Детский центр ИТ-творчества «IT-cube»

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

Казань, 2020 г.

Интерне́т (англ. Internet) — это всемирная система объединённых компьютерных сетей для хранения и передачи информации.

С появлением в 1969 г. Интернета весь мир поделился на два понятия: **ОНЛАЙН (Интернет) и ОФФЛАЙН (обычная, традиционная жизнь).** Практически все, что есть в ОФФЛАЙНЕ, уже присутствует и в ОНЛАЙНЕ.

ВОЗМОЖНОСТИ СЕТИ ИНТЕРНЕТ

Электронная почта

Общение. Существует множество программ и интернет-сервисов, позволяющих общаться. Это программы для обмена сообщениями (ICQ, Mail.ru Агент), социальные сети (Facebook, В Контакте, Одноклассники), тематические форумы и многое-многое другое.

Поиск информации

Поиск людей

Развлечения

Обмен файлами

Обучение

Совершение покупок в интернет-магазинах

Просмотр видео информации

Заработок. Существует множество специализированных сайтов, размещающих вакансии работодателей и резюме соискателей. Кроме того, вы можете работать удаленно.

ОПАСНОСТИ СЕТИ ИНТЕРНЕТ

Угроза № 1. Вредоносные программы (Вирусы).

Вредоносная программа – это любая программа, которая наносит вред компьютеру или пользователю этого компьютера. Некоторые виды рекламы считаются вредоносными программами.

Сегодня вирусы пишутся с расчетом на коммерческую выгоду!

Угроза № 2. Мошенничество.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются новые уловки доступа злоумышленников к компьютерам пользователей с целью выкачивания у них денег.

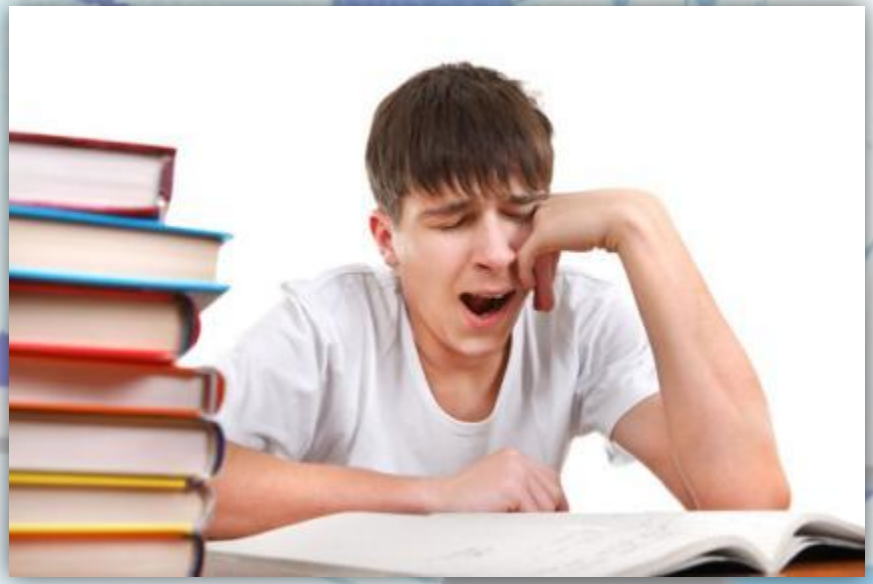
Угроза № 3 . Интернет-зависимость.

Детская и подростковая интернет-зависимость с каждым днем набирает все большие масштабы. Общение в социальных сетях заменяют общение с родителями и сверстниками, подвижные игры и физические занятия. Теряются коммуникационные навыки. Живые эмоции заменяются «веселыми смайликами».

Углубившись в виртуальное общение, человек перестает гулять на улице, встречаться с друзьями и мало двигается, как следствие, наступают проблемы со зрением, пищеварением, опорно-двигательным аппаратом, появляется повышенная утомляемость и головокружения.

Угроза № 4. Пренебрежение к учебе.

