Безопасный Интернет. Советы родителям

Рекомендации экспертов родителям

Уважаемые родители! Если ваши дети пользуются Интернетом, вы, без сомнения, беспокоитесь о том, как уберечь их от неприятностей, которые могут подстерегать в путешествии по этому океану информации. Значительное распространение материалов, предназначенных только для взрослых или неприемлемых для детей по какой-либо другой причине, может легко привести к неприятным последствиям. Кроме того, в Сети нередко встречаются люди, которые пытаются с помощью Интернета вступать в контакт с детьми, преследуя опасные для ребенка или противоправные цели.

Правило 1.

- Внимательно относитесь к действиям ваших детей в «мировой паутине»:

- Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернет, особенно на этапе освоения.

Правило 2.

- Информируйте детей о возможностях и опасностях, которые несет в себе сеть:

- Объясните им, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием от другого пользователя Интернет, ему нужно сообщить об этом близким людям.
- Приучите детей к конфиденциальности. Если на сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним, не раскрывающий никакой личной информации. Расскажите детям о том, что нельзя сообщать какую-либо информацию о своей семье – делиться

проблемами, рассказывать о членах семьи, о материальном состоянии, сообщать

- Научите детей искать нужную им информацию и проверять ее, в том числе с вашей помощью.
- Научите внимательно относиться к скачиванию платной информации и получению платных услуг из Интернет, особенно путем отправки sms, – во избежание потери денег.
- Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если ребенка что-то пугает, настораживает или кто-то угрожает в переписке, в письме, он обязательно должен сообщить об этом взрослым. Ознакомьте ваших детей с этими простыми правилами, и они будут иметь представление о том, с чем могут столкнуться в Интернете, и будут знать, как вести себя в этом случае. Если ребенок будет вам доверять и рассказывать все, что впечатлило его в сети, с кем он познакомился, вы сможете избежать очень серьезных бед, таких, как похищение ребенка посредством сети и сексуальная эксплуатация детей. Но не переборщите – не надо запугивать ребенка Интернетом, говорить, что это очень опасная и страшная штука, но ею надо уметь пользоваться. Ребенок должен усвоить мысль, что Интернет – это друг, и если правильно с ним «дружить», можно извлечь из этого очень много пользы. А правильно «дружить» с ним научить может только взрослый. Так что все карты вам в руки.
- Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ваш ребенок, и посоветуйте их использовать.

Правило 3. Выберите удобную форму контроля пребывания ваших детей в Сети:

- Установите на ваш компьютер необходимое программное обеспечение – решение родительского контроля и антивирус.
- Если ваш ребенок – учащийся младших классов и остается часто дома один, ограничьте время пребывания вашего ребенка в Интернете.
- Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семьи, а не в комнате ребенка.
- Регулярно отслеживайте ресурсы, которые посещает ваш ребенок. Простые настройки компьютера позволят вам быть в курсе того, какую информацию он просматривал.
- Изучите средства фильтрации Интернет-содержимого (такие как Windows Vista, средства родительского контроля Windows 7и Функции

семейной безопасности Windows Live) и используйте их в качестве дополнения к контролю со стороны родителей.

- Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер. Internet Explorer..

Правило 4.

Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей.

Виды информационных угроз для детей и родителей

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Сетевое мошенничество

С развитием сети интернет его стали осваивать и мошенники.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги и получить личные и конфиденциальные данные: к таким данным относятся логины и пароли от различных сервисов, в том числе банковских, номера и пин-коды банковских карт и другие персональные данные.

Сетевое мошенничество имеет множество методов.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) предполагает за счет использования различных методов заманивания пользователя на поддельный сайт, например, через ссылку в письме, баннер или ссылку в тексте.

Вишинг является разновидностью фишинга, в которой используется телефон. Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

Фарминг или скрытое перенаправление является также разновидностью фишинга, но направляет пользователя вирус или взломанная программа на поддельный сайт, являющийся полной копией официального ресурса.

Отдельным подвидом необходимо рассматривать **мобильное мошенничество**, которое в частности предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

- ссылки на фишинговые или зараженные ресурсы;
- информацию о выигрышах, которых не существует;
- ложные просьбы о помощи;
- о переводе денег на сотовый, прямые просьбы о переводе денег;
- SMS из несуществующего банка;
- просьбы перезвонить на платный номер;
- требования выкупа;
- просьбы отправить СМС, которые активируют платные услуги;
- и другую информацию.

Мобильное мошенничество также часто встречается в формах:

Wangiri («Очень дорогой звонок») – когда человек звонит с неизвестного номера, но, как только человек берет трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги;

Требования выкупа – когда кто-то звонит вам с неизвестного номера, но, как только вы берете трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги. Когда вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку: не впадайте в панику, не торопитесь переводить деньги. Перезвоните родным и узнайте, все ли у них в порядке. Уточните, где находятся близкие.

III. Заключение

Необходимо учитывать, что в настоящее время информационная безопасность – важнейший компонент национальной безопасности, она становится одним из элементов национальной, общественной и личной безопасности. Соответственно, важно помнить, что задача родителей не закрыть детям мир информации, а научить брать из этого многогранного мира лучшее!

Электронные ресурсы по теме «Безопасный Интернет»

"Основы безопасности детей и молодежи в Интернете" — интерактивный курс по Интерент-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности.

http://www.nachalka.com/bezopasnost предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям.

- «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». http://www.oszone.net/6213/ - OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль».