Интернет – это безграничный мир информации. Здесь ты найдёшь много интересного и полезного для учёбы. В интернете можно общаться со знакомыми и даже заводить друзей.

Но кроме хорошего, в виртуальном мире есть и плохое. Неправильное поведение в интернете может принести вред не только тебе, но также твоим родным и близким.

Чтобы обезопасить себя в интернете, достаточно соблюдать правила, которые содержатся в этой памятке. В этих правилах нет ничего трудного. Отнесись к ним внимательно – и расскажи о них своим друзьям!

Тест на знание правил поведения в интернете

1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.

   А Попрошу его фото, и потом отправлю своё.
   В Посоветуюсь с родителями.

2) В чате тебя обозвали очень грубыми словами.

   А Скажу в ответ: «Сам дурак».
   В Прекращу разговор с этим человеком.

3) Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.

   А Потребую доказательств, что она плохая.
   В Сразу откажусь.

4) Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.

   А Вышлю только пароль: они сами должны знать логин.
   В Отмечу письмо как Спам.

Посчитай, сколько получилось ответов «А» и сколько «В».

4 «А»
Тебе ещё многому надо научиться.

3 «А» и 1 «В»
Внимательно прочитай эту памятку.

2 «А» и 2 «В»
Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «В»
Ты почти справился, но есть слабые места.

4 «В»
Молодец! К Интернету готов!

Министерство внутренних дел Российской Федерации

Управление «К»

Безопасный интернет – детям!

Полезные советы для тебя и твоих друзей

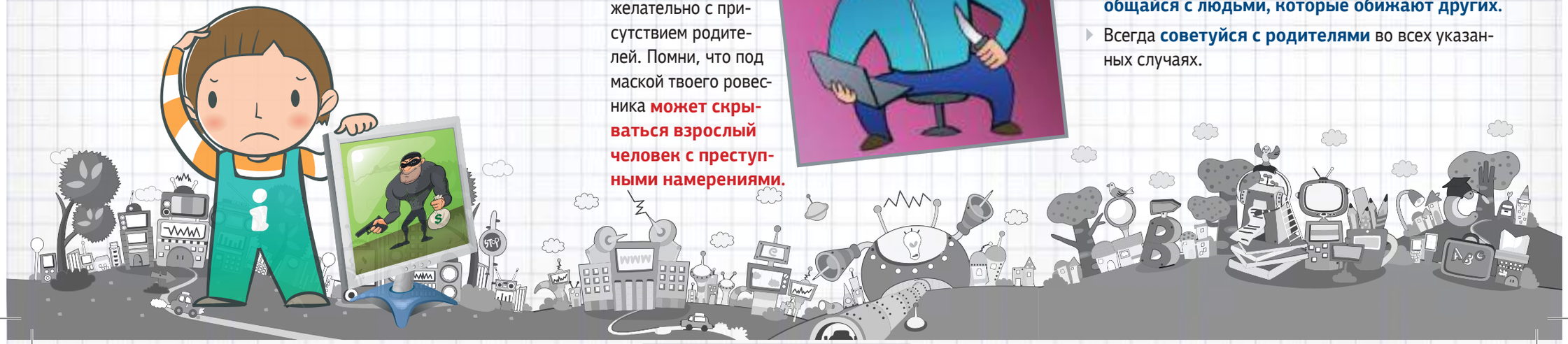
ОСТОРОЖНО:

ВИРУСЫ И ДРУГИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ (ЧЕРВИ, ТРОЯНЫ)

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут **уничтожить** важную информацию **или украсть** деньги через Интернет.

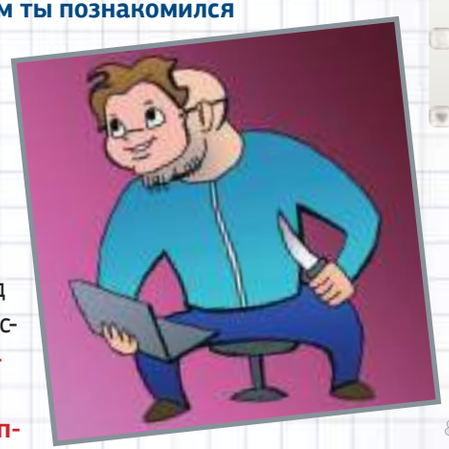
- **Для защиты компьютера** на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- **Не сохраняй подозрительные файлы** и не открывай их.
- Если антивирусная защита компьютера не рекомендует, **не заходи на сайт, который считается «подозрительным».**
- Никому **не сообщай свой логин с паролем** и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.



ВИРТУАЛЬНЫЕ МОШЕННИКИ (ВОРЫ) И ДРУГИЕ ПРЕСТУПНИКИ ИНТЕРНЕТА

Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- **Не сообщай свой адрес или телефон** незнакомым людям и никогда не выкладывай в Интернете. Никогда **не высылай свои фотографии** без родительского разрешения. Помни, что **преступники могут использовать эту информацию** против тебя или твоих родных.
- **Если ты хочешь поучаствовать** в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- Никогда **не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.** Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника **может скрываться взрослый человек с преступными намерениями.**



ГРУБИЯНЫ И ХУЛИГАНЫ (ТРОЛЛЬ, ПРОВОКАТОР) В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- Помни: **ты не виноват**, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение.
- **Если тебе угрожают** по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но **подобные люди боятся ответственности.**

- Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. **Никогда не участвуй в травле и не общайся с людьми, которые обижают других.**
- Всегда **советуйся с родителями** во всех указанных случаях.

БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ

Microsoft®

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома. Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. Для многих, особенно молодых людей, он становится информационной средой, без которой они не представляют себе жизнь. И это неудивительно: ведь в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах.

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

ДЕРГУНОВА Ольга Константиновна,
президент Microsoft в России и СНГ

Скорость распространения информационных технологий в наши дни становится все стремительнее. Сегодня мы говорим уже о 600 миллионах пользователей персональных компьютеров, и в ближайшей перспективе эта цифра может превысить 1 миллиард. Компьютер широко используется не только на рабочем месте, но и в быту, дома, на отдыхе. Причем для домашнего использования персональные компьютеры приобретаются в гораздо больших объемах, нежели для организаций. Это общемировая тенденция, и наша страна не является здесь исключением.

Развитие информационных технологий открывает новые горизонты для нашей молодежи, для подрастающего поколения. В этой связи важно помнить, что дети должны быть защищены от угроз информации агрессивного характера, существующей, к сожалению, в сети Интернет.

Вопросы информационной безопасности и совершенствования технологических решений в этой области постоянно находятся в поле повышенного внимания корпорации Microsoft. Не менее важная задача для нас – научить людей пользоваться новыми современными технологиями так, чтобы они смогли защитить себя и свою семью. Зачастую дети оказываются совершеннее нас, взрослых, в умении использовать информационные технологии. И далеко не всегда взрослые осознают, с какими рисками могут столкнуться дети при использовании Интернета, не всегда могут помочь в использовании технологий, не знают, как обеспечить безопасность своих детей.

Мы надеемся, что предлагаемые вашему вниманию материалы помогут разобраться, какие опасности могут таиться для детей во Всемирной паутине, помогут вооружиться знаниями о том, на что следует обращать внимание, какие меры предосторожности нужно предпринимать и что можно сделать с помощью технологических средств. Все это в конечном итоге повысит безопасность наших детей и защитит их от возможной опасности!

ДЕМИДОВ Алексей Александрович,
заместитель председателя Российского комитета Программы ЮНЕСКО «Информация для всех»

Программа ЮНЕСКО «Информация для всех» создана в качестве основы для международных дискуссий о политических, правовых, этических и социальных проблемах, связанных с построением глобального информационного общества, а также для подготовки проектов, ориентированных на обеспечение всеобщего доступа к информации. Эта деятельность заключается в том числе и в достижении согласия в отношении принципов, применимых к киберпространству.

Сегодня информационно-коммуникационные технологии (ИКТ) предоставляют беспрецедентные возможности для детско-юношеского обучения и творчества. В то же время серьезной проблемой во всем мире стало злоупотребление плодами ИКТ и их использование для совершения преступлений против детей. К настоящему времени проблема безопасности детей в Интернете, без преувеличения, стала глобально значимой проблемой. Вся семья международных организаций системы ООН уже более десяти лет занимается ее решением. Лидеры по внедрению информационных технологий в повседневную жизнь и нормативному регулированию информационных отношений – США и Европейский союз – уже вплотную столкнулись с необходимостью решения всего спектра проблем: как регулировать доступ детей в Интернет и контролировать их пребывание в Интернете? Как защищать детей от преступных действий со стороны злоумышленников, которые очень активно используют Интернет для своих вредных, незаконных и аморальных целей?

Сегодня в мире уже возникло устойчивое понимание того, что проблема детской безопасности в Интернете – это предмет, требующий скоординированного решения на всех уровнях: от семейного и муниципального до регионального и международного. В решении этой проблемы необходимо действовать системно и использовать не только правовые регуляторы, но и нормы обычаев и морали, а также технические и технологические возможности. Новым и самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности – родителей и детей, а также профессиональной информационной культуры журналистов и учителей.

