The State of Spam

A Monthly Report – February 2008

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Charles Var
PR Contact
charles_var@symantec.com

Contributors

Kelly Conley
Manager
Symantec Security Response

Joanne Mulcahy
Manager
Symantec Security Response

Francisco Manzano Pardano
Security Response Technician
Symantec Security Response

Pavlo Prodanchuk
Sr. Security Response Technician
Symantec Security Response

Hitomi Lin
Security Response Technician
Symantec Security Response

Niall O'Reilly
Security Response Technician
Symantec Security Response

Amanda Grady
Sr. Customer Response Analyst
Antispam Engineering

Kevin X Yu
Security Response Lead
Symantec Security Response

Shravan Shashikant
Pr. Business Intelligence Analyst
Antispam Engineering

Frank Kuang
Security Response Technician
Symantec Security Response

Joseph Long
Security Response Lead
Symantec Security Response

Paul O'Hagan
Security Response Lead
Symantec Security Response

Eric Chiu
Security Response Technician
Symantec Security Response

Jessica Lin
Security Response Technician
Symantec Security Response

Mayur Kulkarni
Security Response Lead
Symantec Security Response

Samir Patil
Security Response Lead
Symantec Security Response

Sohan Mirajkar
Security Response Technician
Symantec Security Response

Manish Satalkar
Security Response Technician
Symantec Security Response

Dylan Morss
Mgr, Business Intelligence
Antispam Engineering

Monthly Spam Landscape

While logic would dictate that spam levels would subside after the holidays, they've continued to soar and reached 78.5 percent of al email traffic during January. Another surprise this month was that spam originating in Europe outpaced messages originating from North America.

Highlights from this month included:

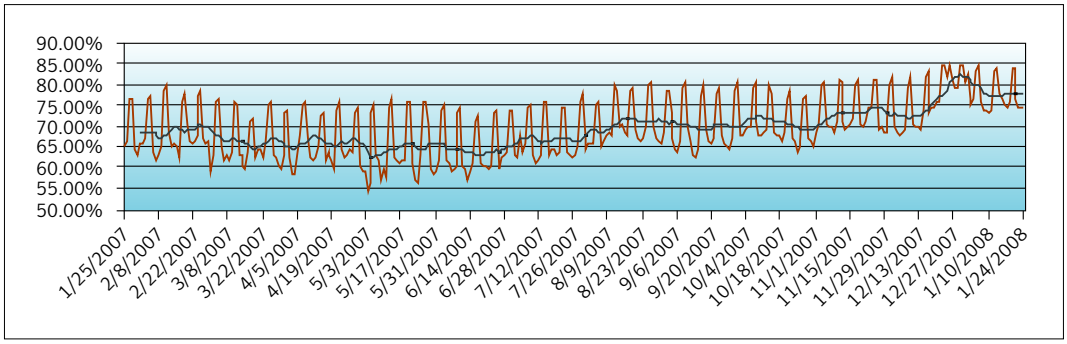
- **Europe Crowned New King of Spam** – The percentage of spam messages originating from Europe surpassed that of North America for the third-month in a row, representing a significant shift in where the bulk of the world's spam is "supposedly" sent from.
- **Will You Be My Valentines** – No Valentines? No problem. With Valentines Day right around the corner, spammers are targeting men with gift-giving ads, only to redirect them to a singles dating site. How romantic.
- **Surprise Tax Refund** – Playing on people's hope for a fat tax refund, spammers sent an official-looking email bearing the logo of the US Treasury Department, promising recipients an early and unexpected tax refund.
- **And Other Notable Activity** –
  - Average spam message size declines
  - Google search abuse by spammers continues
  - Resumes accepted for money laundering
  - Spammers offer a quick-fix solution to visa problems in Europe.
  - Russian spam offers porn site access via SMS message
  - Bizarre spam offerings
    - Naturally improve your genes
    - Rising gas prices lead spammers to bio-fuel

Percentages of Email Identified as Spam

Defined:

Worldwide Internet Mail Gateway Spam Percentage represents the number of messages that were processed and classified as spam versus the total number of messages processed when scanned at the mail gateway. This metric represents SMTP layer filtering and does not include the volumes of email detected at the network layer.

