

БЕЗОПАСНОСТЬ В ИНТЕРНЕТ

Касается всех, касается каждого!



ИНТЕРНЕТ. Вряд ли сегодня кто-то скажет, что в современной жизни можно обойтись без него... В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Для одних он служит источником знаний, для других используется в работе, а кто-то нашел здесь друзей и получил драгоценное общение. Такое явление современного Интернета, как **социальные сети**, приобрело множество поклонников среди самых разных слоев населения. Вместе со взрослыми в глобальную сеть устремили свое внимание и дети. Например, профиль в социальной сети «ВКонтакте» есть практически у каждого ребенка в семье.

Знаете ли вы, что в виртуальном мире любого из нас подстерегает множество опасностей, о которых многие даже не подозревают? Путешествуя в сети, вы можете встретить не только друзей или бывших одноклассников, но и людей, которые, пользуясь вашим незнанием основных правил безопасной сетевой работы, могут осуществить несанкционированный (удаленный) доступ к вашему компьютеру для кражи или уничтожения информации с жесткого диска, исказить или разрушить данные и программы на вашем компьютере. А иногда пользователь и не подозревает, что может стать или уже стал жертвой компьютерных мошенников.

Все опасности интернет- среды объединены в четыре основные группы рисков:

1. **Контентные риски.** Это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.
2. **Коммуникационные риски.** Связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.
3. **Электронные риски.** Это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.
4. **Потребительские риски.** Это злоупотребление в Интернете правами потребителя. Включают в себя следующее: риск приобретения товара низкого качества,

различные подделки, контрафактную и фальсифицированную продукцию, потерю денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества и др.

Соблюдение правил поведения в цифровом пространстве является очень важным для сохранения безопасности. Тому, как преодолеть нежелательное воздействие компьютера, посвящен данный раздел. Мы надеемся, что представленная информация по обеспечению безопасной работы в сети будет полезна и школьникам (раздел "Детям о безопасности") и взрослым (разделы "Родителям о безопасности" и "Педагогам о безопасности"). Но знакомство с материалами лучше начать с раздела "Это должен знать каждый". В разделе "Кинозал" вы найдете информацию в формате видео.

Защитите себя и свой компьютер!



- Всегда следите за обновлениями вашей операционной системы и браузера (или позвольте им обновляться автоматически).
- Используйте последнюю версию антивирусной программы и не забывайте регулярно обновлять вирусные базы.
- Используйте брэндмауэр.
- Внимательно следите за тем, какие веб-сайты вы открываете (не все ссылки безопасны) и что загружаете. Это относится к музыке, фильмам, файлам, плагинам и дополнениям для браузера и т. д.
- Устанавливайте программное обеспечение только из надежных источников
- Не открывайте подозрительные вложения к сообщениям электронной почты и сами сообщения.
- Используйте надежные пароли и храните их надежным способом.
- При совершении Интернет-платежей пользуйтесь только проверенными службами.
- Если вас просят указать личные или финансовые данные по электронной почте, в мгновенном сообщении или на веб-странице, НИКОГДА не делайте этого.
- Соблюдайте осторожность, если вы выходите в Интернет с помощью сети, которую вы не знаете или которой не доверяете, например бесплатное подключение Wi-Fi в кафе. Не включайте общий доступ и подключение к устройствам. Это поможет сделать ваш

компьютер невидимым для других пользователей в сети, и вы будете в большей безопасности.

Детям о безопасности в Интернете



Самые главные правила

1. Научись безопасно использовать свой компьютер

- Убедись, что на твоём компьютере установлены брандмауэр и антивирусное программное обеспечение. Научись их правильно использовать. Помни о том, что эти программы должны своевременно обновляться.
- Хорошо изучи операционную систему своего компьютера (Windows, Linux и т. д.). Узнай, как исправлять ошибки и делать обновления.
- Если на компьютере установлена программа родительского контроля, поговори со своими родителями и договорись о настройках этой программы, чтобы они соответствовали твоему возрасту и потребностям. Не пытайся взломать или обойти такую программу!
- Если ты получил файл, в котором ты не уверен или не знаешь, кто его отправил, НЕ открывай его. Именно так трояны и вирусы заражают твой компьютер

Это должен знать каждый.

2. НИКОГДА и НИГДЕ не указывай личную информацию!

- Когда ты регистрируешься на сайтах, не указывай личную информацию (номер мобильного телефона, адрес места жительства и другие данные).
- Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!

3. Будь начеку!

- Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
- Всегда будь начеку, если кто-то, особенно незнакомец, хочет поговорить с тобой о взрослых отношениях. Помни, что в сети никогда нельзя быть уверенным в истинной сущности человека и его намерениях.