Родители должны понимать, какая информация нужна ребенку для развития. Одно дело – найти хорошую книгу и подтолкнуть ребенка к диалогу с ней, но что, если искомая информация находится в Интернете? Тогда нужно сесть вместе с ребенком к компьютеру и попытаться найти ее вместе. В этом случае ребенок будет позитивно учиться искать, находить и использовать информационные ресурсы и технологии. Надо с первого знакомства с информационными технологиями разъяснять ребенку, как ему жить в информационном пространстве, как избирательно подходить к информации в открытой информационной среде. Важно, чтобы и сами родители, и дети понимали, что в информационном пространстве есть свои плюсы и минусы, плохое и хорошее.

С глубоким удовлетворением отмечаю продолжение сотрудничества Российского комитета Программы ЮНЕСКО «Информация для всех» с офисом Microsoft в России и СНГ, начавшегося в 2004 году с открытия центров доступа к социально значимой информации в Узбекистане. 20 сентября 2005 года в пресс-клубе «РИА Новости» мы провели вместе круглый стол «Безопасность детей в Интернете», организованный при поддержке Международного центра защиты детей от эксплуатации и похищений (ICMEC) и Международной организации уголовной полиции (Interpol). Развивая это важное для нас направление работы, мы реализуем положение Программы ЮНЕСКО «Информация для всех» о необходимости развития сотрудничества с бизнес-сообществом для создания мультиплицирующего эффекта, а также участвуем в реализации соглашения о сотрудничестве, подписанного в 2005 году между Генеральным директором ЮНЕСКО К. Мацуурой и руководителем корпорации Microsoft Б. Гейтсом.

ОПАСНОСТИ И ПРАВИЛА БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Смежная специальность современного родителя – это Интернет-Ангел хранитель.

ПРЕСТУПНИКИ В ИНТЕРНЕТЕ: ЧТО МОЖНО СДЕЛАТЬ ДЛЯ СНИЖЕНИЯ ОПАСНОСТИ

Пользуясь возможностями Интернета, дети подвергаются опасности вступить в контакт со злоумышленниками. Анонимность общения в Интернете способствует быстрому возникновению доверительных и дружеских отношений. Преступники используют преимущества этой анонимности для завязывания отношений с неопытными молодыми людьми. Вы сможете защитить своих детей, если поймете возможную опасность общения через Интернет и будете в курсе того, чем они занимаются в Сети.

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ. Преступники преимущественно устанавливают контакты с детьми 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.

КАК УЗНАТЬ, НЕ СТАЛ ЛИ ВАШ РЕБЕНОК ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА? Приведенные ниже признаки могут означать, что на вашего ребенка обратил внимание злоумышленник.

Ваш ребенок проводит много времени в Интернете. Большинство детей, преследуемых Интернет-преступниками, проводят большое количество времени в Сети, особенно в чатах; подчас закрывают дверь в свою комнату и скрывают, чем они занимаются, сидя за компьютером.

В семейном компьютере появились материалы откровенного содержания. В качестве предлога для начала сексуальных обсуждений злоумышленники могут снабжать детей фотографиями, ссылками на соответствующие сайты и присылать сообщения эротической окраски. Для того чтобы внушить ребенку мысль о естественности сексуальных отношений между взрослыми и детьми, преступники могут использовать фотографии с изображением детской порнографии. Имейте в виду, что ваш ребенок может прятать порнографические файлы на дисках, особенно если другие члены семьи пользуются тем же компьютером.

Вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам незнакомы. Установив в Интернете контакт с вашим ребенком, некоторые злоумышленники могут попытаться вовлечь детей в секс по телефону или попытаться встретиться в реальной жизни. Если дети не решаются дать номер телефона, злоумышленник может сообщить им свой. Не разрешайте своему ребенку лично встречаться с незнакомцем без контроля с вашей стороны.

Ваш ребенок получает письма, подарки или посылки от неизвестного вам лица. Обычно преследователи посылают своим потенциальным жертвам письма, фотографии и подарки. В других странах они порой даже отправляют билеты на самолет, чтобы соблазнить ребенка личной встречей.

Ваш ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый. Интернет-преступники усердно вбивают клин между детьми и их семьями и часто преувеличивают небольшие неприятности в отношениях ребенка с близкими. Кроме того, дети, подвергающиеся сексуальному преследованию, становятся замкнутыми и подавленными.

Ваш ребенок использует чью-то чужую учетную запись для выхода в Интернет. Даже дети, не имеющие доступа в Сеть дома, могут встретить преследователя, выйдя в Интернет у друзей или в каком-нибудь общественном месте, например библиотеке. Иногда преступники предоставляют своим жертвам учетную запись, чтобы иметь возможность с ними общаться.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАШ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА? Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либо свидетельств об общении с сексуальной окраской – это настораживающие признаки.

Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.

Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

Если ваш ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

ЧТО ДЕТИ ДОЛЖНЫ 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. Но хорошо то, что, проявив здравый смысл и предприняв меры по предотвращению опасности, а также объяснив эти опасности своим детям, ваша семья с меньшей вероятностью станет жертвой подобных угроз.

ЧТО ТАКОЕ ВИРУС? Объясните детям, что вирусы – это программы, которые мешают нормальной работе компьютера, перезаписывают, повреждают или удаляют данные. Они также 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 (от вируса Эбола до вируса 24-часового гриппа), 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? Объясните детям, что 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.

Пусть дети будут 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.

Совет: Потребуйте от детей никогда не открывать никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда они ожидают получение вложения и точно знают содержимое такого файла.

Если вы или ваши дети 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, требуйте этого от своих детей. 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.

Если дети регулярно пользуются компьютером, они могут забрести на сайты или скачать файлы, которые могут заразить компьютер. Иногда ваши дети могут 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.

Скажите детям, чтобы они спрашивали у вас разрешение перед тем, как загрузить что-либо из Сети. Если вы полагаете, что дети не понимают, что означает «скачивать только из надежных источников», или считаете, что, возможно, они не будут читать все предупреждения и соглашения, вам, возможно, придется принять дополнительные меры предосторожности: контролировать деятельность ребенка в Интернете или создать для него учетную запись пользователя, которая ограничивает возможности управления компьютером, что поможет предотвратить загрузку программ-шпионов или других нежелательных программ.
Загрузить антивирусное ПО, средства удаления программ-шпионов и многое другое для повышения защищенности компьютера можно на веб-сайте

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.

Более подробную информацию см. на веб-сайте Microsoft по адресу http://www.microsoft.com/Rus/Security/Protect/Default.mspx

Однако нужно помнить, что ничто не может дать стопроцентной гарантии защиты вашего компьютера. Поэтому в любом случае вы и ваши дети 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.

Microsoft по адресу http://www.microsoft.com/rus/athome/security/downloads/default.mspx.

ЧТО ДЕТИ ДОЛЖНЫ ЗНАТЬ ОБ ИНТЕРНЕТ-МОШЕННИЧЕСТВЕ И ХИЩЕНИЯХ ДАННЫХ КРЕДИТНОЙ КАРТЫ

В России мошенничество с помощью Интернета или хищения данных кредитной карты еще не стали очень широко распространены. Однако мы можем стоять на пороге этого явления, и нужно сделать так, чтобы оно не застало нас врасплох.

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing», состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

Кроме того, если вы сами или ваши дети пользуетесь кредитной картой для оплаты товаров и услуг через Интернет, по телефону или даже лично в соседнем магазине, вы уязвимы для мошенников. При любой операции оплаты с использованием кредитной карты компании должны проверить информацию о счете, прежде чем предоставить товары или услуги. Данные о кредитных картах хранятся на крупных серверах. К сожалению, хакеры могут взломать такую систему и завладеть информацией, чтобы воспользоваться ею в корыстных целях, например, оплачивать свои счета, используя деньги с вашей карты.

СНИЖЕНИЕ РИСКА ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ. Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.

ЧТО ДЕЛАТЬ В СЛУЧАЕ ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ? Если вы подозреваете, что ваши личные данные украдены, немедленно принимайте меры:

- Измените пароли.
- Поставьте в известность отдел обслуживания клиентов соответствующих организаций.
- Поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета.
- Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.
- Записывайте и сохраняйте абсолютно все.
- После выполнения всех действий всегда делайте копии документов.

В виртуальном мире есть свои правила Интернет-гигиены.

АЗАРТНЫЕ ИГРЫ В ИНТЕРНЕТЕ: КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ?

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.

КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ ОТ ИГР НА ДЕНЬГИ? Родители должны решить, во что можно играть их детям. Обсудите жанр игр (скажем, только бильярд, стратегии и шахматы) и количество участников (можно ведь играть и одному).

Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают.

Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги.

Объясните, что 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.

