Спам и способы борьбы с ним

История спама

- **1978**
  - первая рассылка по e-mail
- **1994**
  - первая рекламная рассылка в сети Usenet
- **1996-1998**
  - массовое распространение спама
  - более 50% всей почты - спам
- **1997**
  - появление средств для борьбы со спамом (DNSBL, SpamAssassin.org)
- **Наши дни**
  - спам во всех областях электронных коммуникаций

Что такое спам?

- Спам - рассылка сообщений по электронной почте
  - Незапрошенная
  - Массовая
  - Анонимная

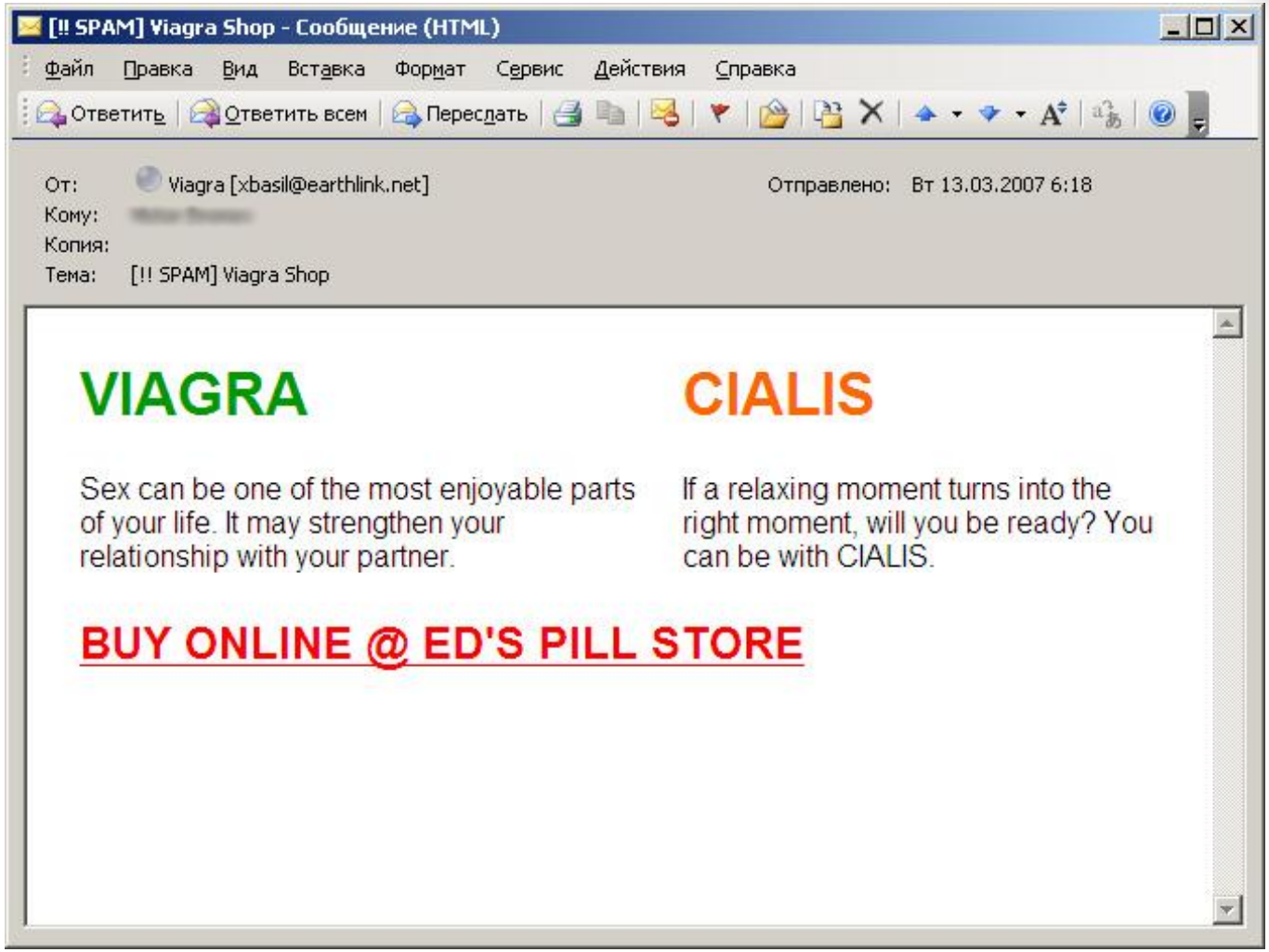
Что НЕ является спамом?