- Если у тебя возникли вопросы или проблемы при работе в онлайн-среде, обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. **Любую проблему можно решить!**

4. Будь дружелюбен.

- Когда общаешься в онлайн, относись к другим людям так, как ты хотел бы, чтобы относились к тебе.
- Избегай сквернословия и не говори вещей, которые заставят кого-то плохо себя чувствовать

Уважаемые родители!

В Интернете вашего ребенка могут обидеть, запугать или даже оскорбить. Важным является предупреждение детей об опасностях Интернета, неоднократное напоминание о том, чтобы они вели себя осторожно.

Обсуждайте с детьми все вопросы, которые могут у них возникнуть при использовании Интернета. Недопустимо дистанцироваться от вопросов детей, а наоборот надо стараться максимально завоевать их доверие, постоянно интересуясь их времяпрепровождением в сети.

Тогда вы будете в курсе той информации, которой владеют ваши дети.

Основные рекомендации

1. Внимательно, но не навязчиво контролируйте деятельность ребёнка в Интернете.

Выберите время для неконфликтного совместного просмотра интернет- страниц.

- Убедите своих детей делиться с вами впечатлениями от работы в Интернете.
- Научите детей доверять интуиции. Если что-нибудь в Интернете будет вызывать у них психологический дискомфорт, пусть дети рассказывают вам об этом.
- Если ваши дети регистрируются на форумах, в чатах или сетевых играх, что требует указания идентификационного имени пользователя, помогите им выбрать это имя и убедитесь в том, что оно не содержит никакой личной информации.
- Запретите своим детям сообщать другим пользователям Интернета адрес, номер телефона и другую личную информацию, в том числе номер школы и любимые места для игр.
- Убедите детей в том, что они не должны встречаться с интернет- друзьями лично. Скажите, что интернет- друзья могут на самом деле быть не теми, за кого они себя выдают.

- Если ваши дети пользуются чатами, вам следует знать, какими именно, и с кем они там беседуют. Лично посетите чат, чтобы проверить, на какие темы ведутся дискуссии. Внушите детям, что никогда нельзя покидать общий чат: многие сайты имеют «приватные комнаты», где пользователи могут вести беседы наедине – у администраторов нет возможности читать эти беседы (такие «комнаты» часто называют «приватом»).
- Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев.
- Объясните детям, что верить всему, что они видят или читают в интернете, нельзя. Скажите им, что при наличии сомнений в правдивости какой-то информации, им следует обратиться за советом к вам.
- Возьмите за правило каждый день проверять, на какие интернет ресурсы заходили ваши дети. Обязательно настройте сохранение истории, журнал браузера. Если заметите попытки редактирования записей журнала, это повод задуматься и поговорить с детьми.

«БЕЗОПАСНЫЙ ИНТЕРНЕТ» - РЕКОМЕНДАЦИИ РОДИТЕЛЯМ

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет – это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них – дети, которые могут не знать об опасностях мировой паутины. Мы хотим сделать Интернет максимально безопасным для подрастающих поколений. Эта цель осуществима, если государство, представители бизнеса, правоохранительные органы и общественность объединят усилия, а родители осознают свое главенство в обеспечении безопасности детей. Данные рекомендации – практическая информация для родителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Правило 1. Внимательно относитесь к действиям ваших детей в «мировой паутине»:

- Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернетом, особенно на этапе освоения.
- Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернета, рассказывайте, как вовремя предупредить угрозы.

Правило 2. Информировать ребенка о возможностях и опасностях, которые несет в себе сеть:

- Объясните ребенку, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием со стороны другого пользователя Интернета, ему нужно сообщить об этом близким людям.

- Объясните ребенку, что размещать свои личные данные (адрес, телефон, место учебы) в социальных сетях и других открытых источниках нежелательно и даже опасно.
- Научите ребенка искать нужную ему информацию и проверять ее, в том числе с вашей помощью.
- Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернета, особенно путём отправки sms, – во избежание потери денег.
- Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ваш ребенок, и посоветуйте их использовать.
- Объясните, что нежелательно переходить по ссылкам в Интернете. Доказано, что за шесть кликов можно перейти от «белого» сайта к «чёрному».
- Научите ребенка самостоятельно вносить адрес в адресную строку браузера. Это позволит избежать сайтов-клонов.