Контролируйте поведение своих детей в Интернете. Следите за тем, какие сайты посещают ваши дети и что они делают в Интернете.

Бесплатный сыр бывает и в Интернет-мышеловках.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ЕСТЬ ЛИ ОНА У ВАШИХ ДЕТЕЙ?

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. Несколько советов ниже помогут вашим детям не впасть в Интернет-зависимость.

СОВЕТЫ ПО ПРОФИЛАКТИКЕ ИНТЕРНЕТ-ЗАВИСИМОСТИ. Обратите внимание на психологические особенности вашего ребенка. Социально дезадаптированные дети имеют повышенную вероятность к приобретению Интернет-зависимости. Причина в том, что Интернет позволяет оставаться анонимным, не бояться осуждения (если что-то сделал неправильно, всегда можно поменять имя и начать все заново), предоставляет гораздо более широкий выбор возможностей к общению, чем реальный мир. В Интернете ребенку гораздо легче выстроить свой виртуальный мир, пребывание в котором ему будет

комфортным. Поэтому, если у ребенка что-то не получается в реальном мире, он будет стремиться к пребыванию там, где ему комфортно. С другой стороны, Интернет может помочь застенчивому ребенку стать более общительным, найти ту среду общения, которая более полно соответствует его уровню развития, и в результате повысить его самооценку. Если ваш ребенок в жизни замкнут, застенчив или склонен к унынию, вам необходимо внимательно следить за его отношением к Интернету, с тем чтобы предотвратить его превращение из средства раскрытия личности ребенка в плохо контролируемую страсть.

Следите за симптомами проявления Интернет-зависимости. Она проявляется в том, что дети до такой степени предпочитают жизнь в Интернете, что фактически начинают отказываться от своей реальной жизни, проводя в виртуальной реальности большую часть своего времени. Интернет-зависимый ребенок чаще всего тих и замкнут, он ждет не дождется, когда можно будет подключиться к Интернету, ему тяжело выйти из него, он впадает в депрессию или становится раздражительным, если на несколько дней его отлучили от Интернета. Интернет-независимый ребенок легко может переключиться на другой канал общения, выйти из Интернета, когда в этом возникает необходимость, он всегда четко различает, где он сейчас общается – в Сети или нет. Спросите себя: оказывает ли времяпровождение в Сети влияние на школьные успехи вашего ребенка, его здоровье и отношения с семьей и друзьями? Выясните, сколько времени ваш ребенок проводит в Интернете.

Обратитесь за помощью к специалистам. Если у вашего ребенка проявляются серьезные признаки Интернет-зависимости, проконсультируйтесь с педагогом или психологом. Навязчивое использование Интернета может быть симптомом других проблем, таких, как депрессия, раздражение или низкая самооценка. И когда эти проблемы будут решены, зависимость от Интернета может пройти сама собой.

Не запрещайте Интернет. Для большинства детей он является важной частью их общественной жизни. Вместо этого установите «Внутрисемейные правила использования Интернета» (см с. 34 данного издания) . В них можно включить следующие ограничения: количество времени, которое ежедневно проводит в Интернете ребенок; запрет на Сеть до выполнения домашней работы; ограничение на посещение чатов или просмотр материалов «для взрослых».

Поддерживайте равновесие. Пусть ребенок почаще играет с другими детьми на свежем воздухе. Мотивируйте его на такое общение.

Помогайте ребенку участвовать в общении вне Интернета. Если ваш ребенок застенчив и испытывает неловкость при общении с ровесниками, почему бы не рассмотреть возможность специального тренинга? Поощряйте участие ребенка в тех видах деятельности, которые объединяют детей с одинаковыми интересами, например, судомодельный или литературный кружок.

Контролируйте своих детей. Существуют программы, которые ограничивают использование Интернета и осуществляют контроль за тем, какие сайты посещаются, например MSN® Premium. Однако сообразительный ребенок, если постарается, может и отключить эту службу. Поэтому ваша конечная цель – развитие у детей самоконтроля, дисциплины и ответственности.

Предложите альтернативы. Если вам кажется, что ваши дети интересуются только онлайновыми развлечениями, попробуйте предложить им автономный аналог одной из их любимых игр. Например, если ваш ребенок получает удовольствие от ролевых игр на тему фэнтези, предложите ему почитать книги той же тематики.

Следите за достижением равновесия у вашего ребенка между временем, проводимым в Интернете и вне его.

ОНЛАЙНОВОЕ ПИРАТСТВО У СЕБЯ ДОМА: КАК ПРЕДОТВРАТИТЬ?

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

СНИЖЕНИЕ РИСКА ПИРАТСТВА У СЕБЯ ДОМА. Предупредите детей о возможных опасностях. Пиратство, по сути, обычное воровство, и, скорее всего, вы вряд ли собираетесь поощрять воровство в своей семье. И чем раньше ваши дети это поймут, тем лучше. Однако не всегда бывает достаточно сказать детям о том, что какая-то деятельность – это плохо. В таком случае попробуйте просто поговорить с ними о возможных последствиях. Объясните вашим детям, что если они незаконно скачивают файлы, то ваш компьютер рискует стать уязвимым для вирусов или программ-шпионов.

Совет: Внушите своим детям, что нельзя незаконно скачивать или распространять фильмы, музыкальные файлы и программы.

Объясните детям, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

Научите своих детей законным методам скачивания. В Интернете существует множество мест, где вы и ваши дети можете скачать программы, фильмы, игры и музыку бесплатно или за небольшую цену. Например, сайт MSN Music предлагает более миллиона записей от разных студий.

Обсудите с детьми допустимые траты на музыкальные записи или игры, чтобы у молодого поколения не было соблазна для незаконного скачивания.

БЕЗОПАСНОЕ ОБЩЕНИЕ ДЕТЕЙ В ИНТЕРНЕТЕ

Интернет предоставляет несколько форм общения между участниками, которые любят использовать дети и подростки: чаты, системы обмена мгновенными сообщениями, блоги или Интернет-дневники.

В ЧЕМ СОСТОИТ ОБЩЕНИЕ ДЕТЕЙ В ЧАТАХ И СИСТЕМАХ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМ? Возможно, вы слышали о чатах, в которых люди встречаются для обмена сообщениями на определенную тему. Может быть, вы даже сами там общались. Комнаты чата, в которых происходит общение, представляют собой виртуальные помещения в Сети, в которых люди могут набирать сообщения, почти мгновенно появляющиеся на экранах компьютеров других участников. Чаты обычно являются анонимными, поскольку участники пользуются псевдонимами.

В Интернете существует множество чатов различной направленности. В них предоставляется потрясающая возможность обсуждать разные темы с людьми со всего мира. Чаты очень популярны среди детей, и, к сожалению, преступникам это известно. Поэтому эта форма общения представляет особенную опасность для детей и подростков.

Многие люди, говоря об общении в системе обмена мгновенными сообщениями, называют это общением в чате, однако все же существует небольшая разница. Первая обычно используется для беседы между двумя собеседниками, в то время как в чате идет разговор с группой людей, но основные правила безопасности остаются одними и теми же.

КАК СДЕЛАТЬ ОБЩЕНИЕ В ИНТЕРНЕТЕ КОМФОРТНЫМ? Контролируйте использование чата вашим ребенком. Помните о том, что дети могут участвовать в чатах, расположенных на сайтах, при помощи программ поддержки чатов, сотовых телефонов и даже некоторых онлайновых игр.

Добейтесь того, чтобы дети никогда не сообщали в чатах свои личные данные. Так, при выборе псевдонима необходимо выбирать имя, не выдающее личные данные детей. Например, вместо псевдонима DetroitSue можно использовать SassySue. Следует настоять на том, чтобы дети не посылали своих фотографий тем, с кем они познакомились в чате.

Дети должны знать, что они всегда могут обратиться к вам за советом или помощью. Предупредите ребенка о том, что, если что-либо в чате вызовет у него чувство дискомфорта, необходимо немедленно его покинуть и сообщить о происшедшем кому-нибудь из взрослых. Пусть дети всегда сообщают вам об участниках чата, которые предлагают им встретиться в приватных комнатах чата.

У детей должно быть настороженное отношение к попыткам собеседников перевести общение из виртуальной плоскости в реальную. Им никогда нельзя соглашаться на личную встречу с незнакомыми людьми, с которыми они познакомились в Интернете.

Скажите детям, чтобы они посещали только модерируемые чаты. Перед тем как вступить в беседу, пусть ознакомятся с положениями и условиями участия в чате, правилах поведения и положением о конфиденциальности.

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.

Правильное ведение дневника может дать детям и их родителям возможность общаться и поделиться друг с другом опытом; дети могут поведать родителям о новых технологиях, а родители могут дать ряд ценных жизненных советов.

Другое преимущество – привитие ответственности и дисциплины ведения дневника; возможность творческого самовыражения; новые возможности общения с друзьями и родственниками, обучение компьютерным и Интернет-технологиям, а также развитие навыков набора на клавиатуре, правописания, письменной речи и редактирования.

ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ ИНТЕРНЕТ-ДНЕВНИКА.
Требуйте от ваших детей никогда не публиковать 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.

Требуйте от ваших детей никогда не помещать 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.

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

Рекомендуйте детям пользоваться веб-журналами только с ясно сформулированными условиями использования и проверять, 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 получить доступ к Интернет-дневнику).

Рекомендуйте вашим детям не стремиться соревноваться с другими детьми, ведущими веб-журналы.

Пусть дети стараются вести свой блог в положительном ключе и не использовать его для злословия или нападок в адрес других детей.

ИГРЫ ЧЕРЕЗ ИНТЕРНЕТ: КАК ИГРАТЬ БЕЗОПАСНО

Компьютерные игры уже давно сравнялись по популярности с телевидением, музыкой и фильмами, а где-то даже превзошли их. Вы можете помочь своим детям играть в занимательные и даже поучительные игры и само собой соответствующие возрасту вашего ребенка. Нужно только придерживаться некоторых советов.

СОВЕТЫ ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ УЧАСТИЯ ВАШИХ ДЕТЕЙ В ОНЛАЙНОВЫХ ИГРАХ ПО СЕТИ.
Получите информацию. Ознакомьтесь с классификацией игр и условиями конфиденциальности, а также прочтите правила на сайте игры. В качестве примера можно познакомиться с кодексом поведения Xbox® Live.

Будьте в курсе, в какие игры и с кем играют ваши дети. Поместите компьютер или игровую консоль (например, Xbox) туда, где экран хорошо просматривается; искренне интересуйтесь, во что дети играют.

Установите правила. Это следует сделать до выхода детей в Интернет; кроме того, убедитесь, что ребенок их понимает. С примером такого рода домашних правил можно ознакомиться, прочитав «Внутрисемейные правила пользования Интернетом» (см. с. 34 данного издания).

Контролируйте чат и сообщения во время игр. Попросите детей сообщать вам, если другой игрок употребляет нецензурные слова; в этом случае можно выделить обидчика в списке и отключить или заблокировать его сообщения. Другой вариант – сообщить о некорректно ведущем себя игроке администраторам игры по электронной почте, в чате или другим способом. Для дополнительной информации о возможных мерах воздействия на таких игроков можно обратиться на официальный сайт игры.

Обучите детей навыкам безопасности. Скажите детям, что, если кто-либо из игроков будет вести себя оскорбительно, игру следует остановить и немедленно сообщить вам. При необходимости – связаться с администратором.

Убедитесь в конфиденциальности. Требуйте от детей никогда не выдавать в игровом чате личную информацию (например, имя, пол или домашний адрес), фотографии и не соглашаться на встречи. Убедитесь, что дети знают о необходимости обратиться к вам за помощью в случае чего.
Выбирайте соответствующие имена. Заставьте ребенка использовать подходящие имена героев, соответствующие игровым правилам. Эти имена не должны раскрывать никакую личную информацию или провоцировать домогательство.

Примечание: Для компьютеров и игровых консолей типа Xbox есть технология маскировки или скрытия голоса, позволяющая изменить настоящий голос ребенка. Имейте в виду, что взрослые также могут пользоваться этой программой и выдавать себя не за того, кто они есть на самом деле.

Берегитесь хулиганов. См. с. 17 данного издания о том, как поступать с задирами (гриферами) в Интернет-играх.

Играйте вместе. Безопаснее всего для детей играть через Интернет вместе с вами. Возможно, им этого хочется меньше всего на свете (особенно тем, кто постарше), но это очень хороший способ научиться общению в Сети.

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 вашего ребенка 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 ДЕТИ СТОЛКНУЛИСЬ С ГРИФЕРАМИ? Пусть ваши дети их игнорируют. Если ребенок не будет реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

Посоветуйте детям изменить параметры игры. Добейтесь, чтобы ребенок играл в игры, правила или режимы которых можно изменить, например, невозможность убить товарищей по команде. Таким образом, тактика гриферов становится бессмысленной.

Порекомендуйте создать частную игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать только друзей.

Пусть дети играют на сайтах со строгими правилами. Там, где установлены строгие правила, администратор сможет немедленно заблокировать хулиганов.

Пусть играют в игры, где от гриферов можно легко избавиться. Предложите ребенку играть в те игры, где сообщения хулиганов можно отключить или проголосовать за их исключение из игры.

Придумайте еще что-нибудь. Если обидчик продолжает беспокоить вашего ребенка, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже.

Сообщайте о «дырах» в игре. Поищите вместе с ребенком уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору.

Пусть ваши дети воздерживаются отвечать огнем на огонь. Убедитесь, что ребенок не использует против обидчиков их же тактику; скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о ребенке впечатление как об обидчике.

Рекомендуйте детям избегать провокаций с именами. Ребенок избежит многих проблем, если не станет использовать псевдоним, который может спровоцировать обидчика.

Пусть дети не выдают личную информацию. Хулиганы (да и вообще кто угодно) могут использовать настоящие имена, номера телефонов, а также домашние или электронные адреса, чтобы причинить ребенку 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 детям, 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.

Расскажите детям, как работает Интернет, и объясните, что каждый может создать сайт и никто ему не задаст никаких вопросов. Научите детей использовать широкий круг источников и проверять все, что они видят в Сети.

КАК НАУЧИТЬ ДЕТЕЙ ОПРЕДЕЛЯТЬ ЛОЖНЫЕ МАТЕРИАЛЫ? Начинайте, когда дети еще маленькие. Теперь, когда даже дошкольники используют Интернет, важно научить их отличать факты от мнений как можно раньше.

Спрашивайте детей о найденной ими в Интернете информации. Например, для чего нужен этот сайт? Для развлечений? Продажи товара? Есть ли на сайте контактная информация или раздел «О нас»? Спонсируется ли сайт кем-то или это место общественной дискуссии? И подумайте: является ли Интернет наилучшим местом для поиска именно этой информации?

Убедитесь, что дети проверяют собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам. Приучите детей советоваться с вами.

Поощряйте использование детьми разных источников. Возьмите их с собой в библиотеку или приобретите для них энциклопедию на диске. Это даст детям доступ к альтернативным источникам информации. Научите детей эффективным способам поиска. Это сильно увеличит их возможности получения качественной информации. Один из способов – приучить детей пользоваться не одной поисковой машиной, а несколькими.

МАТЕРИАЛЫ НЕЖЕЛАТЕЛЬНОГО СОДЕРЖАНИЯ: КАК ИЗБЕЖАТЬ?

ЧТО ЗНАЧИТ НЕЖЕЛАТЕЛЬНОЕ СОДЕРЖАНИЕ. Как правило, большинство родителей не склонны поощрять знакомство своих детей с материалами порнографического, ненавистнического содержания, материалами суицидальной направленности, сектантскими материалами, ненормативной лексикой. Такую информацию относят к материалам нежелательного характера.

Если порнографические материалы или материалы с ненормативной лексикой можно относительно легко идентифицировать и отсечь с помощью средств фильтрации, то от нежелательных материалов других типов детей защитить гораздо сложнее.

Например, на детских сайтах могут встречаться самые разные формы выражения ненависти: от радикального расизма до грубого высмеивания. Такие сайты на первый взгляд могут казаться безобидными, но они вносят свой вклад в формирование детской онлайновой культуры, в которой грубость по отношению к другим считается допустимой.

Расисты и группы ненависти стали использовать Интернет для привлечения молодежи в свои ряды. Последние ищут восприимчивых молодых людей, а

затем вовлекают их в свое сообщество, используя для этого чаты и электронную почту.

Некоторые ненавистнические сайты создают разделы специально для детей. Эта часть сервера специально имеет располагающий вид, предлагает безобидные игровые занятия и дает ссылки на уважаемые сайты.

КАК ПОМОЧЬ СВОИМ ДЕТЯМ ИЗБЕЖАТЬ НЕНАВИСТНИЧЕСКИХ МАТЕРИАЛОВ?

Используйте средства фильтрации нежелательного материала (например, MSN Premium's Parental Controls или встроенные в Internet Explorer®) . Но фильтры могут только помочь в блокировании некоторых нежелательных материалов, они не могут полностью решить проблему. Выражения ненависти, встречающиеся в Интернете, часто принимают мягкие формы и не всегда распознаются фильтрами. Поэтому важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались к вам за помощью.

Контролируйте использование Интернета и наблюдайте за детьми. Как правило, дети, не достигшие десятилетнего возраста, еще не имеют навыков критического мышления, необходимого для самостоятельного посещения Сети.

Расскажите детям о существующих в Интернете способах выражения ненависти. Научите их распознавать материалы с ненавистническим содержанием и символикой, например, изображение свастики, оскорбительные отзывы о расовой принадлежности, карикатурные описания разных этнических и расовых групп. Вашим детям будет легче избежать материалов ненавистнического содержания, если они будут знать об истории расизма, шовинизма и стратегиях распространителей ненависти.

Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред расовых концепций.

Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с вами.

ВОЗРАСТНЫЕ ОСОБЕННОСТИ ДЕТЕЙ И ИНТЕРНЕТ

Гимн продвинутых родителей.

Ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при работе в Интернете. Родителям важно знать, какие особенности имеют дети в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете.

Кроме того, нужно учитывать, что наши дети начинают осваивать Интернет в разном возрасте: кто-то в возрасте 14 – 17 лет, находясь в старших классах, кто-то в 10 – 13 лет, а кто-то еще в дошкольном возрасте получает первый опыт взаимодействия с Интернетом.

ДЕТИ В ВОЗРАСТЕ ДО 7 ЛЕТ И ИНТЕРНЕТ

Последние проведенные исследования показали, что дошкольники являются наиболее быстрорастущим сегментом пользователей Сети. Хотя дети в этом возрасте уделяют Интернету немного внимания, онлайновые изображения и звуки могут стимулировать воображение и развивать их фантазию. Они могут получить доступ к развивающим играм и материалам, размещенным в Интернете, что будет стимулировать их интеллектуальное развитие.

ЧТО ДЕТИ ДО 7 ЛЕТ ОБЫЧНО ДЕЛАЮТ В ИНТЕРНЕТЕ?

На этом этапе деятельность детей в Интернете должна проходить при активном участии родителей. Взрослые могут посадить ребенка к себе на колени во время просмотра семейных фотографий, использования веб-камеры для общения с родственниками или посещения детских сайтов.

У детей этого возраста обычно открытая натура и положительный взгляд на мир. Они гордятся приобретенными начальными умениями читать и считать и любят делиться идеями. Они не только хотят вести себя хорошо, но и доверяют авторитетам и редко в них сомневаются.

Дети в этом возрасте, как правило, легко осваивают Интернет, обучаются основным навыкам при работе с ним. И хотя дошкольники могут быть очень способными в играх, выполнении команд на компьютере и работе с мышью, они сильно зависят от взрослых при поиске сайтов, интерпретации информации из Интернета или отправке электронной почты.

Взрослые играют ключевую роль в обучении детей в этом возрасте безопасному использованию Интернета. Поэтому используйте это время для того, чтобы сформировать у своего ребенка культуру безопасной работы в Интернете.

СОВЕТЫ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДОШКОЛЬНИКОВ ПРИ ПОЛЬЗОВАНИИ ИНТЕРНЕТОМ.

Дети этого возраста должны выходить в Интернет только под присмотром родителей (или других взрослых, например старших братьев и сестер). Ограничивайте время пребывания детей в Интернете, как и время работы за компьютером, в соответствии с рекомендациями врачей и психологов для соответствующего возраста вашего ребенка.

Добавьте сайты, которые вы часто посещаете с вашим ребенком, в список «Избранное» (Favorites), чтобы создать для детей их личную Интернет-среду. У детей в этом возрасте развивается чувство своей территории, поэтому пусть на вашем домашнем компьютере будет их собственный «Интернет-уголок».

Расскажите детям о конфиденциальности. Научите их никогда не выдавать в Интернете информацию о себе и своей семье. Если на каком-то сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним, не раскрывающий никакой личной информации.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

ДЕТИ В ВОЗРАСТЕ ОТ 7 ДО 10 ЛЕТ И ИНТЕРНЕТ (МЛАДШИЙ ШКОЛЬНЫЙ ВОЗРАСТ)

Семи-десятилетние дети обладают сильным чувством семьи. Они только начинают развивать чувство своей моральной и половой индивидуальности и обычно интересуются жизнью старших детей. Они доверчивы и не сомневаются в авторитетах. Как правило, дети, не достигшие десятилетнего возраста, еще не имеют навыков критического мышления, необходимого для адекватного осмысления материалов, встречающихся в Интернете.

ЧТО ДЕТИ В ВОЗРАСТЕ 7 – 10 ЛЕТ ОБЫЧНО ДЕЛАЮТ В ИНТЕРНЕТЕ?

Дети этого возраста начинают активно самостоятельно осваивать виртуальное пространство, любят путешествовать по Интернету, играть в сетевые игры, они начинают общаться в детских чатах, стремятся использовать электронную почту для переписки с друзьями. Однако нужно иметь в виду, что они могут заходить на сайты и чаты, посещать которые родители им не разрешали.

СОВЕТЫ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ 7 – 10 ЛЕТ ПРИ ПОЛЬЗОВАНИИ ИНТЕРНЕТОМ.

Старайтесь держать компьютеры с подключением к Интернету в общих комнатах, в которых можно легко осуществлять визуальный контроль над тем, что делает ваш ребенок в Интернете.

Создайте при участии детей свод домашних правил пользования Интернетом и требуйте его неукоснительного соблюдения.

Приучите детей посещать только те сайты, которые вы разрешили.

Используйте средства блокирования нежелательного материала (например, MSN Premium's Parental Controls) как дополнение, но не замену к родительскому контролю. Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

Создайте семейный электронный ящик, на который будет приходить вся ваша электронная почта, вместо того чтобы позволять детям иметь собственные адреса.

Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.

Научите детей не загружать программы, музыку или файлы без вашего разрешения.

Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением.

Не разрешайте детям этого возраста пользоваться службами мгновенного обмена сообщениями.

Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

ДЕТИ В ВОЗРАСТЕ ОТ 10 ДО 13 ЛЕТ И ИНТЕРНЕТ

10 – 13 лет – младший подростковый и средний школьный возраст – время быстрых изменений в жизни вашего ребенка. И хотя дети в этом возрасте все еще сильно зависимы от своих родителей, они уже стремятся получить некоторую свободу дейс-

твий. Ребята начинают интересоваться миром вокруг них, и отношения с друзьями становятся по-настоящему важными.

ЧТО 10 – 13-ЛЕТНИЕ ДЕТИ ДЕЛАЮТ В ИНТЕРНЕТЕ?

Дети этого возраста начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и заходят на фанатские сайты своих кумиров. Все более часто их любимым способом общения становится мгновенный обмен сообщениями.

Для детей этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Находясь в Интернете, ребенок может попытаться посетить сайты или пообщаться в чатах, разрешения на которые он не получил бы от родителей. Отчеты о деятельности в Интернете от сервиса MSN Premium или других служб могут быть особенно полезными на этом этапе. У детей не будет ощущения, что родители постоянно смотрят на экран через их плечо; однако благодаря отчетам взрослые будут по-прежнему знать, какие сайты посещают их дети.

СОВЕТЫ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ.

Убедитесь в том, что ваш ребенок знает и выполняет правила поведения для детей более раннего возраста, если он только начинает пользоваться Интернетом.

Создайте ребенку собственную учетную запись с ограниченными правами, чтобы он не мог заниматься чем-то посторонним без вашего ведома.

Создайте при участии подростков и поддерживайте соблюдение списка домашних правил при работе в Интернете. Следует указать список сайтов, запрещенных для посещения, часы нахождения в Сети и руководство по общению в Интернете (в том числе и в чатах).

Используйте средства фильтрования нежелательного материала (наподобие MSN Premium's Parental Controls) как дополнение, но не замену к родительскому контролю.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету без вашего присутствия.

Требуйте от детей никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.

Требуйте от детей не загружать из Интернета программы без вашего разрешения. Кроме того, объясните детям, что, делая файлы общими или загружая из Интернета тексты, фотографии или рисунки, они могут нарушать чьи-то авторские права.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, поскольку рассказали вам о новых угрозах. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами. Контроль лучше всего осуществлять ненавязчиво, уважая личное достоинство и право ребенка на самостоятельность.

Расскажите детям об ответственном, достойном поведении в Интернете.

Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

ДЕТИ В ВОЗРАСТЕ 14 – 17 ЛЕТ И ИНТЕРНЕТ

Подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и неохотно слушаются родителей. Более старшие ищут свое место в мире и пытаются обрести собственную независимость; в то же время они охотно приобщаются к семейным ценностям. В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта. Родителям важно продолжать следить, как используют Интернет их дети в этом возрасте.

ЧТО ПОДРОСТКИ 14 – 17 ЛЕТ ДЕЛАЮТ В ИНТЕРНЕТЕ

В этом возрасте дети уже наслышаны о том, какая информация существует в Интернете. И совершенно нормально, что они хотят все это сами увидеть, услышать, прочесть. Доступ к нежелательным материалам (например, порнографическим картинкам или инструкциям по изготовлению взрывчатки) можно легко заблокировать при помощи программных фильтров.

Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Кроме того, подростки активно используют поисковые машины. Большинство пользовалось чатами, и многие общались в приватном режиме. Мальчики в этом возрасте склонны сметать все ограничения и жаждут грубого юмора, крови, азартных игр и картинок для взрослых. Девочкам больше нравится общаться в чатах; и юные дамы более чувствительны к сексуальным домогательствам в Интернете.

Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее участие взрослых тоже необходимо. Особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и ребенком. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Родители должны также помнить о необходимости хранить свои пароли в секрете, чтобы подростки не смогли зарегистрироваться под именем старших.

СОВЕТЫ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ В ВОЗРАСТЕ 14 – 17 ЛЕТ ПРИ РАБОТЕ В ИНТЕРНЕТЕ.

Измените в соответствии с интересами и запросами подростка список домашних правил использования подростком Интернета, требуйте его соблюдения.

Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.

Интересуйтесь, какими чатами и досками объявлений пользуются подростки и с кем они общаются. Поощряйте использование модерируемых чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

Возьмите за правило знакомиться с сайтами, которые посещают ваши дети. Убедитесь, что они не посещают сайты с оскорбительным содержанием, не публикуют личную информацию или свои фотографии.

Настаивайте, чтобы подростки никогда не соглашались на личные встречи с друзьями из Интернета без вашего участия. Напоминайте, какие опасности это может за собой повлечь.

Требуйте от подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

Требуйте от подростков не загружать программы, музыку или файлы без консультаций с вами. Объясните, что иначе подростки могут нарушить авторские права и тем самым закон.

Настаивайте на том, чтобы подростки ставили вас в известность, если что-либо или кто-либо в Сети тревожит или угрожает им. Объясните, что угрозы им – это также и угроза всей семье. Оставайтесь в случае чего спокойными и напомните детям, что они в безопасности, если рассказали вам. Помогайте им решить возникшие проблемы.

Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Постоянно напоминайте, что ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям. Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете.

Обсудите с подростками азартные сетевые игры и связанный с ними риск. Напомните, что детям нельзя в них играть.

Поддерживайте уровень безопасности вашего компьютера на должном уровне. Если ваш ребенок лучше вас разбирается в программном обеспечении, то почему бы не поручить ему заботу о безопасности ваших семейных компьютеров?

Награждается «За защиту семьи от Интернет-напасти».

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, которых также называют Netizens, 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. Если вашим детям не удастся освоить правила существования в Интернете, это будут не просто упущенные возможности: если они скажут неправильные слова в неправильный момент, то могут вызвать агрессию или спровоцировать возникновение других проблем.

Поэтому до того, как новый юный пользователь возьмет в руки мышь, мы предлагаем ему изучить следующие рекомендации:

- 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 полным 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.

ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ ПРИ ПОМОЩИ ТЕХНИЧЕСКИХ СРЕДСТВ

Интернет предоставляет детям доступ к играм и фильмам, а также бесконечные возможности для получения новых знаний и развития исследовательских навыков. Но эти преимущества сопровождаются и рядом сложных проблем. Однако можно предпринять некоторые шаги, которые помогут защитить детей от опасностей в Интернете. Не следует забывать при этом, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются ваши дети за компьютером.

ПОВЫСЬТЕ УРОВЕНЬ ОБЩЕЙ БЕЗОПАСНОСТИ ВАШЕГО КОМПЬЮТЕРА. Если на вашем компьютере установлена операционная система Microsoft® Windows® XP Service Pack 2, то можно использовать Windows Security Center. Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности.

Security Center показывает состояние трех важных компонентов безопасности: брандмауэра Интернета, антивирусных программ и службы автоматического обновления. Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера.
Security Center работает в фоновом режиме, постоянно проверяя состояние трех наиболее важных компонентов.

Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

- *нажмите* кнопку *Пуск/Start*, в открывшемся меню выберите *Панель управления/Control Panel*;
- в панели управления откройте *Центр обеспечения безопасности/Security Center*;
- убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в *Центре обеспечения безопасности*.
Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного програмного обеспечения.

УСТАНОВИТЕ НА ВАШЕМ КОМПЬЮТЕРЕ АНТИШПИОНСКИЕ НАСТРОЙКИ ИЛИ ДОПОЛНИТЕЛЬНОЕ АНТИШПИОНСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Шпионскими называются программы, выполняющие определенные действия (например, сбор личной информации или изменение настроек) без согласия и контроля пользователя. Они могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках. Такие программы трудно удалить.

Антишпионское программное обеспечение поможет избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное для вас время.

Для того чтобы предотвратить появление шпионского программного обеспечения на вашем компьютере, необходимо убедиться в том, что включены основные средства *Центра обеспечения безопасности* вашей операционной системы.

Рекомендуется также для повседневной работы использовать учетную запись с ограниченными правами.

Для удаления шпионского программного обеспечения, попавшего на ваш компьютер, следует воспользоваться специальным антишпионским программным обеспечением, в частности, следующими программами:
Windows Defender;
Malicious Software Removal Tool.
Эти бесплатные программы вы можете загрузить с сайта http://www.microsoft.com/downloads

Для этого в строке *Search* в выпадающем списке выберите *All Downloads*, в строке справа введите название одного из указанных выше продуктов и нажмите кнопку Go.

БЛОКИРУЙТЕ ДОСТУП К НЕПОДХОДЯЩИМ МАТЕРИАЛАМ. Один из наилучших способов защиты от нежелательной информации – это блокирование доступа еще до того, как она может быть получена. Microsoft предлагает несколько таких способов.

Для того чтобы блокировать доступ к нежелательной информации в *Internet Explorer® и MSN Explorer*, нужно выполнить следующее:

- нажмите кнопку *Пуск/Start*, в открывшемся меню выберите *Панель управления/ Control Panel*;
- в панели управления откройте *Свойства обозревателя/Internet Options*;
- в появившемся окне перейдите на вкладку *Содержание/Content*;
- в разделе *Ограничение доступа/Content Advisor нажмите кнопку Включить/Enable*;
- в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;
- в окне *Ограничение доступа/Content Advisor* вы можете блокировать доступ к нежелательной информации.

ПОВЫСЬТЕ УРОВЕНЬ БЕЗОПАСНОСТИ ПРИ РАБОТЕ РЕБЕНКА С ЭЛЕКТРОННОЙ ПОЧТОЙ OUTLOOK® EXPRESS. Для повышения уровня безопасности при работе ребенка с электронной почтой в меню программы Outlook® Express в разделе *Сервис/Tools* выберите команду *Параметры/Options*.
Перейдите на вкладку *Безопасность/Security*.

При помощи переключателя *выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use* вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель *Не разрешать сохранение или открытие вложений, которые могут содержать вирусы/Do not allow attachments to be saved or opened that could potentially be a virus*.

Если же вирус все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку *Предупреждать, если приложения пытаются отправить почту от моего имени/Warn me when other applications try to send mail as me*.

Для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо, кроме указанного получателя, есть возможность Шифровать содержимое и вложения всех исходящих сообщений/Encrypt content and attachments for all outgoing messages и Подписывать все отправляемые сообщения/Digitally sign all outgoing messages.

ЗАБЛОКИРУЙТЕ ПОСТУПЛЕНИЕ СПАМА. Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, hotmail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook).

Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail.

Перейдя по ссылке *Junk E-mail Filter*, вы можете изменить настройки фильтра нежелательной почты.

При помощи ссылки *Block Senders*, находящейся на вкладке *Mail*, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик.

В случае, если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.

Для настройки этого фильтра в меню Microsoft Outlook выберите *Сервис/Tools*, в открывшемся меню выберите команду *Параметры/Options*. В открывшемся диалоговом окне перейдите на вкладку *Настройки/Preferences* и нажмите кнопку *Нежелательная почта/Junk E-mail*.

В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты.

Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

СОЗДАЙТЕ ОТДЕЛЬНЫЕ УЧЕТНЫЕ ЗАПИСИ ДЛЯ РАЗНЫХ ПОЛЬЗОВАТЕЛЕЙ. Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой *«Мои документы»*. Родитель может создать себе учетную запись администратора, дающую полный контроль над компьютером, а детям – ограниченные учетные записи. Пользователи с ограниченными учетными записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение, включая большинство игр, медиаплееров и программ поддержки чатов.

Для того чтобы создать отдельную учетную запись для ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажмите кнопку *Пуск/Start*, в открывшемся меню выберите *Панель управления/Control Panel*;
- в панели управления откройте *Учетные записи пользователей/User Accounts*;
- в открывшемся окне выберите *Создание учетной записи/Create a new account*, введите ее имя;
- на этапе выбора типа учетной записи установите переключатель в положение *Ограниченная запись/Limited*;
- после нажатия кнопки *Создать учетную запись/Create Account* процесс создания учетной записи с ограниченными правами будет завершен и ваш ребенок сможет выбрать ее при следующем входе в систему.

ПОВЫСЬТЕ УРОВЕНЬ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБЩЕНИИ ВАШЕГО РЕБЕНКА В ИНТЕРНЕТЕ С ПОМОЩЬЮ INTERNET EXPLORER.

