Обучение детей основам безопасности при работе с Интернетом

Если у вас есть дети, вы можете помочь им пользоваться Интернетом более безопасно, обучив их некоторым основным правилам. Далее приведены некоторые базовые уроки, которые помогут обучить детей.

- **Научите детей никому не сообщать пароли**

Дети создают имена пользователей и пароли для доступа на сайт школы, игровые сайты, в социальные сети, для публикации фотографий, совершения покупок в Интернете и других операций.

Согласно данным исследования Teen Angels из Wired Safety.org, 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам, 66 процентов девочек в возрасте 7-12 признались, что сообщали свой пароль другим лицам.

Первое правило безопасности при работе в Интернете: пароли следует держать в секрете. Научите детей хранить свои пароли столь же бережно, как информацию, которую они хотя защитить.

Далее приведены некоторые правила, которые дети должны знать и соблюдать.

- **Никогда не сообщайте свои пароли другим.** Не показывайте никому свои пароли, даже друзьям.
- **Обеспечьте защиту для записанных паролей.** Будьте внимательны к тому, где вы храните или записываете пароли. Не храните пароли в рюкзаке или бумажнике. Не оставляйте данные о паролях в местах, где вы бы не хотели оставить информацию, защищенную с их помощью. Не храните пароли в файле на компьютере. Преступники ищут там в первую очередь.
- **Никогда не предоставляйте свой пароль по электронной почте или в ответ на запрос по электронной почте.** Любое сообщение электронной почты, в котором вас просят указать пароль или перейти на веб-сайт, чтобы проверить пароль, может представлять собой разновидность мошенничества, которая называется фишингом.

К ним относятся запросы с сайтов, вызывающих доверие, которые вы можете постоянно посещать. Мошенники часто создают поддельные сообщения электронной почты, содержащие такие же логотипы как и на реальных сайтах и написанных таким языком, чтобы не вызывать сомнения в своей достоверности. Дополнительные сведения о фишинговых сообщениях.

- **Не вводите пароли на компьютерах, которые вы не контролируете.** Не пользуйтесь общедоступными компьютерами в школе, библиотеке, в интернет-кафе или в компьютерных лабораториях, кроме как для анонимного просмотра страниц в Интернете.

Не используйте эти компьютеры с учетными записями, где требуется вводить имя пользователя и пароль. Преступники могут за очень небольшие деньги приобрести устройства, регистрирующие нажатия клавиш, которые устанавливаются в течение нескольких секунд. С помощью подобных устройств злоумышленники могут собирать информацию, вводимую на компьютере, через Интернет. Для получения дополнительной информации см. 5 шагов по использованию общедоступного компьютера.

- **Помощь детям в безопасном использовании социальных сетей**

Ваши дети могут пользоваться сайтами социальных сетей, которые предназначены для детей, такими как Webkinz или Club Penguin, или сайтами, предназначенными для взрослых, такими как Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook и другие.

Дети используют социальные сети для общения с лицами, которые могут проживать на другом конце земного шара, или со своими знакомыми, с которыми они каждый день видятся в школе.

Дети должны понимать, что многие из этих сайтов социальных сетей могут просматриваться всеми, кто имеет доступ в Интернет. В результате публикации ими некоторой информации они могут стать уязвимыми для фишинговых сообщений,, киберугрози похитителей в Интернете. Далее приведены некоторые советы, которые помогут детям безопасно пользоваться сайтами социальных сетей.

- **Беседуйте с детьми по поводу их общения в социальных сетях.** Просите детей рассказывать вам, если им встретится в Интернете то, что вызывает у них беспокойство, неудобство или страх. Сохраняйте спокойствие и убедите детей, что вам можно рассказывать о таких вещах. Дайте детям понять, что вы поможете им успешно разрешить сложившуюся ситуацию.
- **Определите правила работы в Интернете.** Как только ваши дети станут самостоятельно пользоваться Интернетом, установите правила пользования Интернетом. В этих правилах должно быть определено, могут ли ваши дети использовать сайты социальных сетей и каким образом. Для получения дополнительной информации об определении правил см. Использование семейных контрактов для защиты детей в Интернете.
- **Убедитесь в том, что ваши дети соблюдают возрастные ограничения.** Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 и более лет. Если ваши дети не достигли этого возраста, не разрешайте им пользоваться данными сайтами. Вы не должны полностью полагаться на сами службы, чтобы не допустить регистрацию ваших детей на этих сайтах.
- **Учитесь.** 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.
- **Научите своих детей никогда лично не встречаться с теми, с кем они общались только по сети.** Дети подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми они общались только по сети. 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.
- **Попросите детей общаться только с теми людьми, которых они уже знают.** Вы можете помочь защитить ваших детей, попросив их использовать данные сайты для общения с друзьями и никогда не общаться с теми, с кем они лично не встречались.
- **Убедитесь в том, что ваши дети не указывают свои полные имена.** Научите своего ребенка указывать только свое имя или псевдоним и ни в коем случае не использовать псевдонимы, которые могли бы привлечь нежелательное внимание. Кроме того, не разрешайте своим детям публиковать полные имена своих друзей.
- **Относитесь с осторожностью к идентифицирующей информации в профиле вашего ребенка.** На многих сайтах социальных сетей дети могут присоединяться к общественным группам, включающих учеников определенной школы.