Правило 3. Выберите удобную форму контроля пребывания вашего ребенка в Сети:

- Установите на ваш компьютер необходимое программное обеспечение – решение родительского контроля, антивирус Касперского или Doctor Web.
- Простые настройки компьютера позволят вам быть в курсе того, какую информацию просматривал ваш ребенок. Регулярно отслеживайте ресурсы, которые посещает ребенок.
- Пользуйтесь программами семейной безопасности, которые позволяют полностью перекрыть доступ в Интернет или установить веб-фильтры, а также проверить, на какие сайты заходит ребенок, какие программы использует, сколько времени проводит в сети.
- Если ваш ребенок – учащийся младших классов и часто остается дома один, ограничьте ему время пребывания в Интернете.
- Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семьи, а не в комнате ребенка.
- Создавайте разные учетные записи на вашем компьютере для взрослых и детей. Это поможет не только обезопасить ребенка, но и сохранить ваши личные данные.

Правило 4. Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей:

- Используйте удобные возможности повышения уровня компьютерной и Интернет-грамотности, например, посещение курсов, чтение специальной литературы, консультации с экспертами.
- Знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.
- Учитесь у ребенка! Дети XXI века нередко лучше родителей разбираются в вопросах компьютера и Интернета. В форме игры попросите ребенка показать свои возможности и научить вас незнакомым действиям.

Правило 5. Будьте внимательны к поведению ребенка, отслеживайте признаки Интернет-зависимости:

- Уясните, вредные привычки влияют на здоровье, а Интернет-зависимость наносит вред психике человека. По мнению врачей и психологов, зависимость от Интернета является «удобным» типом зависимости для родителей, так как носит неявный характер по сравнению с другими серьезными проблемами, к примеру, алкоголем и наркотиками
- Будьте внимательны к переменам в поведении ребенка Раздражительность, рассеянность, замкнутость, потеря интереса к любимым занятиям, ложь о количестве времени, которое ребенок проводит в сети, частое употребление пищи перед компьютером – все это может быть признаками зависимости от Интернета.
- Придумайте полезную альтернативу Интернету. Это может быть увлекательное занятие, активный отдых, посещение спортивных секций и кружков, обычная прогулка с друзьями или родителями.
- Старайтесь распознать зависимость как можно раньше и при необходимости обратиться к специалисту.

Правило 6. Руководствуйтесь рекомендациями педиатров:

- До 7 лет врачи не рекомендуют допускать детей к компьютеру/Интернету. 7-10 лет — время за компьютером рекомендовано ограничить 30 мин. в день. 10-12 лет — до 1 часа за компьютером. старше 12 лет – не более 1,5 часов с обязательными перерывами.
- Помните, что злоупотребление компьютером рискованно для физического здоровья и может вызвать у ребенка ухудшение зрения, гиподинамию, подверженность аллергиям и даже сердечно сосудистые заболевания. Способы фильтрации
<http://www.ligainternet.ru/filtruyushchii-soft> <http://www.netpolice.ru/filters/?sid=>
<http://www.icensor.ru/>

© Ссылка на источник: http://sch1286sz.mskobr.ru/conditions/bezopasnost_v_internete/

«БЕЗОПАСНЫЙ ИНТЕРНЕТ» - РЕКОМЕНДАЦИИ РОДИТЕЛЯМ

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет – это не только кладёзь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них – дети, которые могут не знать об опасностях мировой паутины. Мы хотим сделать Интернет максимально безопасным для подрастающих поколений. Эта цель осуществима, если государство, представители бизнеса, правоохранительные органы и общественность объединят усилия, а родители осознают свое главенство в обеспечении безопасности детей. Данные рекомендации – практическая информация для родителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Правило 1. Внимательно относитесь к действиям ваших детей в «мировой паутине»:

- Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернетом, особенно на этапе освоения.
- Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернета, рассказывайте, как вовремя предупредить угрозы.

Правило 2. Информировать ребенка о возможностях и опасностях, которые несет в себе сеть:

- Объясните ребенку, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием со стороны другого пользователя Интернета, ему нужно сообщить об этом близким людям.
- Объясните ребенку, что размещать свои личные данные (адрес, телефон, место учебы) в социальных сетях и других открытых источниках нежелательно и даже опасно.
- Научите ребенка искать нужную ему информацию и проверять ее, в том числе с вашей помощью.
- Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернета, особенно путём отправки sms, – во избежание потери денег. • Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ваш ребенок, и посоветуйте их использовать.
- Объясните, что нежелательно переходить по ссылкам в Интернете. Доказано, что за шесть кликов можно перейти от «белого» сайта к «чёрному».
- Научите ребенка самостоятельно вносить адрес в адресную строку браузера. Это позволит избежать сайтов-клонов.

Правило 3. Выберите удобную форму контроля пребывания вашего ребенка в Сети:

- Установите на ваш компьютер необходимое программное обеспечение – решение родительского контроля, антивирус Касперского или Doctor Web.

