БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ

Правовые, психологические, технические аспекты безопасной работы в Интернете

Интернет позволяет:

- общаться с друзьями, семьей, коллегами;
- получать доступ к информации и развлечениям;
- учиться, встречаться с людьми и узнавать новое.

Несомненно, Интернет полезен для детей, однако потенциальные опасности вполне реальны. Узнав больше об этих угрозах, Ваша семья может избежать опасностей и предотвратить неприятности. Опасности Интернета для детей делятся на пять основных категорий.

- **Киберхулиганы**

В Интернете, как и на любой игровой площадке, одни люди приятны, другие — нет. И дети, и взрослые с помощью Интернета могут изводить или запугивать других людей, начиная с присвоения прозвищ и заканчивая физическими угрозами. Например, дети иногда отправляют угрожающие комментарии или неприличные изображения через службы мгновенных сообщений или блоги, незаметно для родителей и общества бесчестя ребенка.

- **Злоупотребление обменом файлами**

Обмен музыкой, видео и другими файлами рискован. Ваши дети случайно могут загрузить неуместные материалы, компьютерные вирусы или программы-шпионы. Некоторые программы для обмена файлами дают доступ к компьютеру в любое время, пока он в сети.

- **Доступ к неприличному контенту**

Дети зачастую не в силах противостоять любопытству. Пользуясь Интернетом, они могут столкнуться с информацией или изображениями, доступ к которым Вы бы хотели ограничить, например, с контентом неприличного характера, недопустимым для детей или не соответствующим ценностям Вашей семьи. Это может случиться при нажатии на рекламные или непонятные ссылки на поисковой странице либо при обмене файлами через Интернет

- **Киберхищники**

Киберхищники используют Интернет для сближения с детьми. Их цель — изолировать детей и убедить их встретиться лично. О людях в сети известно только то, что они сами сообщают о себе. Киберхищники пользуются этой анонимностью для обмана детей, притворяясь другим ребенком или кем-то еще, кто заслуживает доверия. Эти люди могут также использовать подростковые стремления к приключениям и романтике, чтобы завязать с ними недопустимые дружеские отношения.

- **Вторжение в частную жизнь**

Некоторые организации используют регистрацию или формы опроса для сбора личных сведений. При заполнении различных форм в Интернете без присмотра дети могут предоставить конфиденциальные сведения о себе или Вашей семье. Дети также могут случайно предоставить личные сведения или фотографии в блогах, на персональных веб-страницах или при игре через Интернет.

Множество полезных и приятных сервисов Интернета требуют делиться сведениями о себе. Одни требует совсем немного, другие больше. Не всегда легко понять, кто и зачем собирает эту информацию. Иногда предоставление сведений приносит непредвиденные и нежелательные результаты. Эти результаты могут просто раздражать (например, нежелательные сообщения электронной почты) или быть чем-то серьезным, например попыткой кражи идентификационных сведений, нанесением ущерба Вашей репутации, а также попыткой кражи денег.

Кража идентификационных сведений и интернет-мошенничество

Интернет-мошенники хотят, чтобы вы отдали им с трудом заработанные деньги или предоставили личные сведения, которые позволят им украсть Ваши идентификационные сведения. Преступники давно поняли, что Интернет может помочь им обманывать доверчивых людей, иногда весьма изощренными методами. Большинство афер в Интернете основано на мошенничестве и краже идентификационных сведений — и лишь от Вас зависит, предоставлять или нет личные сведения, отправлять деньги или нет. Таким образом, зная, на что обращать внимание и что делать, Вы не станете жертвой этих преступлений.

Фишинг

Чрезвычайно подлое мошенничество, известное как фишинг, начинается с сообщения электронной почты от источника, которому Вы доверяете. Поддельное сообщение электронной почты — «наживка» — обычно содержит ссылку на поддельную веб-страницу, очень похожую на страницу компании, которой Вы доверяете. Этот веб-узел может запросить у вас личные сведения, например номер кредитной карты. Это «крючок». Если Вы заглотили крючок — Вы попали в неприятности, потому что предоставили преступникам достаточно сведений для кражи Ваших идентификационных сведений и получения доступа к Вашим учетным записям, деньгам или счетам.

Мистификация

Мистификация — еще один тип мошенничества. Например, «нигерийское мошенничество» — тип авансового мошенничества, долгое время пользовавшийся «популярностью». Жертва получала сообщение электронной почты от кого-либо, выдающего себя за нигерийского чиновника, деловую персону или выжившего супруга прежнего лидера правительства, просящего помощи в вывозе денег из страны. Мошенники, отправившие это сообщение, предлагали перечислить на банковский счет жертвы миллионы долларов в обмен на небольшое вознаграждение. Если жертва отвечала на первое письмо, мошенники могли прислать официально выглядящие документы или другие «доказательства» и просьбу предоставить чистый фирменный бланк, номера банковских счетов и как можно больше денег, чтобы покрыть затраты на перевод и судебные издержки. Если жертва продолжала отвечать, мошенники предоставляли дополнительные «свидетельства», подтверждавшие их намерения, и тревога поднималась только, когда мошенники запрашивали больше денег и задерживали перевод обещанной суммы на счет жертвы. В конечном счете мошенники исчезали с деньгами жертвы, оставляя ее с носом.