- Регулярные подписные рассылки
- Автоматические ответы серверов
- Рассылки «вручную» от менеджеров по продажам
- Просто «нежелательные» сообщения

Цели рассылки спама

- Реклама
- Мошенничество
  - фишинг
  - «нигерийские письма»
- Рассылка вредоносного ПО
- Черный PR, игра на бирже
- Политическая агитация

Пример рекламного спама



Спам – это выгодно

- Дешевый контакт с получателем для рекламодателя
- Доходы от рекламы для спамера
- Продажа/использование похищенных банковских данных
- Косвенные доходы от спама
  - при игре на бирже
  - агитации
  - PR и т.д.

Ущерб от спама

- Потеря времени сотрудников
  - до 2% общего рабочего времени
- Затраты времени ИТ-персонала
  - до 50% при работе с почтовыми системами
- Инвестиции в ИТ-инфраструктуру
  - до 90% нагрузки на сервера - спам
- Увеличение интернет-трафика
  - 70-90% всего почтового трафика - спам
- Риск вирусных атак и фишинга в спаме

Технологии рассылки спама

- Прямая рассылка
- Рассылка с выделенного сервера
- Рассылка через dial-up провайдеров
- Использование открытых релеев (Open Relay)
- Использование зомби-сетей

Длительность рассылки

- Дни
  - Прямая рассылка
  - Dial-up аккаунты
  - Открытые релеи
- Часы
  - Собственный сервер на площадке провайдера
  - «Медленные» зомби-сети
- Менее часа
  - «Быстрые» зомби-сети

