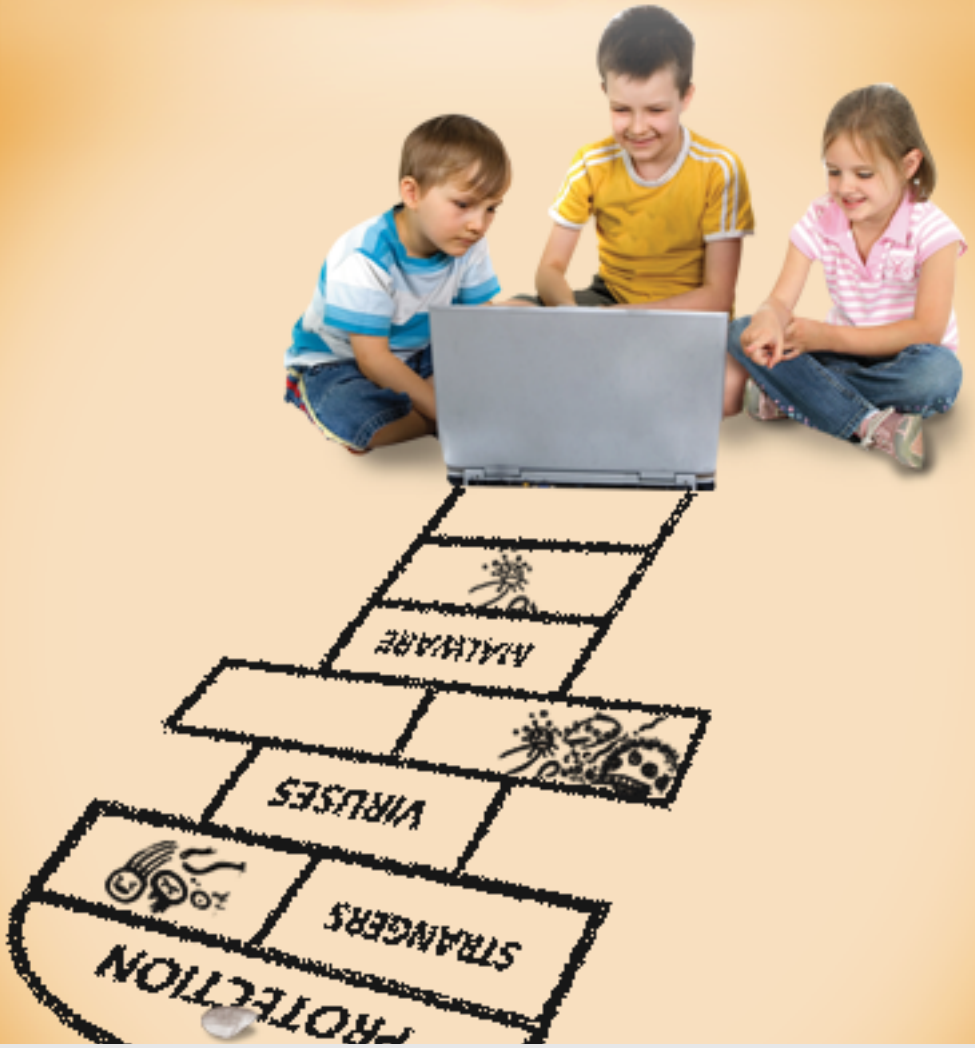
РЕБЕНОК В СЕТИ. РЕБЕНОК ИГРАЕТ?



PANDA SECURITY | The Cloud Security Company

Количество новых вредоносных программ (вирусов, шпионов и другого вредоносного кода), которое появилось в последние годы, на порядок больше, чем за все предыдущие годы. Более того, кибер-преступники нашли новые способы инфицирования пользователей и кражи их персональной информации, такие как системы обмена мгновенными сообщениями (такие программы, как MSN Messenger, Yahoo! Messenger или ICQ), программы для обмена файлами (например, eMule или Kazaa) и блоги.

Другими словами, риски в Интернете постоянно растут, а дети, даже если они имеют какие-то инструкции по использованию Интернета, являются все более уязвимыми.

