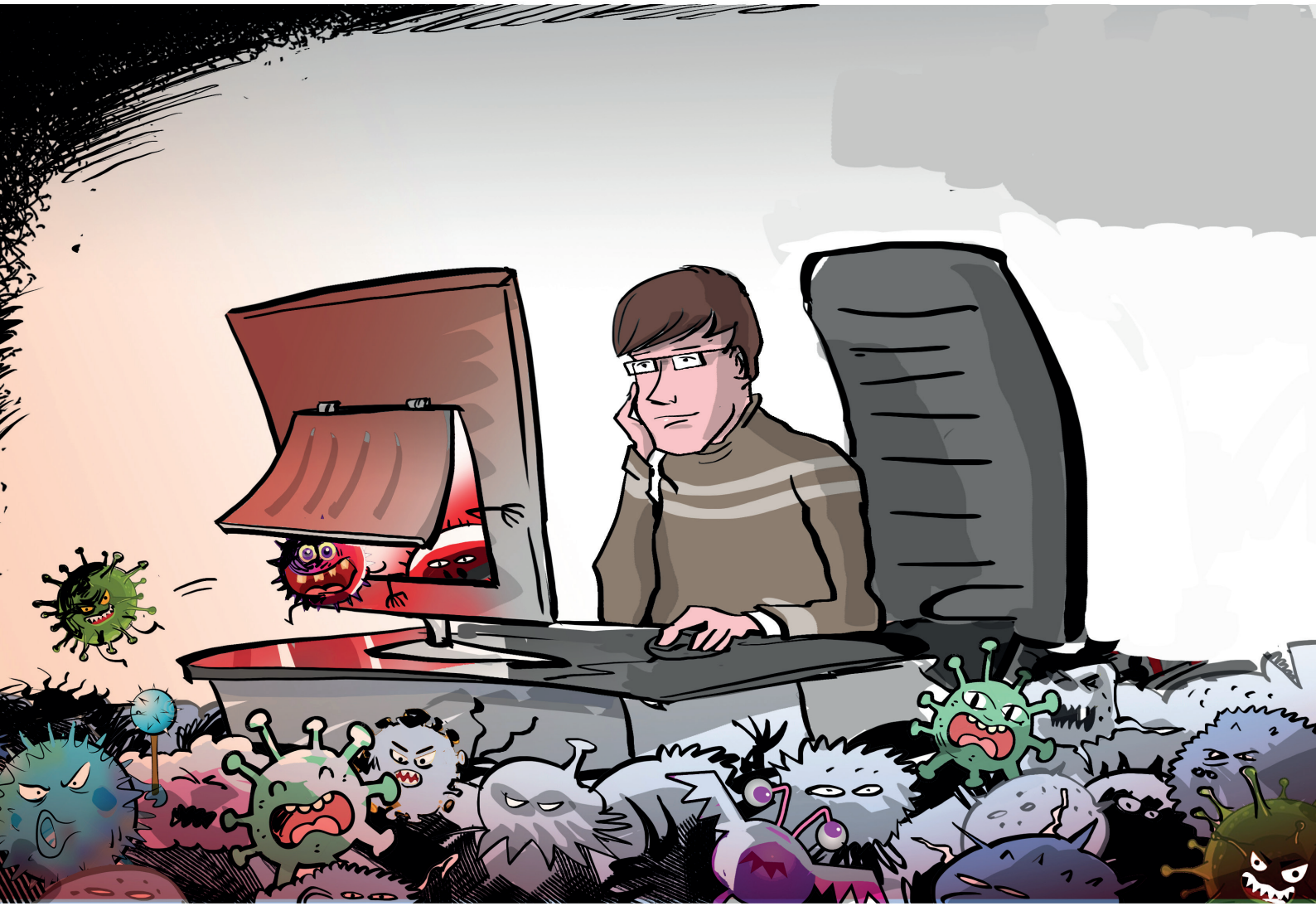
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт
ligainternet.ru

