ПАМЯТКА ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

- Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не

выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

- Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.

- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

- Используйте фильтры электронной почты для блокирования спама и нежелательных

сообщений.

- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.

- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.

ПРАВИЛА ИНТЕРНЕТ-ЭТИКЕТА

Путешествие по Сети может быть и развлечением, и полезным занятием, и способом общения как для взрослых, так и для детей. Однако важно, чтобы все новые пользователи Интернета, помнили о том, что они в Интернете не одни и, как и в реальной жизни, в Сети существуют правила поведения, или этикет, который необходимо соблюдать.

- Помните золотое правило: обращайтесь с другими так, как вы хотели бы, чтобы обращались с вами.

- Помните о том, что ваше сообщение получает живой человек.

- Не забывайте о том, где вы находитесь, и ведите себя подобающим образом.

- Прощайте ошибки другим людям, в особенности новичкам.

- Всегда сохраняйте спокойствие, особенно если кто-нибудь вас обижает (или вы думаете, что вас обидели).

- Избегайте написания текста ТОЛЬКО ЗАГЛАВНЫМИ БУКВАМИ с целью усиления его значения – некоторые пользователи видят в этом способ выражения крика.

- Не используйте неподходящую или оскорбительную лексику.

- Пользуйтесь постоянным онлайновым именем или псевдонимом и подписывайте им все сообщения (и наоборот, чтобы защитить свои личные данные, никогда не пользуйтесь своим пол-

ным именем).

- Никогда не отправляйте и не пересылайте нежелательные электронные письма (обычно их называют спамом).

- Держитесь в стороне от затяжных, эмоциональных споров или «флейма».

- Проверяйте правильность написанного, четко и коротко формулируйте свои сообщения.

- Во время общения в чатах не прерывайте других и не уходите от темы.

- Придерживайтесь тех же правил хорошего тона, которым вы следовали бы в реальной жизни.

ИНТЕРНЕТ-ХУЛИГАНСТВО: КАК ПРИ ЭТОМ СЕБЯ ПРАВИЛЬНО ВЕСТИ?

Так же как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета.

КТО ТАКИЕ ИНТЕРНЕТ-ХУЛИГАНЫ И ЧТО ОНИ ДЕЛАЮТ? Их называют гриферами, задирами, дурными игроками, повернутыми и т.д. Есть вероятность, что один из таких злодеев по крайней мере единожды побеспокоит вас в таких многопользовательских играх, как Halo 2, EverQuest, The Sims Online, SOCOM и Star Wars Galaxies. Обидчики (гриферы), по сути, те же дворовые хулиганы; они получают удовольствие, хамя и грубя окружающим. Обычно хулиганы издеваются над другими, особенно над начинающими (чайниками); мешают играть товарищам по команде; используют нецензурную лексику; жульничают; создают вместе с другими гриферами бродячие банды; блокируют выходы из комнат; выманивают монстров на неосторожных игроков или используют игру, чтобы досаждать, кому только можно, или изводить конкретного человека.

Хотя они составляют лишь малую часть от общего числа пользователей, из-за гриферов некоторые

компании потеряли клиентов. В итоге многие разработчики игр не жалеют этих хулиганов и используют любые методы для их вычисления.

КАК ПОСТУПАТЬ, ЕСЛИ ВЫ СТОЛКНУЛИСЬ С ГРИФЕРАМИ? Игнорируйте. Если не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут. Попробуйте изменить параметры игры. Играйте в игры, правила или режимы которых можно изменить, например, невозможность убить товарищей по команде. Таким образом, тактика гриферов становится бессмысленной. Создайте частную

игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать толь-

ко друзей. Играйте на сайтах со строгими правилами. Там, где установлены строгие правила, администратор сможет немедленно заблокировать хулиганов. Играйте в игры, где от гриферов можно легко избавиться, а также где сообщения хулиганов можно отключить или проголосовать за их исключение из игры. Придумайте еще что-нибудь. Если обидчик продолжает беспокоить вас, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже. Сообщайте о «дырах» в игре. Поищите уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору. Воздерживайтесь отвечать огнем на огонь. Не используйте против обидчиков их же тактику; скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о вас впечатление как об обидчике. Избегайте провокаций с именами. Вы избежите многих проблем, если не станете использовать псевдоним, который может спровоцировать обидчика. Не выдавайте личную информацию. Хулиганы (да и вообще кто угодно) могут использовать настоящие имена, номера телефонов, а также домашние или электронные адреса, чтобы причинить вам неприятности.