Сохранение конфиденциальности личной информации вашего ребенка при его работе в Интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении вашего ребенка в Интернете, выполните следующие действия:

- нажмите кнопку *Пуск/Start*, в открывшемся меню выберите *Панель управления/Control Panel*;
- в панели управления откройте *Свойства обоз-*

ревателя/Internet Options;
- в появившемся окне перейдите на вкладку *Конфиденциальность/Privacy*;
- при помощи ползунка выберите необходимый уровень конфиденциальности.

КОНТРОЛИРУЙТЕ ТО, ЧТО ДЕЛАЮТ В ИНТЕРНЕТЕ ВАШИ ДЕТИ.

Невозможно всегда находиться рядом с детьми, когда они путешествуют по Интернету. Однако есть возможность проверить, на каких сайтах они проводят время.

Когда вы перемещаетесь по Интернету, браузер (например, Internet Explorer или Netscape Navigator) собирает всю информацию о посещенных местах и сохраняет ее на компьютере. Современные браузеры обычно ведут журнал последних посещенных сайтов.

Проверить, чем ребенок занимался в Интернете, можно следующим образом:
- запустите *Internet Explorer®*;
- в его меню выберите раздел *Вид/View*, в нем – раздел *Панели обозревателя/Explorer Bar*. В этом разделе выберите команду *Журнал/History*.

В окне Internet Explorer'а появится журнал, в котором вы сможете увидеть список всех посещенных ребенком страниц.

Совет: Помните о том, что дети без труда могут отключать или изменять указанные функции контроля. В вопросах технологии они, скорее всего, всегда будут на шаг впереди вас.

Мы должны понимать, что открытый и доброжелательный диалог с детьми гораздо конструктивнее, чем тайная слежка за ними. Хотя и негласный, но ненавязчивый контроль часто делает свое доброе дело по своевременному обнаружению признаков нарушения безопасности вашего ребенка.

БЛОКИРУЙТЕ ВОЗМОЖНОСТЬ НЕИЗВЕСТНЫХ КОНТАКТОВ В ПРОГРАММАХ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ.

Чаты и система обмена мгновенными сообщениями предоставляют детям замечательные возможности для обсуждения интересующих их тем и установления дружеских контактов. Однако анонимность Интернета может представлять серьезную опасность; ваш ребенок рискует стать жертвой обманщиков и преступников.

Для предотвращения попыток контакта с вашими детьми со стороны незнакомых людей во время обмена мгновенными сообщениями настройте программу так, чтобы были доступны только проверенные контакты.

Для того чтобы блокировать возможность неизвестных контактов в MSN Messenger®, нужно проделать следующее:
- в главном окне программы в меню *Сервис/Tools выбрать пункт Параметры/Options;*
- на панели слева перейти на вкладку *Конфиденциальность/Privacy*;
- установить флажок *«Видеть мое состояние и отправлять мне сообщения могут только люди, внесенные в белый список»/Only people on my Allow list can see my status and send me messages*.

СОЗДАВАЙТЕ НАДЕЖНЫЕ ПАРОЛИ.

Пароли – это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени. Вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/privacy/password.mspx

БЕЗОПАСНЫЙ ИНТЕРНЕТ ВНЕ ДОМА

Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ-шпионов и других возможных атак.

В настоящее время все большее распространение получают беспроводные сети. Это дает возможность путешествовать по Интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома или собираетесь активно использовать беспроводными сетями общего назначения, прочитайте соответствующие разделы брошюры и обратите особое внимание на информацию по безопасности.

Принимайте необходимые меры предосторожности, пользуясь беспроводной связью!

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ:

Повысьте меры компьютерной защиты до максимально приемлемого уровня на компьютере, который ваш ребенок предполагает использовать вне дома. Особое внимание обратите политике конфиденциальности. Для этого можно воспользоваться мерами, которые описаны в соответствующем разделе данной брошюры.

Установите надежный пароль. Пароль защищает компьютер и блокирует возможность его использования без разрешения его владельца. Напомните вашему ребенку, что ему нельзя сообщать этот пароль своим друзьям, а если он стал им известен, то пароль должен быть изменен.

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ.

Требуйте от детей всегда блокировать доступ к компьютерной системе на то время, когда он с ней не работает. Чтобы «запереть» компьютер с операционной системой Windows, удерживайте нажатыми клавиши «Windows + L». Когда понадобится возобновить работу, необходимо следовать инструкциям на экране.

Просите детей всегда делать резервные копии результатов работы, когда они возвращаются со своим компьютером домой, и тем более, если они работают на общественном компьютере (а также игр и других развлекательных программ). Образ студента, оставшегося без своей курсовой работы из-за того, что он забыл сделать резервную копию, стал уже почти штампом. Тем не менее многие до сих пор не находят времени на копирование. Пользователи операционной системы Windows XP могут воспользоваться программой «Архивация данных», которая выполнит за вас эту работу.

Пусть ваши дети всегда тщательно «заметают свои следы» при работе на общественных компьютерах. Никогда не сохраняют свои пароли, удаляют следы своей работы в Интернете: ссылки на посещаемые ресурсы, просмотренную информацию и пр. По этой информации о вашем ребенке можно узнать много личных данных, чем могут воспользоваться злоумышленники

ПАМЯТКА РОДИТЕЛЯМ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ В ИНТЕРНЕТЕ

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но, как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, им следует уяснить некоторые моменты.

Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций. В заключение беседы установите определенные ограничения на использование Интернета и обсудите их с детьми. Сообща вы сможете создать для ребят уют и безопасность в Интернете.

Если вы не уверены, с чего начать, вот несколько мыслей о том, как сделать посещение Интернета для детей полностью безопасным.

- Установите правила работы в Интернете для детей и будьте непреклонны.

- Научите детей предпринимать следующие меры предосторожности по сохранению конфиденциальности личной информации:
  - Представляясь, следует использовать только имя или псевдоним.
  - Никогда нельзя сообщать номер телефона или адрес проживания или учебы.
  - Никогда не посылать свои фотографии.
  - Никогда не разрешайте детям встречаться со знакомыми по Интернету без контроля со стороны взрослых.

- Объясните детям, что разница между правильным и неправильным одинакова как в Интернете, так и в реальной жизни.

- Научите детей доверять интуиции. Если их в Интернете что-либо беспокоит, им следует сообщить об этом вам.

- Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

- Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

- Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.

- Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

- Скажите детям, что не все, что они читают или видят в Интернете, – правда. Приучите их спрашивать вас, если они не уверены.

- Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

- Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Регулярно посещайте Интернет-дневник своего ребенка, если он его ведет, для проверки.

- ***Будьте внимательны к вашим детям!***

ПАМЯТКА ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, ребенок должен предпринимать следующие меры предосторожности при работе 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.

ВНУТРИСЕМЕЙНЫЕ ПРАВИЛА ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА

ВНУТРИСЕМЕЙНЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ. Перед тем как дети начнут осваивать Интернет, неплохо убедиться, что все понимают, что следует и чего не следует делать в Сети. Можно написать кодекс поведения, которому все согласны будут следовать. Кроме того, можно составить правила пользования для каждого ребенка в семье – в зависимости от их возраста. Каждый подписывает свое соглашение, чтобы показать, что понимает правила и соглашается следовать им в Интернете.
Ниже приведен образец. Его можно скопировать, пересмотреть для нужд именно вашей семьи и напечатать для личного использования. Семейные правила пользования Сетью можно прикрепить около компьютера. Для напоминания.

СОГЛАШЕНИЕ О КОДЕКСЕ ПОВЕДЕНИЯ В ИНТЕРНЕТЕ.

Я обязуюсь: Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в Интернете (___ минут или ___ часов).
Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.
Всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в Интернете.
Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей.
Никогда не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет или обычной почтой.
Никогда никому, кроме своих родителей, не выдавать пароли Интернета (даже лучшим друзьям).
Вести себя в Интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречить закону.
Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без должного разрешения.
Никогда не делать без разрешения родителей в Интернете ничего, требующего оплаты.
Сообщить моим родителям мое регистрационное имя в Интернете и имена в чате, перечисленные ниже:

_____

_____

_____

Имя (ребенок) _____ Дата _____

Родитель или опекун _____ Дата _____

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ПО БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ПО БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВАС, ВАШЕЙ СЕМЬИ, ВАШИХ ДЕТЕЙ МОЖЕТ БЫТЬ ПОЛУЧЕНА:
на веб-сайте «Безопасность детей в Интернете» по адресу http://www.microsoft.com/rus/childsafety, а также на веб-сайте «Безопасность дома» по адресу http://www.microsoft.com/rus/athome/security/.

Получить консультацию о том, как с помощью программного обеспечения Microsoft повысить безопасность детей и всей семьи при пользовании Интернетом, можно по телефону **8-800-200-800-1** (бесплатный номер для территории России).

САЙТ-ДУБЛЁР –

это сайт, который внешне на 99% повторяет настоящий сайт благотворительной организации или активиста, собирающего средства на доброе дело.