Другой известный мистификатор предлагал жертве купить билеты международной лотереи и использовать «секретную систему» для выигрыша большой суммы денег. Или посылал сообщение электронной почты, извещающее получателя об огромном выигрыше в международную лотерею, даже если он не участвовал в ней, требующее только номер его банковского счета, чтобы перечислить выигрыш. Конечно же, не было никакой «секретной системы», а большинство лотерей, упомянутых в этих сообщениях, были вымышленными.

Нежелательная почта

Один из инструментов, используемых мошенниками и преступниками — нежелательная почта, то есть сообщения электронной почты, мгновенные сообщения и даже электронные поздравительные открытки, которые Вы не запрашивали. Нежелательная почта может содержать ссылки на поддельные веб-узлы или рекламные объявления о бесполезных продуктах, в которых Вы не заинтересованы.

Необходимые шаги для безопасности в Интернете — внимательность, здравый смысл и умение распознавать жульничество и интернет-мошенничество и избегать их.

Что вы можете предпринять

- Включите интернет-брандмауэр Windows.
- Используйте Центр обновления Microsoft для автоматической загрузки новейших обновлений Windows.
- Установите и регулярно обновляйте антивирус-ное программное обеспечение.
- Установите и регулярно обновляйте Защитник Windows (Microsoft Windows Defender)
- Поговорите с детьми о том, что они делают в Интернете.
- Установите четкие правила использования Интернета.
- Держите личные сведения в секрете.
- Используйте настройки семейной безопасности в программном обеспе-чении Microsoft.
- Выработайте линию поведения в Интернете, снижающую риски.
- Аккуратно обращайтесь с личными сведениями.
- Используйте технологии антифишинга и защиты от нежелательной почты, встроенные в Windows Vista, Windows XP SP2, Windows Live и Microsoft Outlook.

Четыре следующих шага **обезопасят компьютер** от большинства вредоносных программ. Эти шаги просты.

1. Используйте Интернет-брандмауэр и держите его включенным

2. Регулярно обновляйте операционную систему, желательно при помощи функции автоматического обновления Windows
3. Установите и регулярно обновляйте антивирусное программное обеспечение
4. Установите и регулярно обновляйте антишпионскую программу, например Защитник Windows (Microsoft Windows Defender)

Для защиты Вашей семьи при использовании Интернета необходимо знать об опасностях, часто открыто говорить с детьми, приучая их правильно себя вести в Интернете, и использовать технологии, которые помогут снизить интернет-риски для Вашей семьи. Четыре следующих шага помогут защитить Вашу семью в Интернете.

1. Поговорите с детьми о том, что они делают в Интернете.
2. Установите четкие правила использования Интернета.
3. Держите личные сведения в секрете.
4. Используйте программы для обеспечения семейной безопасности.

Защита ваших личных сведений подразумевает соблюдение правил безопасности при использовании Интернета, контроль и нейтрализацию вредоносных источников, а также защиту от более серьезных проблем, таких как кража идентификационных сведений.

Для этого необходимо:

1. Быть осмотрительным в Интернете, выработать линию поведения, которая поможет снизить риск.
2. Аккуратно обращаться с личными сведениями.
3. Использовать технологии, реагирующие на опасность, для предотвращения угроз.

Давайте рассмотрим эти шаги подробнее.

ДОПОЛНИТЕЛЬНО

Для детей Интернет — это и виртуальный учебный класс, и игровая площадка — он прекрасно подходит как для обучения, так и для развлечения. Дети растут, и часто Интернет становится местом, где они заводят новые знакомства, обмениваясь электронной почтой и мгновенными сообщениями с друзьями, читая блоги и оставляя в них собственные записи, создавая персональные веб-страницы, обмениваясь музыкой и видео и играя в игры.

Многие из этих развлечений могут помочь детям развить общительность, научиться самовыражению и обрести уверенность в себе. К несчастью, эти же развлечения могут стать источником серьезных неприятностей для них, включая угрозы личной безопасности и частной жизни, наряду с воровством и нарушением безопасности компьютера.

И хотя Интернет — бесспорно превосходный источник знаний, в нем можно найти вещи, не подходящие для ребенка, подобно тому, как в любом городе есть места, небезопасные или недопустимые для детей. Кроме того, определенные действия в Интернете подходят взрослым, но не детям, или подходят одним детям, но не подходят другим.

Только Вы знаете лучше всех, что подходит Вашим детям. Нужно быть в курсе опасностей для детей в Интернете и знать, что предпринять для снижения или устранения этих опасностей, чтобы принимать взвешенные решения об использовании Интернета и обеспечивать защиту Вашей семьи.]

- **Обсудите с детьми опасности Интернета**

Открыто поговорите с детьми об опасностях Интернета, в том числе о недопустимом контенте, вторжении в частную жизнь и нежелательных связях с другими детьми или взрослыми. Объясните им, как их собственное поведение может снизить угрозу и обеспечить безопасность в Интернете. Эти знания очень помогут детям.