КАК УБЕРЕЧЬСЯ ОТ НЕДОСТОВЕРНОЙ ИНФОРМАЦИИ?

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете. Это, в частности, относится к тем, которые

склонны думать: «Раз в Интернете – значит, правильно. У газет или журналов есть проверяющие

люди: корректор и редактор. Но Интернет не сможет проверить, насколько правдива размещенная информация. В Интернете каждый может создать сайт и никто ему не задаст никаких вопросов. Используйте широкий круг источников и будьте осторожны с тем, что видите в Сети.

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

Преступники преимущественно устанавливают контакты в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и

даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить

сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

ЧТО НУЖНО ЗНАТЬ О ВРЕДОНОСНЫХ И НЕЖЕЛАТЕЛЬНЫХ ПРОГРАММАХ В ИНТЕРНЕТЕ

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

ЧТО ТАКОЕ ВИРУС? Вирусы – это программы, которые мешают нормальной работе компьютера, перезаписывают, повреждают или удаляют данные. Они распространяются между компьютерами в Сети и через Интернет, часто замедляя их работу и вызывая другие неполадки. Так же как вирусы человека различаются по степени опасности, так и компьютерные вирусы могут быть как

слегка неприятными, так и безусловно разрушительными. Однако у них есть и хорошая сторона: настоящий вирус не может распространяться без участия человека. Для продвижения вируса кто-то должен распространить файл или отправить электронное письмо. Более сложные вирусы, например черви, могут автоматически самовоспроизводиться на других компьютерах, устанавливая контроль над программами (например, приложениями электронной почты).

Некоторые вирусы – «троянские кони» (названные так в честь легендарного Троянского коня) – выглядят как полезные программы и обманом убеждают пользователей загрузить их. Отдельные «троянские кони» способны даже работать как полезная программа, одновременно нанося вред системе или другим компьютерам, подключенным к Сети. Иметь представление о разновидностях вирусов и принципах их функционирования необходимо, но гораздо важнее регулярно устанавливать на компьютере последние обновления безопасности и антивирусные средства.

ЧТО ТАКОЕ НЕЖЕЛАТЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ?

Под выражением «нежелательное программное обеспечение» понимаются программы, которые выполняют на компьютере некие задачи без вашего согласия. Они могут показывать рекламные сообщения, объявления или собирать личные данные о вас и вашей семье.

КАК МОЖНО ОПРЕДЕЛИТЬ, ЧТО ВАШ КОМПЬЮТЕР ЗАРАЖЕН?

Ваш компьютер может начать работать медленнее или прекращать работать и перезагружаться каждые несколько минут. Иногда вирус атакует файлы, необходимые для запуска компьютера.

В подобном случае вы можете, нажав кнопку запуска, обнаружить, что смотрите на пустой экран.

Все эти симптомы являются типичными признаками заражения компьютера вирусом, хотя они могут вызываться также проблемами в аппаратной части или программном обеспечении, не имеющими ничего общего с вирусным заражением. Совет: Помните, что, открыв и запустив зараженный файл, вы можете не сразу узнать, что получили вредоносную программу, так как вирусы часто начинают свою разрушительную работу не сразу. Будьте внимательны к сообщениям о том, что они отправили электронное письмо,

содержащее вирус. Это может значить, что вирус указал ваш электронный адрес в качестве отправителя зараженного письма. Это необязательно означает, что на вашем компьютере есть вирус. Некоторые вирусы умеют фальсифицировать электронные адреса. Если компьютер внезапно начал медленно работать или вы видите всплывающие окна, даже если не подключены к Интернету, то, возможно, вы стали жертвой программ-шпионов и других нежелательных программ. Они автоматически загружаются в

систему без всякого уведомления. Часто они бывают прикреплены к другому файлу, который вы скачали или установили. Программа-шпион может загрузиться на ваш компьютер, даже если вы просто щелкнули по баннеру.

