Информационная безопасность.

В век глобальной информатизации неуклонно возрастает роль сети Интернета в жизни каждого человека, и в частности ребенка. Современный интернет — это очень агрессивная среда, которая полна различными хакерами и кибер-преступниками. В социальных сетях детям зачастую преподносится по специально отработанной тактике информация, формирующая у подростков 10-18 лет деструктивное восприятие мира. Самое страшное явление человечества - это массовое вовлечение детей в суицидальные группы.И воздействие на ребенка происходит не только через социальные сети, но и через предложения просмотра видео, обсуждения сериалов,и даже в помощи решения домашнего задания, в предложениях онлайн книг.

По мере взросления ребенку понадобится все больше учебной информации из Интернета. Поэтому нужно :

-сформировать у детей правильное отношение к возможностям компьютера, -донести им всю степень опасности .

-выработать правила контроля потока информации и воспитывать культуру получения ее ребенком.

-необходимо обучать детей компьютерной грамотности для их безопасности и защищенности.

 У каждого ребенка уже с младшего школьного возраста есть своя страничка в соцсетях. Нужно научить детей правильно настроить страницу в соцсети, приватность и безопасность, ограничить доступ к странице. Ведь соцсети имеют интуитивно понятный интерфейс***.***

***В соц.сетях необходимо соблюдать следующее:***

-***Устанавливайте надежный пароль:*** должно быть не меньше восьми знаков: заглавные и строчные буквы, цифры, специальные знаки.

- ***Просматривайте периодически, с кем «дружит» ребенок в соцсетях и что публикует в открытом*** ***доступе.***

 - ***Удалите из друзей пользователей***, с которыми он не знаком лично.

 -***Настройте конфиденциальность*** соцсети и регулярно проверяйте ее, чтобы посты и личную информацию видели только доверенные лица.

 -***Не стоит публиковать личную информацию***. Полное имя, номер телефона, домашний адрес и другие данные лучше оставить в тайне и придумать вместе интересный **псевдоним**.

 -***Не встречаться с сетевыми «френдами» в реальной жизни***. *О подобных приглашениях лучше сразу сообщать родителям.*

-***Не открывать сообщения от неизвестных***, *уверенно говорить «нет».*

 - ***При получении ссылки в посте или письме от незнакомца*** ,то по ней лучше не переходить.

 - ***-Договоритесь всегда обсуждать странные или пугающие происшествия***. Так как дети могут пострадать от ***кибербуллинга*** – сетевой травли.

 -***Игнорировать*** ***оскорбительные сообщения и комментарии*** - даже если очень хочется возразить и трудно сдержать эмоции.

 - ***Не удаляйте оскорбительные письма***.Могут пригодиться в качестве доказательства..Если угрозы или оскорбления исходят от посторонних, перешлите сообщения в службу технической поддержки соцсети Если он пользуется «Вконтакте», безопасность детского аккаунта можно бесплатно проверить на сайте **socialmediascanner.eset.com** .

 *«Запрещать ребенку регистрацию в социальных сетях - неразумно и несовременно. Особенно в подростковом возрасте, когда общение со сверстниками выходит у детей на первый план. И если все одноклассники поддерживают связь в интернете, а ему нельзя - он может чувствовать себя изгоем в коллективе и не на шутку обидеться на родителей. Поэтому доверяйте своему ребенку, но контролируйте время пребывания в сети, деликатно интересуйтесь, в каких группах он состоит, с кем дружит, что смотрит.*

Давайте теперь поговорим о том, какие опасности могут поджидать во время работы за компьютером. Если на вашем ПК происходят какие-то странности, то возможно заражение вирусами.

**Признаками заражения являются:**

* Вывод на экран странных сообщений или изображений;
* Неожиданное открытие и закрытие лотка дисковода;
* Произвольный запуск каких-либо программ;
* Неожиданная перезагрузка и завершение программ;
* Повышенная нагрузка и «зависание» устройства;
* Этого можно избежать, если соблюдать простые правила!

**Соблюдайте 10 простых , но эффективных правил**:

1*.Использовать современные операционные системы, имеющие серьезный уровень защиты;*

*2.Своевременно обновлять программы только с сайтов разработчиков и их надежных источников, включать автообновление. Так как иногда программы имеют ошибки. Зачастую эти ошибки исправляют сами разработчики. Если вовремя не обновлять, то эти ошибки используют взломчики и хакеры.*

*3.Использовать антивирусные продукты известных производителей*

*4.Применять брандмауэр.*

*5.Не устанавливать програмные продукты с подозрительных сайтов;*

*6.Работать на своем компьютере под правами пользователя под своей учетной записью, а не администратора. Большинство вредоносных программ работают только от имени администратора.*

*7.Ограничить доступ физических лиц к своему компьютеру для посторонних;*

*8.Использовать внешние носители (флешкарты ,диски) только от проверенных источников или проверять их на наличие вирусов;*

*9.Не открывать файлы, полученные от ненадежных, неизвестных источников, и если даже от знакомых. Надо вначале уточнить, действительно ли знакомые высылали вам их.*

*10.Создавать резервные копии важных файлов, желательно на внешние накопители.*

Вредоносные программы (сетевые черви, руткиты, шпионские программы)

могут нанести колоссальный урон: похищать пароли, логины, контакты, данные банковских карт, делать скрытые скриншоты, отправлять данные злоумышленникам, рассылать с вашего ПК спамы, рассылки, звонки ,СМС на платные номера, включать удаленное управление компьютером.

