Безопасность детей в интернете.

Отношения между родителями и потомками изменились из-за появления **Интернета**, так как технологии увеличивают разрыв между поколениями. **Дети в Интернете** ежедневно находятся часами. **Безопасность детей в интернете** зависит от микроклимата в семье. Поэтому важно проявить активное участие в борьбе с противоправным контентом, в том числе как противоречащему законодательству РФ.

*В России запрещено распространение порнографии, экстремизма, пропаганды наркосодержащих средств, самоубийств, а также данных о несовершеннолетних **детях**, уже пострадавших от противоправных действий.*

Перечисленные пункты определены ФЗ РФ No 139 «О защите **детей** от информации, причиняющей вред здоровью и развитию». Столкнувшись с противоправной информацией, вы

можете направить жалобу в отдел Роскомнадзора, после чего будут приняты действия.

Таким образом вы защитите и своих, и других **детей** от «черного» контента в **Интернете**.

Безопасность детей в интернете: статистика

1. По показателям исследований Фонда по вопросам Развития **Интернета**, молодежь в 2 с лишним раза чаще обращается ко Всемирной Паутин, чем взрослое поколение.

2. **Дети** намного быстрее осваивают новые **Интернет** технологии, уверенно используют информационные ресурсы.

3. Из-за огромной занятости или скромных знаний цифровых технологий, родители не объясняют своим **детям** о правилах безопасности в интернете.

4. В свою очередь **дети** желают быть самостоятельными и хотят решать проблемы через **Интернет**, не обращаясь за советами к родителям. Но в действительности, им необходимы и поддержка, и помощь.

5. **Дети** редко делятся со взрослыми из-за того, что боятся наказания или просто хотят быть независимыми.

6. Некоторые **дети** думают, что родители и взрослые не способны помочь решить какую-либо проблему.

В подобных ситуациях вы должны сделать первый шаг и поговорить с ними об особенностях интернета и обсудить **безопасность детей в интернете**

Дети в интернете: Общие риски

Покупая товары или пользуясь услугами можно встретиться с обманом в форме товаров низкого качества, подделками или вовсе потерять средства.

При неправильном использовании сети, могут возникнуть технические повреждения ПК:

• сбой системы;

• ошибки Windows;

• заражение вирусами.

В результате обычно страдают системные параметры, возможна кража конфиденциальной информации и личных данных.

Дети в Интернете: основные проблемы

Дети думают о себе, как о всезнающих пользователях **Интернета**, на самом деле это иллюзия, по уровню знаний новых информационных технологий **дети** стоят примерно на одном уровне со взрослыми.

*Проблемы в **Интернете** появляются у **детей** из-за большой активности и уверенности в своих знаниях.*

Мошенничество легко распространяется в **Интернете** из-за анонимности, здесь велики риски столкнуться с преследованием и слежкой. Нередко активные **дети** встречаются с различного вида унижениями, оскорблениями личности или шантажом, и это только малая часть неприятностей.

Техническое решение подобных проблем в Интернете еще не найдено. Единственной надежной защитой служат доверительные отношения между детьми и взрослыми.

Основная задача взрослых обеспечить, чтобы **дети** не получали «грязную» информацию, которая часто попадает в **Интернет**. И отстранение от компьютера — не выход. **Интернет** нужен как помощник в учебе.

*Когда **дети** вместе с родителями путешествуют по **Интернету**, рождается доверие, крепнет взаимное уважение, повышается уровень знаний, навыков. А также предотвращаются риски столкновения с мошенниками и другими негативными ситуациями.*

Для безопасного нахождения в **Интернете** интересуйтесь занятиями **детей**, хвалите за успехи, поддерживайте в трудностях. Чтобы **дети** испытывали к вам доверие, нужно уважительно отнестись к их деятельности и не осуждать.

Родители должны набраться терпения, особенно когда возраст чада 13-14 лет. Со скрытными подростками потребуется проявить хитрость. Тему происшествий в **Интернете** можно использовать в виде предлога для важного разговора. Или подать информацию в форме рассказа третьему лицу. Расскажите другому члену семьи о происшествии, которое якобы случилось с ровесником вашего ребенка. Но сделайте так, чтобы ваш ребенок услышал разговор. Поданную таким опосредованным способом информацию принимают самые упрямые максималисты.

Безопасность детей в интернете: практическая защита

Доверие и теплые отношения в семье важно и необходимо поддерживать постоянно. **Дети** должны чувствовать, что ваша цель лишь научить и помочь, а ни в коем случае не наказать. Тогда в любой ситуации **дети** будут вам доверять. При этом вы должны грамотно контролировать процесс выхода в **Интернет**.

