БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ – очень важная проблема нынешнего времени. И касается она всех, от детей до пенсионеров. Она становится все актуальнее в связи с массовым приходом в интернет пользователей, почти, а то и совсем, не подготовленных к угрозам, их поджидающим.

Поэтому данные рекомендации будут посвящены такому вопросу, как безопасность детей в сети Интернет.

ДЕТИ И ИНТЕРНЕТ

В связи с развитием современных технологий все большее количество детей получает возможность выхода в Интернет. И если раньше они в основном играли в игры, даже не выходя в сеть, то теперь все совсем по-другому, да вы и сами все знаете. Поэтому появилась новая задача – обеспечить безопасность детей в этой глобальной сетке.

Это достаточно сложно, так как Всемирная паутина изначально развивается полностью бесконтрольно. В ней есть очень много информации, доступа к которой у детей быть не должно. Ко всему прочему, их нужно научить, как не "наловить" вирусов и троянов.

БУДЬТЕ БДИТЕЛЬНЫ

Кто же им поможет с этим, как не взрослые. К тому же очень важна и информационная безопасность в сети интернет, так как дети – совсем неискушенные пользователи. Они легко могут попасться на удочку опытного мошенника или злоумышленника, или еще хуже, попасть под влияние экстремистской или иной деструктивной организации.

КАК НАУЧИТЬ ДЕТЕЙ ПРАВИЛЬНО ПОЛЬЗОВАТЬСЯ ИНТЕРНЕТОМ.

Самый первый совет заключается в том, что первые сеансы в сети ребенок должен проводить с кем-нибудь из взрослых. Желательно пользоваться такими программами, как "Родительский контроль", чтобы контролировать все действия детей в интернете.

ЭТО МОЖЕТ БЫТЬ ОПАСНО.

Нужно ограничивать самостоятельное использование почты и чатов, ведь это может быть опасно. Так как там, например, преступники и мошенники могут искать себе жертв. Дадим несколько рекомендаций относительно того, как можно постараться обеспечить максимально безопасность детей в сети интернет.

Основные угрозы личной безопасности в Интернете

Фишинг
Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные сведения

Мистификация
Сообщения электронной почты, отправленные, чтобы обманом вынудить пользователя отдать деньги

Кража идентификационных сведений
Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту

Нежелательная почта
Нежелательные сообщения электронной почты, мгновенные сообщения и другие виды коммуникации

Основные угрозы безопасности компьютера

Вирусы и программы-черви
Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных

Программы-трояны
Вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений

Программы-шпионы
Программы, отслеживающие ваши действия в Интернете или отображающие навязчивую рекламу

Защита. Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах.
Безопасность. Наше поведение должно защищать от опасностей Интернета.

Основные угрозы безопасности детей в Интернете

Киберхулиганы
И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей

Злоупотребление общим доступом к файлам
Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ

Неприличный контент
Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить

Хищники
Эти люди используют Интернет для того, чтобы заманить детей на личную встречу

Вторжение в частную жизнь
Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или свой семье

Советы для родителей:

1.Установите на компьютер антивирусную программу. Они бывают не только платные, но и абсолютно бесплатные, однако защищающие нисколько не хуже.

2. Следите за тем, что выкладывает ваш ребенок в сеть (фото, видео, сообщения, геопозицию). Эти материалы несут информацию нежелательную для просмотра посторонними людьми.

3. Обращайте внимание на сообщения, которые приходят вашим детям в сети, не угрожают ли они их безопасности.

4. Старайтесь ограничить бесполезное использование Интернета детьми. Как правило онлайн игры и социальные сети не несут ничего полезного. Узнайте, почему ребенок посещает те или иные сайты, и обсудите с ним альтернативные варианты проведения досуга.

5. Если с вашей карты произошло списание за покупку в AppStore, Google Play или другом онлайн магазине, а вы ее не совершали, проверьте, к какой кредитной карте привязаны мобильные устройства и аккаунты вашего ребенка.

6. Если вы не всегда можете контролировать использование Интернета вашим ребенком и переживаете, что он может столкнуться с вредной информацией, установите родительский контроль или подключите такую услугу у мобильного оператора или провайдера.

7. Убедитесь, что контент-фильтр установлен в учебном учреждении, которое посещают ваши дети. Спросите родителей друзей ваших детей, используют ли они систему родительского контроля у себя дома.

