
БЕЗОПАСНЫЙ
ИНТЕРНЕТ

Перед подключением к Интернет, Вы должны подумать о том, как обезопасить себя и свои данные!

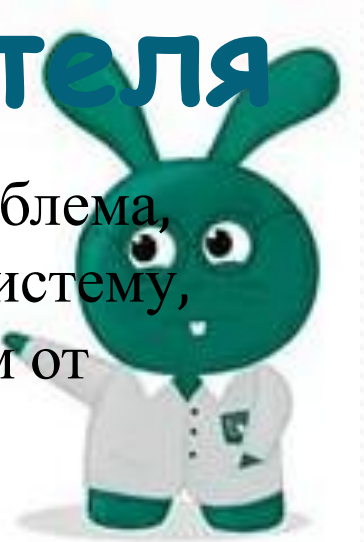
За очень короткий промежуток времени в интернете без надлежащей защиты, можно серьезно навредить своему компьютеру

Вирусы

- Компьютерные вирусы, сетевые и почтовые черви **распространяются самостоятельно**
- Троянские программы самостоятельно не распространяются, хотя они могут распространяться с помощью компьютерных вирусов.
  - Их основные цели – КРАСТЬ И УНИЧТОЖАТЬ


Credit Caru
John Smith
1234 5678 9101 1

Неосторожное поведение пользователя



- **Неосторожность пользователя –** это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере.

- ***Например***, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления важных данных.

Ошибки пользователей:

- Регистрация в социальной сети с предоставлением полной информации о себе (личные данные, контактный телефон, паспортные данные)
- Переход на сайт по активной ссылке рекламного блока
- Оплата сомнительных товаров с помощью банковской карты по непроверенным сайтам
- Предоставление посторонним лицам логина и пароля от своего компьютера, электронной почты
- Скачивание материала с непроверенных источников

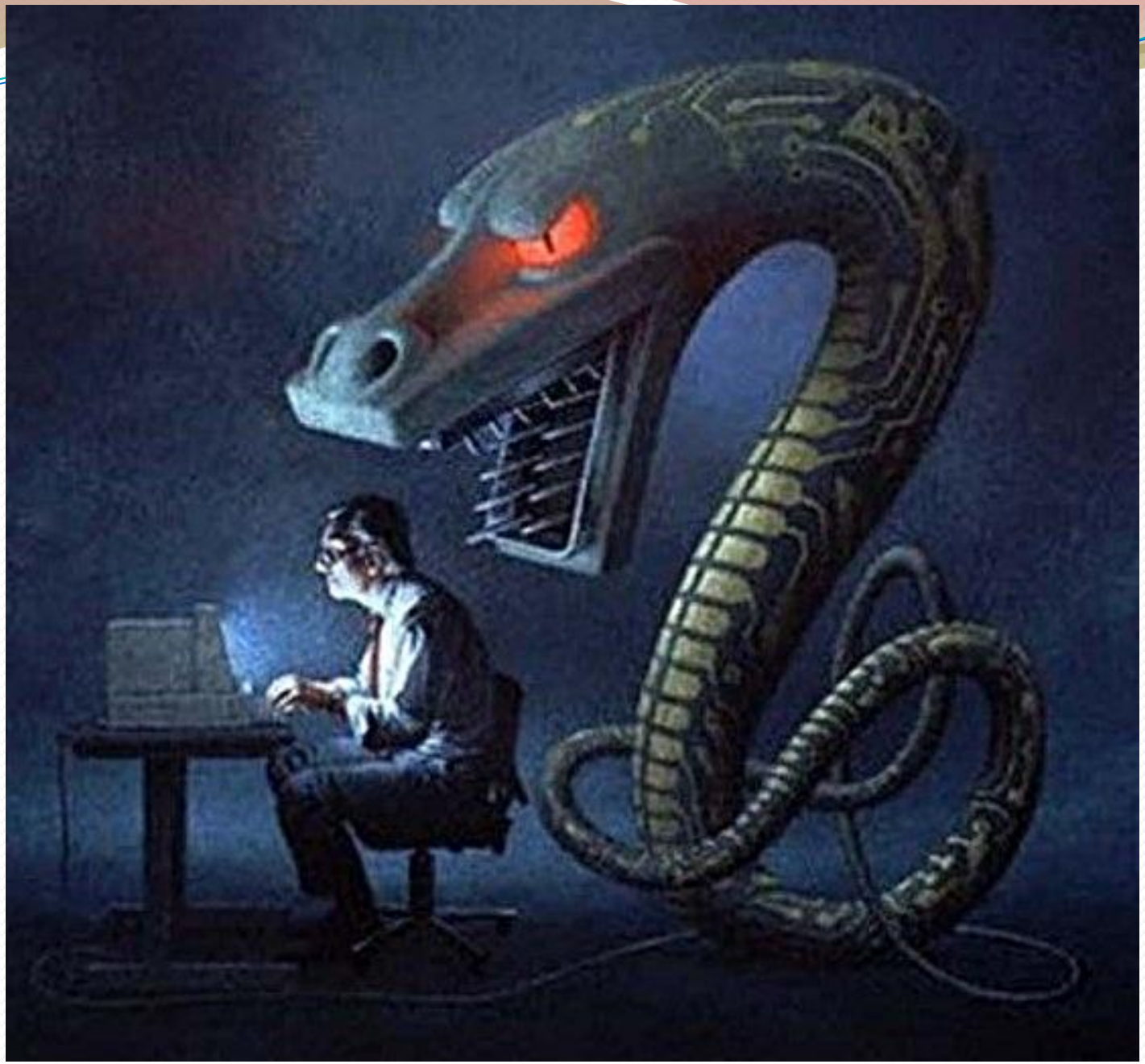
Источники опасностей

- **Социальная инженерия —** метод, основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение
- **Список уловок, придуманных хакерами в расчёте на доверчивость пользователей**. Вам могут прислать письмо от имени администрации сервиса с просьбой выслать им якобы утерянный пароль или письмо, содержащее безобидный, якобы файл, в который на самом деле спрятан троян, в расчёте на то, что из любопытства вы сами его откроете и запустите вредоносную программу.

- **Трояны и вирусы** могут быть **спрятаны в различных бесплатных, доступных для скачивания из интернета программах** или на пиратских дисках, имеющихся в свободной продаже.

- Взлом вашего компьютера может быть произведён через «дыры» в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно

- **Фишинг** - создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д. Цель - украсть данные вашего аккаунта (т. е. логин и пароль), которые вы обычно вводите на странице настоящего сайта.



Безопасность

- Использование антивирусных программ
- Своевременное скачивание и установка всех критических обновлений для Windows, Internet Explorer и т. п.
- Не устанавливайте или удалите лишние ненужные службы Windows, которые не используете
- Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы и не переходите по содержащимся в них подозрительным ссылкам
- Не используйте простые пароли
- Будьте осторожны при выходе в интернет из мест общего пользования (например, интернет-кафе), а также при использовании прокси-серверов
- При использовании электронных платёжных систем, работа с ними через веб-интерфейс является менее безопасной, чем если вы скачаете и установите специальную программу
- Не посещайте порносайты и прочие подобные им ресурсы сомнительной тематики
- Даже если у вас безлимитный доступ, всё равно следите за трафиком

Спасибо за внимание ☺