1. Вы вправе установить определенное время для использования сети на устройствах.

2. Нужно обсудить следующие вопросы:

• Что можно делать в сети?

• Когда и где можно использовать гаджеты?

• Сколько времени разумно проводить в **Интернете**?

3. Чаще разговаривайте с **детьми** о Всемирной Паутине. Предупредите о возможных опасностях и угрозах, которые ожидают в **Интернете**. Достоверность и точность информации — важная деталь защиты от рисков.

Вы должны быть осведомленными о событиях жизни **детей** как в реальном, так и виртуальном мире.

*Искренний интерес к активности и действиям **детей в Интернете** — лучшее преимущество.*

4. В качестве объединяющего шага попросите создать для вас страницу в социальной сети ВКонтакте или Одноклассниках, или зарегистрироваться в любимой ребенком игре.

5. Нужно рассказать о том, как правильно вести себя в сети, что вежливость и дружелюбие превыше всего.

6. Необходимо донести до **детей**, что анонимность в виртуальном мире — это иллюзия, а каждое действие может оставить последствия, не всегда положительные.

7. Защита персональных данных и информации считается необходимым. Любые данные могут быть использованы в корыстных целях и даже против него самого.

8. Следует сообщить о средствах зашиты, помочь установить приватность в настройках на любимых сайтах.

9. Расскажите **детям**, куда можно обратиться с проблемами, например, к администраторам сайтов, технической поддержке.

Взрослый человек должен быть примером ответственного **Интернет** пользователя. Повышайте свой уровень знаний и навыков пользования, а также соблюдайте правила, это будет эффективным примером для **детей**.

Безопасность детей в интернете: Социальные сети

После того, как вы узнали, что ваши **дети** завели страницу в социальной сети, не ругайтесь. Сообщите **детям**, что представляют собой социальные сети в **Интернете**.

Наиболее частые случаи регистрации в социальных сетях происходят из-за подражания ровесникам, которые заводят профиль, а также, чтобы выглядеть круто и по-взрослому. Если вы попросите удалить аккаунт,**дети** могут создать новый и сделать так, что вы не узнаете. Именно поэтому расскажите о том:

• что такое социальная сеть;

• как и для чего её используют;

• кто там может находиться;

• как она устроена.

Настройте **детям** приватность, сообщите почему нельзя делать профиль доступным для любой публики, а также помогите придумать запоминающийся надежный пароль.

Но не следите и не проверяйте личные переписки детей, дайте им свое пространство.

Следует обязательно рассказать про угрозы, которые могут возникнуть при общении в социальных сетях:

- Главной проблемой считается общение с незнакомыми людьми и небрежное обращение с личной информацией.
- **Дети** возраста от 10 до 13 лет разговаривали в сети с пользователями, с которыми не были знакомы лично. Причем так поступает большая часть ребятишек.

Риск состоит в том, что **дети** наивны и доверчивы, могут рассказать о себе практически любую информацию.

По статистике **дети** в 60% случаев так и поступают. Называют контактные номера, адрес, учреждение в котором учатся, рассказывают о хобби, увлечениях, легко отправляют свои фотографии.

Безопасность детей в интернете: как противостоять мошенникам?

Судя по практике линии помощи «Онлайн **Дети**» по номеру 8-800-250-00-15, личная информация может быть использована мошенниками, для шантажа, сексуальных домогательствах и других противоправных действий.

Обеспечить безопасное нахождение в сети **Интернет** своим **детям** и домашним пользователям вы можете, лишь предупредив о всевозможных проблемах, угрозах и рисках. Проследите, чтобы в непредвиденной ситуации

ваши **дети** не растерялись и обратились, в первую очередь, к вам.

Не следует пытаться бороться с мошенниками самим. Чаще всего хакеры и сетевые злоумышленники, это опытные люди, хорошо знающие **Интернет** и программное обеспечение компьютеров. Они способны оценить риск, на который идут.

Сообщите о проблемном сайте администрации официальных авторитетных ресурсов, и, если данные подтвердятся, такой источник связи заблокируют. Для противодействия мошенникам напишите любой службе из нижеперечисленных:

1. Яндекс помощь:

webmaster.yandex.ru/delspam.xml

2. Служба Гугл:

www.google.com/safebrowsing/report_phish/?hl=ru

3. Лаборатория Касперского:

virusdesk.kaspersky.ru

4. Служба безопасности Avira:

analysis.avira.com/ru/submit-urls

Защита детей в интернете

Как защитить детей в Интернете от некачественной информации

Защита детей в Интернете сравнима с реализацией целого комплекса мер и способов. В статье Безопасность детей в интернете, мы поговорили насколько важно общение с ребенком на темы изучения интернета. В данной статье хотелось бы рассказать о способах практической защиты детей в интернете от запрещенной информации, мошенничества.