Internet E-mail Spam Percentage



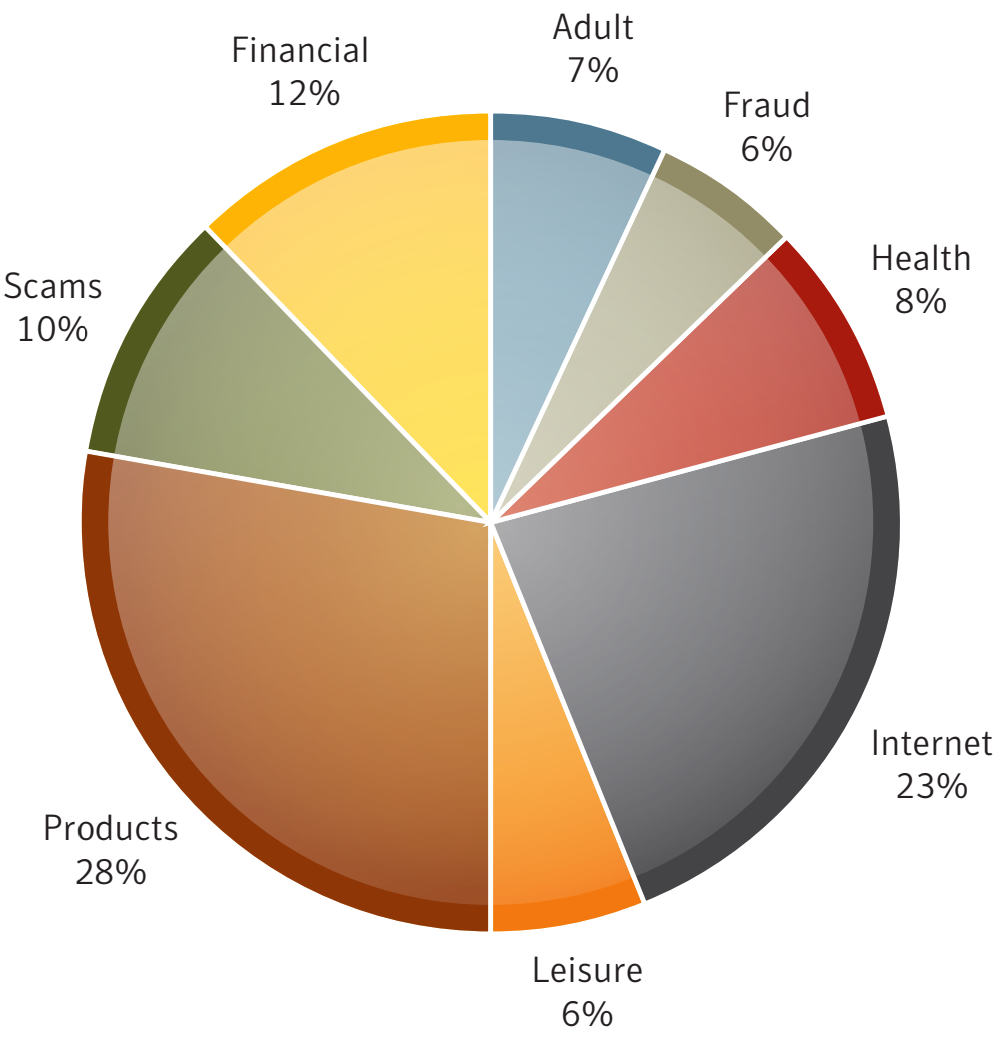
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

Spam category data is collected from classifications on messages passing through the Symantec Probe Network.

Global Category Count



Category Definitions

- **Product Email attacks** offering or advertising general goods and services. **Examples: devices, investigation services, clothing, makeup**

- **Adult Email attacks** containing or referring to products or services intended for persons above the age of 18, often offensive or inappropriate. **Examples: porn, personal ads, relationship advice**

- **Financial Email attacks** that contain references or offers related to money, the stock market or other financial "opportunities." **Examples: investments, credit reports, real estate, loans**

- **Scams Email attacks** recognized as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender. **Examples: Nigerian investment, pyramid schemes, chain letters**

- **Health Email attacks** offering or advertising health-related products and services. **Examples: pharmaceuticals, medical treatments, herbal remedies**

- **Fraud Email attacks** that appear to be from a well-known company, but are not. Also known as "brand spoofing" or "phishing," these messages are often used to trick users into revealing personal information such as email address, financial information and passwords. **Examples: account notification, credit card verification, billing updates**

- **Leisure Email attacks** offering or advertising prizes, awards, or discounted leisure activities. **Examples: vacation offers, online casinos, games**