Ниже мы постараемся объяснить самые основные Интернет-угрозы, которым подвержены дети, а также посмотрим, как наилучшим образом мы можем их защитить. Основное бремя защиты лежит, конечно же, на родителях и учителях, которые должны быть способны контролировать, что дети делают в Интернете, а также рассказать им о том, как можно пользоваться новыми технологиями безопасным и ответственным способом.

Важные данные: Дети и Интернет

Согласно данным Save the Children, свыше 13 миллионов детей в Европе регулярно пользуются Интернетом. Как правило, они впервые выходят в Интернет в возрасте до 10 лет.

Согласно исследованию Kleiner and Lewis, проведенному еще в 2004 году, 90% детей в США в возрасте от 6 до 10 лет регулярно пользуются Интернетом. В 2006 году Американская Ассоциация психологов (APA) в своем исследовании говорит о том, что регулярно пользуются Интернетом, общаются в чатах или используют системы обмена мгновенными сообщениями от 75% до 90% детей.

Данные, которые приводятся по Евросоюзу, практически идентичны. Евробарометр показывает, что 64% детей в Дании, Голландии и Великобритании являются пользователями Интернет, в Швеции – 63%, в Финляндии – 62%, в Эстонии – 60%. За исключением ряда стран (Греция – 15%, Кипр – 20%, Словакия – 30% и Португалия – 31%), в других странах Евросоюза уровень использования Интернета детьми примерно такой же.

Если говорить про абсолютные значения, то согласно данным Save the Children, свыше 13 миллионов детей в Европе регулярно пользуются Интернетом: четыре миллиона детей в возрасте до 12 лет и девять миллионов детей в возрасте от 12 до 17 лет. Возглавляет этот рейтинг – Великобритания, в котором самое большое количество детей, регулярно пользующихся Интернетом.

Что касается рисков, то около 49% детей, принявших участие в опросе Save the Children, сказали, что получали через Интернет информацию, которая пугала или беспокоила их.

Короче говоря, Интернет – это часть ежедневной жизни наших детей. Они часами подключены к Интернету, находясь дома или в школе. Именно поэтому родители и дети должны быть осведомлены о рисках в Интернете, а также должны знать о том, как их можно избежать.

Основные риски

Дети и молодые люди подвергаются рискам в Интернете, от элементарного заражения компьютера вредоносными программами до знакомства с людьми, которые используют чужие персональные данные и предлагают встретиться в реальной жизни.

В данном документе мы рассмотрим список основных угроз и обсудим, как родители и дети могут бороться с ними.

Системы мгновенного обмена сообщениями и электронная почта

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messsenger, Google Talk, ICQ…) стали широко используемым каналом общения для молодых людей. Это не могло остаться незамеченным со стороны кибер-преступников, которые быстро сделали его основным каналом для своей деятельности.

Одна из самых опасных угроз заключается в том, что преступники, используя данные программы, обманывают детей и подростков и представляются им другим человеком, чем они есть на самом деле. Смотрите, в этих программах пользователи авторизуются с использованием адреса электронной почты и пароля. Например, если кто-то узнает данные другого пользователя и подключится к программе от его лица, то остальные люди, с которыми этот пользователь общается, будут думать, что они общаются именно с данным пользователем, хотя это не так. Если Вы обмениваетесь информацией или файлами с этим псевдо-пользователем, то преступник сможет легко ими завладеть. Именно по этой причине очень важно не распространять любую конфиденциальную информацию (персональные данные, фактический адрес проживания, банковские реквизиты и пр.) через подобные небезопасные каналы связи, как системы обмена мгновенными сообщениями.

Системы обмена мгновенными сообщениями используют адрес электронной почты и пароль для идентификации пользователей. Поэтому сложно узнать, кто в действительности находится на другой стороне.

Другая опасность состоит еще в том, что к подобным преступлениям часто прибегают педофилы. Их задача – собрать сведения о детях и подростках, а затем договориться с ними о реальной встрече или заставить их пойти на встречу. Педофилы зачастую представляются другими молодыми людьми, профессиональными фотографами или т.п.

Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайне, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.

