

## Памятка для родителей

В памятке представлены практические рекомендации о том, как помочь юным пользователям оставаться в безопасности в киберпространстве и избежать существующих рисков. Что делать, если ребенок все же столкнулся с какими-либо рисками?

### Как защитить ребенка от нежелательного контента в Интернете

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 булимиа, суицида, азартных игр, наркотических веществ и т.д.

### Как помочь ребенку избежать столкновения с нежелательным контентом:

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. Страйтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами. Включите программы родительского контроля и безопасного поиска, которые помогут оградить ребенка от нежелательного контента.

Постоянно объясняйте ребенку правила безопасности в Сети. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Используйте специальные настройки безопасности (инструменты родительского контроля, настройки безопасного поиска и др.).

Выработайте «семейные правила» использования Интернета. Ориентируясь на них, ребенок будет знать, как поступать при столкновении с негативным контентом.

Будьте в курсе того, что ваш ребенок делает в Интернете. Чаще беседуйте с ребенком о том, что он делает в Сети.

### 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. Общаюсь 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, страйтесь 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 пересыпать 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 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.

### Объясните ребенку основные правила поведения в Сети:

- ✓ нельзя делиться с виртуальными знакомыми персональной информацией, а встречаться с ними в реальной жизни следует только под наблюдением родителей;
- ✓ если интернет-общение становится негативным – такое общение следует прервать и не возобновлять.

## Как избежать кибербуллинга

Кибербуллинг – преследование сообщениями, содержащими оскорблении, 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 так же неприятно, как и слышать;
- научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем;
- если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.
- 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.

### Как защититься от кибербуллинга:

Не провоцировать. Общаться в Интернете следует этично и корректно. Если кто-то начинает оскорблять ребенка в Интернете – необходимо порекомендовать уйти с такого ресурса и поискать более удобную площадку.

Если по электронной почте или другим каналам кто-то направляет ребенку угрозы и оскорблений – лучше всего сменить электронные контакты (завести новый e-mail, Skype, ICQ, новый номер мобильного телефона).

Если кто-то выложил в Интернете спену киберуничения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию. 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.

Что на что следует обращать внимание родителям, чтобы вовремя заметить, 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 причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое).

### 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.