**Источниками вирусов могут быть:**

*-переходы по непроверенным ссылкам,*

*-посещение сомнительных и зараженных сайтов;*

*-клики по опасным баннерам;*

*-скачивание файлов с непроверенных ресурсов;*

*-установка программ непроверенных и сомнительных ресурсов, использование зараженных накопителей информации и другое.*

 У каждого пользователя есть электронная почта. Советую соблюдать следующие правила  **относительно электронной почты:**

1.Никогда не открывайте подозрительные сообщения или вложения электронной почты. Сразу удалите их.

2.Никогда не отвечайте на спам. Они приводит к перегрузке систем электронной почты и может заблокировать почтовые ящики. В них могут быть вирусы - черви электронной почты.

3.Применяйте фильтры от спама и рассылок .

4.Создайте несколько почтовых ящиков с разными паролями для разных целей.

*5.*Используйте псевдоним для защиты реальной личности;

*6.*Используйте надежные пароли и регулярно их меняйте!

*7.*Не следует разглашать в Интернете личную информацию *(полное имя, почтовый адрес и номер телефона, название школы, спортивного клуба, места проживания и т.д.) Вместо фото на аватаре лучше вставлять нарисованные картинки. После публикации в Интернете текста или фотографии их невозможно контролировать. Их можно легко скопировать во множество разных мест, и их полное удаление может оказаться невозможным*

*8.*Никогда никому не сообщайте пароли, даже друзьям.

9.Применяйте аутентификацию.*.*

 *Для безопасности личных данных в соцсетях и электронной почте применяйте двухэтапную* ***аутентификацию.*** *Двухэтапная* ***аутентификация,*** *которую еще называют двухэтапной* ***авторизацией****, – это использование для входа в компьютерную систему сочетания двух видов паролей: текста, отпечатка пальца, кода, который приходит на ваш смартфон, числа, которое генерируется специальной программой, и т.д. Это безопасность в квадрате.*

 В интернете помимо нужной информации много информационного мусора, которая затрудняет доступ к нужной информации. Источниками информ.мусора являются: спам, реклама, репостинг, много искаженной информации. Поэтому нужно уметь определять источники поиска и проверять достоверность и достаточность по разным источникам;

Оценить достоверность информации помогут здравый смысл и собственная грамотность пользователя.

Информация анализируется по сотням параметров. На разных поисковых устройствах, на разных браузерах будут найдены разные источники и будут отличаться. Для быстрого поиска инфо нужно задать корректный вопрос поисковику. Он должен состоять как минимум из двух ключевых слов, тогда ему будет гораздо проще отыскать нужную информацию. Несмотря на то, что все поисковики построены на общих принципах, алгоритмы у них могут различаться. Поэтому может случиться так, например, что не смог найти Yandex, выдаст Google.

**Для ускоренного поиска информации можно использовать параметры расширенного поиска:**

***1.Исключение из Google поиска****. Чтобы исключить из поиска какое либо слово, фразу, нужно перед ним поставить знак «-» (минус). Например,«бесплатный хостинг -ru» .*

***Поиск по синонимам****. С помощью символа «~» можно подобрать синонимы.*

***Неопределённый поиск****. если не знаете точное определение,то ставьте оператор «\*».*

***Поиск на выбор из вариантов.*** *Используя оператор «|», можно найти несколько запросов.*

***Значение слова****. Чтобы узнать значение того или иного слова, достаточно ввести в поисковую строку «define:» и после двоеточия искомую фразу.*

***Точное совпадение****. Для точного совпадения фразы с запросом нужно заключить слова в кавычки.*

***Поиск по определённому сайту****. Чтобы искать только по конкретному сайту нужно добавить слово «site:».*

***Цифровая репутация****. После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.*

*Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.*

*Благоразумно ли размещать личную информацию на собственном веб-сайте, если невозможно быть уверенным в целях ее использования?*

*Имена учеников, их фотографии и другая личная информация из школьного журнала может публиковаться на веб-сайте школы только с согласия учеников и их родителей.*

Все ,что вы делаете в интернете, анализируется.На основе сложенной цифровой репутации могут возникнуть проблемы при поступлении на учебу, при устройстве на работу .У каждого пользователя формируется цифровой портрет, который может повлиять на судьбу и будущее человека!

Благодарю за внимание!

**Всего вам самого светлого и доброго!**

**Пять правил для родителей:**

1. Разместите компьютер в общей комнате — таким образом, обсуждение Интернета станет повседневной привычкой, и ребенок не будет наедине с компьютером, если у него возникнут проблемы.

2. Используйте будильник, чтобы ограничить время пребывания ребенка в Сети — это важно для профилактики компьютерной зависимости.

3. Используйте технические способы защиты компьютера: функции родительского контроля в операционной системе, антивирус и спам-фильтр.

4. Создайте «Семейные Интернет-правила», которые будут способствовать онлайн-безопасности для детей.

5. Обязательно обсуждайте с детьми все вопросы, которые возникают у них в процессе использования Сети, интересуйтесь друзьями из Интернета. Учите критически относиться к информации в Интернете и не делиться личными данными онлайн.

Популярные программы родительского контроля:

¦ «Дополнительная безопасность» в Windows 7 — обеспечит сохранность личных данных от всех возможных угроз;

¦ «Семейная безопасность» в Windows Live — поможет уследить за контактами и интересами вашего ребенка даже с другого компьютера;

¦ «Родительский контроль» в Windows Vista — с ее помощью вы можете определить время, когда ребенок может зайти в систему, а также с помощью фильтра установить запрет или к отдельным играм, узлам, программам.

¦ «Родительский контроль» в Kaspersky Cristal — помимо антивирусной программы, она позволяет следить за тем, по каким сайтам ходит ребенок, и ограничивать посещение «неугодных». Кроме того, программа поможет вам сохранить личную информацию (семейные фото, пароли, файлы) от вторжения и хищения.