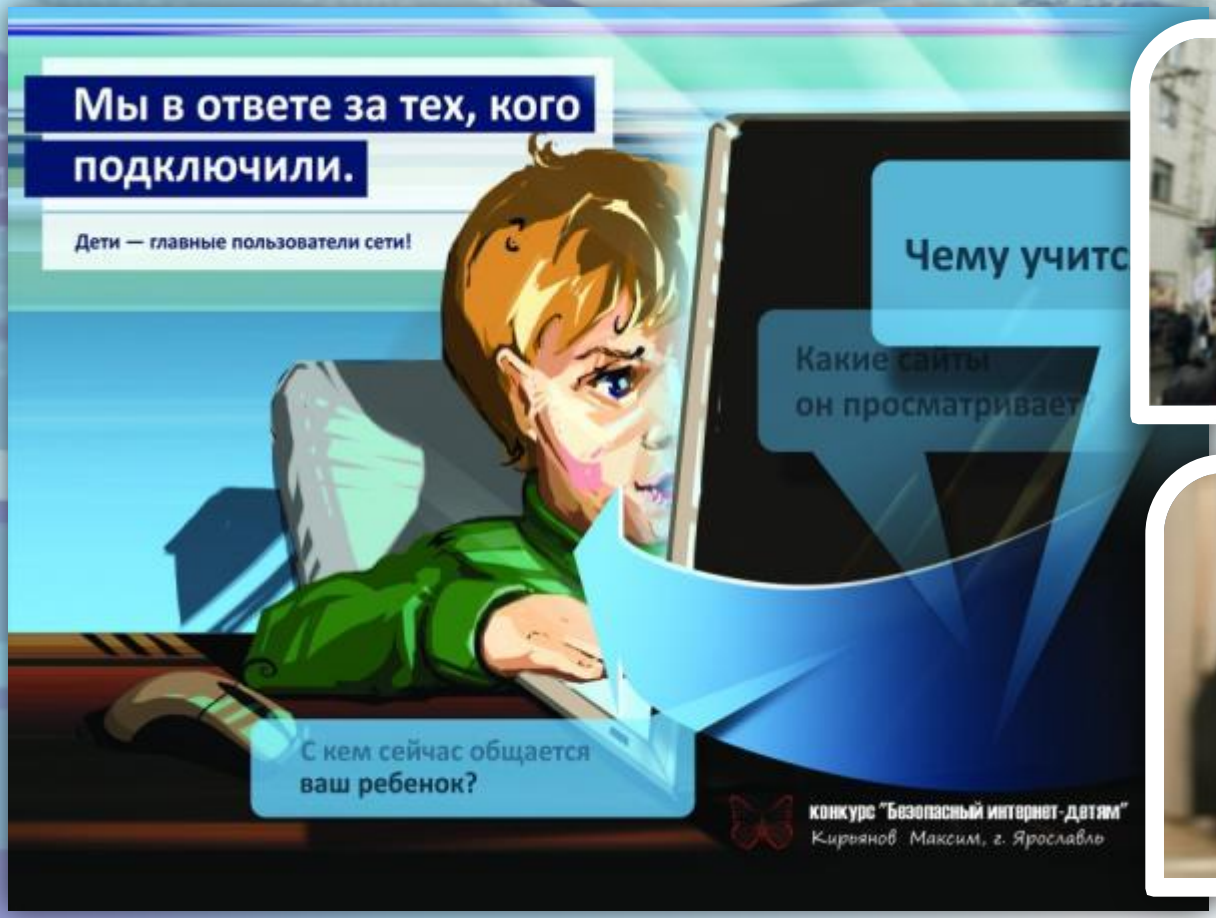
В Интернет много учебного материала, который становится доступным для студентов после процедуры скачивания, занимающей не более пяти минут. Подростки распечатывают нужный реферат и сдают его преподавателю, даже не удосужившись его прочитать. Таким образом, никакие знания получены не будут. Не в помощь студенту и «решебники» по любым дисциплинам. Студент, привыкший регулярно списывать, самостоятельно перестает учить, а значит усваивать материал и развиваться.



Угроза № 5. Доступ к сайтам, содержащим опасную информацию.

