Общие правила безопасности при работе в Интернете

Ребенку не следует давать частной информации о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей.

Не разрешайте ребенку предоставлять личную информацию через ИнтернетРебенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность - отличный способ защиты. Не выкладывайте фотографии ребенка на веб-страницах или публичных форумах.

Безопасное общение детей в Интернете

Не делайте ваши письма длиннее, чем они должны быть. У каждой мысли есть начало и конец. Да и 15-20 слов в одном предложении электронного послания – именно та норма, которую получатель e-mail, а может воспринимать в Интернете без напряжения для глаз и психики. Довести проверку до автоматизма. Послания без знаков препинания вышли из моды, настала эпоха онлайн-справочников, электронных словарей и всесторонней проверки правописания. Ввести многократную компьютерную проверку перед отправкой в привычку/

Опытные пользователи также вносят шаблонные приветствия и благодарности, которые вставляются в начало или конец каждого послания, в награду «за уделенное время». Так что даже в Интернете не стоит пренебрегать этикетом, вне зависимости о темы переписки. Ведь электронное послание лишь создается в Сети – прочитает его, все равно, живой человек/ Посылая возмущенные письма в ответ на спам, юзер, вопреки частому заблуждению, не мстит виртуальному обидчику. Напротив, поступая таким образом, пользователь подтверждает, что его электронный адрес является «живым». Что спамеру и нужно. В итоге спамовых сообщений будет приходить только больше. Поэтому, разумнее выбрать удаление и функцию игнорирования. Или использовать программное обеспечение электронной почты, чтобы мусорные сообщения удалились автоматически.А если ответ не приходит на ум сразу? На этот случай у пользователя есть помощники: шаблоны и дежурные фразы. Этим стоит воспользоваться хотя бы по той причине, что отправитель будет традиционно терпимее к вежливой просьбе об ожидании, чем к банальному и грубому игнорированию. Есть также смысл в том, чтобы цитировать предшествующую переписку с пользователем. Такой вежливый жест поможет юзеру вспомнить все детали виртуальной беседыНепосредственно перед отправкой, специалисты советуют всегда производить контрольное прочтение. Уверенность в том, что приложены все файлы, а в сообщении все же написано то, что запланировано значительно, сократит время в Сети при «расхлебывании» всех этих естественных и популярных ошибок в будущем.Интернет-этикаУзнайте правила прежде, чем что-нибудь сказать или сделать.

Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.

Не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила. Если Вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и Вы когда-то были новичком.

Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам. Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использоваться опцию «Отправить по электронной почте». Не используйте без

разрешения чужой пароль.Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).
Программы-фильтры KidsControl (http://soft.mail.ru/program_page.php?grp=47967)Предназначение KidsControl – контроль времени, которое ребенок проводит в интернете.

Содержание Опасности, с которыми дети могут столкнуться в Сети

1Безопасное общение детей в Интернете
2Профилактика Интернет-зависимости у учащихся
3Технологии безопасной работы в сети
4Тест на интернет-зависимость http://www.psyhelp.ru/texts/iad_test.htm

Тревожная статистика

44% детей подвергались сексуальным домогательствам в Интернете
28% детей посещают порнографические веб-страницы
50% детей выходят в Интернет одни
Программы-фильтры iProtectYouPro (http://soft.mail.ru/program_page.php?grp=5382)
Программа-фильтр интернета позволяет родителям ограничивать по разным параметрам сайты, просматриваемые детьми.

БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ

Преодоление Интернет-зависимости
1. Признайте свою зависимость. «Патологическое использование компьютера» можно распознать по «симптомам» навязчивой потребности, пропущенным урокам и встречам, забытой и несделанной домашней работе, потере контакта с друзьями и родственниками.
2. Определите проблемы, лежащие в основе зависимости. В зависимости от возраста человека, такие моменты, ,как неуверенность в будущем, трудность успевать в школе или проблемы социальных отношений, могут подвигнуть ребенка на побег в гостеприимные виртуальные миры.
3. Решайте реальные проблемы. Стараясь избежать стрессовых ситуаций, мы только усложняем их. Вы можете найти репети-тора, который поможет с домашним заданием, поможет начать решать социальные трудности, написать о том, что вас «гложет», или даже обратиться к специалисту.
4. Контролируйте работу на компьютере. Совсем не обязательно полностью выключать его — можно просто ограничить время нахождения в Интернете. В зависимости от возраста родители или сам учащийся могут взять на себя эту ответственность. Все виды деятельности должны быть выстроены по их приоритетности. Общение в Интернете не должно происходить до выполнения домашней работы или других обязанностей.
5. Проводите различие между интерактивной фантазией и полезным использованием Интернета.
www.themegallery.com
www.themegallery.com

Опасности, с которыми дети могут столкнуться в Сети

Доступ к неподходящей информации:
сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;
сайты, размещающие изображения порнографического или иного неприемлемого сексуального
контента, к которым дети могут легко получить доступ;
сайты с рекламой табака и алкоголя;
сайты, посвященные изготовлению взрывчатых веществ;
сайты, пропагандирующие наркотики;
сайты, пропагандирующие насилие и нетерпимость;
сайты, публикующие дезинформацию;

сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;
сайты, позволяющие детям принимать участие в азартных играх онлайн
сайты, на которых могут собирать и продавать частную информацию о Ваших детях и Вашей семье.
Любопытная детская природа может завести их на сайты расистского, дискриминационного, сексуального, насильственного содержания или на сайты, содержащие материалы, побуждающие ребенка к действиям, которые могут поставить под угрозу его психологическое или физическое здоровье.
Общие правила безопасности при работе в Интернете:
Установите несколько четких и жестких правил для ребенка, чтобы контролировать расписание, время подключения и способ использования им Интернета. Убедитесь, что установленные правила выполняются. Особенно важно контролировать выход ребенка в Интернет в ночное время.
Хороший антивирус – союзник в защите Вашего ребенка от опасностей Интернета.
Ребенку не следует давать свой пароль кому-либо, за исключением взрослых членов семьи.
Следует объяснить ребенку, что он не должен делать того, что может стоить семье денег, кроме случаев, когда рядом с ним находятся родители.
Программы-фильтры Power Spy 2008 (http://www.securitylab.ru/software/301944.php)
Программу удобно использовать, чтобы узнать, чем заняты дети в отсутствие родителей.

