Осторожно, соцсети! 8 правил безопасности

Вот что надо сделать родителям, чтобы общение в социальной сети было для ребенка безопасным со всех точек зрения.

1. Заведите ребенку личную электронную почту (если таковой еще нет, конечно). Аккаунт в соцсети останется с ребенком навсегда (ну или на очень продолжительное время). Регистрировать его на свою почту или на какой-то специально заведенный для этого временный вариант не имеет никакого смысла.

2. Объясните ребенку, что пароли основной электронной почты и социальной сети должны быть , во-первых, **надежными** (состоять как минимум из 8, а лучше из 12 символов, содержать буквы в разном регистре, специальные символы и цифры), во-вторых, **запоминающимися** (придумайте какой-то алгоритм, который позволит запомнить пароль), в-третьих, **разными и уникальными** , чтобы в случае получения злоумышленниками доступа к паролю от почты социальная сеть не была также утеряна и наоборот.

И уж тем более чтобы ребенок не потерял аккаунты от этих важных ресурсов из-за утечки базы паролей с малозначимого интернет-магазина.

3. Установите по возможности и в электронной почте, и в соцсети подтверждение входа с помощью одноразового СМС-пароля.

4. Установите специальную программу для детской онлайн-безопасности, которая умеет работать с соцсетями. Такие программы не должны уметь читать личную переписку ребенка, их задача – помочь вам мониторить его активность в соцсети. Это так же важно, как знать о его действиях в реальной жизни.

Программа поможет вам быть в курсе того, кого ребенок добавляет в друзья, в какие группы он вступает и что размещают на его стене.

5. Настройте вместе с ребенком безопасность и приватность его аккаунта – доступ к его странице и к возможности писать ему личные сообщения должен быть только у его друзей.

6. Заполните страницу ребенка вместе с ним, объяснив, что такую важную информацию, как адрес и телефон, а также текущее местоположение или номер школы, нельзя публиковать на своей странице даже в том случае, если увидят ее только друзья. Взломы аккаунтов «ВКонтакте» не такая уж и редкая история, и, если это случится с аккаунтом ребенка или кого-то из его друзей, вся опубликованная информация станет доступна злоумышленнику.

7. Объясните дочери или сыну, что в соцсети, даже если не публиковать такие данные, как номер телефона и адрес, все равно **огромное изобилие личной информации** – получив доступ к странице, можно увидеть фото ребенка, его имя и фамилию, с кем он дружит, где учится (даже если ребенок не указал эти данные, их довольно легко найти на страницах друзей или они наверняка «всплывут» в диалогах или фотографиях).

8. Поговорите с ребенком о том, что дружить в социальной сети – это практически то же самое, что и дружить в реальной жизни. Соответственно, и к выбору друзей в соцсети надо подходить очень ответственно, даже ответственнее, чем в реальности. В соцсети никогда точно не знаешь, кто находится «по ту сторону монитора»,

действительно это такой же школьник или это человек (или даже несколько людей) значительно более старшего возраста и с нехорошими намерениями.

В итоге знакомиться в соцсети с совершенно новыми людьми нельзя ни в коем случае и в список друзей можно добавлять только тех, кого встречал в жизни. Исключение составляют лишь случаи, когда реальный друг знакомит ребенка в соцсети с человеком, которого сам знает в офлайне (например, лучшая подруга вашей дочери дает ей ссылку на аккаунт их сверстника, с которым она ходит вместе на курсы английского языка).

Если вы объяснили все это ребенку и установили соответствующую программу, можете считать, что малыш находится в относительной безопасности, по крайней мере, не подвергается большему риску, чем в офлайн-пространстве. А программа будет подсказывать вам, если ребенок все-таки добавляет в друзья новых людей или среди групп, в которые он вступил, замечены опасные сообщества.