Путешествуя по просторам Интернета легко можно оказаться на сайтах, содержащих опасную для подростков информацию. Например: *порнография, суициды, сцены насилия и жестокости, призывы к экстремистским действиям и прочее.*

Отсечь доступ к сайтам с этим содержанием помогают поисковые фильтры, настройки приватности и программы «Родительский контроль".



Угроза № 6. Виртуальное общение.

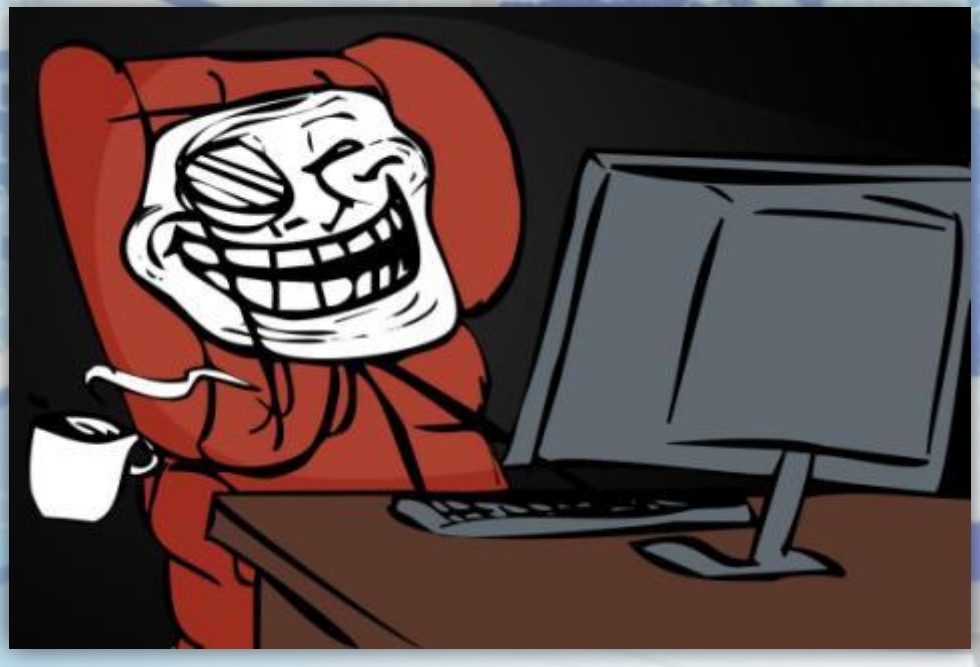
Виртуальное общение - это мир фантазий. Собеседник в Интернете может выдавать себя за кого-то другого. Здесь почти у каждого есть своя маска, свой тип поведения, причем он отличается часто от реальности. Почти каждый скрыт под аватарками, вымышленными именами и своими фантазиями.

Важно знать, что по закону ответственность за содержание текста несёт не только автор, опубликовавший информацию, но и пользователь, распространивший её — поставивший отметку «Мне нравится» или скопировавший её на свою страницу.

Угроза № 7. Интернет-хулиганство.

Одна из проблем, с которой можно столкнуться в социальных сетях - это оскорбления - *троллинг.*

Иногда это выглядит как обычное развлечение, своеобразная переписка, но очень часто *тролль* (так называют таких людей) выходит за рамки дозволенного и давит на самые болевые точки. Очень часто молодые люди, которые имеют влияние на определенную аудиторию, начинают терроризировать человека через интернет. Порой это приводит к необратимым последствиям.



Троллинг – это способ общения в сети, целью которого является провоцирование других его участников к конфликтам, выведение их из душевного равновесия, снижение интереса пользователей к ресурсу, где проходило общение.

