

Правила безопасности в сети Интернет для детей и родителей

Научите ваших детей соблюдать основные правила безопасности работы в сети Интернет. По мере взросления детей добавляются новые разъяснения безопасного поведения в Сети, о которых нужно помнить родителям.

1. Не входите на незнакомые сайты. Не переходите по подозрительным ссылкам. Не отвечайте на «спам».
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Никогда не посылайте никому свой пароль. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв, а также периодически меняйте их.
4. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник). При общении лучше выбирать ник, не позволяющий определить половую принадлежность и возраст (не стоит делать частью виртуального псевдонима год своего рождения). Никогда не давай информацию о себе, которая может указать, что ты — ребенок.
5. Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире. в виртуальном пространстве необходимо вести себя абсолютно так же, как в реальности. Не грубить, не сквернословить и не оскорблять других.
6. Незаконное копирование продуктов труда других людей (музыки, игр, программ и т.д) считается плагиатом (умышленное присвоение авторства чужого произведения).
7. Не верьте всему, что вы видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым. Учите ребенка избирательно относиться к информации в Сети и всегда проверять ее.
8. Нельзя сообщать другим пользователям интернета свою личную информацию (адрес, номер телефона, номер школы, любимые места для игр, местоположение ребенка и родителей, планы, касающиеся длительных путешествий, каникул и отпусков, фото дорогих вещей, фото квартиры, автомобиля или дома, информация о личных документах, номерах автомашин, фото личных документов, банковских карт и т. д. Не отправляйте фотографии людям, которых вы не знаете. Не надо, чтобы незнакомые люди видели ваши личные фотографии.
9. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в интернете чем-то, что требует указания идентификационного имени пользователя, тогда выберите это имя вместе со взрослыми, чтобы убедиться, что оно не содержит никакой личной информации.
10. Не сохраняйте важные сведения на общедоступном компьютере. Расскажите ребёнку, что если он использовал чужой компьютер (планшет, смартфон) для просмотра своей странички в социальной сети, то должен обязательно выходить из аккаунта по окончании работы. Нельзя на чужих устройствах сохранять пароли — это могут использовать злоумышленники.
11. Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями лично. Главный принцип: если незнакомец кажется подозрительным, угрожает, обещает подарки, деньги или настойчиво просит о чем-то, общение в Сети с ним необходимо моментально прекратить.
12. При возникновении чувства неловкости или тревоги при виртуальном диалоге, а также, если собеседник навязчиво настаивает на перенос отношений в реал, следует прекратить общение и сообщить старшим; Виртуальное знакомство не должно перерасти в реальное. Если такое решение принято, встреча должна состояться в общественном месте и под контролем родителей;
13. Научитесь доверять интуиции. Если что-нибудь в интернете будет вызывать у вас психологический дискомфорт, поделитесь своими впечатлениями с взрослыми.
14. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть вас во время разговора, т.к. он может быть записан.
15. Не добавляйте незнакомых людей в свой контакт лист (ICQ, MSN messenger, соцсети и т.д.).

Блоги

Ведение блогов, иными словами «сетевых дневников», очень популярно среди подростков. Многие из них ведут блоги втайне родителей. Если же ваш ребёнок является автором блога, то необходимо проследить, чтобы юный автор не слишком много выкладывал в сеть информации личного характера о себе и семье. Избежать проблем поможет следование рекомендациям:

1. **Предварительный просмотр.** Родителям следует предварительно посмотреть содержание того, что собирается публиковать в блоге ваш сын или дочь, и только после этого одобрять или нет публикацию.
2. **Адекватна ли информация?** Если да, то право на жизнь у такой статьи (фотоподборки) есть.
3. **Проверяем блог.** Время от времени знакомьтесь с содержанием блога ребёнка, читайте комментарии.
4. **Мониторинг.** Сделайте подборку лучших блогов и продемонстрируйте ребёнку хороший вариант при возникновении какой-то проблемы.

Советы по безопасности в сети Интернет для родителей

1. Соблюдайте время нахождения ребенка в сети интернет.
2. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
3. Используйте специальные детские поисковые машины, типа MSN Kids Search.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
6. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
7. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
8. Научите детей не загружать файлы, программы или музыку без вашего согласия.
9. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
10. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
11. Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
12. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Семейное соглашение

Соберитесь вместе, всей семьей, и предложите разработать своеобразный документ, в котором будут отражены все права и обязанности каждого из участников интернет-сообщества, то есть каждого из домашних, так или иначе использующих ПК с целью выхода в Сеть, в том числе и правила безопасности детей в Интернете. Пусть вас не пугает столь официальный подход к житейским делам. Дети любят, когда к ним относятся "по-взрослому". Поэтому их отношение к семейному соглашению будет принято со всей доступной детскому пониманию серьезностью. Такое мероприятие по интернет-безопасности позволит ребенку проникнуться уважением к оказанному ему вниманию. Результат не заставит себя ждать.

- *Какие именно интернет-ресурсы (сайты) могут посещать ваши дети и с какой целью.*
- *Сколько времени ребенок может находиться в Сети (имеется в виду общее время с учетом критерия периодичности).*
- *Какие действия необходимо предпринять в случае обеспокоенности ребенка.*
- *Научите ребенка пользоваться браузером и мессенджерами. Именно на этом умении и базируются основы безопасности в Интернете.*

Антивирусная защита

Трудно представить, что может произойти с пользовательской машиной (ПК) при работе в Сети, если на ней не установлен соответствующий софт, который способен противодействовать зловредному коду в виде разнообразных программных вирусов. А ведь информационная безопасность детей в Интернете напрямую зависит от эффективности антивирусной защиты. Антивирусы обычно имеют в своем арсенале массу встроенных фильтров, в том числе собственный «Родительский контроль», так сказать, повышенной бдительности.

Для осуществления родительского контроля важно применять и различное программное обеспечение. Установите любую из программ в зависимости от операционной системы вашего компьютера — это поможет отфильтровать вредоносное содержимое; выяснить, какие сайты посещает ваш ребенок; установить временные рамки использования компьютера (или Интернета); блокировать нежелательные действия маленького пользователя в Сети.

Популярные программы родительского контроля

- *«Дополнительная безопасность» в Windows 7 — обеспечит сохранность личных данных от всех возможных угроз;*
- *«Семейная безопасность» в WindowsLive — поможет уследить за контактами и интересами вашего ребенка даже с другого компьютера;*
- *«Родительский контроль» в WindowsVista — с ее помощью вы можете определить время, когда ребенок может зайти в систему, а также с помощью фильтра установить запрет или к отдельным играм, узлам, программам.*
- *«Родительский контроль» в KasperskyCristal — помимо антивирусной программы, она позволяет следить за тем, по каким сайтам ходит ребенок, и ограничивать посещение «неудобных». Кроме того, программа поможет вам сохранить личную информацию (семейные фото, пароли, файлы) от вторжения и хищения.*