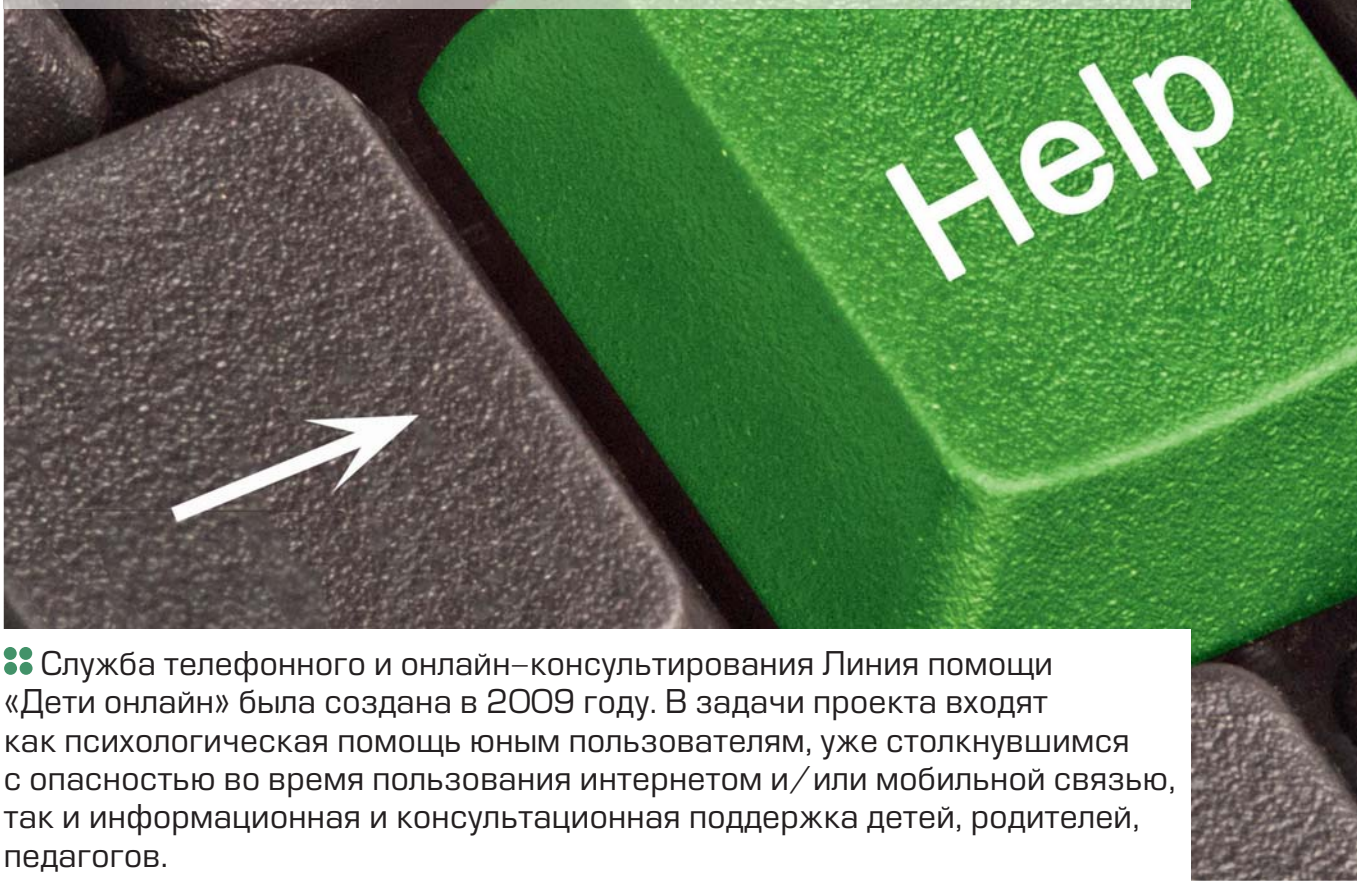
Глобальная сеть: правила пользования

Как защитить ребенка от столкновения с вредоносной информацией в сети? Как научить его справляться с последствиями таких встреч? Линия помощи «Дети онлайн» представляет рекомендации для родителей



