

Безопасность в сети Интернет



Интернёт (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

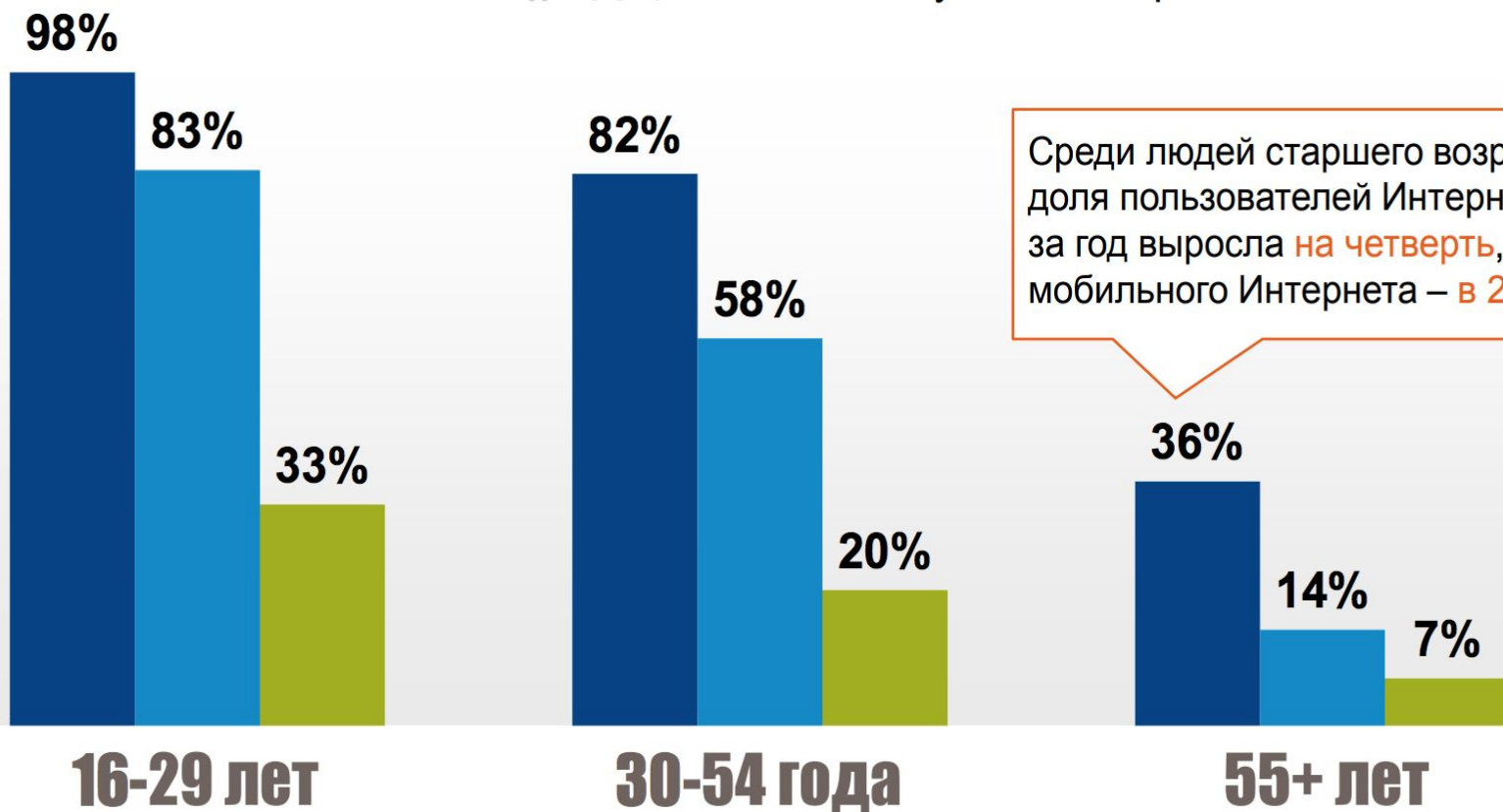
Заработок. Существует множество специализированных сайтов, размещающих вакансии работодателей и резюме соискателей. Кроме того, вы можете работать удаленно.



В связи с массовой популярностью сети Интернет важной проблемой сегодня является безопасность в глобальной сети. Касается данная проблема абсолютно всех, начиная от детей и заканчивая



- Пользуются Интернетом
- Пользуются Интернетом **на смартфонах**
- Пользуются Интернетом **на планшетах**



Среди людей старшего возраста доля пользователей Интернета за год выросла **на четверть**, мобильного Интернета – **в 2 раза**

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!