Другой потенциальный риск в обмене мгновенными сообщениями – это инфицирование вирусами и вредоносными кодами. Почти 60% червей (вредоносные коды, которые распространяют сами себя), обнаруженных антивирусной лабораторией PandaLabs на протяжении первого полугодия, были созданы для распространения через системы обмена мгновенными сообщениями. Некоторые из них созданы для кражи паролей к онлайн-банкам. В этом случае в большей степени рискуют сами родители, потому что будут украдены их банковские данные, и, следовательно, могут пропасть их деньги.

Существуют простые способы, которые могут быть полезны для предотвращения случаев проникновения вредоносных кодов на компьютеры через системы обмена мгновенными сообщениями: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через эти системы. По крайней мере, не делайте этого, пока точно не убедитесь, что человек, который их Вам прислал, является именно тем, кем он себя называет.

Лучший способ защиты от вредоносных программ, распространяющихся через почтовые приложения – это не открывать файлы и не нажимать на ссылки, которые Вы получили через этот канал общения.

Электронная почта – это другой источник опасности для молодых ребят. В этом случае также существует несколько угроз:

Во-первых, это спам. Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств. Дети более подвержены доверять сообщениям, которые представлены в данных письмах, со всеми вытекающими отсюда последствиями. Они могут получить доступ к онлайн-казино и проиграть большую сумму денег, или они могут купить лекарства или даже наркотики с большим риском для своего здоровья.

Далее, существуют ложные предложения работы. Это не представляет серьезную опасность для детей, но может являться таковой для подростков. Обычно эти сообщения содержат фантастические условия работы. Они обещают большие зарплаты без каких-либо усилий. Все, что в таких случаях необходимо, - это номер банковского счета, куда будут перечисляться деньги, а затем, в обмен на комиссию, получателя попросят перевести эти средства на другой банковский счет. Это выглядит слишком хорошо, чтобы быть правдой, и любой здравомыслящий взрослый человек насторожиться от такого предложения. Однако молодые люди ищут легких денег. В результате этого они непроизвольно становятся соучастником преступления, т.к. целью подобных финансовых переводов является «отмывание» преступных денег.

Другой риск связан с вирусами и вредоносными программами, которые могут попасть на компьютер. Как правило, они распространяются через сообщения в электронной почте, которые имеют определенную тематику (реклама новых фильмов, эротические фотографии, скачивание игр и т.д.) и предлагают пользователям нажать на ссылку или скачать файл, являющиеся причиной инфекции. Данная техника известна как «социальная инженерия». Многие взрослые люди становятся жертвами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.

Лучший способ защитить детей и подростков от этих угроз – это **научить их быть бдительными по отношению к письмам из неизвестных источников**. Они должны знать, что большинство из написанного в этих письмах является ложью, и что они никогда не должны открывать файлы или нажимать на ссылки в письмах подобного рода.

Программы обмена файлами (Emule, Kazaa и другие)

Обмен файлами в P2P-сетях является еще одним из основных источников распространения инфекций. Большинство вредоносных кодов (преимущественно, черви) копируются в папки с этими программами под заманчивыми именами (названия фильмов, программ и т.д.) для того, чтобы привлечь внимание других пользователей, которые захотят скачать эти файлы и запустить их на своих компьютерах.

По сути дела, это еще один вариант социальной инженерии: названия файлов могут быть умышленно созданы таким образом, чтобы привлечь именно детей и подростков, которые по незнанию скачают вредоносные программы на свои компьютеры.

Именно по этой причине детям следует знать, какие файлы они могут скачивать, а какие скачивать нельзя. Более того, очень хорошая идея – это **проверять каждый скаченный файл с помощью решения безопасности** до момента их первого открытия / запуска. Если при запуске файла возникает ошибка или открывается диалоговое окно с вопросом о лицензии или предложением скачать дополнительный кодек, то подобные действия должны сразу же Вас заставить быть бдительным, потому что, скорее всего, данный файл содержит в себе вирусы или другое вредоносное программное обеспечение.

Многие вредоносные коды копируют себя на самые посещаемые веб-страницы для того, чтобы пользователи скачали их и запустили.

