**Наши краткие рекомендации помогут вам обеспечить безопасность членов вашей семьи в Интернете, даже если вам вечно не хватает времени.**

1. **Поговорите с ребенком о безопасности в Интернете**. Объясните основные правила, возможности различных технологий и последствия нарушений. Самое главное: убедите ребенка, что в любой непонятной или пугающей ситуации ему следует обращаться к родителям, чтобы найти безопасное решение.
2. **Используйте компьютер и смартфон вместе с детьми**. Это хороший способ научить их правилам безопасности в Интернете. При этом дети поймут, что решать возможные проблемы лучше всего вместе.
3. **Расскажите детям больше о сайтах и сервисах в Интернете**. Поговорите о том, что их интересует в Интернете и какие страницы им можно посещать.
4. **Безопасные пароли**. Помогите своей семье приобрести правильные привычки в отношении паролей. Расскажите об их использовании. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.
5. **Используйте настройки конфиденциальности и управления доступом**. В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации. Поговорите с членами своей семьи и определите, о чем не следует рассказывать всем. Научите детей уважать конфиденциальность друзей и родных.
6. **Проверьте возрастные ограничения**. Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет. Прежде чем ваш ребенок зарегистрируется на том или ином сайте, самостоятельно проверяйте условия его использования и соответствие материалов правилам, принятым в вашей семье.
7. **Научите детей ответственному поведению в Интернете**. Помните золотое правило: то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.
8. **Посоветуйтесь с другими взрослыми**. Привлеките к обсуждению этой темы друзей, родственников и педагогов. Другие родители и специалисты по работе с детьми могут оказать вам неоценимую помощь в том, как научить детей и родственников правильному использованию самых разных информационных технологий.
9. **Защитите свой компьютер и личные данные**. Используйте антивирусное программное обеспечение и регулярно его обновляйте. Поговорите со своей семьей о типах личной информации – например, номер социального страхования, номер телефона или домашний адрес – эти данные не должны быть размещены в Интернете. Научите свою семью не принимать файлы или открывать вложения в электронной почте от неизвестных людей.
10. **Не останавливайтесь на достигнутом**. Безопасность в Интернете требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе. Пересматривайте правила пользования Интернетом в семье, следите за тем, как ваши близкие осваивают новые технологии, и время от времени давайте им советы.

**Технологии безопасной работы в сети**

* **Безопасность при навигации по сайтам и по приему почты**

1. Не ходите на незнакомые сайты.

2. Если ходите, то выключайте (на всякий случай) поддержку языка Java и использование cookies.

3. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

4. Если пришел **exe-файл**, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов. Вот недавно хакерами был вскрыт один из крупнейших узлов бесплатной почты Hotmail. Так что не исключено, что с адреса вашего знакомого придет вирус.

5. Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).

6. Никогда, никому не посылайте свой пароль.

7. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше сгенерируйте его специальной программой или попросите сделать это своего провайдера.

* **Пять советов по безопасности при работе на общедоступном компьютере**

*1. Не сохраняйте свои учетные данные для входа в систему*.

 2. *Не оставляйте без присмотра компьютер с важными сведениями на экране***.**

*3.Заметайте свои следы***.**

*4.Опасайтесь подглядывания через плечо.*

*5.Не вводите важные сведения на общедоступном компьютере.*

* **Программы-фильтры**
1. **Power Spy 2008 (**[**http://www.securitylab.ru/software/301944.php**](http://www.securitylab.ru/software/301944.php)**) Программу удобно использовать,** чтобы узнать, чем заняты дети в отсутствие родителей.
2. **iProtectYou Pro (**[**http://soft.mail.ru/program\_page.php?grp=5382**](http://soft.mail.ru/program_page.php?grp=5382)**) Программа-фильтр интернета,** позволяет родителям ограничивать по разным параметрам сайты, просматриваемые детьми.
3. **KidsControl (**[**http://soft.mail.ru/program\_page.php?grp=47967**](http://soft.mail.ru/program_page.php?grp=47967)**) Предназначение KidsControl –** контроль времени, которое ребенок проводит в интернете.
4. **CYBERsitter (**[**http://www.securitylab.ru/software/240522.php**](http://www.securitylab.ru/software/240522.php)**) CYBERSitter дает взрослым возможность ограничивать доступ детей к нежелательным ресурсам в Internet.**
5. **КиберМама 1.0b (**[**http://www.securitylab.ru/software/273998.php**](http://www.securitylab.ru/software/273998.php)**) КиберМама** проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет.

**КиберМама поддерживает следующие возможности:**

* Ограничение по суммарному времени работы
* Поддержка перерывов в работе
* Поддержка разрешенных интервалов работы
* Возможность запрета интернета
* Возможность запрета игр/программ