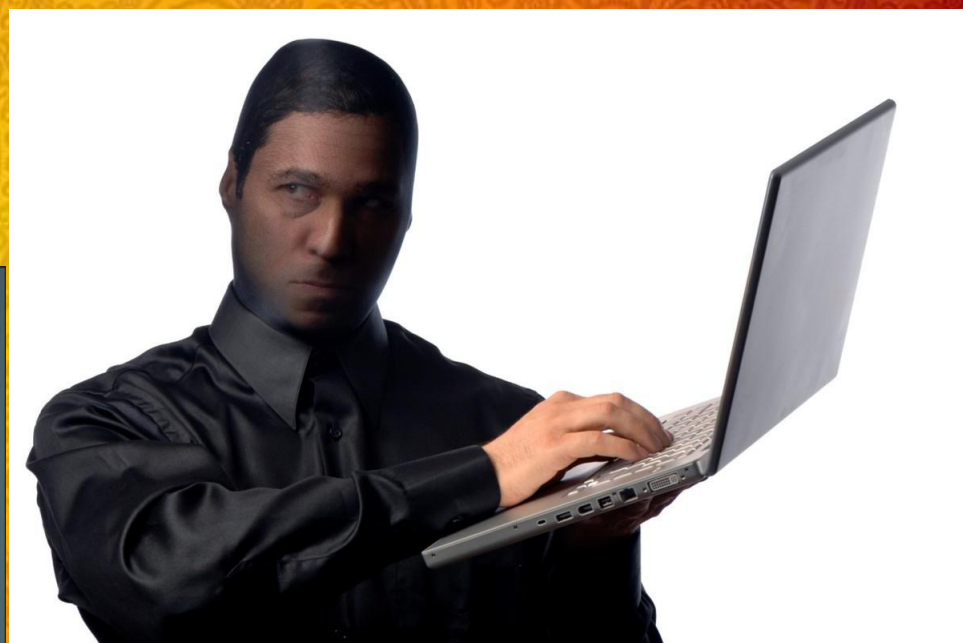
СИМПТОМЫ ЗАРАЖЕНИЯ ПК ВИРУСОМ

- ❑ ПК долго загружается и долго выключается;
- ❑ автоматическое открытие окон с незнакомым содержимым при запуске ПК;
- ❑ блокировка доступа к официальным сайтам антивирусных компаний;
- ❑ появление новых неизвестных процессов в окне «Процессы» диспетчера задач ;
- ❑ запрет на изменение настроек компьютера в учётной записи администратора;
- ❑ невозможность запустить исполняемый файл (выдаётся сообщение об ошибке);
- ❑ появление всплывающих окон или системных сообщений с непривычным текстом;
- ❑ перезапуск компьютера во время старта какой-либо программы;
- ❑ случайное или беспорядочное отключение компьютера;
- ❑ случайное аварийное завершение программ.



Угроза № 2. Мошенничество.

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



КАКИМ ОБРАЗОМ ЗЛОУМЫШЛЕННИКИ МОГУТ ПОЛУЧИТЬ ДОСТУП К ВАШЕМУ КОМПЬЮТЕРУ?

Первый приём. Социальная инженерия.

Это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.

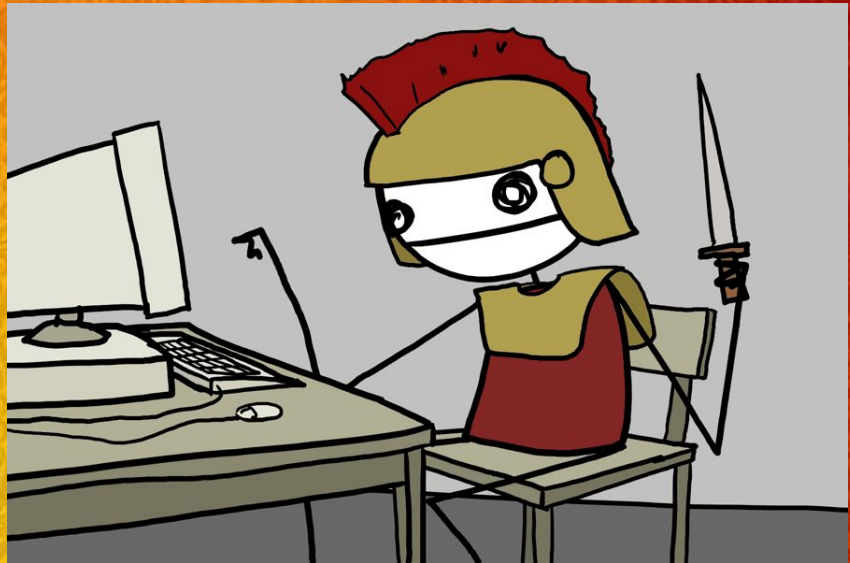
Сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации, или информации, которая представляет большую ценность. Благодаря использованию уловок и психологических приемов, вы открываете присланное хакерами письмо, содержащее вирус.