Такой процесс требует от родителей уверенного уровня владения Интернетом.

1. Если вы совсем плохо ориентируетесь в Сети как **интернет** пользователь и заводите компьютер ради **детей**, то для начальных настроек пригласите системного администратора.
2. Если у вас дома один общий программный компьютер, создайте отдельную учетную запись для себя. **Защитите** надежным паролем и правами администратора, чтобы **дети** не смогли изменить настройки и пользоваться в **Интернете** всеми ссылками подряд.

Обязательно проведите следующие **защитные** процедуры:

- установите в Яндексе или Гугл фильтрацию контентной информации.
- сделайте запрет на посещение взрослых **Интернет** сайтов.
- можно ограничить для **детей** время доступа к **Интернету**.
- отслеживайте действия **детей** по истории, просматривайте список операций.
- заблокируйте сомнительные поисковые страницы, баннеры, рекламу в **Интернете**.
- установите антивирусную программу, в которой есть родительский контроль.

Защита детей в Интернете с использованием фильтров

Существуют разные уровни фильтрации контента в **Интернете**:

1. Провайдер по запросу подключает услуги фильтрации контента, **защиту** от негативного воздействия на устройства с выходом в **Интернет**.
2. Приложения и специальные программы для родительского контроля и **защиты** ПО устанавливают на устройства, с которых **дети** выходят в **Интернет** – это могут быть планшеты, смартфоны, компьютеры, ноутбуки и так далее.
3. Есть **Интернет** ресурсы, сервисы, поисковые системы и социальные сети, которые обеспечивают **защиту** настройкой безопасного режима работы.

Риски в Интернете для детей важно предупредить

Вы должны с критикой отнестись к информации, наполняющей **Интернет** и научить своих **детей** такому же отношению.

*Следует объяснить **детям**, что немалое количество информации, находящейся в **Интернете**, считается неправдоподобной.*

Чаще всего многие опубликованные материалы нуждаются в проверке. Сообщите **детям** правила, по которым можно разделить информацию на достоверную и недостоверную.

Оценка достоверности информации в интернете

Получив новые сведения в сети, следует найти источник и обратить свое внимание на автора информации. Проанализировать другие публикации по теме.

Яркий, красочный сайт – еще не показатель того, что ему можно доверять и верить в написанное. Объясните **детям**, какой могла быть цель создания сайта, возможно всего лишь привлечение публики.

Расскажите **детям** правило «трех источниках» – прочитав новую информацию, не доверяйте сразу, проверьте что пишут еще в других **Интернет** источниках по этому-же вопросу.

Если дополнительной информации не найдено или в **Интернете** отсутствует первоисточник, то можно принять факты, но не стоит распространять другим пользователям сети.

Необходимо выбирать проверенные сайты

Сегодня в **Интернете** существуют белые списки, где находится полезный и безопасный контент, то есть перечень сайтов пригодных для изучения. К ним относятся образовательные, развлекательные, информационные ресурсы, а также с услугами и товарами.

Не предвзято общайтесь с детьми

Откровенный и доброжелательный диалог с **детьми** – лучший вариант предотвратить **Интернет** риски. Порой даже постоянный контроль не дает стопроцентной гарантии **защиты детей** от некачественной, негативной информации. Ведь столкнуться с ней можно на каждом шагу, например, у друзей, знакомых или случайно найти в домашнем **Интернете**.

*Лучший метод **защиты** — разговаривать честно и откровенно*

Тактично и аккуратно расспросите **детей**, что они увидели и прочитали в **Интернете**, а затем обсудите ту или иную проблему вместе. Лучше всего, когда **дети** узнают поясняющую информацию от взрослых, а не от знакомых сверстников на улице.

Защита детей в Интернете от технических рисков

По исследованиям Фонда Развития **Интернета** можно сказать, что почти каждый третий школьник России сталкивается с техническими угрозами. Даже несмотря на то, что сегодня много различных платных и бесплатных программ, которые позволяют **защитить** устройства от негативного воздействия, риски все-таки есть.

Обращения в службу помощи «**Дети** Онлайн» с техническими коллизиями происходят очень часто. Вирусы и вредоносные программы могут содержаться на любых сайтах и в любых файлах.

Эффективно и просто **защитить Интернет** можно благодаря правилам пользования, о которых следует помнить, как взрослым, так и **детям**.