Социальные сети и блоги

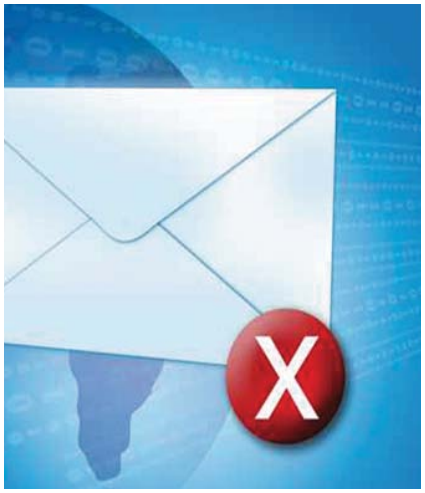
Сайты социальных сетей (например, Facebook, MySpace) широко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д.

Детям следует постоянно напоминать, что необязательно предоставлять эту информацию, а достаточно только указать адрес электронной почты и имя, которое может быть псевдонимом. Нельзя распространять такую информацию, как возраст, адрес проживания, а также свои фотографии и видео.

Многие подростки используют блоги в качестве своих персональных дневников. Как правило, такие онлайн-журналы содержат значительно более широкую информацию, чем следовало бы публиковать. Крайне важно предотвратить публикацию любых данных, которые могли бы идентифицировать пользователя как ребенка или подростка, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию.

Аналогично, в некоторых социальных сетях, например в MySpace, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание ребенка на то, какими файлами он может обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье.

Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей. Родители также должны быть способны проинструктировать своих детей о том, как использовать эти сервисы правильно и безопасно.



Такие функции смартфонов как Bluetooth и выход в Интернет сделали их уязвимыми для кибер-атак.

Новый риск: мобильные телефоны с выходом в Интернет

Согласно исследованию Frost & Sullivan, стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак.

В настоящее время сотовые телефоны широко используются детьми и подростками. Соответственно, они сталкиваются с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.

Во-первых, сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Дети могут войти в чаты в любой момент, при этом не важно, где они находятся физически, и столкнуться с теми рисками, о которых мы подробно говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.

Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии. Это означает, что дети могут столкнуться с подобной информацией не только при выходе в Интернет со своего компьютера, но и при использовании собственного мобильного телефона.

В результате, родители также должны контролировать то, как дети пользуются своими сотовыми телефонами. Поэтому мы рекомендуем родителям покупать своим детям сотовые телефоны без встроенных функций, которые могли бы подвергать их такому риску (подключение к Интернету, SMS, наличие Bluetooth и т.д.), а подросткам необходимо объяснять, как следует безопасно использовать свой сотовый телефон. Постоянно напоминайте им, чтобы они не отвечали на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

Риск инфекции

В предыдущих главах мы рассмотрели различные способы, которыми молодые пользователи могут инфицировать свои компьютеры (ссылки в письмах или мгновенных сообщениях, скачивание зараженных файлов через P2P). Существует огромное количество опасностей, содержащих вредоносный код, который запускается в операционной системе компьютера.

Во-первых, как говорилось выше, если ребенок пользуется тем же компьютером, что и родители, то он может инфицировать компьютер банковским трояном или любым другим подобным вредоносным кодом. Эти угрозы могут украсть банковские данные (номера и пароли доступа к банковским картам, регистрационные данные для подключения к интернет-банку и пр.) в то время, когда взрослые пользуются компьютером.

Но вредоносные программы представляют угрозу не только для взрослых, но и для самих детей. Например, рекламное ПО может легко проникнуть на компьютер. Этот тип вредоносных программ используется для показа на зараженных компьютерах баннеров, всплывающих окон и других видов рекламы. Для взрослых это может быть очень большим раздражающим фактором (хотя таких угроз следует серьезно остерегаться, потому что они могут скачивать различные другие угрозы, например, трояны), но для детей и подростков риск значительно выше, т.к. некоторые из показываемых реклам могут вести на сайты с порнографическим содержанием. Более того, порнография может оказаться на компьютерах детей даже в том случае, если они ее не смотрели.