Если вы хотите подготовиться к разговору с детьми или узнать, чему их нужно научить, обратитесь к следующим полезным ресурсам.

- www.microsoft.com/rus/protect/
- http://www.content-filtering.ru/
- http://www.friendlyrunet.ru/
- http://www.saferunet.ru
- **Держите личные сведения в секрете**

- **Научите детей советоваться с Вами, прежде чем предоставить личные сведения в Интернете**, пока Вы не разрешите им это. Личные сведения включают настоящие имена Ваших детей, их возраст, пол, номер телефона, адрес, школу, спортивную команду, любимые места развлечений, чувства и эмоции, а также фотографии. Хищники ориентируются на эмоциональную уязвимость, например печаль, одиночество или гнев. Они знают, как использовать казалось бы несвязанную информацию для определения местонахождения людей.
- **Следите за детьми в Интернете**

Убедитесь, что знаете, с кем Ваши дети делятся сведениями через мгновенные сообщения, блоги и другие сообщества. Друзья ли эти люди, друзья друзей или неограниченный круг лиц?

- **Научите детей сообщать Вам о подозрительных действиях**

Убедите детей немедленно сообщать Вам, если кто-либо начал задавать им вопросы личного характера или попытался договориться о личной встрече. Убедитесь, что дети не будут отвечать на сообщения электронной почты с запросами личных сведений, например номеров кредитных карт и банковских счетов.

- **Помогите детям выбрать подходящие псевдонимы и адреса электронной почты**

Помогите детям выбрать псевдонимы и адреса электронной почты, не содержащие никаких личных сведений и не намекающие на разного рода непристойности — «музыкальный_фанат» или «спортсмен» вместо «женя13» или «сексуальная Света».

- **Установите четкие правила использования Интернета.**

Как только Ваши дети начнут пользоваться Интернетом, необходимо установить четкие правила в отношении того, когда и как они могут его использовать, как и в случае с их первым велосипедом. Расскажите им об опасностях и о том, почему им необходимо соблюдать семейные правила, чтобы избежать неприятностей и весело проводить время в Интернете. Обсудите следующие рекомендации по защите Вашей семьи в Интернете.

- **Не открывайте файлы для общего доступа и не щелкайте по вложениям и ссылкам в сообщениях электронной почты**

Вы учите детей не принимать подарки от незнакомцев в реальном мире. Это относится и к Интернету. Открывая вложения сообщений электронной почты, щелкая по ссылкам в мгновенном сообщении или блоге, а также обмениваясь музыкальными и видеофайлами, дети могут открыть вирус, загрузить вредоносную программу или непристойное изображение. К несчастью, даже сообщения, приходящие от друзей, могут быть опасными. Преступники в Интернете могут выдать себя за кого-то из знакомых Ваших детей, или компьютер друга может быть инфицирован вирусом, рассылающим сообщения электронной почты без его ведома.

- **Относитесь к другим так, как хотите, чтобы относились к вам**

Это основное правило человеческих взаимоотношений. Отдавайте то, что хотите получить обратно. Пытаться смутить или запугать других людей непристойными замечаниями — грубо и недопустимо. К тому же это вопрос обычной вежливости, а запугивание людей в Интернете может стать преступлением, если зайдет слишком далеко.

- **Защищайте себя**

Если кто-либо неуважительно относится к Вам или пытается запугать Вас, проигнорируйте его и воспользуйтесь программой для блокировки возможности общаться с Вами или играть в ту же игру. Если ситуация выходит из-под контроля, сообщите об этом администратору веб-узла или другому представителю администрации.

- **Уважайте собственность других людей**

То, что в Интернете легко найти и просмотреть любое содержимое, не означает, что это содержимое можно бесплатно копировать или разместить. Напомните детям, что несанкционированное копирование музыки, игр и других охраняемых авторскими правами объектов загрузки и обмен ими — это пиратство. Плагиат и проникновение в компьютер также незаконны.

- **Никогда не отправляйтесь на личную встречу с «другом» из Интернета.**

Люди, с которыми Ваши дети познакомились в Интернете, могут быть совсем не теми, кем представились. Если ребенок настаивает на встрече, необходимо пойти вместе с ним и убедиться, что встреча проходит в людном публичном месте.

- **Используйте программы для семейной безопасности, чтобы контролировать детей в Интернете**

Windows Vista, Windows Live OneCare Family Safety и Xbox 360 предусматривают настройки семейной безопасности, чтобы помочь Вам следить за детьми и контролировать их поведение в Интернете. Используя эти настройки, можно задать те веб-узлы, программы, игры и DVD-фильмы, которые могут использовать Ваши дети. Можно установить ограничения в зависимости от содержимого, названий сайтов или рекомендаций независимых рейтинговых сайтов либо руководствуясь собственными соображениями. Программы для семейной безопасности также позволяют задавать индивидуальные, соответствующие возрасту настройки для каждого члена семьи.

- **Узнайте больше о доступных средствах семейной безопасности**

Единого технологического решения, удовлетворяющего запросы каждой семьи, не существует, поэтому необходимо изучить множество различных средств и выбрать те, которые обеспечат безопасность детей в Интернете.