Защита программных устройств

1. Пароль.

Защита *создается надежным сложным паролем для входа в компьютер, мобильное устройство или планшет.*

Научите **детей** создавать пароль на своем устройстве. Чтобы посторонние люди не смогли воспользоваться данными, попросите не сообщать никому данные, даже друзьям и близким людям. Регулярно напоминайте **детям** о смене паролей на каждом устройстве, и сами не пренебрегайте дополнительной **защитой**. Так вы обеспечите безопасность данных.

2. Учетная запись.

*На программном компьютере следует создать для **детей** отдельную учетную запись, но без административных прав.*

Чтобы нельзя было сменить настройки. Это **защитит** ваши документы, снизит риск попадания на компьютер вирусов и шпионских программ, **защитит** программное обеспечение, а также **дети** не смогут сменить настройки безопасности в браузере.

3. Антивирусники

Защита детей в интернете *с помощью антивирусных установок необходима, ПО позволяют комплексно **защитить** и проанализировать компьютер.*

Антишпион вычисляет шпионские программы, сетевой и онлайн сканер также необходимы во время использования **Интернета**. Нельзя забывать о том, что **защищать** следует не только ПК, но и мобильные устройства, планшеты.

Обновляйте операционные системы и программное обеспечение, пользуйтесь лицензионным ПО. Не забывайте обновлять антивирусные программы, браузеры и операционную систему ПК. Качать и устанавливать программы следует только с проверенных и надежных источников. Нельзя переходить по сомнительным рекламным баннерам и ссылкам.

Защита детей в интернете: Осторожность

Расскажите своим **детям**, что нельзя кликать на незнакомые сайты, ссылки и яркие рекламные вставки, так как таким

способом можно попасть на вредоносный сайт, страницу и так далее. Намного безопаснее будет найти нужный продукт через поисковую строку в Яндексе — ввести запрос самостоятельно.

*Часто посещаемые сайты удобно добавить в закладки или на панель быстрого доступа, а **защищенное** соединение – залог хорошей работы в **Интернете**.*

Используя Wi-Fi сеть для доступа в **Интернет**, следует убедиться в безопасности
соединения. **Защитить** домашний **Интернет** можно посредством пароля и логина. Расскажите **детям**, что
пользование **незащищенным** соединением может привести к потере данных с компьютера или другого устройства, на котором выходили в **Интернет**.

Важные советы для защиты детей в интернете

Интернет наполнен разнообразными пользователями, которые преследуют свои цели и не только хорошие. Существует большое количество мошенников, цель которых – украсть у людей финансовые средства путем получения их персональных данных или какой-либо важной информации.

Сегодня с такой проблемой сталкиваются и взрослые, и **дети**. Кража денег происходит через онлайн-игры, рекламные сайты, через заказ товара и так далее. Персональные данные вскрываются еще чаще.

Чтобы не стать жертвой мошенников, необходимо привить **детям** правила:

4. Игнорировать сомнительные сообщения от незнакомых или малознакомых людей. В том числе письма, которые приходят на электронную почту с неизвестных ресурсов.
5. Если письмо несет в себе информацию о каком-либо выигрыше, призе или о беде с близкими людьми, поясните **детям**, что следует рассказать о форс-мажорной информации родителям.
6. Часто мошенники ловят наивных людей на благотворительном сборе средств.
7. Не следует переходить по ссылкам, которые имеются в подозрительном сообщении от незнакомого человека.
8. Не следует заполнять формы и откликаться на всплывающие окна. При взломе страниц социальных сетей, мошенники просят **детей** сделать простые действия, но втайне от взрослых и очень срочно, нельзя вестись на эти уловки.
9. Сообщения от друзей или знакомых о срочной проблеме следует проверять через звонок.

Взрослые могут найти сайт или телефон компании, от которой якобы приз и позвонить или написать. Когда вы вместе с **детьми** потратите время на обратную связь и продемонстрируете, что никаких бонусов нет, **дети** сами перестанут обращать внимание на спам.

С помощью разных приемов и источников можно установить правдивость информации в **Интернете** по благотворительности. Покажите **детям** — как делается проверка.

Если есть какие-то подозрения, что компьютер или аккаунт взломаны, нужно менять пароли и написать администрации ресурса. С проблемой аккаунта **детям** лучше обратиться за помощью к родителям. Тогда, чаще всего, аккаунт удается восстановить, затем компьютер нужно сканировать. Если по отчету вы видите, что остается много фрагментов разных файлов, пригласите опытного администратора. Специалист

приведет компьютер в порядок и подскажет, какими программами его лучше **защитить**.