Угрозы сети Интернет
Угроза заражения вредоносным ПО.
Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.
Множество вебсайтов, электронных сообщений или программ обмена файлами позволяют пользователям скачивать все виды музыки, игр, документов и т.д. Однако, несмотря на их кажущуюся безобидность, многие из них содержат вирусы.

Пять советов по безопасности при работе на общедоступном компьютере
1. Не сохраняйте свои учетные данные для входа в систему
2. Не оставляйте без присмотра компьютер с важными сведениями на экране
.3.Заметайте свои следы
.4.Опасайтесь подглядывания через плечо.
5.Не вводите важные сведения на общедоступном компьютере.
Программы-фильтры КиберМама 1.0b(http://www.securitylab.ru/software/273998.php)
КиберМама проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет.
КиберМама поддерживает следующие возможности:
Ограничение по суммарному времени работы
Поддержка перерывов в работе
Поддержка разрешенных интервалов работы
Возможность запрета интернета
Возможность запрета игр/программ

Общие правила безопасности при работе в Интернете:
Встреча в реальной жизни со знакомыми по Интернет-общению не является очень хорошей идеей, поскольку люди могут быть разными в электронном общении и при реальной встрече, и, если ребенок желает встретиться с ними, родителям следует пойти на первую встречу вместе.
Ребенок должен понять, что его виртуальный собеседник может выдавать себя за другого. Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. И 10-летний друг Вашего ребенка по чату в реальности может оказаться злоумышленником. Поэтому запретите ребенку назначать встречи с виртуальными знакомыми.

Профилактика Интернет-зависимости у учащихся
экономический аспект: неспособность и нежелание отвлечься даже на короткое время от работы в Интернете; досада и раздражение, возникающие при вынужденных отвлечениях, и навязчивые размышления об Интернете в такие периоды; стремление проводить за работой в Интернете все увеличивающиеся отрезки времени и неспособность спланировать время окончания конкретного сеанса работы; побуждение тратить на Интернет все больше денег, не останавливаясь перед влезанием в долги; межличностный аспект: готовность лгать друзьям и членам семьи, преуменьшая длительность и частоту работы в Интернете, способность и склонность забывать при работе в Интернете о домашних делах и учебе, важных личных встречах, пренебрегая занятиями; стремление и способность освободиться на время работы в Интернете от ранее возникнувших чувств вины или беспомощности, от состояний тревоги или депрессии, обретение ощущения эмоционального подъема и своеобразной эйфории; нежелание принимать критику подобного рода образа жизни; готовность мириться с потерей друзей и круга общения из-за поглощенности работой в Интернете; аспект здоровья: резкое сокращение длительности сна; избегание физической активности, пренебрежение личной гигиеной; постоянное забывание о еде.
За проявлениями зависимости от Интернета нередко скрываются другие аддикции, либо психические отклонения.
Расширение симптоматики, преувеличение количества потенциальных пациентов, шумиха в прессе удобны на данный момент специалистам по психическому здоровью и исследователям этого феномена.
Угрозы сети Интернет
Контакты с незнакомыми людьми с помощью чатов или электронной почты . Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.
Неконтролируемые покупки.
Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.
К сожалению уже было много случаев, когда педофилы выдавали себя за одного из детей или выдуманных персонажей, чтобы войти к ним в доверие и завести пошлые или открыто сексуальные беседы с ними или даже договориться о личной встрече.
Если Ваши дети имеют доступ к Вашим банковским данным или номеру кредитной карты, они могут приобрести практически что угодно через Интернет, от постера до роскошной машины, или оплатить услуги, варьирующиеся от онлайновых игр до путешествия вокруг света.
Общие правила безопасности при работе в Интернете:
Не следует открывать письма электронной почты, файлы или Web-страницы, полученные

от людей, которые не знакомы или не внушают доверия. Оградите ребенка от ненадлежащего веб-содержимого Научите его, как следует поступать при столкновении с подозрительным материалом, расскажите, что не нужно нажимать на ссылки в электронных сообщениях от неизвестных источников, открывать различные вложения. Такие ссылки могут вести на нежелательные сайты, или содержать вирусы, которые заразят Ваш компьютер. Удаляйте с Вашего компьютера следы информации, которую нежелательно обнаружить Вашему ребенку.

Инструкции по безопасному общению в чатах

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

Технологии безопасной работы в сети

Безопасность при навигации по сайтам и по приему почты

1. Не ходите на незнакомые сайты.
2. Если ходите, то выключайте (на всякий случай) поддержку языка Java и использование cookies

.3. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

4. Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов. Вот недавно хакерами был вскрыт один из крупнейших узлов бесплатной почты Hotmail. Так что не исключено, что с адреса вашего знакомого придет вирус.
5. Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).
6. Никогда, никому не посылайте свой пароль.
7. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше сгенерите его специальной программой или попросите сделать это своего провайдера.

Программы-фильтры CYBERsitter (http://www.securitylab.ru/software/240522.php)

CYBERSitter дает взрослым возможность ограничивать доступ детей к нежелательным ресурсам