

Прямо по курсу – Интернет: правила, советы и рекомендации по безопасному использованию сети



Проблема обеспечения информационной безопасности детей и подростков в Интернете становится все более актуальной. Дети и подростки – одна из самых активных групп пользователей Интернета: они используют Интернет как в образовательных целях, так и для проведения досуга. Но дети и подростки по большей части не осознают тех проблем, которые могут возникнуть при бесконтрольном и беспечном использовании Сети. Находясь в социальных сетях, форумах, дети часто оказываются незащищенными от негативной и даже агрессивной информации. Дети активно пользуются электронной почтой и получают спам, совершенно не задумываясь о проблемах, с которыми они могут столкнуться в виртуальном пространстве. Содержание многих сайтов не соответствует требованиям информационной безопасности. Часто дети становятся легкой целью грабителей, мошенников, сталкиваются с порнографическим контентом и сексуальными предложениями.

На сегодняшний день Интернет является важной составляющей информационных ресурсов современной библиотеки. Библиотека в дополнение к печатным ресурсам предоставляет доступ к электронным информационным ресурсам, и что немаловажно, помогает ориентироваться в них. Библиотекари, работающие с детьми – это просветители и консультанты по безопасности в Интернете, а также лоцманы-навигаторы в киберпространстве.

Некоторые правила, советы и рекомендации безопасного пользования Интернетом позволяют повысить уровень онлайн-грамотности и обезопасить свою жизнь, создав комфортные условия для пользования сетью Интернет.

Кибербуллинг



В сети Интернет, как и в обычной жизни, встречаются злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, устроить травлю. Такие люди могут встретиться на форумах и чатах. Сложное слово «кибербуллинг» в

современном мире как раз и означает преследование человека сообщениями, содержащими оскорблении, агрессию, запугивание.

Лучшая защита – предупреждение.

1. Помни: ты не виноват, если получил оскорбительное сообщение! Ни в коем случае не стоит общаться с таким человеком и тем более пытаться ответить ему тем же. Просто прекрати общение.
2. Страйся быть дружелюбным с другими пользователями, ни в коем случае не пиши грубых слов, не провоцируй собеседника. Нельзя использовать сеть для хулиганства и угроз!
3. Если тебе угрожают по Интернету, обязательно расскажи об этом родителям, учителю или близкому человеку, которому ты доверяешь! Это неправильно, когда тебя запугивают, унижают или оскорбляют.
4. Коллективное преследование – это крайнее проявление жестокости. Никогда не участвуй в травле и не общайся с людьми, которые обижают других.
5. Помни: твои родители всегда готовы тебя выслушать, помочь и защитить.

Онлайн-общение



В сети Интернет, так же как и вне дома и школы нужно помнить о личной безопасности и вести себя осторожно, чтобы не попасть «в лапы» злоумышленников. Вот несколько советов:

Никогда не сообщай свое полное имя, домашний адрес и телефон, не высыпай свои фотографии незнакомым людям. Помни: преступники могут использовать эту информацию против тебя или твоих родных.

Встречаться с виртуальным знакомым либо не следует вовсе, либо только в присутствии родителей. Если назначается встреча, она должна проходить в людном месте и, желательно, так же в присутствии родителей. Помни: под маской своего «друга» – ровесника может скрываться взрослый человек с преступными намерениями.

Если Интернет-общение становится негативным – такое общение следует прекратить и не возобновлять.

Скачивание/хранение информации

Воровать — нехорошо. Этому нас учат дома, в школе, пишут в книгах, в гражданском и даже в уголовном кодексе. Любой материал, выставленный в сети Интернет: фото, видео, музыка, картинки и тексты, – имеет своего автора, а значит – охраняется законом (часть 4 Гражданского кодекса Российской Федерации).

То, что на web-сайте нет надписи о защите авторских прав, совсем не означает, что можно свободно использовать материалы. Не нужно думать, что если ты не продаешь чужую информацию, то ты ничего не нарушаешь.

Обязательное условие при копировании материалов – указать источник информации. Это относится к текстам, изображениям, музыкальным, видео- и прочим файлам, независимо от целей использования.

Перед копированием необходимо обязательно ознакомиться с дополнительными условиями, которые могут быть указаны на сайте-источнике. Если такие условия есть, то при копировании они должны быть обязательно соблюдены. Если же указан прямой запрет на использование материалов, то от копирования необходимо отказаться. Следует запрашивать специальное разрешение у авторов или информировать их о копировании файлов.

Используй на домашнем компьютере лицензионное программное обеспечение или их бесплатные аналоги (свободно распространяемые версии).

Помни: путешествуя в сети Интернет, необходимо соблюдать закон!

Личные данные



Волку дверь не открывайте! У интернет-мошенников ничего не получится, если только мы сами не откроем им дверь – не сообщим им наши пароли, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям.

