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 программного 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).