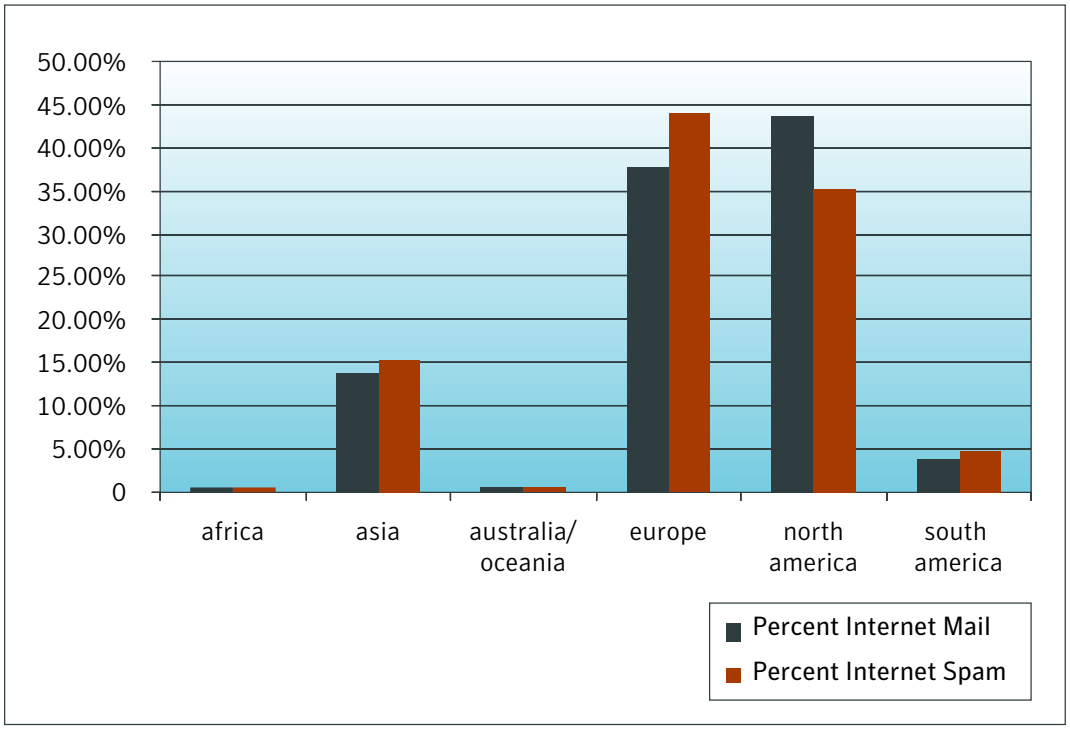
- **Internet Email attacks** specifically offering or advertising Internet or computer-related goods and services. **Examples: web hosting, web design, spamware**

Regions of Origin

Defined:

Region of origin represents the percentage of messages reported coming from each of the following regions in the last 90 days: North America, South America, Europe, Australia/ Oceania, Asia, and Africa.

Global Claimed Region of Origin



Europe Crowned New King of Spam

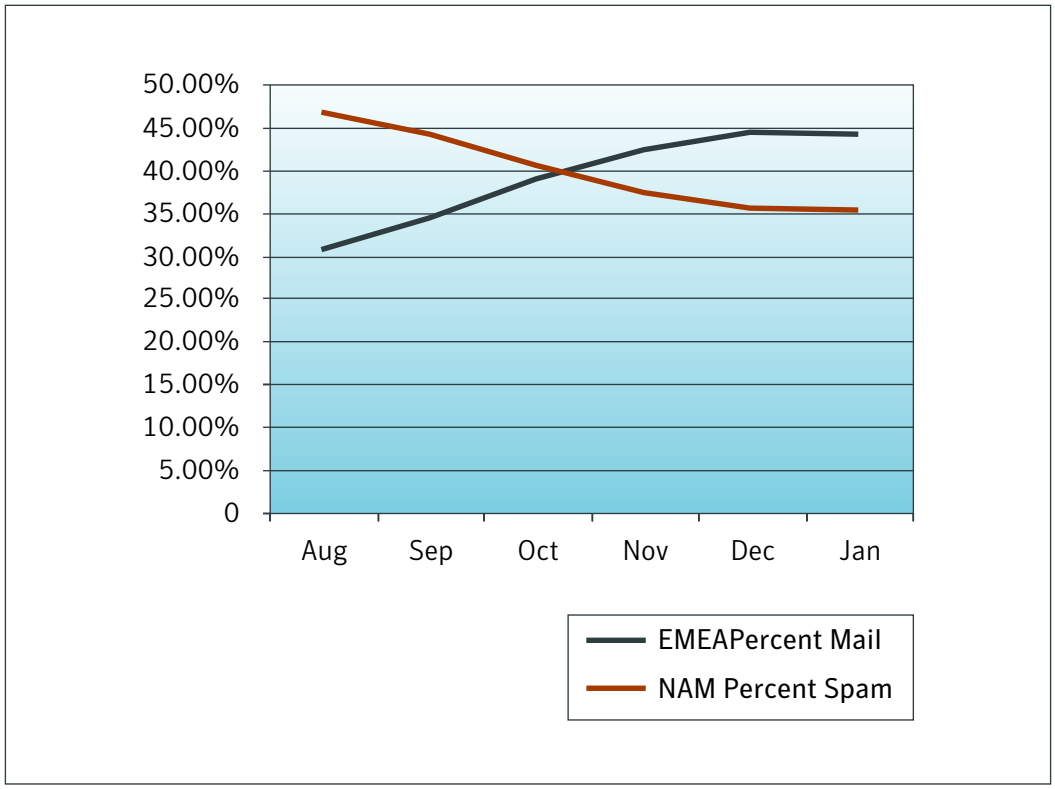
The percentage of spam messages that claimed to originate from Europe is now significantly greater than the percentage of spam messages originating from North America. Approximately 44 percent of all spam email now claims to originate from Europe versus 35.1 percent claiming to originate from North America. This new trend has occurred and remained constant in each of the last three months, beginning in November 2007. When Symantec first started recording this data in August of 2007, 30.6 percent of spam originated in Europe while 46 percent originated in North America.