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ПК

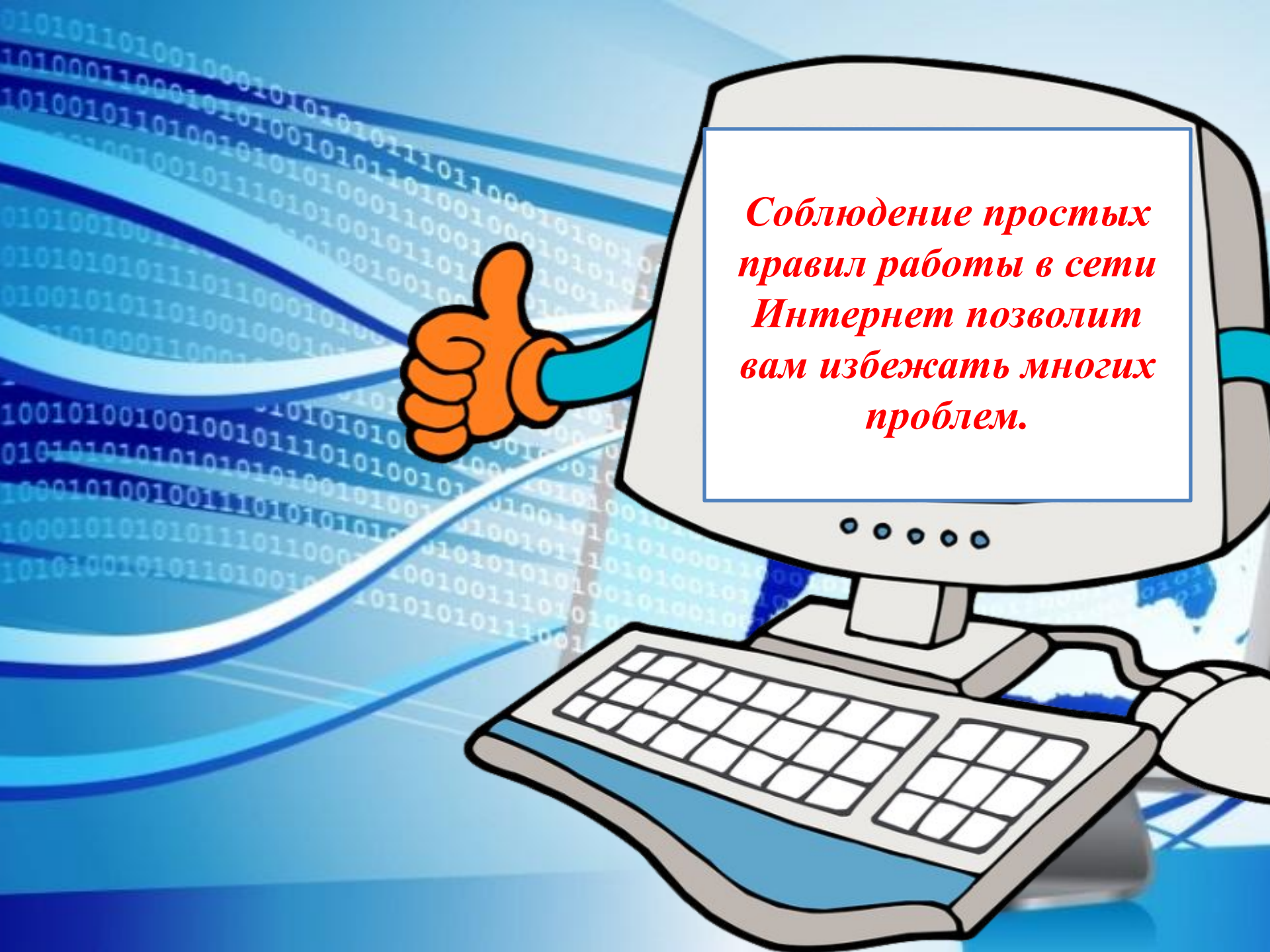
Пользователь, который только что приобрел персональный компьютер, прежде чем начать покорять Интернет-просторы, должен:

- установить антивирус и антишпионское программное обеспечение. После установки обновить их и настроить автоматическое обновление. Лучше если обновление антивируса запускается автоматически вместе с операционной системой.
- проверять антивирусом любую устанавливаемую на ПК программу.

ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

- Не заполняйте все поля вашего профиля.
- Не нужно выкладывать в социальных сетях откровенные фотографии.

- Не регистрируйтесь под чужими данными. Если хотите сохранить инкогнито – прибегните к вымышленному имени.
- Не используйте чужие изображения без разрешения этих людей.
- Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации.


Соблюдение простых правил работы в сети Интернет позволит вам избежать многих проблем.


Спасибо за внимание!