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

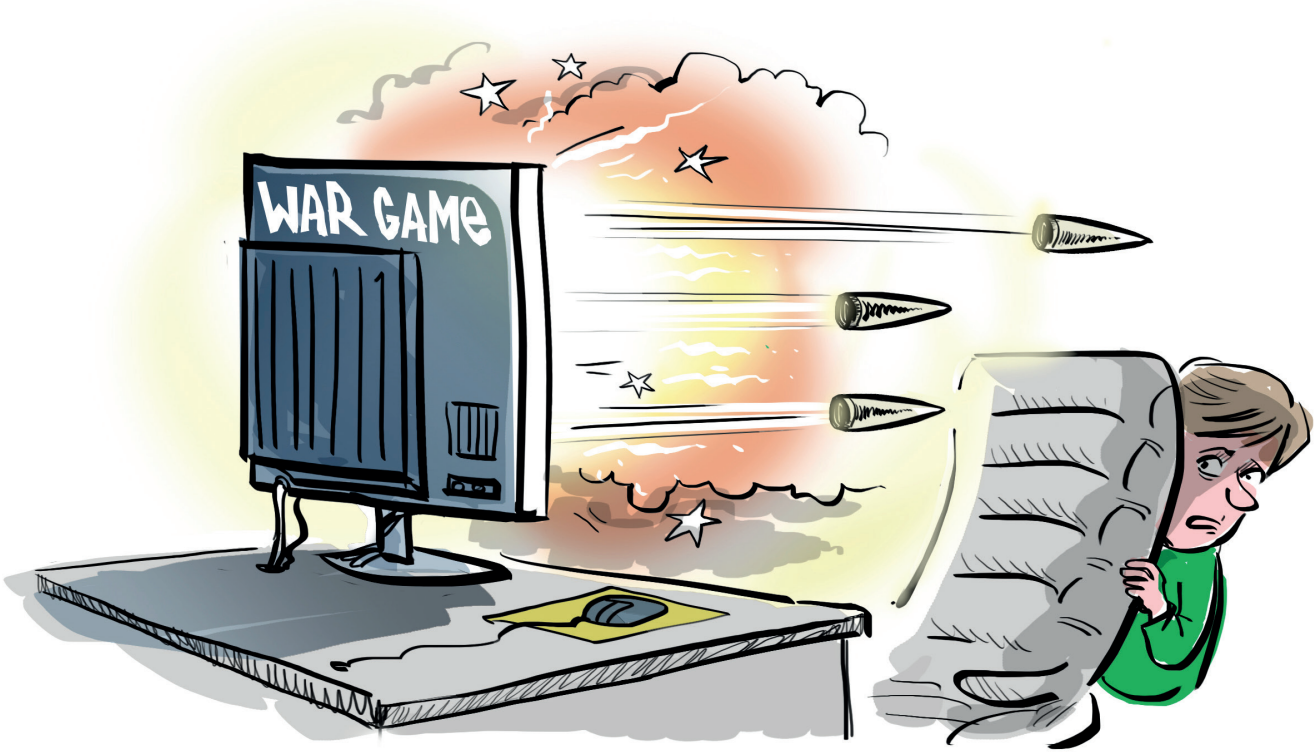
Сайт ligainternet.ru

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

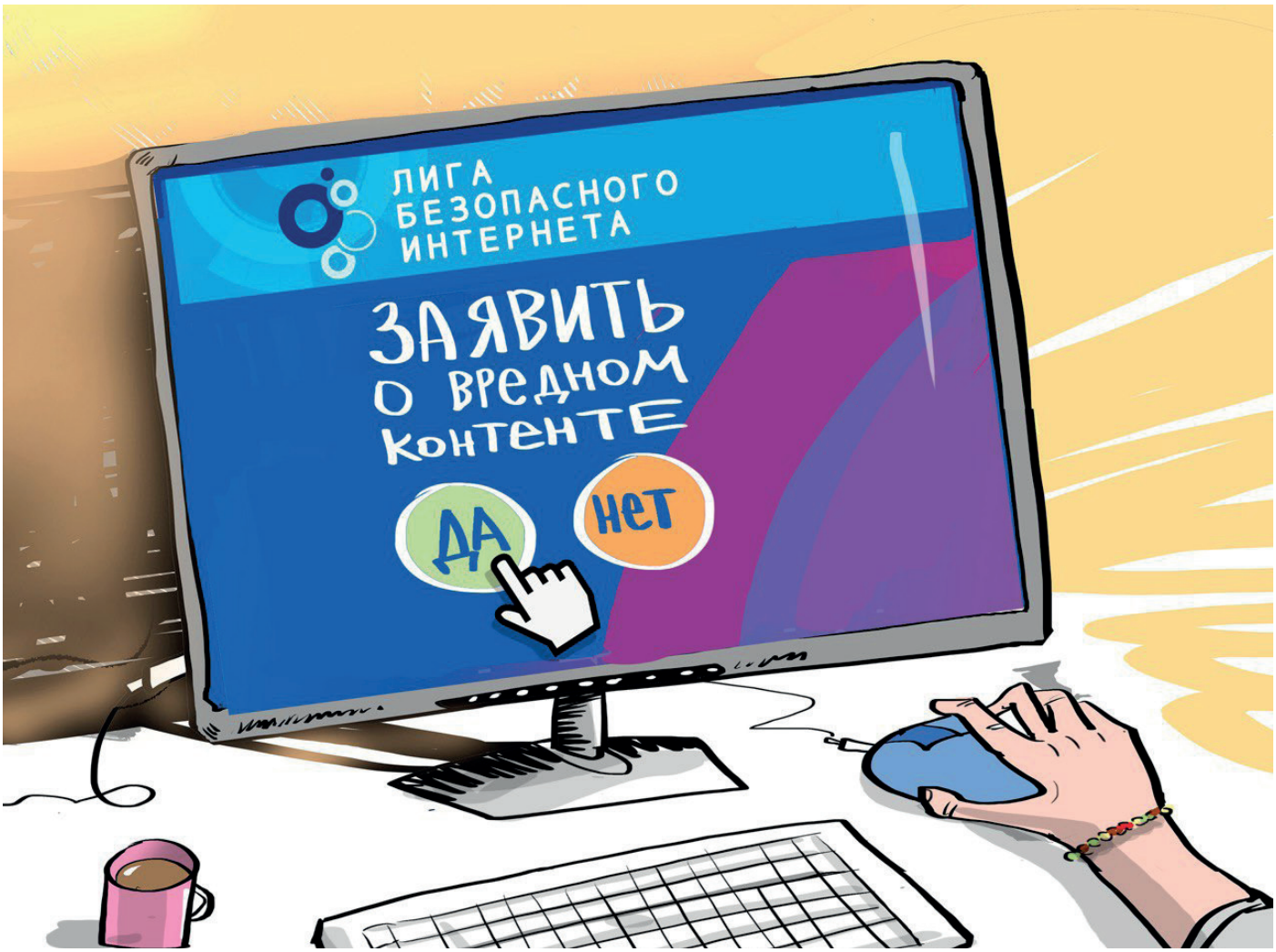
ОПАСНЫЕ ПУБЛИКАЦИИ В СОЦИАЛЬНОЙ СЕТИ: ПОЧЕМУ НЕЛЬЗЯ ПРОМОЛЧАТЬ!

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

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