It should be noted, however, that the nature of spam and its distribution on the Internet presents challenges in identifying the location of the people sending it. Many spammers redirect attention away from their actual geographic location. In an attempt to bypass DNS block lists, they use Trojans to relay email, allowing them to send spam from sites in different geographic locations. Therefore, the region in which spam originated may not always correspond with the region in which the spammers are located.

This sizeable increase in spam appearing to originate from Europe is significant but not altogether surprising when you consider the massive growth of broadband users in Europe in the last few years. The OECD report published June 2007 notes that while the United States has the highest number of broadband users at 66 million, Europe holds six out of the top ten countries for broadband users in the world. This phenomenal growth in percent spam originating in Europe may also be considered when you look at countries ranked by broadband subscribers per 100 inhabitants – European countries take eight of the top ten places.

Month Recorded	EMEA Percent Spam	NAM Percent Spam
August	30.6	46.5
September	34.2	44
October	38.7	40.3
November	42.2	37.3
December	44.4	35.3
January	44	35.1

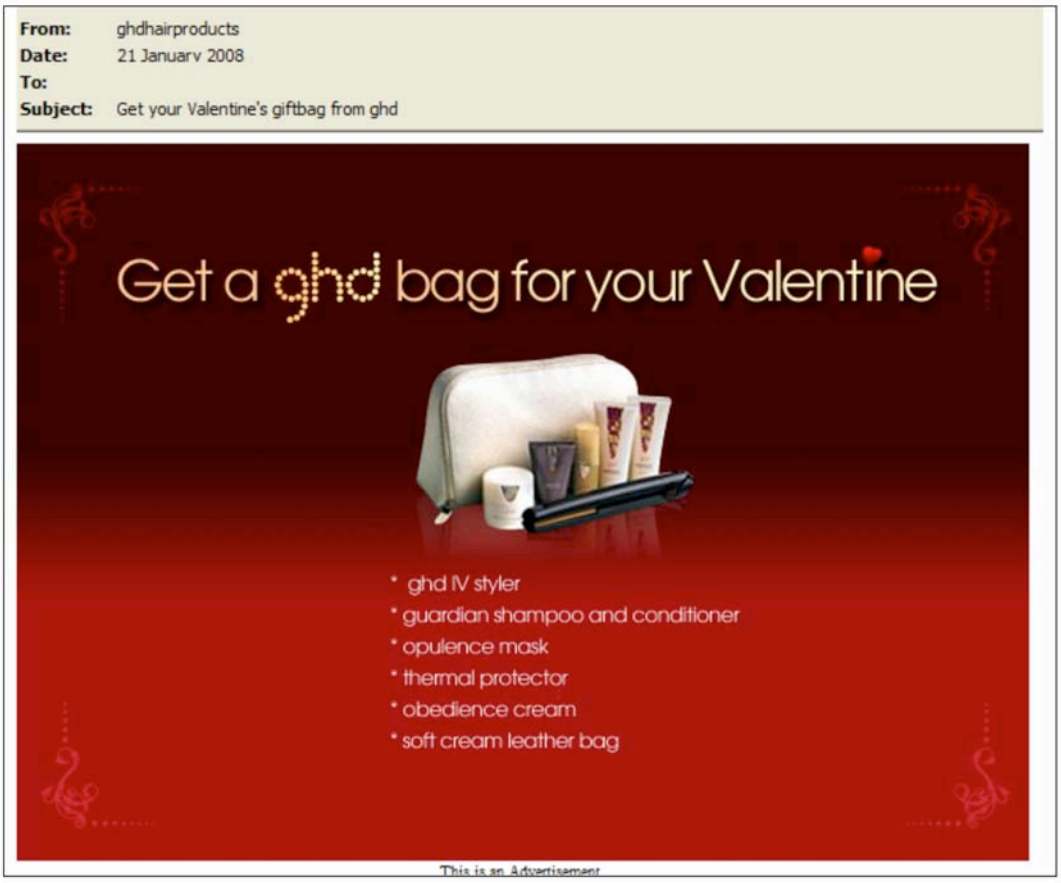
Claimed Region of Origon



Will You Be My Valentines

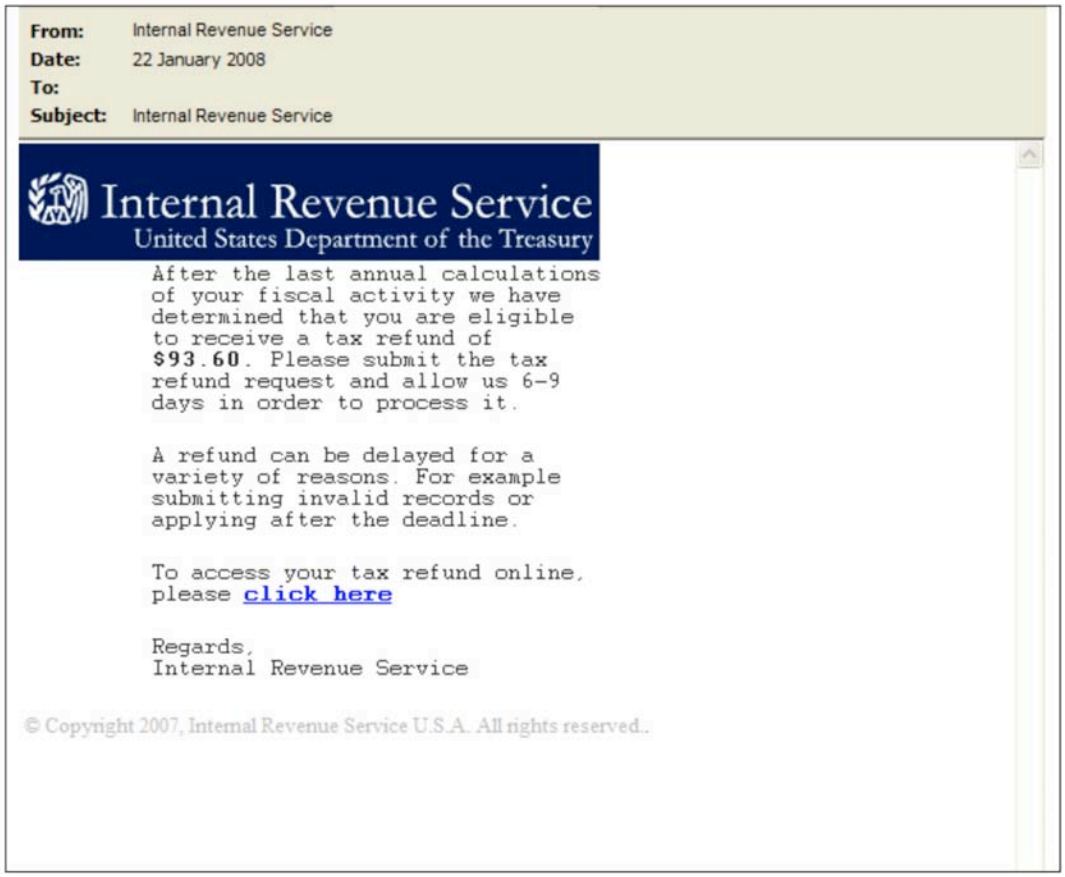
With Valentine's Day approaching and with most people not even thinking about what to get their loved ones until the 13th of February, the spammers are already out in force advertising their wares.