Если ребенок пользуется тем же компьютером, что и его родители, то существует риск, что неосторожное обращение может привести к заражению компьютера.

РЕБЕНОК В СЕТИ. РЕБЕНОК ИГРАЕТ?

Практические советы для родителей

1 **Поговорите с Вашими детьми**. Начальной точкой для защиты Ваших детей должен стать разговор с ними. Вы должны знать, какие сайты они посещают, с кем они общаются, что они любят смотреть и т.д. Вы не должны позволять им уходить из дома и не предупреждать Вас, куда и с кем они пошли. Соответственно, Вы не должны разрешать им пользоваться Интернетом, если они не знают, как с ним обращаться.

2 **Обучите себя и поделитесь этими знаниями с Вашими детьми**. Для многих родителей Интернет является все еще неизвестным миром. Кто-то использует его для поиска информации, чтения газет или скачивания музыки, фильмов и других файлов, но для большинства родителей те сервисы и сайты, которыми пользуются их дети, остаются для них неизвестными. По этой причине очень важно знать о тех утилитах, которые Интернет предлагает детям, о рисках, которые они могут в себе нести, а также о том, как их можно избежать. Узнав, Вы сможете затем советовать Вашим детям, как безопасно использовать Интернет.

3 **Установите правила для использования Интернета**. Вы должны установить четкие и понятные правила, которые описывают расписание выхода в Интернет, максимальную продолжительность работы в Интернете, а также способ его использования. Убедитесь, что Ваши дети следуют этим правилам, особенно при использовании Интернета ночью. Также следует обратить внимание на расположение компьютера дома: если у Вас только один ПК на всю семью, то он должен располагаться в общей комнате, а не в спальне Вашего ребенка.

4 **Запретите детям предоставлять конфиденциальную информацию**. Вы должны проинструктировать Ваших детей о том, что им нельзя предоставлять кому-либо в Интернете такие данные, как их имя, адрес или свои фотографии. Посоветуйте им использовать псевдоним или ник и покажите им, как можно создать сложные безопасные пароли (сочетание букв с нижним и верхним регистром, цифр, символов и т.д.), которые помогут предотвратить кражу регистрационных данных детей для доступа к почте, системам обмена сообщениями, форумам и пр.

5 **Научите своих детей быть осторожными**. Информация в Интернете может быть обманчивой. Выше мы рассматривали с Вами, каким образом вредоносный код может маскироваться в виде различных кодеков и видеофайлов, как педофилы представляются другими людьми, чтобы установить контакт с детьми, и как сообщения, которые пришли от знакомого человека, могут оказаться зараженными. Зачастую в Интернете многие вещи выглядят не так, как они нам представляются. Научите Ваших детей быть осторожными и приучить их не делать ничего такого, что могло бы поставить под угрозу их безопасность и конфиденциальность.

6 **Установите эффективное решение безопасности**. Чтобы защитить Ваших детей от вредоносных программ, лучший способ – это использовать обновляемое и эффективное решение безопасности. Panda предлагает решения для домашних пользователей, которые не только уничтожают вредоносные программы, но также блокируют доступ к тем веб-сайтам, которые могли бы заразить компьютер, фильтруют спам и, в случае с Panda Internet Security 2011, содержат функцию Родительского контроля, которая позволяет Вам решить, какие сайты будут доступны для Ваших детей.

PANDA SECURITY

РЕБЕНОК В СЕТИ. РЕБЕНОК ИГРАЕТ?

Практические советы для детей

1 **Не нажимайте на ссылки**. Когда Вы общаетесь в чате с помощью систем обмена мгновенными сообщениями или если Вы получили письмо, никогда не нажимайте непосредственно на ссылку. Если сообщение или письмо пришло к Вам от известного человека, то скопируйте адрес ссылки и поставьте его в адресной строке Вашего браузера. Если сообщение или письмо пришло к Вам от неизвестного человека, то лучше не открывать эту ссылку. Даже если Вы поставите ее в адресную строку браузера, то может открыться сайт с вредоносными программами, которые загрузятся на Ваш компьютер.