КАК СНИЗИТЬ РИСК ЗАРАЖЕНИЯ?

Необходимо постоянно улучшать защиту вашего компьютера. Есть три основных шага, которые необходимо сделать, чтобы обеспечить защиту своего компьютера:

- применяйте межсетевой экран;
- выполняйте обновления;
- применяйте новейшие антивирусные программы.

Однако нужно помнить, что ничто не может дать стопроцентной гарантии защиты вашего компьютера. Поэтому в любом случае вы должны быть крайне внимательны к получению сообщений от неизвестного адресата с вложением. Практически все вирусы и многие черви не могут распространяться, пока вы не откроете или не запустите инфицированную программу.

Многие из наиболее опасных вирусов распространялись преимущественно через вложения в электронные письма – файлы, отправляемые вместе с электронным сообщением. Вирус запускается в тот момент, когда вы открываете вложенный инфицированный файл.

Совет: никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда ожидаете получение вложения и точно знаете содержимое такого файла.

Если вы получили электронное письмо с вложением от неизвестного лица, немедленно

его удалите. К несчастью, иногда небезопасно открывать даже вложения, полученные от знакомых вам людей. Вирусы и черви обладают способностью красть информацию из почтовых программ и рассылать себя по всем адресам, указанным в адресной книге. Проверяйте всю информацию, которая поступает на ваш компьютер из других источников. Вирусы могут распространяться с помощью программ, которые вы загружаете из Интернета, или через зараженные компьютерные диски, которые вы можете взять у друзей. Но в большинстве случаев вредоносные программы попадают на компьютеры пользователей, когда они открывают и запускают вложения в электронные письма, полученные от неизвестных им корреспондентов.

Иногда вы можете случайно заразить компьютер программой-шпионом, даже не осознавая этого.

Совет: Ключевое правило, которого следует придерживаться, – это скачивать файлы из надежных источников и обязательно читать предупреждения об опасности, лицензионные соглашения и

положения о конфиденциальности

АЗАРТНЫЕ ИГРЫ В ИНТЕРНЕТЕ. В ЧЕМ СОСТОИТ ОТЛИЧИЕ МЕЖДУ ИГРОВЫМИ САЙТАМИ И САЙТАМИ С АЗАРТНЫМИ ИГРАМИ.

Множество детей обожают искать развлечения (например, игры) в Интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако им нельзя играть в азартные игры на деньги.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

В основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. К играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ:

То, что дети проводят в Интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветствовали появление Сети, полагая, что она – безграничный источник новых знаний. Вскоре выяснилось, что подростки не столько пользуются Интернетом для выполнения домашних заданий или поиска полезной информации, сколько общаются в чатах и играют в онлайновые игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями

всегда было испытанием для родителей; Интернет сделал это еще более трудной задачей. Общение в Интернете и интерактивные игры могут настолько затягивать детей, что они часто теряют ощущение времени.

ИНТЕРНЕТ-ДНЕВНИКИ: ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара,

особенно среди подростков, которые порой ведут Интернет-дневники без ведома взрослых.

Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

При этом все больше молодых пользователей создают собственные дневники, и каждый стремится привлечь как можно больше внимания аудитории. Иногда это приводит к тому, что дети размещают в блогах такой неуместный материал, как провокационные фотографии – свои или друзей.

ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ ИНТЕРНЕТДНЕВНИКА.

Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения.

Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверять, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

Знайте, что публикуемая в Интернете информация остается там надолго и кто угодно может легко распечатать веб-журнал или сохранить его на своем компьютере.

Пользуйтесь веб-журналами с ясно сформулированными условиями использования и проверяйте, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользователя (даже если это так, лучше держать в уме, что любой человек может получитьдоступ к Интернет-дневнику).

Не стремиться соревноваться с другими детьми, ведущими веб-журналы.

Старайтесь вести свой блог в положительном ключе и не используйте его для злословия или нападок в адрес других детей.