



Уполномоченный по правам ребенка

в Томской области



Мегабезопасность  
советы родителям



Уважаемые родители!

Вместе с радостью отцовства и материнства мы приобретаем огромную ответственность за своего ребенка. Быть родителем это одна из основных, наиболее важных и чрезвычайно сложных функций взрослого человека. Это тяжелая, но необычайно увлекательная работа.

Родители стремятся вырастить здорового и самостоятельного ребенка, приносящего пользу самому себе и обществу и реализовывающего свои таланты и возможности. Родители удовлетворяют его физические потребности и создают условия для наилучшего духовного и общественного развития ребенка.

Именно для развития ребенка мы и знакомим его с сетью Интернет, это не только огромная база увлекательных знаний, полезной информации, развлечений и среда для ведения бизнеса и совершения покупок. К сожалению, Интернет может представлять большую опасность для любого пользователя: огромное количество вредоносных программ и различных угроз, с помощью которых кибер-преступники способны красть персональную и конфиденциальную информацию, нарушать работу Вашего компьютера или использовать его для реализации своих преступных замыслов. Именно по этой причине безопасность в Интернете это ключевой момент, который должен приниматься во внимание любым пользователем. Несмотря на большой выбор антивирусных решений и наличие огромного объема информации о том, как следует защищаться при использовании Интернета, миллионы взрослых людей ежегодно становятся жертвами кибер-преступлений. А что уж говорить о детях, которые значительно более наивные и доверчивые, чем мы, взрослые.

Помочь обезопасить себя в сети, стать добрым помощником в исследовании Интернета - задача настоящего родителя.

С уважением,

**Людмила Эфтимович,**

Уполномоченный по правам ребенка в Томской области.

## **1.Как выбрать компьютер для ребенка?**

- Постарайтесь понять, для каких задач требуется компьютер. Поговорите об этом с ребенком. От его ответов будет зависеть Ваше удовлетворение покупкой и радость ребенка. Абсолютно все современные обучающие программы, офисные приложения и, тем более, Интернет отнюдь не требуют от компьютера выдающихся характеристик в плане производительности и скорости работы. Однако, зная это, мы ведь не будем лишать ребенка удовольствия слушать музыку, смотреть на компьютере видео, осваивать (может быть, в совсем недалеком будущем) более сложные и поэтому требовательные к ресурсам программы и время от времени играть в компьютерные игры? Если все в меру, то ничто не повредит;

- Позаботьтесь о хорошем мониторе. От плохого монитора у ребенка будут слезиться и сильно уставать глаза, а медлительность агрегата при работе с современными программами ничего, кроме раздражения, не вызовет;

- Отнеситесь внимательно к "начинке" системного блока. Конечно, вам не нужно срочно становиться специалистом по компьютерам. Ваша задача - найти разбирающегося в теме знакомого, которому можно было бы доверять. Однако в любом случае, хотя бы в общих чертах, представлять, из чего состоит компьютер, полезно, да и знакомому будет легче объяснить, что вам нужно.

## **2. Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете, избежать столкновения с нежелательным контентом<sup>1</sup>?**

- Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации;
- Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете является правдой. Приучите их спрашивать о том, в чем они не уверены;
- Старайтесь спрашивать ребенка об увиденном в Интернете. Бывает, открыв один сайт, ребенок захочет познакомиться и с другими схожими ресурсами.

## **Предупреждение груминга<sup>2</sup>**

- Чтобы защитить и обезопасить своего ребенка, будьте в курсе, с кем контактирует в Интернете Ваш ребенок, старайтесь регулярно проверять список его контактов, чтобы убедиться, что он лично знает всех, с кем общается;
- Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать Интернет-знакомым, которых он никогда не встречал в жизни, свои фотографии;
- Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;

- Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым Интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
- Интересуйтесь тем, куда и с кем ходит Ваш ребенок.

### **Предупреждение кибербуллинга<sup>3</sup>**

- Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов, ведь читать плохие слова также неприятно, как и слышать их;
- Научите детей правильно реагировать на обидные слова или действия других пользователей;
- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- Старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также наблюдайте за его настроением после пользования Сетью;

***На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:***

- Беспокойное поведение: даже самый замкнутый и стеснительный ребенок будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу или на прогулку – самые явные признаки того, что ребенок подвергается агрессии;

- Неприязнь к Интернету: если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире;

- Нервозность при получении новых сообщений: негативная реакция ребенка на звук поступления письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих посланий.

### **Предупреждение кибермошенничества<sup>4</sup>**

- Расскажите ребенку о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;

- Прежде, чем совершить покупку в Интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности: изучить отзывы покупателей, проверить реквизиты и название юридического лица – владельца магазина, уточнить, как долго существует магазин. Посмотреть эту информацию можно в поисковике или по дате регистрации домена (сервис WhoIs).

