Правила безопасности в интернете

Залог безопасности ребенка в социальных сетях - *доверительные отношения* с родителями и *исполнение* некоторых правил. Эти правила нужно разобрать вместе с ребенком.

1. **К выбору социальной сети нужно подходить ответственно**. Не следует регистрироваться во всех найденных социальных сетях. Перед регистрацией нужно собрать сведения о социальной сети, прочесть правила. Отзывы желательно искать на независимых интернет-ресурсах. Например, популярные социальные сети **Facebook**, **ВКонтакте**, **Одноклассники** способны быть достаточно безопасными для ребенка при выполнении правил.
2. **При регистрации в социальной сети нужно использовать сложный пароль**. Это - залог того, что учетную запись не взломают. В данном случае взлом учетной записи опасен, во-первых, тем, что злоумышленник может узнать конфиденциальные данные ребенка. Это могут быть сведения о городе проживания, фотоальбомы, скрытые от общего просмотра. Во-вторых, контроль над учетной записью перейдет злоумышленнику, и он сможет от имени ребенка совершать какие-либо действия. Если при регистрации в социальной сети используется система восстановления пароля с указанием секретного вопроса и ответа, убедитесь, что ответ на вопрос сложно узнать или подобрать. Иначе взлом учетной записи может быть осуществлен через подбор ответа.
3. **Не рекомендуется использовать при регистрации в социальной сети возможность указания данных почтового ящика ребенка**. Это может привести к неконтролируемому оповещению о его учетной записи тех, с кем когда-либо велась переписка. Как результат, будет сложнее управлять списком друзей ребенка.
4. **Нельзя никому сообщать данные для входа в учетную запись в социальной сети**. В частности, пароль нужно держать в секрете от всех. Мошенники иногда рассылают пользователям социальных сетей электронные письма, в которых под разными предлогами просят сообщить пароль. Например, письмо может выглядеть так, как будто оно отправлено от имени администрации сайта или от имени интернет-провайдера. Ни администрация социальной сети, ни провайдер никогда не попросят о подобном. Такие сообщения следует игнорировать.
5. **После завершения работы в социальной сети нужно выполнять процедуру выхода**. Для этого служит команда **Выход** или другая подобная. Она обычно расположена в правой верхней области окна. Если не выйти из учетной записи, а, например, просто закрыть окно браузера, доступ к учетной записи могут получить посторонние. Особенно это справедливо при работе с учетной записью социальной сети на чужом компьютере.
6. **Очень внимательно подходите к выбору друзей в социальных сетях**. Рассматривайте каждую кандидатуру вместе с ребенком. Для наибольшего уровня безопасности следует добавлять в друзья только тех пользователей, которых

вы знаете в реальной жизни. Учителя, одноклассники, родственники - вот те люди, с которыми можно установить дружеские отношения в социальных сетях. С ними можно безопасно общаться. К любым другим пользователям, особенно к тем, которые сами предлагают добавиться в друзья, следует относиться с большой осторожностью. Не зная человека лично, вы не можете быть уверены в том, что он - тот, за кого себя выдает.

7. **Воспользовавшись настройками учетной записи, ограничьте возможность связи с ребенком посторонних**. Ниже мы рассмотрим такие настройки. Это позволит ребенку получать сообщения только от тех людей, которые, с вашим участием, добавлены в список его друзей. От посторонних ребенок может получить сообщение любого содержания, с любыми изображениями или видеоклипами. Если подобные настройки не предусмотрены, предложите ребенку не открывать сообщения от незнакомцев без вашего участия.

8. **Расскажите ребенку о том, что переходить по ссылкам, которые кто-либо отправил ему в сообщении, опасно**. Эти ссылки могут вести на сайты, распространяющие вредоносные программы. Если ссылку отправил, например, одноклассник в ходе беседы - по такой ссылке можно перейти. Если же сообщение со ссылкой пришло неожиданно, прежде чем переходить по ней, следует уточнить у автора сообщения, куда она ведет. Если ответа получить не удается, возможно, учетная запись автора сообщения взломана и сообщение отправил мошенник. Опасно скачивать и открывать файлы, приходящие в сообщениях.

9. **Объясните ребенку, что он не должен никому сообщать каких-либо личных сведений о себе**. К таким сведениям относятся номер телефона, домашний адрес, время начала занятий в школе и другие подобные. Эти данные могут быть использованы злоумышленниками. Такие сведения не следует публиковать даже в том случае, если опубликованная запись предназначена только для друзей. Злоумышленник, взломавший учетную запись одного из друзей, может получить к ним доступ.

10. **Попросите ребенка с осторожностью относиться к приложениям, которые можно устанавливать в социальных сетях**. Обычно это игры или другие развлекательные приложения. Они могут собирать данные о пользователях, либо, если они созданы злоумышленниками, использоваться для взлома учетных записей. Заранее сказать, окажется ли опасным приложение, нельзя. Надежнее всего не пользоваться ими.

11. **Расскажите ребенку о том, что если он заметил что-то странное в своей учетной записи, то пароль к ней нужно немедленно сменить**. На взлом учетной записи могут указывать следующие признаки: исчезли какие-нибудь фотоснимки, или, наоборот, появились новые, которых никто не выкладывал, на стене появились неожиданные записи.

Пользуясь этими рекомендациями и ознакомив с ними ребенка, вы значительно повысите уровень его безопасности в социальных сетях. Еще более безопасной работу может сделать использование специального программного обеспечения, о

котором мы поговорим на одном из следующих занятий. Но главное в безопасности ребенка, который работает в Интернете, - *доверительные отношения* с родителями.