

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

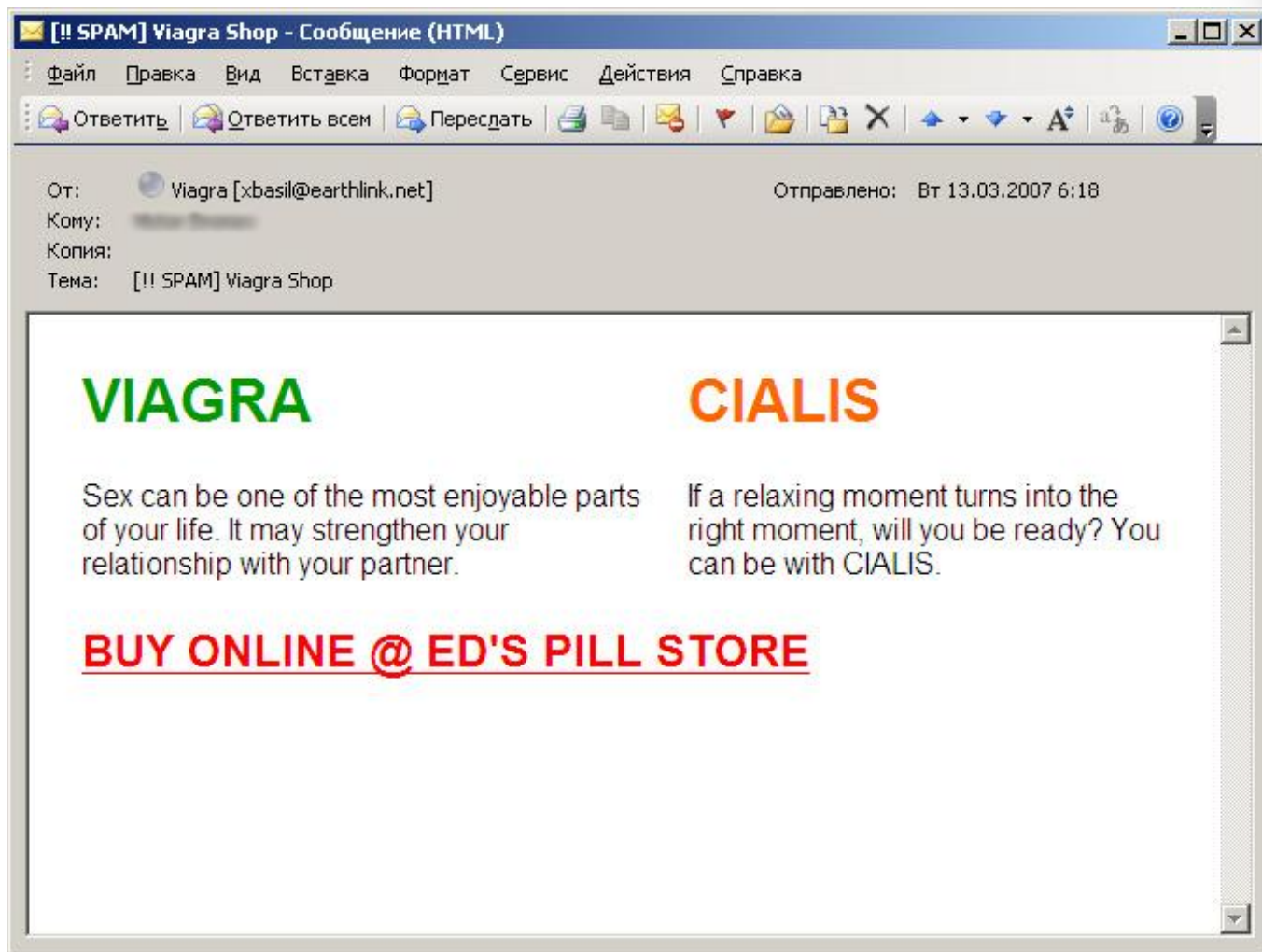
Что НЕ является спамом?