## **Предупреждение Интернет-зависимости<sup>5</sup>**

- Оцените, сколько времени Ваш ребенок проводит в сети, не пренебрегает ли он, из-за работы за компьютером, своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками;
- Узнайте у ребенка о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости — чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить: ответить на все сообщения, проследить за всеми событиями, показать себя;
- Выясните, поддерживается ли интерес ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями;
- Понаблюдайте за сменой настроения и поведения Вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройство сна, снижение физической активности, потеря аппетита;
- Поговорите со школьным психологом и классным руководителем о поведении Вашего ребенка, его успеваемости и отношениях с другими учениками.

Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт;

- Узнайте, есть ли у Вашего ребенка навязчивое стремление выйти в Интернет с помощью телефона или иных мобильных устройств во время урока.

### **3. Как научить ребенка не загружать на компьютер вредоносные программы<sup>6</sup>**

#### ***Предупреждение столкновения с вредоносными программами:***

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения;

- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр:

- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелегальный контент;

- Периодически старайтесь полностью проверять свои домашние компьютеры;

- Делайте резервную копию важных данных;



- Старайтесь периодически менять пароли (например, от электронной почты), не используйте слишком простые пароли.

#### **4. Что делать, если ребенок все же столкнулся в сети Интернет с какими-либо рисками?**

- Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось;
- Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать;
- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно случившееся и насколько серьезно это могло повлиять на ребенка;
- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате Интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации: что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете;

## **5. Что делать, если ситуация связана с насилием в Интернете по отношению к ребенку?**

- Выясните всю возможную информацию об агрессоре;
- Узнайте историю взаимоотношений ребенка и агрессора, а именно: существует ли договоренность о встрече в реальной жизни; были ли такие встречи и что может быть известно агрессору о ребенке: реальное имя, фамилия, адрес, телефон, номер школы и т.п.;
- Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств: зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения;
- Скопируйте и сохраните всю собранную информацию: в дальнейшем это может помочь при обращении в правоохранительные органы;
- Настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;

### **Общие рекомендации по обеспечению безопасности детей и подростков в Интернете**

- Расположите компьютер Вашего ребенка в месте общей доступности: столовой или гостиной. Так вам будет проще уследить за тем, что делают дети в Интернете;
- Следите за тем, какие сайты посещают Ваши дети;

- Если у вас маленькие дети, знакомьтесь с Интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и обсудите, что допустимо, а что запрещено в Вашей семье;
- Список сайтов, которые посещает Ваш ребенок, можно найти в истории браузера;
- Воспользуйтесь инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube;
- Расскажите детям о безопасности в Интернете. Вы не сможете все время следить за тем, что Ваши дети делают в Сети;
- Помогите ребёнку научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом;
- Используйте и регулярно обновляйте антивирусное программное обеспечение;
- Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей;
- Научите детей ответственному поведению в Интернете;

Помните золотое правило: «То, что Вы не сказали бы человеку в лицо, не стоит отправлять ему по SMS, электронной почте, в чате или размещать в комментариях на его странице в Сети»;

- Оценивайте Интернет-контент критически. То, что содержится в Интернете, не всегда правда;
- Объясните ребёнку, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

## **Полезная информация**

*- Если Вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если Ваш ребенок уже столкнулся с рисками в Сети, можете обратиться:*

Линия помощи “Дети Онлайн”: сайт: [www.detionline.com](http://www.detionline.com); телефон: 8-800-2500-015 (звонок по России бесплатный). На линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет.

Всероссийский детский телефон доверия: 8-800-2000-122

(звонок с любого телефонного номера, в том числе мобильного — бесплатный).

*- Если Вы столкнулись с ситуацией, когда необходимо обратиться в правоохранительные и надзорные органы:*

Правоохранительный портал РФ: [www.112.ru](http://www.112.ru) — Общественная приёмная МВД России

Дежурная часть УМВД России по Томской области  
8(3822) 27-12-20;

Управление Роскомнадзора по Томской области: горячая линия  
8(3822)97-60-03

## Словарь терминов

---

<sup>1</sup> **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.

<sup>2</sup> **Груминг** - установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

<sup>3</sup> **Кибербуллинг** — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных Интернет-сервисов.

<sup>4</sup> **Кибермошенничество** — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

<sup>5</sup> **Интернет-зависимость** - навязчивое желание войти в Интернет, и неспособность выйти из интернета. (Гриффит В., 1996). По своим симптомам Интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером,

---

досада и раздражение при невозможности выйти в Интернет.

<sup>6</sup> **Вредоносные программы** (вирусы, шпионские программы и др.) - это программы, наносящие какой-либо вред компьютеру, на котором они запускается или другим компьютерам в сети. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.