БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Шумейко И.А. преподаватель ВАМК

Дикий мир интернета

Опасности интернета:

- Контакты с нежелательными людьми
- Нежелательные для просмотра или использования материалы
- Угроза безопасности компьютера

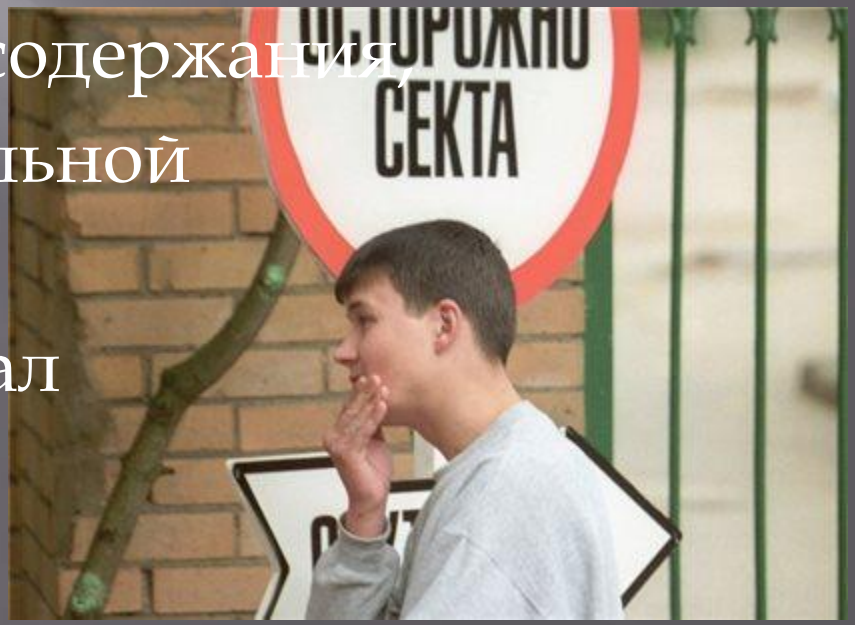
Контакты с нежелательными людьми, в том числе:

угроза со стороны интернет-хулиганов;

ики, расставляемые
для
ной
ас и вашей

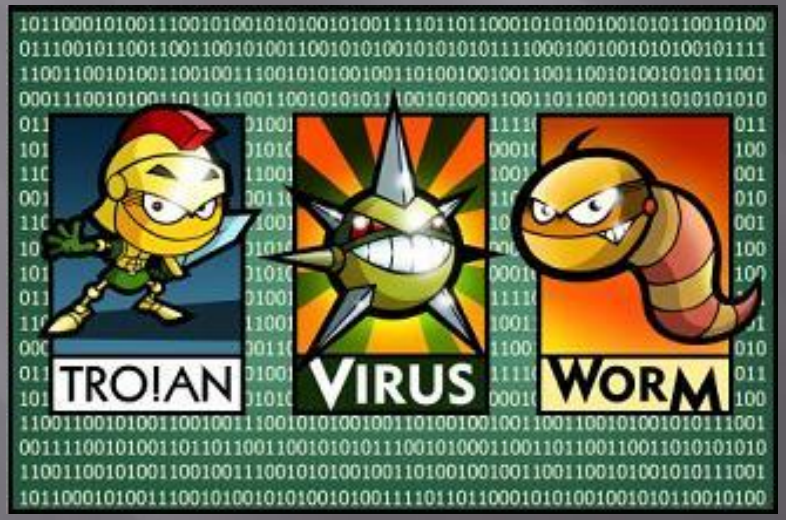
Нежелательные для просмотра или использования материалы

- материалы с ненормированной лексикой
- порнографического,
- ненавистнического содержания,
- материалы суицидальной направленности,
- сектантский материал

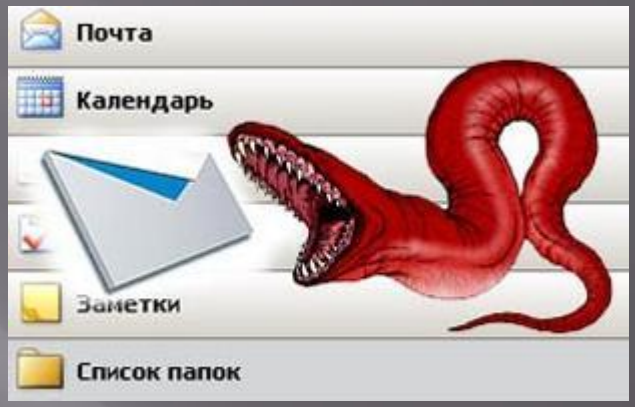


Угроза безопасности компьютера.

- **Попутная загрузка** – когда при простом посещении веб-сайта на компьютер автоматически загружается вредоносная программа.



- **Заражение через пиринговые сети (P2P)** – может предоставить доступ к компьютеру посторонним лицам.



- **Нежелательная реклама, всплывающие окна и рекламное ПО** – могут автоматически быть установлены при скачивании бесплатных программ или программ для обмена данными.

Спам и фишинг

Спам — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга.

Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками, цель которых:

- выудить деньги у некоторого количества получателей, ответивших на сообщение;
- провести фишинговую атаку, чтобы обманным путем получить пароли, номера кредитных карт, банковские учетные данные и т.д.;
- распространить вредоносный код на компьютерах получателей.

Защити себя:

- Никогда не предоставляйте секретные сведения (номер счета или пароль) в ответе на сообщение электронной почты, в чате и социальной сети
- Прежде чем вводить секретные сведения (номер счета или пароль) обратите внимание на адресную строку: куда уходят ваши сведения;
- Никогда не отвечайте на просьбы прислать деньги от «членов семьи», сообщений из лотерей, оставление задатков в намечающейся сделке и тд.;
- Используй сложные пароли.

Защити свой компьютер:

- Установите лицензионное антивирусное программное обеспечение;
- Постоянно обновляй свое программное обеспечение;
- Не переходи по ссылкам и не нажимай кнопки во всплывающих сообщениях, которые кажутся подозрительными;
- Не вставляй неизвестные флеш-носители в свой компьютер.

Используемые материалы:

- http://www.kaspersky.ru/internet-security-center/internet-safety/kids-online-safety
- http://www.google.ru/safetycenter/families/start/
- nruo.ru/bezeych.html
- Видео с конкурса «безопасный интернет – детям». – Автор: Евгений Бакал