

Безопасность в интернете: краткая инструкция для родителей

В пёстром Интернете найти можно всё что угодно, даже если не искать. Взрослый человек регулярно борется с навязчивыми баннерами, всплывающими из ниоткуда окнами, неизвестными программами, которые бонусом идут к скачанному фильму. Чтобы потреблять Интернет-контент, необязательно даже уметь писать – спасибо голосовому поиску – и дети сталкиваются с теми же угрозами и проблемами, что и взрослые. Единственная проблема – они дети, и не всегда знают, как грамотно поступить.

Бытует мнение, что учить детей безопасному поведению на улице нужно, а в Интернете – само сложится. Написан ведь закон о защите детей от информации. Можно еще надеяться на школу, недаром есть отдельный предмет – информатика. Там школьники забивают формулы в Excel, делают сайты в Блокноте, иногда показывают учителю, как монтировать видео. Тут не до безопасности. Вот и получается, что в семье меры предпринимаются только после экстренных ситуаций : ребенок опустошил родительскую карту, случайно оформив подписку на платный контент, был пойман за просмотром «видео для взрослых», познакомился с кем-то и пошел на свидание...

Актуальность тех или иных Интернет-угроз меняется вместе с возрастом ребенка. Дошкольники и младшие школьники рискуют нажать «не туда» и увидеть то, что не должны были бы видеть, ребята постарше запросто оставляют открытыми странички «Вконтакте» на школьных компьютерах, и подростка не заставишь игнорировать друзей, которых он не знает в реальной жизни. Это лишь малая часть опасностей. Кибербуллинг и киберсуицид, секстинг, фишинг, вредоносное программное обеспечение , трекинг данных – список огромный, и далеко не со всем разберётся антивирусная программа.



Если вы заинтересованы в безопасном пребывании ребенка в Интернете, к вопросу стоит подойти **комплексно**:

1) Оцените масштаб рисков. Поймите, с чем вам предстоит иметь дело. Сколько устройств у вас в доме, к которым имеет доступ ребенок? Есть ли у них выход в Интернет? Если да, каким образом они защищены от кибер-атак? Игровая приставка тоже считается. Какими из этих устройств чаще пользуются дети? В вашем присутствии и когда вас нет рядом – это могут быть разные девайсы. Кстати, кристально чистая история посещений не означает, что браузер никто не открывал.

2) Разберитесь в вопросе. Для дошкольников и младших школьников родитель – авторитет и эксперт, и они ждут помощи взрослых в деле освоения Сети. Это потом оказывается, что страничку эксперта несколько раз взламывали и что такое брандмауэр он не представляет. Не менее половины подростков помогают старшим осваивать Интернет, что снимает ответственность с родителя, ведь какой смысл объяснять, если «он всё знает лучше меня». Но «знает» не означает «применяет на практике». Да и в теории бывают пробелы: их помогает обнаружить даже нехитрый тест по безопасности в Интернете на Яндексe.

3) Используйте специальные настройки и программы. В большинстве десктопных и портативных устройств есть встроенные в систему функции защиты и родительского контроля, позволяющие выставить ограничение на использование и скачивание программ. А в браузерах можно блокировать нежелательные для посещения сайты и выставить фильтры для поисковых запросов. Существуют и комплексные решения от разработчиков антивирусного ПО: с их помощью возможно контролировать присутствие ребенка в Сети на всех устройствах, получать уведомления о «подозрительной» активности и следить за изменениями на персональных страничках в социальных сетях.

4) Установите понятные нормы и правила поведения в Интернете. Любые ограничения должны быть четко сформулированы, а главное – обоснованы (здравым смыслом, объективной угрозой, логикой). И если у младших школьников создание отдельного безопасного аккаунта не вызовет протеста, то с подростками такие жесткие меры не пройдут. Хотя и они, наверняка, предпочтут бездушную программу маме, тайком просматривающей переписку с друзьями. Любые правила необходимо время от времени пересматривать и расширять зону самостоятельности ребенка.

5) Будьте примером. Ваш пароль электронной почты – дата рождения ребенка? В открытом Инстаграме красуется фото дорогого подарка с прикреплённой геометкой? Отправляете скан паспорта коллегам в общий чат? Не стоит ждать от детей того, что не могут выполнять взрослые.

6) Учитесь вместе. Если вы рассказали ребенку обо всех опасностях, что знаете сами, пришло время стимулировать его собственную поисковую активность. Попросите найти интересные видео-уроки или мультфильмы и устройте семейное обучение. Спрашивайте, что вызывает трудности, и помогайте разобраться. Обсуждайте сложные случаи, которые были у вас или спорные вопросы из СМИ. Ключевая задача – научить ребенка самостоятельно определять, что можно и нельзя делать на просторах Сети, и поэтому информация должна быть им активно переработана, осмыслена и обсуждена.

7) Стройте открытые и доверительные отношения. Универсальных способов по борьбе с Интернет-угрозами не существует: технологии не стоят на месте, опасности меняются. А вот честные отношения с ребенком – инвестиция вечная. Старайтесь прийти к тому, чтобы дети свободно рассказывали обо всём, что вызывает у них непонимание или дискомфорт в Интернете. Уверенность детей в том, что помощь и поддержка всегда рядом – ваша уверенность в их безопасности.