

## **Проблемы информационной безопасности детей**

Выделим ключевые рекомендации, которые могут помочь родителям в решении проблемы безопасного пользования Интернет-ресурсами.

### **Как защитить ребенка от нежелательного контента в Интернете**

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

### **Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете**

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Специалисты используют специальный термин «груминг», обозначающий 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.

### **Предупреждение груминга:**

- Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;
- 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 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 отсутствие 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.

### **Как избежать кибербуллинга**

*Кибербуллинг* — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

- Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать;
- 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 следите за его настроением после пользования Сетью.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

Родителям следует обратить внимание на ряд признаков в поведении ребенка, которые могут свидетельствовать о том, что ребенок стал жертвой кибербуллинга:

- **Беспокойное поведение**

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – 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 письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

## **Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников**

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

Предупреждение кибермошенничества:

- Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных

системах, наиболее частым из которых является кража конфиденциальных данных.

### **Безопасное совершение покупок в Интернет-магазинах**

- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
- Необходимо вместе с ребенком познакомиться с отзывами покупателей;
- Проверьте реквизиты и название юридического лица – владельца магазина;
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить

### **Как распознать интернет-и игровую зависимость**

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого онлайн;
- увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

### **Как научить ребенка не загружать на компьютер вредоносные программы**

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. 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.

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) и не используйте слишком простые пароли.

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

1. **Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной.** Так вам будет проще уследить за тем, что делают дети в Интернете.
2. **Следите, 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 недопустимо в вашей семье. Список сайтов, которые посещает ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube.
3. **Расскажите детям о безопасности в Интернете.** Вы не сможете все время следить за тем, что ваши дети делают в Сети. Им необходимо научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом.
4. **Установите защиту от вирусов.** Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.
5. **Научите детей ответственному поведению в Интернете.** Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по MS, электронной почте, чате или размещать в комментариях на его странице в Сети.
6. **Оценивайте интернет-контент критически.** То, что содержится в Интернете, не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую

они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

7. Если Вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если Ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи “[Дети Онлайн](http://www.detionline.com)” ([www.detionline.com](http://www.detionline.com)), по телефону: 825 000 15 (звонок по России бесплатный).

### **Пять правил безопасного пользования электронной почтой:**

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
2. Никогда не отвечайте на спам.
3. Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
5. Никогда не пересылайте «письма счастья». Вместо этого сразу удалите их.

В приложении 1 помещены ответы на актуальные вопросы родителей по проблемам безопасного пользования Интернет-ресурсами, которые могут быть рассмотрены в ходе собраний, консультаций, а также размещены на школьных сайтах в рубрике «Для Вас, родители».

В приложении 2 помещены информационные материалы для педагогов к проведению с детьми разных возрастных групп классных часов, бесед по проблемам безопасности в сети Интернет.

### **Актуальные вопросы родителей Сколько времени ребенок может проводить за компьютером?**

Все родители, наверняка, часто говорят о том, что их дети много времени проводят за домашними заданиями или что их дети мало гуляют и, в основном, сидят дома. Поэтому родители вряд ли удивятся результатам исследований, показывающим, что дети проводят за компьютером слишком много времени. Этому вопросу родителям надо уделить особое внимание. Сегодняшним детям компьютер заменил множество разнообразных действий. Эта машина помогает им в выполнении домашних заданий, а при необходимости предоставляет услуги телефонной связи, «игровой площадки», музыкального и видео сервиса и других развлечений.

Ваше беспокойство должно зависеть от того, каким образом ваш ребенок использует отведенное ему для компьютера время и много ли времени ему остается для других занятий и развлечений. Если ребенок, просыпаясь утром или

вбегая домой после школы, в первую очередь включает компьютер и сидит за ним до тех пор, пока не ляжет спать, у вас, скорее всего, будут проблемы.

