# Безопасность детей в интернете. 10 советов родителям

Что же делают дети в интернете? Давайте обратимся к результатам исследования Лаборатории Касперского, проведенного в 2016 году. Дети сегодня гораздо более зависимы от своих гаджетов. По результатам опроса, 44% детей в возрасте от 8 до 16 лет остаются онлайн постоянно. Что же касается США, то там эта цифра составляет 83%, в России и Беларуси еще больше – 88%.

Какие данные разглашают наши дети:

- 40% детей разглашают конфиденциальные данные о себе или своей семье.
- 57% из них используют в Сети свое настоящее имя
- 47% вводят настоящий возраст
- 40% указывают школу, в которой учатся
- 14% детей приводят свой точный адрес проживания
- 11% не скрывают, сколько зарабатывают их родители.
- 31% детей использовали телефон для совершения финансовых операций онлайн (в том числе и для оплаты встроенных покупок в приложениях) и хотели бы сделать это снова.

Безопасность в интернете безусловно важна, поэтому КВ подготовили для родителей 10 советов.

**Совет 1. Доверяйте своему ребенку, иначе технические средства будут бессильны!**

Если по какой-то причине вы не можете доверять вашему ребенку или он не доверяет вам, все остальные советы можно уже не читать. Вы упустили воспитание. Ребенка нельзя держать в клетке. У вас это просто не получится. Все средства родительского контроля вспомогательные. Они просто помогают вам узнать, чем занят ваш ребенок.

Безусловно, вы сможете оградить его от тех или иных опасностей при использовании ПК или гаджетов. Но кто и что убережет его от похода к другу (подружке), в интернет-кафе? Там нет мамы и папы. И если он (она) не имеет собственных воспитательных тормозов, то ваш контроль будет бессилен.

**Совет 2. Заведите отдельную учетную запись на ПК для вашего ребенка**

Прежде чем говорить о родительском контроле, заведите ребенку отдельную учетную запись с правами обычного пользователя на вашем ПК.

Убедитесь, что ваша учетная запись (то ли общая для родителей, то ли отдельная для каждого из них защищена устойчивым паролем). Под устойчивым имеется ввиду пароль длиной не менее 8 символов, содержащий большие и маленькие буквы латинского алфавита, а также цифры или спецсимволы.

После этого вы сможете довольно легко задать расписание доступности вашего ПК для ребенка. То есть, например, в рабочие дни с 18-00 до 20-00 или в любое другое время, когда кто-то из взрослых будет дома.

**Совет 3 Объясните ребенку, что не следует давать частной информации о себе без разрешения родителей**

Ребенок не должен в интернете выкладывать следующие сведения:

- Имя
- Возраст
- Номер телефона
- Номер школы
- Домашний адрес и прочие персональные данные

Убедитесь, что у него нет доступа к вашим банковским данным.

Научите ребенка использовать ники (прозвища) при использовании интернета. Анонимность – хороший способ защиты. Не выкладывайте фотографии ребенка в социальных сетях.

**Совет 4. Не следует открывать письма электронной почты, файлы или web-страницы, полученные от людей, которые не знакомы или не внушают доверия**

Научите его, как следует поступать при столкновении с подозрительным материалом, расскажите, что не нужно нажимать на ссылки в электронных сообщениях, полученные из неизвестных источников, открывать различные вложения.

**Совет 5. Ребенок должен понять, что его виртуальный собеседник может выдавать себя за другого**

Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. И 10-летний друг вашего ребенка в реальности может оказаться злоумышленником. Поэтому запретите ребенку назначать встречи с виртуальными знакомыми.

**Совет 6. Заведите ребенку его собственный адрес электронной почты**

Научите вашего ребенка правильным способам аутентификации при работе с почтой. Постарайтесь заводить электронный адрес на почтовых серверах, использующих двухэтапную аутентификацию(Hotmail.com, Outlook.com, Gmail.com, Mail.ru, Yandex.ru).

Поясните ребенку, что в случае необходимости регистрации для прохождения игрушек лучше использовать специальный, игровой адрес. А еще лучше – специальный алиас к основному адресу. Это довольно легко как настраивается, так и удаляется на Hotmail.com или Outlook.com.

Постарайтесь, чтобы он регистрировался на таких серверах в вашем присутствии и не указывал свои реальные данные.

**Совет 7. Поясните детям что не все что они видят или читают в интернете обязательно правда**

Приучите их спрашивать вас, если вдруг они сомневаются в прочитанном.

**Совет 8. Проведите беседу об интернет-этике**

Не ссылайтесь на то, что вы никогда не увидите своего собеседника. Отсутствие возможности видеть и слышать собеседника - это не повод для хамства.

**Совет 9. Контролируйте детей с помощью специального ПО родительского контроля**

Да, безусловно, вы доверяете своему ребенку. Но все же учтите, что это все еще ребенок и вы, безусловно, должны его контролировать. Применяйте для этого специализированное

программное обеспечение родительского контроля. Сегодня выбор такого ПО огромен. Безусловно, вы можете применять как бесплатное, так и платное ПО.

**Совет 10. Не забывайте о том, что ваш ребенок — это личность!**

Применяя ПО родительского контроля, легко скатиться в другую крайность и лишить ребенка права на ошибку. Учтите, ваш ребенок может легко обидеться на вас и обязательно так и будет, если поймет, что вы просто ему не доверяете. Поэтому обязательно обговаривайте ограничения вместе с ним, чтобы он понимал, почему вы делаете так, а не иначе.

Вообще, разговор о детской безопасности, на мой взгляд, требует не столько усилий специалистов по информационной безопасности, сколько простого разговора с ребенком. Ребенок должен понимать почему вы решились на принятие тех или иных правил.

Наиболее сложная задача, стоящая перед каждым из нас - это быть достойными папами и мамами, дедушками и бабушками. И если вы сами этому не научитесь, то никакой специалист по информационной безопасности и никакой психолог вас этому не научит.

**Владимир Безмалый**

**Microsoft Security Trusted Advisor,**

**MVP Consumer Security**