Второй приём. Фишинг («рыбалка»).

В интернете создаются подделки популярных сайтов и пользователи «клюют на эту наживку». Так вместо официальной страницы своего банка вы можете оказаться на его поддельной копии со всеми вытекающими последствиями.

Третий приём. Предложение бесплатного программного обеспечения.
Это как правило уловки, содержащие в себе множество вирусов и троянов.

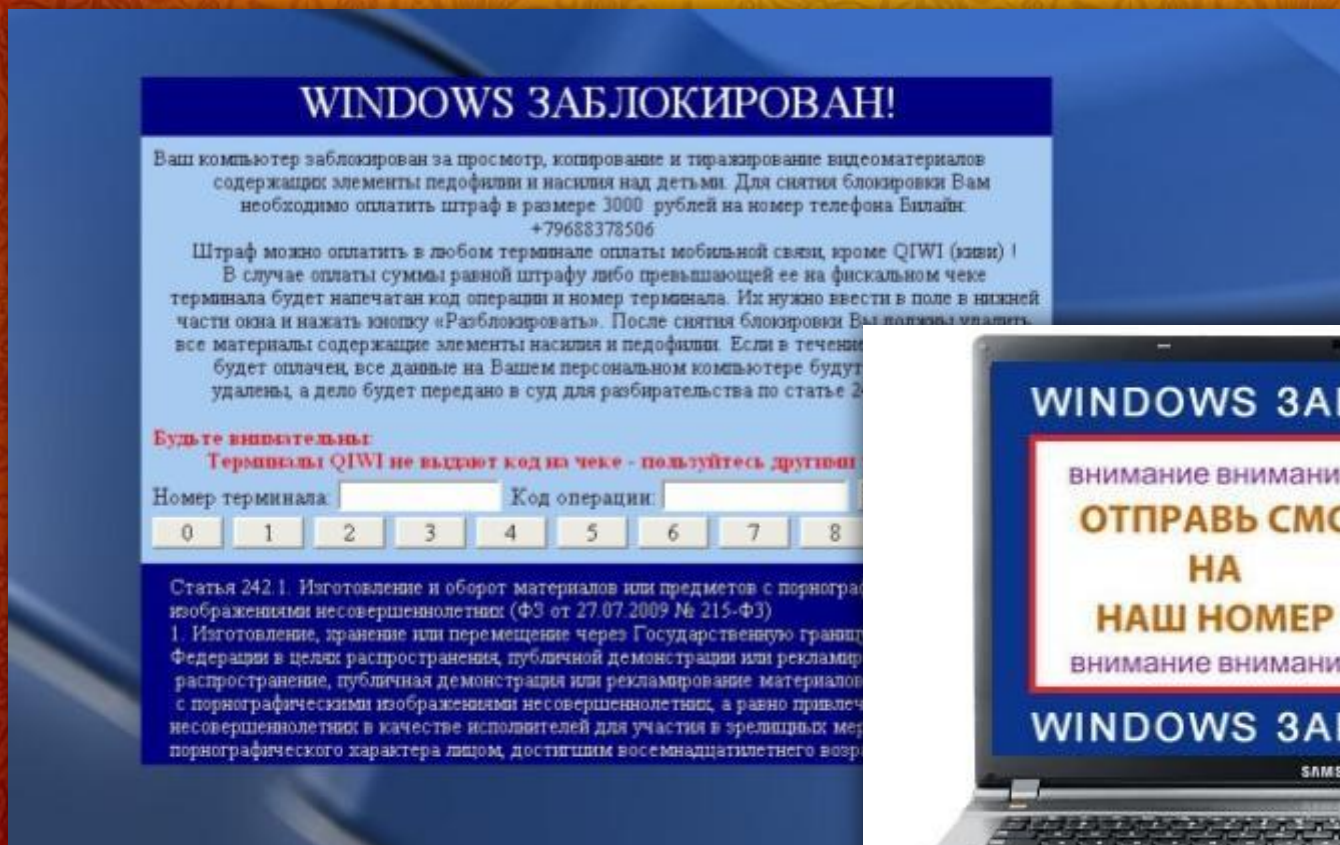


Троя́нская программа (также — троя́н, троя́нец, троя́нский конь) — это разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от *вирусов* и *червей*, которые распространяются самопроизвольно.