2 **Не скачивайте и не открывайте файлы из подозрительных источников**. Несомненно, Вы получаете много сообщений, которые приглашают Вас скачать фото, песню или видео. Иногда такие сообщения могут отправляться без ведома человека, от которого они пришли к Вам, потому что его компьютер был заражен вредоносными программами, которые стали автоматически себя распространять среди других пользователей. В этом случае, лучше спросить знакомого Вам отправителя, действительно ли он отправил Вам это сообщение или файл. Если он не делал этого, то сообщите ему, что возможно его ПК заражен, и пусть он сообщит всем, чтобы не смотрели и удалили это сообщение или файл, которое якобы пришло от него другим пользователям.

3 **Не общайтесь с незнакомцами**. Пользуясь чатами и системами обмена мгновенными сообщениями, Вы никогда не знаете, с кем Вы общаетесь на самом деле. Особенно это касается онлайн-сообществ, где люди никогда не видели друг друга в реальной жизни. Никогда не дружите с незнакомцами, и ни под какими предлогами не соглашайтесь на встречу с ними в реальной жизни.

4 **Не распространяйте через Интернет свою конфиденциальную информацию**. Никогда не отправляйте личную информацию (Ваши данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуйте такого рода информацию в блогах и форумах. Кроме того, будьте внимательны при создании профилей в таких сервисах, как Facebook или MySpace. Вы никогда не должны размещать такую конфиденциальную информацию, как Ваш возраст и Ваш адрес. Также рекомендуем Вам не использовать свое настоящее имя, а пользоваться псевдонимом или ником.

5 **Будьте бдительны**. Как правило, никто ничего не дает просто так. В Интернете если что-то выглядит очень привлекательно, то вряд ли оно есть таким на самом деле. Поэтому если Вы получили фантастическое предложение работы от неизвестных пользователей, то не обращайте на него внимания.

6 **Не запускайте подозрительные файлы**. Если Ваше решение безопасности скажет Вам, что файл может содержать (или содержит) вредоносную программу, не открывайте этот файл. Просто удалите его.

7 **Поговорите с Вашими родителями или учителями**. Если у Вас возникли вопросы обо всем этом, если Вы столкнулись с чем-то подозрительным, если Вы получили оскорбительные или опасные письма, то обсудите это с взрослыми. Они смогут Вам помочь.

Практические советы для учителей

Учителя также играют важную роль в воспитании детей и могут показать им, как правильно и безопасно использовать новые технологии и, прежде всего, компьютеры, которые есть в большинстве школ и домов. Именно поэтому мы предлагаем учителям серию следующих рекомендаций:

1. **Узнайте подробнее**. Найдите и изучите информацию об Интернет-угрозах. Узнайте, что они собой представляют, и какие от них последствия могут быть. Подумайте, как Вы сможете донести эту информацию до своих учеников и студентов.

2. **Разработайте образовательный план по ИТ-безопасности**. Т.к. молодые люди изучают, как обращаться с компьютерами и работать в Интернете, им следует также знать и о потенциальных опасностях. Таким образом, Вы должны быть уверены, что они способны соблюдать свою безопасность при работе с ПК и Интернетом. Составьте план обучения, определитесь с тем, что Вы им будете рассказывать, найдите требуемую информацию и документацию.

3. **Сделайте Ваши рассказы интересными и практичными**. Лучший способ донести эту информацию – это использовать практические примеры. Вы можете продемонстрировать некоторые опасности в Интернете, показав Вашим ученикам, какие негативные последствия они имеют. Расскажите новости и истории, которые связаны с подобными инцидентами.

4. **Научите их защищать себя**. Во время практических занятий расскажите о том, как настроить антивирусные программы, создавать сложные пароли, объясните им, как можно безопасно совершать интернет-покупки, и пр.

5. **Практикуйте то, что Вы преподаете**. Чтобы помочь детям избежать рисков, важно, чтобы Вы сами были осведомлены об этих рисках и избегали их. Используйте надежное решение безопасности, которое позволяет не только защититься от вирусов, спама, хакеров, мошенников и других угроз, но и содержит в себе функцию Родительского контроля, обеспечивающую безопасное использование Интернета детьми.

www.detionline.ru