Будьте осторожны, если ваши дети предоставляют информацию, по которой их можно идентифицировать, например школьное животное-талисман, рабочее место или город проживания. Если указано слишком много информации, ваши дети могут подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных. Для получения дополнительных сведений 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 написанное ими сможет прочесть любой, кто имеет доступ в Интернет, и похитители часто ищут эмоционально уязвимых детей.

- **Расскажите детям об интернет-угрозах.** Как только ваши дети станут достаточно взрослыми для использования сайтов социальных сетей, расскажите им о них киберугроз. 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 отказываются соблюдать установленные вами правила для защиты их безопасности, и вы безуспешно пытались помочь им изменить свое поведение, можно обратиться на веб-сайт социальной сети, которую использует ваш ребенок, с просьбой 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.

Хотели ли бы вы получить дополнительную информацию о том, как защитить своего ребенка в Интернете? Подробные инструкции см. Помощь по защите детей в Интернете: 4 вещи, которые вы можете сделать.

- **Если ваши дети пишут блоги, убедитесь в том, что они не рассказывают слишком много о себе.**

Практика написания блогов (сокращение от англ. "web log" – дневник в сети) или личного интерактивного журнала очень быстро стала популярной среди подростков, многие из которых ведут свои блоги без ведома родителей или опекунов.

Социальные сети сейчас обошли по популярности блоги среди большинства подростков, однако многие дети по-прежнему ведут свой блог на своем сайте социальной сети. Недавние исследования показали, что на сегодняшний день примерно половину всех блогов пишут подростки, при этом каждые двое из троих указывают свой возраст, каждые трое из пяти сообщают о месте своего проживания и дают контактную информацию, а каждый пятый указывает свое полное имя. Разглашение подробной личной информации сопряжено с риском.

Несмотря на то, что ведение блога дает возможные преимущества, включая развитие навыков письма и общения, очень важно рассказать детям об Интернете и научить их писать блоги еще до того, как они начнут этим заниматься аналогично тому, как все сначала оканчивают курсы по вождению, прежде чем самостоятельно садятся за руль автомобиля. Далее приведены некоторые начальные советы.

- **Определите правила пользования Интернетом** с детьми и проявите настойчивость.
- **Просматривайте то, что дети планируют опубликовать в Интернете, прежде чем они опубликуют эти материалы.** Внешне безобидную информацию, например

школьное животное-талисман и фотография города, можно собрать воедино и понять, в какую школу ходит автор.

- **Спросите себя (и проинструктируйте детей делать то же самое), насколько комфортно вы будете чувствовать себя, показывая эти материалы незнакомцу.** Если имеются сомнения, исключите такие материалы.
- **Проведите оценку службы блогов** и выясните, обеспечивает ли она возможность написания личных блогов, защищенных с помощью паролей.
- **Сохраните интернет-адрес блога вашего ребенка** и регулярно проверяйте его.
- **Просматривайте другие блоги, отыскивая положительные примеры** для подражания для ваших детей.
- **Помните об интернет-мошенниках**

Согласно данным Федеральной торговой комиссии США, 31 процент жертв похищения личных данных составляют молодежь. Подростки становятся привлекательными объектами для мошенников, поскольку у них хорошие кредитные оценки и малый долг, по сравнению со взрослыми они меньше заботятся о безопасном хранении информации.

Некоторые моменты, о которых должны знать ваши дети, чтобы стать разумными потребителями и избежать интернет-мошенничества.

- **Никогда не разглашайте личную информацию.** Никогда не указывайте свою личную информацию, например полное имя или город проживания во время общения с помощью мгновенных сообщений или в чатах, если вы полностью не уверены в личности человека, с которым вы общаетесь.
- **Обязательно завершайте сеанс с выходом из системы при работе на общедоступном компьютере.** Если вы используете компьютер в библиотеке или в интернет-кафе, прежде чем покинуть компьютер, полностью завершите все сеансы с выходом из системы. Вы не знаете, какое программное обеспечение установлено на этих компьютерах, а также что оно выполняет. Кроме того, может быть установлено программное обеспечение, фиксирующее нажатие клавиш.
- **Придумывайте безопасные пароли и держите их в секрете.** Для получения дополнительных сведений см. пункт 1 выше.
- **Используйте только безопасные сайты.** Если ваши дети совершают покупки в Интернете, то им следует каждый раз убеждаться в том, что URL-адрес сайта, на котором они вводят финансовую информацию, начинается с префикса https://, в правом нижнем углу имеется желтый значок замка или адресная строка отображается зеленым цветом. Они могут щелкнуть по значку замка или в адресной строке, чтобы проверить сертификат безопасности данного сайта.
- **Распознавание мошенников и сообщение о фактах мошенничества.** Расскажите своим детям о признаках подделки идентификационных данных: предложение утвержденных кредитных карт, звонки из агентств по сбору информации или незнакомые финансовые документы. Если у вашего ребенка возникнет подозрение на подделку личных данных, немедленно предпримите соответствующие действия, чтобы ограничить ущерб. Обратитесь в свою кредитную компанию, банки или все три организации по кредитной отчетности, а также в полицию. Закройте все счета, которые подвергались фальсификации, и попросите детей поменять пароли для всех своих учетных записей в Интернете. Ведите журнал всех выполняемых действий.