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: *сбор информации и её передачу злоумышленнику, её разрушение или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях.*

Четвёртый приём. Блокирование операционной системы.

Еще один простой вариант получить доступ к ПК пользователя и его деньгам – заблокировать операционную систему и потребовать некоторые сведения и некоторую сумму за ее разблокировку.



Угроза № 3 . Интернет-зависимость.

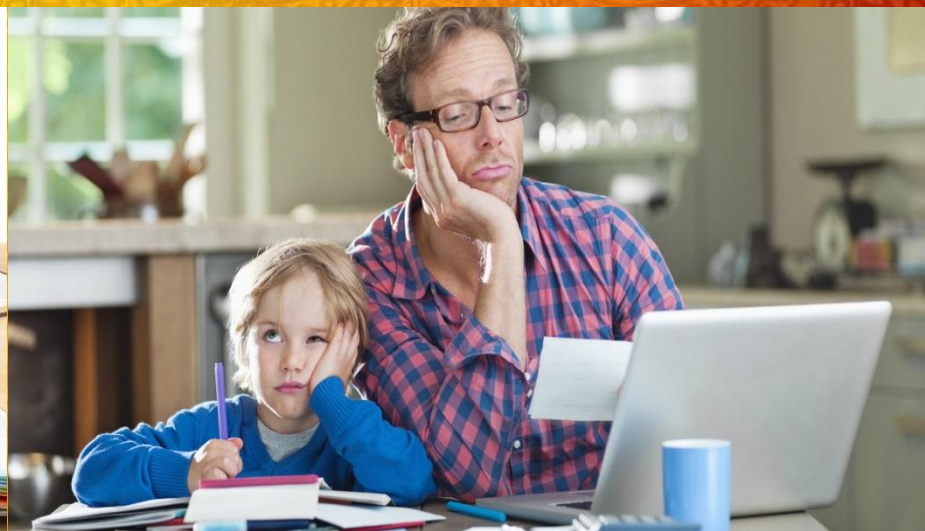
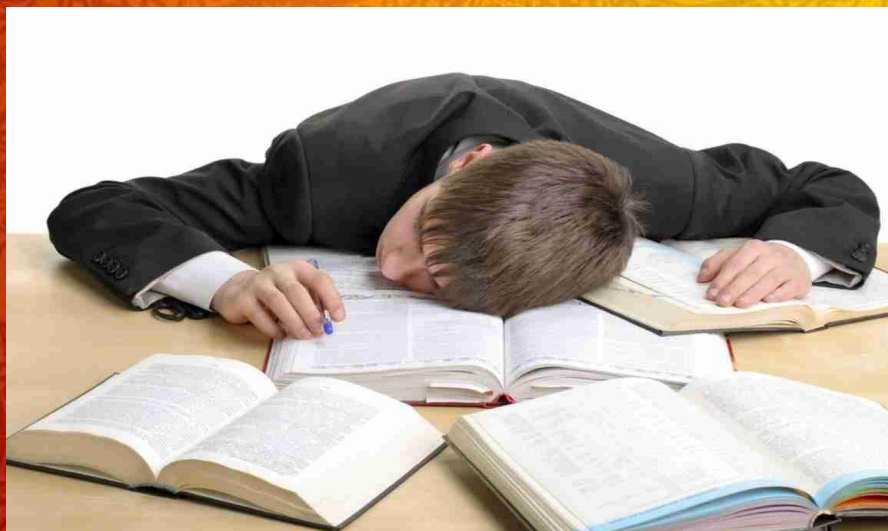
Детская и подростковая интернет-зависимость с каждым днем набирает все большие масштабы. Общение в социальных сетях заменяют общение с родителями и сверстниками, подвижные игры и физические занятия. Теряются коммуникационные навыки. Живые эмоции заменяются «веселыми смайликами».

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.

