«Безопасный интернет»

РОДИТЕЛЬСКОЕ СОБРАНИЕ

Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

На сегодняшний день практически каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Результаты анкетирования учащихся группы

- 98 % учащихся имеют дома компьютер.
- В среднем ежедневно проводят за ним от 4 часов до 6 в день.
- Из видов деятельности, преобладающих в общении с компьютером, на первое место поставили компьютерные игры.
- На втором месте – общение в сети.
- другие виды - прослушивание музыки, рисование, печать документов.

Зависимости от сети Интернет - одна из важнейших проблем современных подростков.

Зависимость в медицинском смысле определяется как навязчивая потребность в приеме привычного вещества, сопровождающаяся ростом толерантности и выраженными симптомами. Рост толерантности означает привыкание ко всё большим и большим дозам.

Интернет-зависимость – это навязчивая потребность в использовании Интернета.

типы Интернет-зависимости

• бесконечный веб-серфинг — постоянные «путешествия» по Интернету с целью поиска информации.
• пристрастие к виртуальному общению и виртуальным знакомствам, характеризуется большими объёмами переписки, постоянным участием в чатах, форумах, избыточностью знакомых и друзей из Интернета.
• игровая зависимость — навязчивое увлечение сетевыми играми.
• навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах.
• киберсексуальная зависимость — навязчивое влечение к посещению порносайтов.

- Интернет-зависимость характеризуется сильным желанием подростка быть в сети, что приводит к нежеланию проводить время с семьей и друзьями, спать, посещать и делать уроки. Ребенок может перестать следить за своим внешним видом, начинает болезненно реагировать на просьбы отвлечься от компьютера, терять контроль за своим временем, лгать, причем уход от реальности может усиливаться день ото дня.

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников

Родители должны уметь распознать признаки надвигающейся зависимости, прежде чем она станет реальной проблемой. Но это легче сказать, чем сделать…

Основные угрозы для детей в сети Интернет

1. Системы мгновенного обмена сообщениями

- 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. 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. 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.

2. Электронная почта

- 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.
- Существуют также ложные предложения работы. Это не представляет серьезную опасность для детей, но может являться таковой для подростков.
- 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.
- 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.

3. Программы обмена файлами

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.

4. Социальные сети и блоги

Сайты социальных сетей 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

5. Мобильные телефоны с выходом в Интернет.

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибератак 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

Как обеспечить безопасность детей в сети Интернет?

Установите комплексную систему защиты

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление

Будьте осторожны с электронной почтой.

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

Обновляйте операционную систему Windows.

Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

Не отправляйте SMS-сообщения.

- Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.
- При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.
- Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

Пользуйтесь лицензионным ПО.

- Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.
- Лицензионные программы избавят Вас от подобной угрозы!

Используйте сложные пароли.

- Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

Делайте резервные копии

- При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.
- Функция «Родительский контроль» обезопасит вас .

- ***Соблюдая эти несложные правила, вы сможете избежать популярных сетевых угроз.***

- **<u>И самое главное – будьте внимательны к своим детям!</u>**