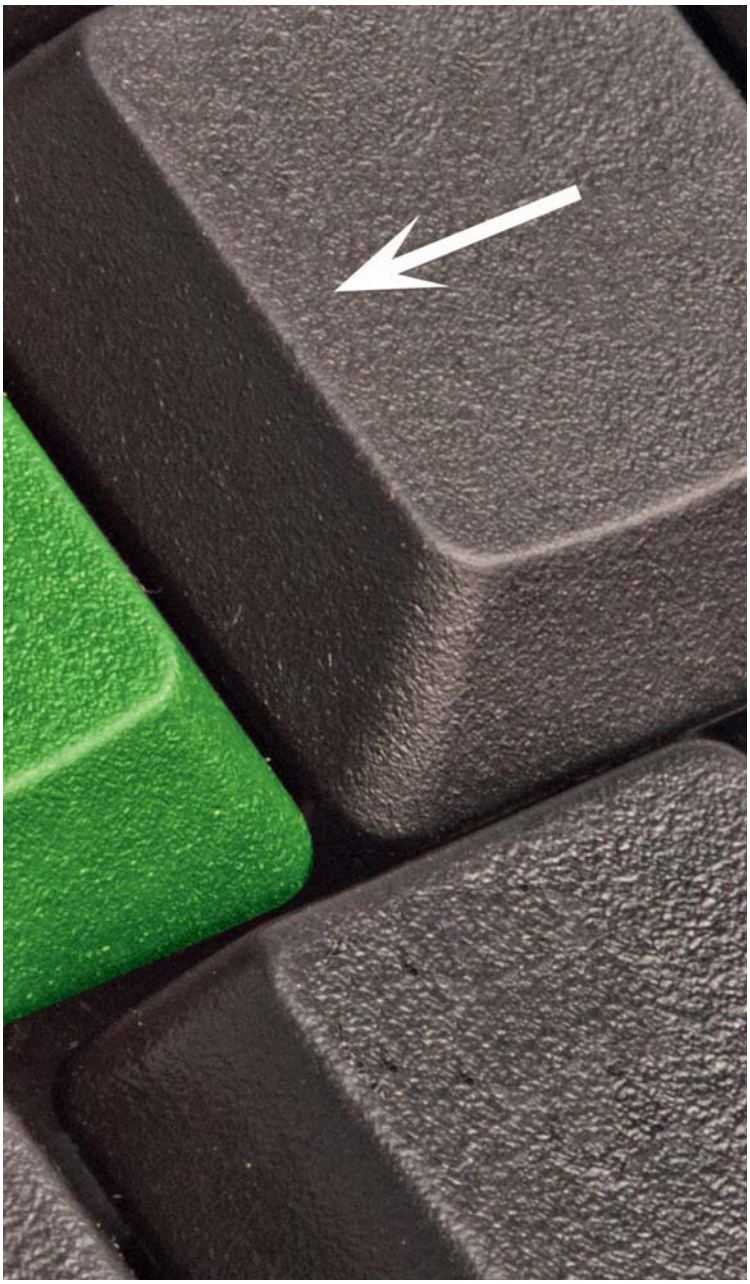
Служба телефонного и онлайн–консультирования Линия помощи «Дети онлайн» была создана в 2009 году. В задачи проекта входят как психологическая помощь юным пользователям, уже столкнувшимся с опасностью во время пользования интернетом и/или мобильной связью, так и информационная и консультационная поддержка детей, родителей, педагогов.

Обратиться на Линию помощи можно:

- по телефону 8–800–250–00–15 (с 9 до 18 по рабочим дням). Звонки по России бесплатные
- по электронной почте helpline@detionline.com
- на сайте www.detionline.com

Знакомства в интернете

При общении в сети существует угроза подвергнуться рискам, связанным с контактами с другими людьми, не всегда знакомыми в реальной жизни. Особенно опасен грумминг — установление дружеских отношений с ребенком с целью вступления в сексуальные отношения. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), преступник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.



Предупреждение груминга:

1. Будьте в курсе, с кем взаимодействует в интернете ваш ребенок. Старайтесь регулярно проверять список его контактов, чтобы убедиться, что он лично знает всех, с кем общается.

2. Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии.

3. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн–играх), нельзя использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.

4. Если ребенок интересуется контактами с людьми намного старше его, следует обратить на это внимание и провести с ним разъяснительную беседу.

5. Не позволяйте 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.

6. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Кибербуллинг

Кибербуллинг – преднамеренное и протяженное во времени агрессивное поведение по отношению к жертве, осуществляемое одним человеком или группой людей посредством различных электронных сервисов.

Предупреждение кибербуллинга:

1. Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова — читать грубости так же неприятно, как и слышать.

2. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

3. Научите детей правильно реагировать на обидные слова или действия других пользователей.

4. Объясните детям, что информация, которую они выкладывают в интернете, может быть использована против них.

5. Старайтесь следить за тем, что ваш ребенок делает в интернете, а также следите за его настроением после пользования сетью.

Кибермошенничество

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

Предупреждение кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться с взрослыми перед тем, как воспользоваться теми или иными услугами сети.

2. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.

3. Интернет-магазины:

- Ознакомьтесь с отзывами покупателей.
- Избегайте предоплаты.
- 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 выдачей кассового чека.
- Сравните цены в разных интернет-магазинах.
- Позвоните в справочную магазина.
- Обратите внимание на правила интернет-магазина.
- Выясните, сколько точно вам придется заплатить.

Противозаконный и неэтичный контент

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 наркотиков и действий, причиняющих вред физическому и психическому здоровью. Столкнуться с рисками такого рода можно практически везде: сайты, социальные сети, блоги, торренты, видеохостинги. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Предупреждение столкновения с неэтичным или противозаконным контентом:

- Установите на компьютер специальные программные фильтры (при нажатии на вылетающий баннер вместо страницы будет всплывать пустое окно) или специальные программы, называемые системами родительского контроля (они позволяют родителям решать, какое содержимое могут просматривать их дети).

- Приучите ребенка советоваться с взрослыми и немедленно сообщать о появлении подобного рода нежелательной информации.

- Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете — правда. Научите 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.

Вредоносные программы

Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру

и нарушить конфиденциальность хранящейся в нем информации. Они также способны снижать скорость обмена данными с интернетом и даже использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой–либо социальной сети.

Предупреждение столкновения с вредоносными программами:

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

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

3. Периодически старайтесь полностью проверять свои домашние компьютеры.

4. Делайте резервную копию важных данных.

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

Если ребенок все же столкнулся с какой–либо угрозой в сети, и она оказала на него негативное влияние

- Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.
- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и в какой степени 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 деньги в результате интернет–мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату — непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.
- Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об агрессоре, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Жестко настаивайте на том, чтобы ребенок избегал встреч с незнакомцами, особенно без свидетелей. Проверьте все новые контакты ребенка за последнее время.
- Соберите наиболее полную информацию о происшествии как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.
- Если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, если ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, если вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться, если требуется вмешательство психолога, полиции или других служб и организаций.

С более подробными рекомендациями вы можете ознакомиться на сайте www.detionline.com