- 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

The image displays several screenshots of email clients and a multi-part message. The top row shows two windows: 'Breaking News - Western European (ISO)' and 'NOTIFICATION - News Release - Western...'. Both windows show a 'BUY ALERT ISSUED FOR FRIDAY JAN 13th !!!' for Remington Ventures Inc. (RMVN.PK) with a current price of \$0.63 and a status of 'Strong Buy'. The 'NOTIFICATION' window also features a red, stylized header: 'Ma Bachelors, Masters, MBA, and Doctorate (PhD) diploma' and promotional text: 'Have you ever thought that the only thing stopping you from a great job and better pay was a few letters behind your name? Well now you can get them! Within 4-6 weeks! No Study Required! 100% Verifiable! They are fully verifiable and certified transcripts are also available.' Below this is a window titled 'coup d'etat - Western European (Windows)' showing a 'STOCK ALERT!' for America Asia Petroleum (AAPM) on Tuesday, July 11, 2006, with a price of \$0.105 and 'SALES AND EARNINGS!!!'. The bottom section shows a blue terminal window with a multi-part message header: '-----_NextPart_000_0E21_6C536161.0E35F629 Content-Type: text/plain; charset="iso-8859-1"'. The body of the message is a grid of 4x4 alphanumeric characters.

-----_NextPart_000_0E21_6C536161.0E35F629
Content-Type: text/plain;
charset="iso-8859-1"

00nb	vee6	sxFc6y6m	j97jygn	kfzs	gli6	
z1kr	5egz	bvglzspd	ro0s7v4oyo	urhu	6qr9	
ji2y	6s6k	6iaabrg0	9u6zxzxd8bjg	f9ju	0g4z	
8b68	u7n1	cowr	zgcxc	fw	onlg	dzcx
b23w	1znf	h59r	fzx3a	j9eg	ew0e	
mse8m5wqjg85	e25h	w5vn	y37cblakeenw			
t3odvug38zax	xuyk	mcxg	j76dsp	26fj5q063n1x		
a51934ohu8of	0oui	9rd0	two2wo	onyxknb4mmrm		
mh41	50zm	wxog	c3qw	13gns3	rse2	k2k7
qbwg	xu3k	p13l	q7qb3	7oby	r2Fo	F49i
oya3	4xwz	ucxh	yh76a	j9d3	h9zi	fise
24mb	wfjp	vqntckqc	ou5itcc1oe54	wbqn	43e6	
uw76	m9ew	gz6ikouh	2x3m61984xd	pi2c	alot	
wh6t	oju8	83dtvmx1	xlobohg	x3o0	sk7h	
149zidu	ljum	b6kj	uj9mxd321g	rku63sc9ox	jr7gb6dl	
c6fdixq671	ij4q0	mcnz	f9ukdsb5ed	zeq437bt8t	4fiwcnmkw	

Анимированный спам: отдельные кадры

Buy!!!

BUY

Buy

BUY

Buy!!!

BUY BUY!

BullsEye Financial Weekly Report September Issue:

Make no mistake, our mission at BullsEye Financial is to sift through the thousands of underperforming companies out there to find the golden needle in the haystack.

The micro-cap diamond that can make you a fortune. More often than not, the stocks we profile show a significant increase in stock price, sometimes in days or hours, not months or years.

We have come across what we feel is one of those rare deals that the public has not heard about yet.

Trade Date: Tuesday, September 5, 2006

Company : TRIMAX CORPORATION

Ticker : TMXO

Current Price : \$0.38

Short Term Target Price : \$1.50

Long Term Target Price : \$2.50

Recommendation: STRONG BUY

Brokers and Day-Traders are gonna be scrambling Tuesday Morning.

Don't let them beat you to the punch, get in EARLY on Tuesday morning!!!

We all know that in the this business it's the big announcements that makes these explode!

Buy!

BUY!!!

BUY

Buy

BUY

Buy!!!

Buy

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.