Отличия сайта-дублёра от оригинального минимальны: одна или две буквы в доменном имени сайта (имени, которое указано в адресной строке браузера) и другой номер счёта, куда перечисляют средства.

Изготовить такой сайт-дублёр очень просто: он может появиться в самое кратчайшее время после публикации настоящего – оригинального сайта. Поэтому мошенники всё чаше прибегают к этой схеме обмана.

На сегодняшний день Интернет является очень эффективным инструментом для использования его в благотворительных целях.

Развитие электронных кошельков и расширение возможностей по перечислению денежных средств, упрощает участие в благотворительной деятельности для каждого пользователя Интернета.

Одновременно злоумышленники приспособились использовать сбор средств на благотворительных сайтах в своих мошеннических схемах.

Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

ПОЛЬЗОВАТЕЛЯМ ИНТЕРНЕТА

Будьте осторожны!

МОШЕННИЧЕСКОЕ ДУБЛИРОВАНИЕ БЛАГОТВОРИТЕЛЬНЫХ САЙТОВ

КАК ОРГАНИЗОВАНО МОШЕННИЧЕСТВО:

Вы узнаёте о трагической ситуации, в которой требуется помощь.

Достаточно зайти на некий сайт и перевести деньги на указанные реквизиты.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Злоумышленники отслеживают социальную ситуацию и активно используют темы, которые являются заведомо выигрышными с точки зрения возможных откликов граждан.

Тематика благотворительных сайтов может быть самой разной:

- помощь больным детям – сбор средств на операцию;
- помощь жертвам терактов;
- помощь пострадавшим во время стихийных бедствий – землетрясений, цунами, сходов лавин и оползней;
- восстановление храмов;
- помощь приютам, заботящимся о брошенных животных.

Для осуществления своих противоправных замыслов мошенники создают сайты-дублеры, которые являются точной копией официальных сайтов с той лишь разницей, что на них указаны другие расчетные счета, по которым гражданам предлагается направлять денежные средства.

Учащаются случаи создания полностью выдуманных историй, созданных на основе правдивых.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Не поленитесь перепроверить информацию в Интернете.

Ей можно будет доверять только в том случае, если на нескольких сайтах будет указан один и тот же расчетный счет и номер телефона.

Если вы планируете постоянно участвовать в благотворительной деятельности, используйте сайт, принадлежащий благотворительной организации или группе активистов. Помогайте тем, кто даёт информацию «из первых рук» и известен своей надёжной репутацией.

Посмотрите, указан ли на сайте номер телефона для связи.

Если да, то следует позвонить по нему и уточнить все детали. Например, если необходимы деньги на операцию ребенку, спросите о диагнозе, узнайте имя лечащего врача, номер больницы, в которой наблюдается ребенок и т.д.

Задавайте как можно больше уточняющих вопросов: если на другом конце провода вам не смогут ответить на поставленные вопросы, либо ответы будут уклончивыми и неуверенными, или ответы вообще не будут совпадать с тем, что указано на сайте, то, скорее всего, вы общаетесь с мошенниками.

Зачастую мошенники вообще не указывают никаких телефонных номеров, чтобы их было сложнее вычислить.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

Телефонный номер-«грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества множатся с каждым годом.

В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

Мошенники разбираются в психологии и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении.

Управление «К» МВД РФ напоминает, что чаще всего в сети телефонных мошенников попадаются пожилые люди или доверчивые подростки. При этом **каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.**

Министерство внутренних дел Российской Федерации

Управление «К»
МВД РФ предупреждает:

ТЕЛЕФОННЫЕ МОШЕННИКИ

Телефонные мошенники используют мобильные телефоны для обмана и изъятия денежных средств граждан.

- **Основные схемы**
- **Тактика мошенников**
- **Как реагировать**

ТАКТИКА ТЕЛЕФОННЫХ МОШЕННИКОВ

Для общения с потенциальной жертвой мошенники используют либо SMS, либо телефонный звонок.

SMS – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – в надежде на доверчивого получателя.

Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом.

Цель мошенников – заставить Вас передать свои денежные средства «добровольно». Для этого используются различные схемы мошенничества.

Изъятие денежных средств может проходить разными способами. Вас попытаются заставить:

1. **передать деньги из рук в руки или оставить в условленном месте;**
2. **приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;**
3. **перевести деньги на свой счёт и ввести специальный код;**
4. **перевести деньги на указанный счёт;**
5. **позвонить на специальный телефонный номер, который окажется платным, и с Вашего счёта будут списаны средства;**

КАК ПРАВИЛЬНО РЕАГИРОВАТЬ НА ПОПЫТКУ ВОВЛЕЧЕНИЯ В МОШЕННИЧЕСТВО

Мошенники очень хорошо знают психологию людей. Они используют следующие мотивы:

а. Беспокойство за близких и знакомых.

б. Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.

в. Желание выиграть крупный приз.

г. Любопытство – желание получить доступ к SMS и звонкам других людей.

Чтобы противодействовать обману, достаточно знать о существовании мошеннических схем и в каждом случае, когда от Вас будут требовать перевести сумму денег, задавать уточняющие вопросы.

Телефонные мошенники рассчитывают на доверчивых, податливых людей, которые соглашаются с тем, что им говорят, и выполняют чужие указания. Спокойные, уверенные вопросы отпугнут злоумышленников.

ЧТО НАДО ЗНАТЬ, ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Если Вы сомневаетесь, что звонивший действительно ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

Помните, что никто не имеет права требовать коды с карт экспресс-оплаты!

Оформление выигрыша никогда не происходит только по телефону или Интернету. Если Вас не просят приехать в офис организатора акции с документами – это мошенничество.

Не ленитесь перезванивать своему мобильному оператору для уточнения правил акции, новых тарифов и условий разблокирования якобы заблокированного номера.

Для возврата средств при якобы ошибочном переводе существует чек. Не возвращайте деньги – их вернет оператор.

Услуга «узнайте SMS и телефонные переговоры» может оказываться исключительно операторами сотовой связи и в установленном законом порядке.

ЕСТЬ НЕСКОЛЬКО ПРОСТЫХ ПРАВИЛ:

- отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
- не реагировать на SMS без подписи с незнакомых номеров;
- внимательно относиться к звонкам с незнакомых номеров.

ТАКТИКА БОРЬБЫ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ

Вредоносные программы представляют собой файлы, которые срабатывают при активировании на компьютере. Тактика борьбы с ними достаточно проста:

а) не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

б) если они к Вам все-таки попали, ни в коем случае не запускать их;

в) если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.

Самый действенный способ оградить от вредоносных программ свой почтовый ящик – запретить прием сообщений, содержащих исполняемые вложения.

РАСШИРЕНИЕ ФАЙЛА – ЭТО ВАЖНО!

Особую опасность могут представлять файлы со следующими расширениями:

- ***ade, *adp, *bas, *bat; *chm, *cmd, *com, *cpl; *crt, *eml, *exe, *hlp; *hta, *inf, *ins, *isp; *jse, *lnk, *mdb, *mde; *msc, *msi, *msp, *mst; *pcd, *pif, *reg, *scr; *sct, *shs, *url, *vbs; *vbe, *wsf, *wsh, *wsc.**

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети.

Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы.

ВРЕДОНОСНЫЕ ПРОГРАММЫ

способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами.

Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

Управление «К» МВД РФ напоминает: для защиты пользователей от вредоносных программ разработано множество действенных контрмер. Надо лишь знать их и своевременно использовать.

Министерство внутренних дел Российской Федерации

Управление «К» МВД РФ предупреждает:

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ

- Правила поведения в Интернете
- Безопасное использование электронной почты
- Защита от вредоносных программ

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ

1. АНТИВИРУСНЫЕ ПРОГРАММЫ – ВАШИ ПЕРВЫЕ ЗАЩИТНИКИ

Установите современное лицензионное антивирусное программное обеспечение.

Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. ОБНОВЛЕНИЯ – ЭТО ПОЛЕЗНО И БЕЗОПАСНО

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки.

Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления.

Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

3. НАСТРОЙТЕ СВОЙ КОМПЬЮТЕР ПРОТИВ ВРЕДОНОСНЫХ ПРОГРАММ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети.

Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

4. ПРОВЕРЯЙТЕ НОВЫЕ ФАЙЛЫ

Будьте очень осторожны при получении сообщений с файлами-вложениями.

Обращайте внимание на расширение файла.

Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.

Подозрительные сообщения лучше немедленно удалять.

Чтобы удалить сообщение в почтовой программе полностью:

- удалите сообщение из папки «Входящие»;
- удалите сообщение из папки «Удаленные»;
- выполните над папками операцию «Сжать» (Файл/Папка/Сжать все папки).

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять.

Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

5. БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ

По возможности не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.

При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

6. РЕЗЕРВНОЕ КОПИРОВАНИЕ – ГАРАНТИЯ БЕЗОПАСНОСТИ

Регулярно выполняйте резервное копирование важной информации.

Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.