Никогда не разглашайте личную (персональную) информацию. Персональная информация — это номер вашего мобильного телефона, фамилия, имя и отчество, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

Если ты используешь общедоступный компьютер в библиотеке или в интернет-кафе, прежде чем покинуть компьютер, полностью заверши все сеансы с выходом из системы.

Придумывай безопасные пароли, часто меняй их и держите в секрете.

Используй псевдонимы в сети Интернет, они обеспечивают безопасность и конфиденциальность.

Вредоносные программы

Что нужно знать об угрозе заражения вредоносным программным обеспечением?



Загружаемые из сети Интернет файлы могут быть носителями вредоносных программ, которые могут нанести вред тебе или другим пользователям сети Интернет через твой компьютер. Это так называемые вирусы, черви, программы-шпионы – небольшие программы, которые распространяются с компьютера на компьютер и вмешиваются в работу операционной системы, могут даже уничтожить все, что находится на жестком диске.

Легче всего вирусы распространяются во вложениях сообщений электронной почты и мгновенных сообщений. Поэтому очень важно никогда не открывать вложения, если ты не ожидал их получить или не знаешь, кто их отправил.

Нежелательная почта (спам) – получение абсолютно не нужных сообщений или мошеннических предложений, рассылаемых с помощью специальных программ-роботов.

Не попадайся на предложение «отписаться» от рассылки, нажав на предложенную ссылку! Игнорируй его! Иначе впоследствии тебя завалят спамом, так работают мошенники.

Не стоит, не глядя, переходить по ссылкам, содержащимся в сообщениях электронной почты. Прежде чем щелкнуть по ссылке, просмотрите, куда она ведет, проверь ее конечный адрес.

Будь внимателен при загрузке бесплатных файлов и игр на компьютер, тебя могут обмануть: нажав на ссылку, ты можешь попасть в «небезопасную зону» или загрузить на свой компьютер вирус или программу-шпион.

Антивирусные программы – твои защитники. Установи их на своем компьютере и регулярно обновляй.

Окружи себя реальными друзьями! Научись использовать Интернет с пользой для учебы, самообразования и любимых увлечений. Тот, у кого много друзей, есть любимое занятие, вряд ли окажется в онлайн-западне.

Безопасного тебе путешествия в сети, дорогой друг!

Рекомендации подросткам: как избежать зависимости от интернета

- ❖ Используйте реальный мир для общения. Ищите друзей в реальности. Виртуальный мир дает только иллюзию принадлежности к группе и не развивает никаких действительных навыков общения.
- ❖ Наполняйте жизнь положительными событиями, поступками.
- ❖ Избегайте лживости и анонимности в виртуальной реальности.
- ❖ Имейте собственные четкие взгляды, убеждения.
- ❖ Научитесь контролировать собственное время и время за компьютером.
- ❖ Найдите любимое занятие, увлечение, хобби в реальной жизни.
- ❖ Больше гуляйте, проводите время на свежем воздухе, займитесь спортом.
- ❖ Прислушивайтесь к советам родителей, если они говорят, что вы слишком много времени проводите за компьютером.

Полезные ссылки

<https://www.edu.yar.ru/azbuka> Азбука цифрового мира расскажет простым языком о сложных вещах из необъятного мира цифровых технологий. Увлекательные комиксы, специализированные тренажёры и интересные игры!

www.edu.yar.ru/safety/sites/region Региональный сегмент реестра безопасных Интернет-ресурсов для детей

Родителям

Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р Об утверждении Концепции информационной безопасности детей в РФ и признании утратившим силу распоряжения Правительства Российской Федерации от 2 декабря 2015 г. N 2471-р

Правительство утвердило новую концепцию информационной безопасности детей в России.

Ее стратегические цели - развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия. Концепция предусматривает, в частности:

- введение в российских школах уроков информационной безопасности и цифровой грамотности;
- проведение просветительских мероприятий для родителей, учителей, работников детских и юношеских библиотек;
- расширение спектра возможностей услуги "Родительский контроль" на стационарных и мобильных устройствах, которыми пользуется ребенок.

[Указ Президента Российской Федерации от 17.05.2023 № 358 "О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года"](#)

17 мая 2023 года Президент России Владимир Путин подписал указ об утверждении Стратегии комплексной безопасности детей в РФ на период до 2030 года.

[Дети в интернете: риски, о которых нужно знать родителям](#)

Эксперты Альянса по защите детей в цифровой среде рассказали, какие интернет-риски сейчас наиболее актуальны и как защитить от них ребенка.

Использованные источники:

Материал из сети интернет:

- Безопасный Интернет: <http://www.saferinternet.ru>
- <https://sites.google.com/site/family0first/negativnoe-vlianie-interneta-na-organizm-celoveka-i-ego-psihiku>
- <https://geektimes.ru/post/252244/>
- <https://rg.ru/2015/11/19/internet-site.html>