Совсем маленьким детям до пяти лет не следует проводить много времени за компьютером. Жизненно важным для них является развитие познавательных способностей и изучение других видов деятельности. Дети 10-летнего возраста должны совмещать компьютер с другими занятиями. В отношении раннего школьного возраста трудно сказать, сколько точно времени отвести ребенку на компьютер, т.к. в этом возрасте дети очень различаются по развитию. Некоторые дети пытаются в любую свободную минуту выйти в чат (наподобие тех из нас, взрослых, которые любят болтать по телефону). Других притягивает сам компьютер: учебные программы, создание веб-страниц, устройство компьютера.

Наш совет – внимательно следите за поведением ребенка. Какие-либо изменения в его поведении станут лучшим индикатором негативных явлений, которые должны насторожить Вас. Например, если ребенок перестал общаться с друзьями, заниматься спортом или просто выходить на улицу, или же у него резко упала успеваемость в школе – все это вы должны проанализировать. Если ваш ребенок замкнут или необщителен, то вы должны со всей серьезностью отнестись к увлечению Вашего ребенка компьютером. Поэтому, решение вопроса лимита времени, проводимого Вашим ребенком за компьютером, зависит, прежде всего, от Вас самих, с учетом того, что Вы будете внимательно следить за поведением ребенка и хорошо представлять себе, для чего именно ребенок использует компьютер. При этом некоторые медики предлагают четкие возрастные схемы максимально допустимого времени пользования компьютером.

### **С какого возраста можно разрешать ребенку пользоваться своей собственной электронной почтой?**

Не существует жесткого возрастного ограничения. Самый простой ответ: вы можете допустить ребенка к e-mail в том случае, если он выражает желание пообщаться с кем-нибудь модным образом. Прежде чем зарегистрировать почтовый ящик, предложите ему для начала использовать ваш и под присмотром написать, например, брату или лучшему другу.

Электронная почта – это здорово, потому что она преодолевает все географические и возрастные барьеры. Как правило, дети становятся готовыми к использованию e-mail с 7-8 летнего возраста.

### **Следует ли использовать программу контроля за поведением ребенка в Интернете?**

Родители, в целом, еще не пришли к единому мнению по этому вопросу и, как правило, делятся на два лагеря. Одна сторона считает, что контроль за поведением дает детям гарантию безопасности, другие категорически возражают им тем, что это равносильно организации слежки за детьми.

Программы контроля предназначены для того, чтобы точно знать, что ваш ребенок делает в Интернете. Они позволяют Вам вести запись адресов, которые ваш ребенок посещает в Интернете. Известны даже случаи, когда ведение подобных записей помогало представителям правоохранительных органов.

Видимо, вывод может быть следующий. Если вы решились поставить компьютерную деятельность Вашего ребенка под контроль, вам следует поставить его в известность. Если же вы контролируете своего ребенка без его ведома, вы, действительно, шпионите за ним. Скорее всего, если вы расскажете ребенку, что установили программу контроля в целях его собственной безопасности, он поймет вас. И, наконец, помните, что вашей основной целью является воспитание молодого человека, который сможет правильно пользоваться Интернетом, даже если никто не будет его контролировать.

### **Ваш личный Интернет рекомендует:**

- Не публикуйте свои личные данные и личные данные своих друзей.
- К личным данным относятся номера мобильного и домашнего телефонов, адрес электронной почты и любые фотографии, на которых изображены ты, твоя семья или друзья.
- Если Вы публикуете фото- или видеоматериалы в Интернете – любой желающий может скопировать их и потом воспользоваться в своих целях.
- Не верьте спаму (нежелательной электронной рассылке) и не отвечай на него.
- Не открывайте файлы, полученные от людей, которых Вы не знаете. Неизвестно, что они могут содержать: это может быть как вирус, так и незаконный материал.
- Следите за тем, что пишете. Не пишите людям то, что никогда бы не сказали им в лицо.
- Не забывайте, что люди в Интернете могут говорить неправду.
- Лучше не встречайтесь со своими виртуальными друзьями в реальной жизни без присутствия взрослых, которым Вы доверяете.
- Никогда не поздно рассказать родителям, если что-то смущает или настораживает.