Правила безопасной работы в сети ИНТЕРНЕТ

Интернет *- это полезная и интересная вещь, если правильно ею пользоваться, но у всякой медали есть своя оборотная сторона. В виртуальном мире нас подстерегает множество опасностей, о которых мы не имеем ни малейшего понятия. Поэтому надо знать основные правила работы в Интернет и соблюдать их.*

Общие правила безопасной работы в интернете:
Поставьте на свой компьютер брандмауэр/firewall (это первое, с чего нужно начинать работу в интернете; брандмауэр позволяет отслеживать и предотвращать/блокировать атаки хакеров на ваш компьютер); регулярно проверяйте свой компьютер на вирусы (как можно чаще обновляйте базы программ-антивирусов); не открывайте вложенные в письма файлы, присланные вам по почте (в этих файлах могут содержаться вирусы; если файл вам прислал знакомый, то перед тем как открыть этот файл сначала проверьте его на наличие вирусов); старайтесь не пользоваться публичными proxy-серверами (владельцу proxy-сервера не составит труда перехватить ваш трафик и узнать пароль (это же относится и ко всем локальным сетям, компьютерным клубам и прочим местам общего пользования компьютерами, где системные администраторы могут отслеживать весь трафик посетителей)); если незнакомец просит что-то сделать на вашем компьютере (поставить какую-то программу, изменить какие-то настройки и т.п.), то сначала посоветуйтесь со знакомыми специалистами на предмет безвредности этих действий; при регистрации на новом сайте всегда придумывайте новый уникальный пароль (часто под благовидным предлогом хакеры заставляют регистрироваться на их сайтах (для возможности начать пользоваться их форумами, чатами, библиотеками документов и т.п.), чтобы потом использовать ваши пароли для доступа к вашим аккаунтам на других сайтах); не создавайте простых/очевидных паролей; если вы сохраняете пароль в файле или записываете на бумаге, то постарайтесь, чтобы он не был доступен посторонним людям; никому ни при каких обстоятельствах не давайте свой пароль (в том числе друзьям и знакомым); пароль - это ваш маленький секрет ;-) (администратор сайта никогда не попросит у вас пароля, потому что он и так имеет полный доступ ко всему своему сайту); отключите в вашем браузере автозапоминание паролей (в противном случае любой человек, севший за ваш компьютер, сможет войти в ваши аккаунты, даже не зная ваших паролей, а войдя - изменить эти пароли на свои).

Информация для родителей:

Если ваши дети пользуются Интернетом, вы, без сомнения, беспокоитесь о том, как уберечь их от неприятностей, которые могут подстерегать их в путешествии по этому океану информации. Хотя значительная часть ресурсов Интернета не может нанести вреда детям, распространение материалов, предназначенных только для взрослых или неприемлемых по какой-либо другой причине, может легко привести к неприятным последствиям. Кроме того, к сожалению, встречаются люди, которые пытаются с помощью Интернета вступать в контакт с детьми, преследуя опасные для ребенка или противоречащие закону цели.
Возможные опасности, с которыми сопряжен доступ детей к Интернету:
- Неприемлемые материалы. В Интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий;

- Неприятности, связанные с нарушением законов или финансовыми потерями. У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов;
- Разглашение конфиденциальной информации. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол, и информация о семье могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации;
- Проблемы технологического характера. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, "червь", "троянский конь", "зомби" или другой код, разработанный со злым умыслом.

Меры предосторожности:

Побеседуйте с детьми. Первое, что необходимо сделать, — это объяснить детям, что нахождение в Интернете во многом напоминает пребывание в общественном месте. Многие опасности, подстерегающие пользователя Интернета, очень схожи с риском, возникающим при общении с чужими людьми, и дети должны понимать, что, если они не знают человека, с которым вступили в контакт, лично, это означает, что они общаются с незнакомцем, что запрещено и в реальной, а не только в виртуальной действительности.

Разработайте правила пользования Интернет:

- Четко объясните детям, посещение каких веб-узлов является приемлемым и какими правилами нужно руководствоваться при пользовании Интернетом. Приведите ясные и наглядные примеры того, что следует искать, и убедитесь в том, что дети обратятся к вам, если столкнутся с не внушающими доверия или смущающими их материалами;
- Пароли. Предупредите детей о том, что они не должны никому сообщать свои пароли, даже если человек утверждает, что является сотрудником вашего поставщика Интернет-услуг (например представляется вашим провайдером). Поставщик услуг Интернета никогда не будет спрашивать, какой у вас пароль;
- Разработайте "домашнюю" политику. Составьте список того, что можно и чего нельзя делать любому члену вашей семьи при использовании Интернета. Например: Нельзя разглашать информацию личного характера. Объясните детям, что они не должны сообщать свою фамилию, адрес, номер телефона или давать свою фотографию. Ребенок ни в коем случае не должен соглашаться на личную встречу с "виртуальным" другом без разрешения и присутствия родителей. Нельзя ничего покупать через веб-узел, деятельность которого осуществляется через небезопасный сервер. Перед тем как совершить покупку, необходимо всегда спрашивать разрешения взрослых;
- Следует либо не допускать использования ребенком чата, либо контролировать это занятие. Кроме того, нужно убедиться в том, что выбранный им чат является управляемыми и поддерживается заслуживающей доверия компанией или организацией;
- Установите компьютер в помещении, используемом всеми членами семьи, а не в

комнате ребенка. Это упростит контроль за пребыванием детей в Интернете. Воспользуйтесь современными технологиями;
- Контролируйте входящие и выходящие сообщения электронной почты своего ребенка. Знакомьтесь с его "виртуальными" друзьями подобно тому, как вы знакомитесь с "реальными";
- Регулярно просматривайте журнал веб-обозревателя. Из него вы узнаете, какие веб-узлы посещали ваши дети и как часто они это делали;
- Настройте веб-обозреватель в режиме обеспечения безопасности.

Помните!

Эти простые меры, а также доверительные беседы с детьми о том, каких правил им следует придерживаться при использовании Интернета, позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное и безопасное путешествие по Всемирной сети.