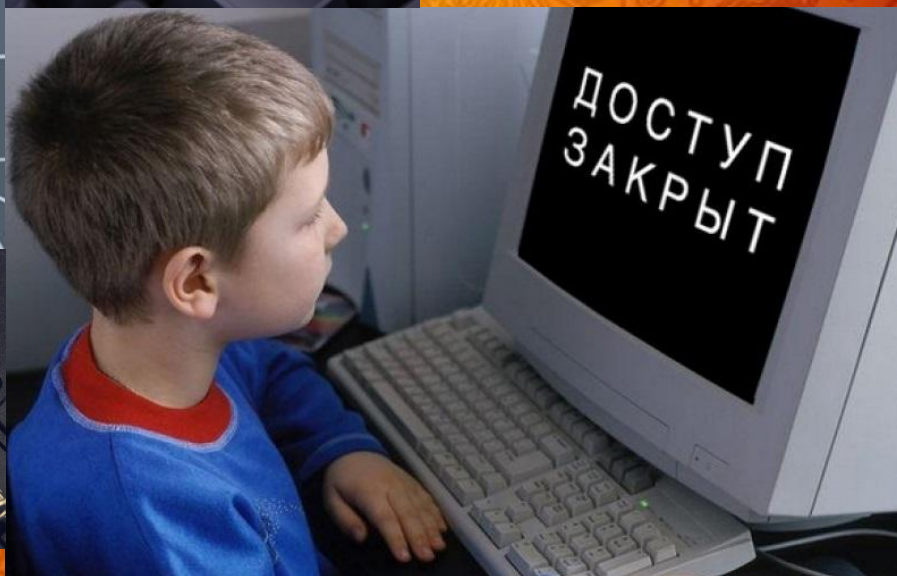
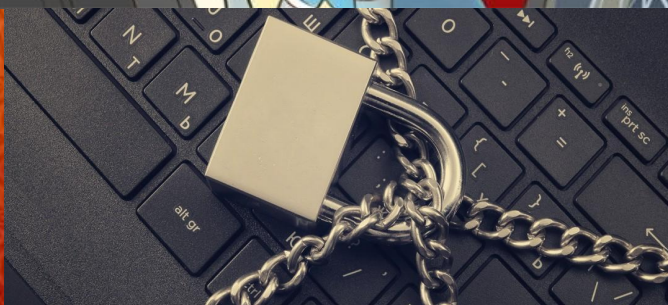
В Интернет много учебного материала, который становится доступным для студентов после процедуры скачивания, занимающей не более пяти минут. Подростки распечатывают нужный реферат и сдают его преподавателю, даже не удосужившись его прочитать. Таким образом, никакие знания получены не будут. Не в помощь 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.

Expectation Vs Reality

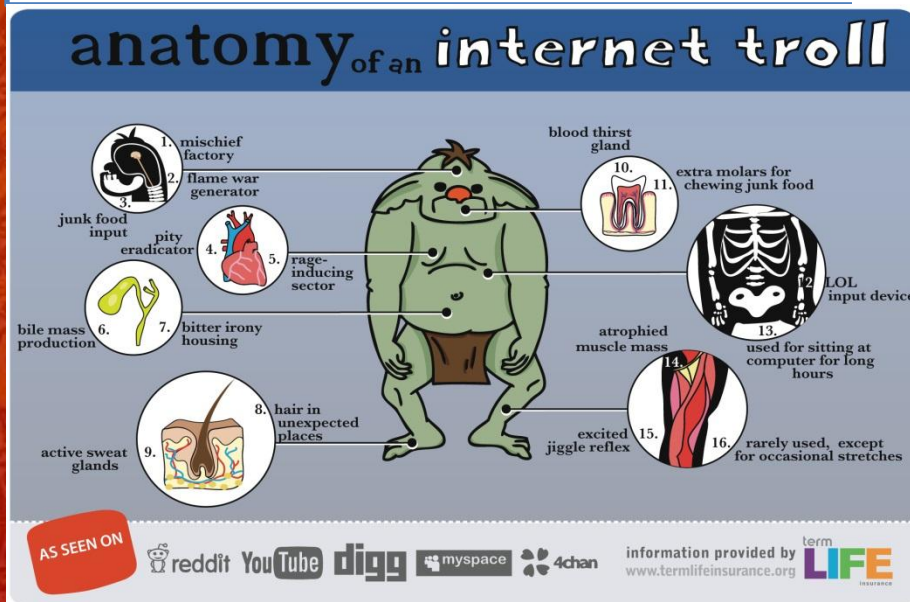


Важно знать, что по закону ответственность за содержание текста несёт не только автор, опубликовавший информацию, но и пользователь, распространивший её — поставивший отметку «Мне нравится» или скопировавший её на свою страницу.

