Презентация по информатике.

Безопасность в интернете.

Что такое интернет и с чем его едят?

Интернет-всемирная система объединенных компьютерных систем для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. Построена на базе стека протоколов TCP/IP. На основе интернета работает Всемирная паутина (World Wide Web, WWW) и множество других систем передачи данных. 29 октября 1969 года в 21:00 между двумя первыми узлами сети ARPANET, находящимися на расстоянии в 640 км-в Калифорнийском университете Лос-Анджелеса (UCLA) и в Стэнфордском исследовательском институте (SRI)-провели сеанс связи. Чарли Клайн пытался выполнить удаленнок подключение из Лос-Анджелеса по компьютеру в Стэнфорде.

Безопасное пользование интернетом для детей.

- Никогда не загружайте картинки из незнакомых источников-они могут иметь откровенно сексуальное содержание.
- Используйте фильтры электронной почты.
- Всегда и немедленно сообщайте взрослым, если во время общения онлайн что-то заставляет вас чувствовать себя неуютно или пугает.
- Выбирайте нейтральное экранное имя, не содержащее сексуального подтекста и не отображающее никакой персональной информации.
- Никогда и никому не сообщайте онлайн свою персональную информацию или информацию о своей семье и не заполняйте персональные профили.

Безопасное пользование интернетом для детей.

- Прекращайте любое общение по электронной почте и обмен мгновенными сообщениями или разговоры в чатах, если кто-то начинает задавать вам вопросы, являющиеся слишком личными или имеющие сексуальный подтекст.
- Разместите рядом с компьютером семейное соглашение о работе онлайн, которое будет напоминать вам о защите от опасности в интернете.

Какие угрозы для детей существуют в интернете?

Хакеры, трояны, перезагрузка сайта или сети, подмена адресов, анализ пакетов, социотехника, подмена веб-страницы, вирусы, спамы. Всё это может нанести большой ущерб компьютеру и вам.

Как защититься от вирусов и спамов?

Существуют программы, созданные для защиты аппаратной составляющей и операционной системы компьютеров, компьютерных сетей и данных, которые хранятся и обрабатываются на нём. К этой группе программного обеспечения относятся ***антивирусы, фаерволы, антишпионы и программы для шифровки и сохранения данных.***

На каждом компьютере, даже на не подключённом к интернету, обязательно должна быть установлена программа, которая обеспечивает защиту от вирусов. Для этого можно использоватьАнтивирус Касперского, Norton Antivirus или Eset NOD32.

Как предотвратить заражение вирусами?

- Не вступайте в сомнительные контакты.
- Не вставляйте свои устройства внешней памяти в чужой компьютер. Не разрешайте посторонним работать на вашем компьютере со своими устройствами. Избегайте компьютерных игр-основных носителей вирусов. Для заражения компьютера достаточно прочитать содержание заражённого носителя информации.
- Вступая в контакт, избегайте возможного заражения.

Как предотвратить заражение вирусами?

- Если контакта не избежать, сначала проверьте чужие устройства на вирусы. На чужом компьютере работайте после его антивирусной проверки или с устройствами памяти, на которых заблокирована запись.
- Периодически проводите профилактические проверки.
- Проверьте свои устройства внешней памяти на вирусы после контакта с чужим компьютером. На своём компьютере после каждой загрузки операционной системы полезно проводить предварительный антивирусный контроль винчестера после контакта, вызывающего сомнения, желательно проводить антивирусный контроль всех дисков винчестера. Рекомендуется время от времени обновлять антивирусные программы.

Как предотвратить заражение вирусами?

- Создавайте архивные копии важных программ и данных.
- Копии информации размещают на дисках или других съёмных носителях с помощью программ-архиваторов. Если вирусы «съедят» информацию на винчестере, то после лечения его содержимое можно возобновить из архивных копий.

Какие правила безопасности следует соблюдать при передаче информации по интернету?

- Защищённые сайты обычно требуют ввода имени пользователя и пароля. Делайте его длинным как минимум 8 символов, комбинируя буквы и числа. И главное, паролем не должно быть очевидное, какие-то слова или даты.
- Удобно иметь два пароля: один для так называемых развлекательных сайтов, то есть игр, чатов и прочее; а другой-для более важных действий, например приобретение товаров. Тогда снизится вероятность того, что ваши важные действия будут подвержены риску. И никогда не используйте для паролей такие данные, как дата рождения, номер телефона или имя.

Какие правила безопасности следует соблюдать при передаче информации по интернету?

- Пользуйтесь последней версией браузера. В более новых браузерах реализованы последние достижения в отрасли шифровки и других технологий защиты и безопасности.
- Внимательно читайте правила безопасности сайта. Ведь вряд ли вам понравится, если информацию, предоставленную вами о себе, организация впоследствии продаст владельцам рассылок.
- Записывайте информацию о действиях, связанных с покупкой или заказом товаров через интернет.

Безопасны ли для детей социальные сети?

Социальные сети обретают всё большую популярность у детей и подростков. Немало существующих соцсетей поощряют пользователей предоставлять как можно больше личной и конфиденциальной информации. Мошеннику нетрудно выбрать потенциальную жертву и выучить её по предоставленной в профайле информации. Пользователи выкладывают подобную информацию в большинстве случаев добровольно, не осознавая возможных последствий такой неосторожности. Дети охотно размещают фотографии, которые могут также быть использованы мошенниками в собственных целях. Иногда подростки охотно размещают свои пикантные фотографии, не задумываясь над тем, что опубликованное в интернете информация остаётся в сети ***навсегда***.

Презентация подготовлена для конкурса «Интернешка» http://interneshka.org/

Список литературы: «Википедия» и научно-методический журнал И.Н. Лещук «Безопасность в интернете: вопрос-ответ.

Работу выполнил ученик 8 класса
Кисельников Михаил.