Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей

Сегодня многие дети не делают различий между реальной жизнью и виртуальной жизнью в Интернете. Они могут пользоваться сайтами социальных сетей, предназначенных для детей, такими как Webkinz или Club Penguin, или сайтами социальных сетей, предназначенных для взрослых, такими как Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другими. Что бы они не делали, они должны понимать, что многие из этих веб-страниц могут просматривать кто угодно, кто обладает доступом в Интернет.

Дети могут использовать эти сайты для:

- чата;
- игр;
- публикации и просмотра фотографий и видео;
- Блог
- публикации профиля в Интернете.

К сожалению, часть информации, которые дети публикуют на своих страницах, может также делать их уязвимыми для фишинговых сообщений, киберугроз и интернет-похитителей. Далее описано несколько способов, как вы можете помочь детям более безопасно пользоваться сайтами социальных сетей.

- **Поговорите с детьми об опыте их общения в социальных сетях.** Попросите детей рассказывать вам, если они столкнутся на этих сайтах с чем-либо, что вызывает у них беспокойство, неудобство или страх. Проявляйте спокойствие и напомните детям, что их никогда не накажут за то, что они вам расскажут. Дайте детям понять, что вы вместе с ними постараетесь найти удачный выход из сложившейся ситуации.
- **Установите собственные правила пользования Интернетом у вас дома.** Как только дети начнут самостоятельно пользоваться Интернетом, желательно подготовить список правил пользования Интернетом, которые будут приняты всеми. В этих правилах должно быть указано, могут ли дети использовать сайты социальных сетей и каким образом. Для получения дополнительных сведений о том, как установить правила, см. Использование семейных контрактов для защиты детей в Интернете.
- **Проследите за тем, чтобы дети соблюдали возрастные ограничения на сайте.** Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 или более лет. Если ваши дети не достигли рекомендуемого возраста, указанного для данных сетей, не разрешайте им пользоваться сайтами. Важно помнить, что вы не должны полностью полагаться на службы сайта, которые не допускают регистрации детей, не достигших нужного возраста.
- **Научитесь пользоваться сайтом.** Оцените сайты, которые планирует использовать ваш ребенок, и убедитесь, что вы и ваш ребенок понимают политику конфиденциальности и правила поведения. Узнайте, существует ли на сайте контроль над публикуемым содержимым. Кроме того, периодически просматривайте страницу вашего ребенка. Для

получения дополнительных предложений см. Советы по безопасному ведению блогов для детей и родителей.

- **Настаивайте на том, чтобы дети никогда лично не встречались с тем, с кем они общались только по Интернету, и просите их общаться только с теми, кого они знают лично.** Дети подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми они общались только по сети. Вы можете защитить своих детей, попросив их общаться в Интернете со своими друзьями и не общаться с теми, с кем они лично не встречались.
  Иногда бывает недостаточно просто сказать детям, чтобы они не разговаривали с незнакомыми людьми, поскольку дети могут не считать незнакомым человека, с которым они «встречались» в сети. Для получения дополнительных советов по защите ваших детей в Интернете см. Интернет-преступники: что можно сделать, чтобы уменьшить риск.

- **Убедитесь в том, что ваши дети не указывают свои полные имена.** Проследите за тем, чтобы дети использовали только свои имена или псевдонимы, но никогда не использовали псевдонимы, которые бы вызывали ненужное внимание. Кроме того, не разрешайте своим детям публиковать полные имена своих друзей.

- **Опасайтесь наличия в профиле ребенка информации, по которой можно идентифицировать его личность.** На многих сайтах социальных сетей дети могут присоединяться к общественным группам, включающих учеников определенной школы. Будьте бдительны, если дети разглашают эту и другую информацию, которую можно использовать для их идентификации, например школьный питомец-талисман, рабочие места и название города проживания. Если указано слишком много информации, ваши дети могут подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных. Для получения дополнительной информации см. Распознавание фишинговых и поддельных сообщений электронной почты.

- **Постарайтесь выбрать сайт, который не столь широко используется.** Некоторые сайты позволяют защитить вашу страницу с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только тем лицам, которых знает ваш ребенок. Например, с помощью Windows Live Spaces вы можете настроить разрешения, указав тех, кто может посещать ваш сайт. При этом возможны самые различные настройки – от всех пользователей Интернета до ограниченного списка людей.

- **Следите за деталями на фотографиях.** Объясните детям, что фотографии могут раскрывать много личной информации. Попросите детей не публиковать фотографии себя или своих друзей, на которых имеются четко идентифицируемые данные, такие как названия улиц, государственные номера автомобилей или название школы на одежде.

- **Предостерегите своего ребенка относительно выражения своих эмоций перед незнакомцами.** Вероятно, вы уже предупреждали своих детей не общаться с незнакомыми людьми напрямую по сети. Однако дети используют сайты социальных сетей для написания журналов и стихотворений, в которых часто выражают сильные чувства. Объясните детям, что многое из публикуемого сможет прочесть любой пользователь, имеющий доступ в Интернет, а также что похитители часто ищут

эмоционально уязвимых детей. Для получения дополнительной информации см. Чему следует научить детей, чтобы повысить их безопасность при работе в Интернете.

- **Расскажите детям об интернет-угрозах.** Как только ваши дети станут достаточно взрослыми для использования социальных сетей, поговорите с ними о киберугрозах. Расскажите детям, что если у них возникнет ощущение, что им угрожают через Интернет, то им сразу же следует сообщить об этом родителям, учителю или другому взрослому человеку, которому они доверяют. Кроме того, очень важно научить детей общаться по сети точно так же, как они общаются лично. Попросите детей относиться к другим людям так же, как они хотели бы, чтобы относились к ним самим.
- **Удаление страницы вашего ребенка.** Если ваши дети откажутся следовать установленным правилам, которые предназначены для их безопасности, и вы безуспешно пытались их убедить следовать им, то вы можете обратиться на сайт социальной сети, который использует ваш ребенок, и попросить удалить его страницу. Можно также обратить внимание на средства фильтрации интернет-содержимого (например, Функции семейной безопасности Windows Live) в качестве дополнения и ни в коем случае не замены для контроля со стороны родителей.