*Повесьте эту памятку рядом с компьютером вашего ребенка.

Все еще переживаете за работу ваших детей и других членов семьи в сети Интернет? Узнайте как защитить все устройства подключенные к вашей домашней сети.

Зайдите на сайт www.skydns.ru и прочитайте о возможностях бесплатной системы родительского контроля.

Вы сможете навсегда забыть об угрозах, подстерегающих членов вашей семьи в Интернете. Теперь это наша забота.

SkyDNS

Мы делаем Интернет безопаснее...

www.skydns.ru

Правила безопасности в Интернете для детей и родителей

Интернет - это не просто сеть компьютеров, это сеть людей — огромная вселенная идей, творчества и информации, которая объединяет всех нас. И чтобы ваше нахождение в этой вселенной было безопасным, прочтите и используйте эти простые правила для детей и родителей.

ТВОЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

В Европе свыше 13 миллионов детей, как ты, регулярно пользуются Интернетом. Если ты ищешь информацию по своему домашнему заданию или только хочешь повеселиться, то Интернет – замечательное место, но ты должен знать об опасностях и следовать советам:

НЕ НАЖИМАЙ НЕИЗВЕСТНЫЕ ССЫЛКИ

Когда ты общаешься в чатах и интернет-пейджерах или получаешь письмо, никогда не нажимай непосредственно на ссылку. **ЕСЛИ ОНА ПРИШЛА ОТ НЕЗНАКОМОГО ЧЕЛОВЕКА, ЛУЧШЕ НЕ ОБРАЩАТЬ НА НЕЕ ВНИМАНИЯ.**

НЕ СКАЧИВАЙ ФАЙЛЫ ИЗ НЕИЗВЕСТНЫХ ИСТОЧНИКОВ

Без сомнения, ты часто получаешь сообщения, предлагающие тебе скачать фото, песню или видео. **ИНОГДА ТАКИЕ ФАЙЛЫ МОГУТ ОТПРАВЛЯТЬСЯ НЕ ЧЕЛОВЕКОМ ИЗ ТВОИХ КОНТАКТОВ, А ВИРУСОМ, КОТОРЫЙ ЗАРАЗИЛ ЕГО КОМПЬЮТЕР И ПЫТАЕТСЯ РАСПРОСТРАНИТЬСЯ СРЕДИ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ.**

Именно по этой причине ты должен всегда спрашивать своего знакомого, действительно ли он отправил тебе сообщение или файл. Если он этого не делал, сообщи ему, что его компьютер заражен. Пусть он сообщит своим знакомым, которые получили от него подобное сообщение или файл, чтобы они не открывали их и

НЕ ОТКРЫВАЙ ПОДОЗРИТЕЛЬНЫЕ ФАЙЛЫ

Если твое решение безопасности говорит тебе, что файл содержит или может содержать угрозу, не открывай файл. **ПРОСТО УДАЛИ ЕГО.**

НЕ ОБЩАЙСЯ С НЕЗНАКОМЦАМИ

В чатах или системах обмена мгновенными сообщениями **ТЫ НИКОГДА НЕ МОЖЕШЬ БЫТЬ УВЕРЕН В ТОМ, КТО С ТОБОЙ ОБЩАЕТСЯ.** Никогда не заводи дружбу с незнакомцами, и ни под какими предлогами не соглашайтесь на встречу с ними в реальной жизни.

НЕ РАСПРОСТРАНЯЙ В ИНТЕРНЕТЕ ЛИЧНУЮ ИНФОРМАЦИЮ

Никогда не отправляй свою личную информацию (твои данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуй такого рода информацию в блогах и форумах. Кроме того, будь внимательным при создании профилей в таких сервисах, как Facebook или MySpace.
Ты никогда не должен размещать такую конфиденциальную информацию, как твой возраст и твой адрес проживания. Также рекомендуем тебе не использовать свое настоящее имя, а пользоваться псевдонимом или ником.

ОСТЕРЕГАЙТЕСЬ ЗАМАНЧИВЫХ ПРЕДЛОЖЕНИЙ РАБОТЫ

Как правило, никто ничего не дает просто так. Если ты получил фантастическое предложение работы от неизвестных пользователей, то **НЕ ОБРАЩАЙ НА НЕГО ВНИМАНИЯ.**