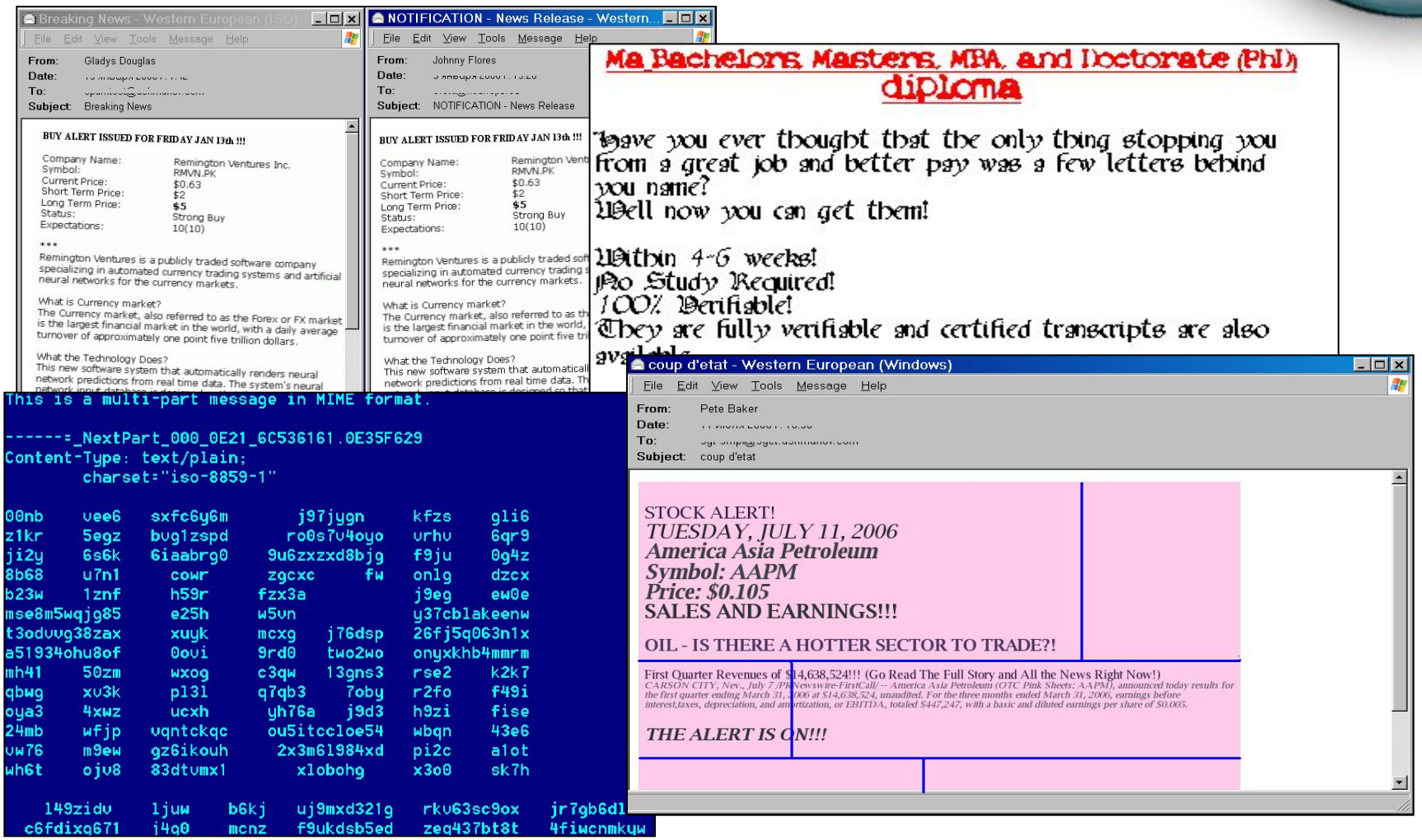
Базы адресов для рассылки

- Программы-роботы
  - поиск адресов на веб-страницах
  - в форумах
  - блогах и т.д.
- Продажа спамерам баз email-адресов своих клиентов нечистыми на руку компаниями
- Генерация случайных имен и использование словарей наиболее популярных имен (info@, sales@, john@ и т.д.)

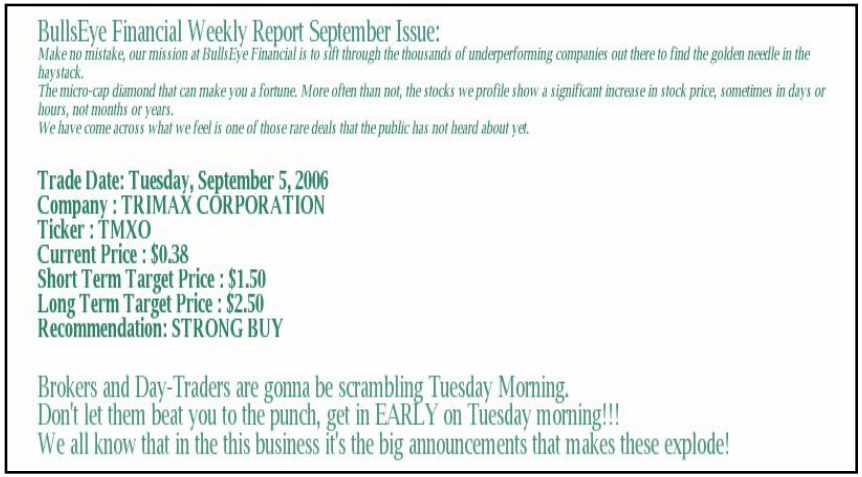
Приемы для обмана спам-фильтров

- Подмена адреса отправителя
- Искажения текста: V!A_GrA
- Мусорный текст – в конце письма, белый на белом и др.
- Спам в картинках
- Анимированный спам
- … множество других способов

Примеры графического спама



Анимированный спам: отдельные кадры



Приемы социальной инженерии

- Социальная инженерия – методы манипулирования человеком для побуждения его к неким действиям.

- Применение в спаме
  - Фишинг
  - Нигерийские письма
  - «Биржевой спам»

Спасибо!

Ваше мнение.