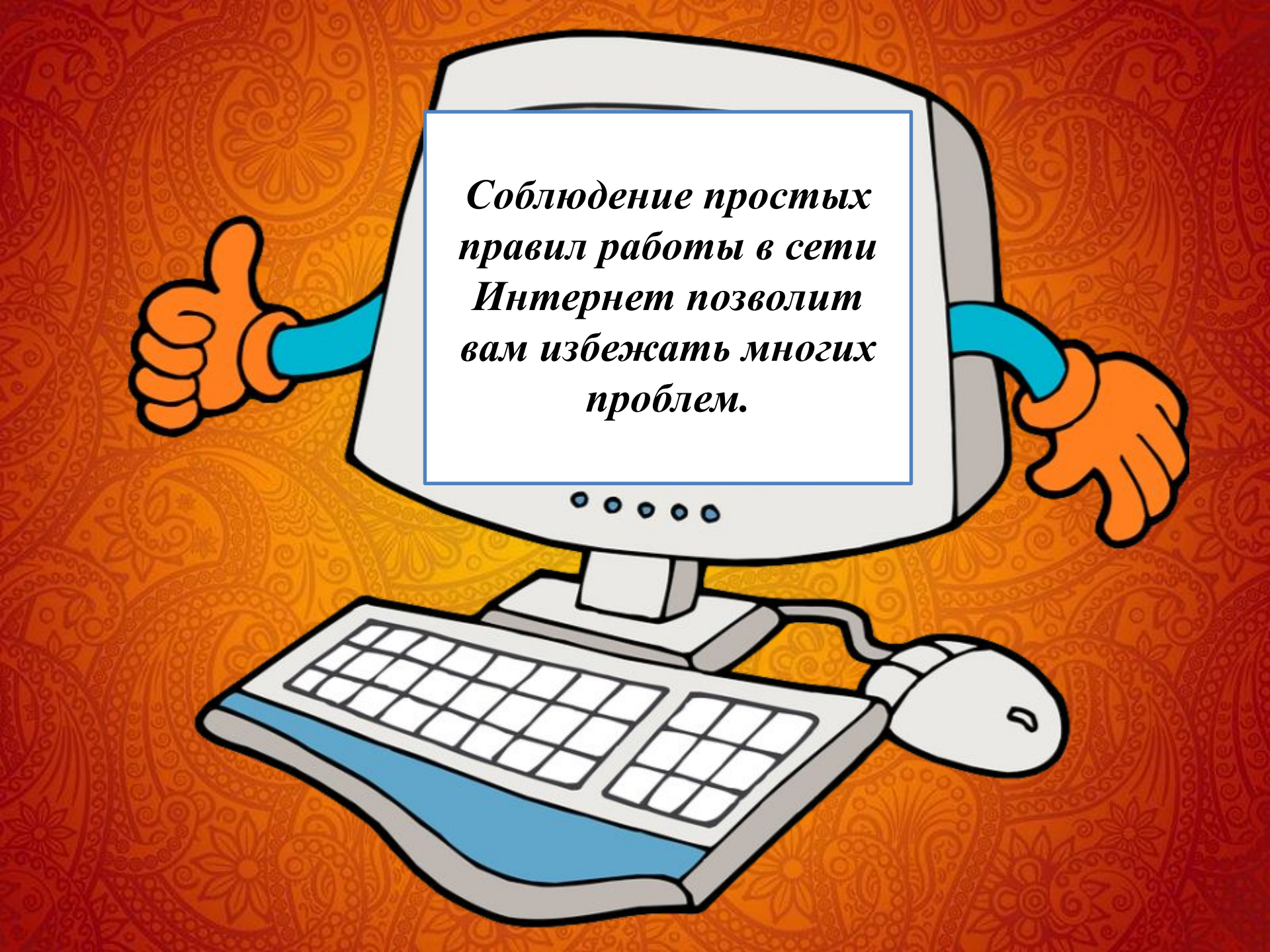
Угроза № 7. Интернет-хулиганство.

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

Иногда это выглядит как обычное развлечение, своеобразная переписка, но очень часто *троль* (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.



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