A recent spam trend is targeting men by urging them to "Get your Valentine's gift bag from ghd". The image in the email contains a picture of a designer hand bag filled with beauty care products. However when the image is clicked upon the recipient will see a message stating 'We're sorry this offer is not available in your area.' Depending on your location the recipient will be redirected towards another site. In Europe and some parts of Asia the user will be re-directed to a dating website. In North America the user is redirected to a bonus offer site and in India the user is redirected to a friends networking site. This modus operandi providing localized content that is 'relevant' to the users IP address location is a practice that has been used by some web sites/search engines for some time now so its not altogether surprising that the technique is now being utilized in some spam attacks.



Surprise Tax Refund

Instead of a tax rebate this tax season, US Citizens should beware of a sinister scam that may arrive in their inboxes. An email currently being circulated by spammers to look like it's from the IRS has been observed by Symantec. This spam email which seems to bear the logo of the US treasury department explains that a tax refund is due to the recipient. It encourages the recipient to click upon a URL link to access the refund online. The URL opens a webpage which asks the user if they want to want to "Get Tax Refund on your Visa or Mastercard". The recipient is then asked to enter their Social Security number, valid Visa or Mastercard number, name, address and many more personal details. The recipient is "helpfully" advised that "a refund can be delayed for a number of reasons". This allows the spammer enough time to use the personal information collected as they see fit.



From: Internal Revenue Service
Date: 22 January 2008
To:
Subject: Internal Revenue Service

Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **$93.60**. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access your tax refund online, please **click here**

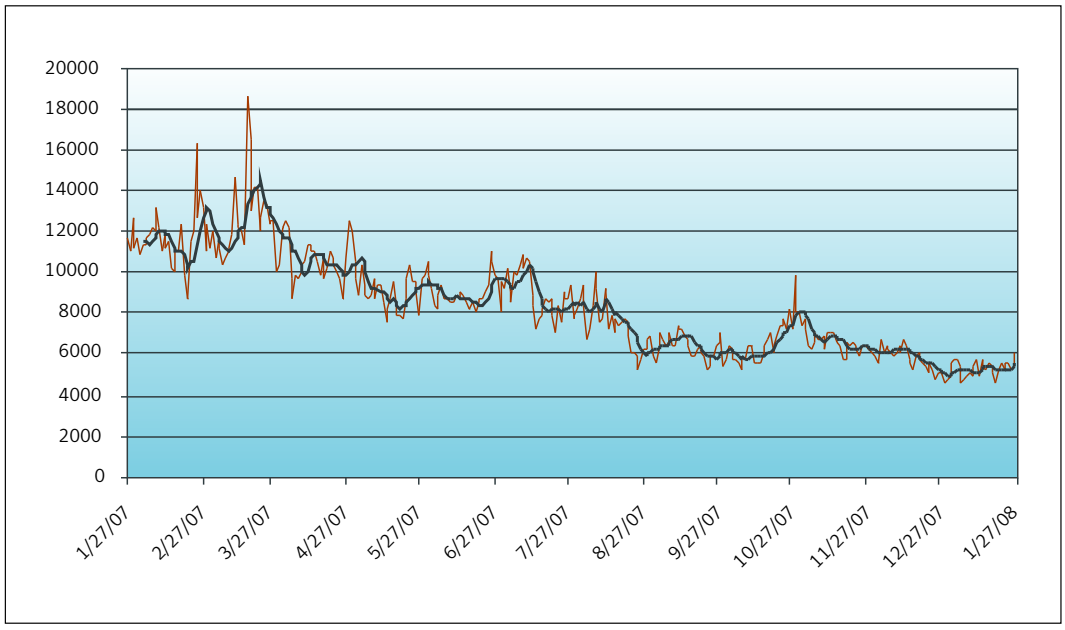
Regards,
Internal Revenue Service

Average Spam Message Size Declines

January 2007 saw Image spam reach its highest peak accounting for 52% of all spam. As Image spam decreased Symantec has observed that the average message size has also decreased significantly.

Average Message Size (bytes)

By analyzing Image spam recorded in the last 90 days Symantec notes that 84% of Image spam has an average size of between 10kB-50Kb. When you consider spam messages in total between November 2007 and January 2008, only 5% now fall into the 10kB- 50Kb with the majority (64%) of messages falling into the 2kB-5KB range. Large message size can put inordinate strains on mail infrastructures and could possibly prevent end users from receiving legitimate email. Further analysis by Symantec shows that the percentage of total spam that contains an attachment such as an Image accounted for less than 8% of all Spam in January 2008.



All Spam

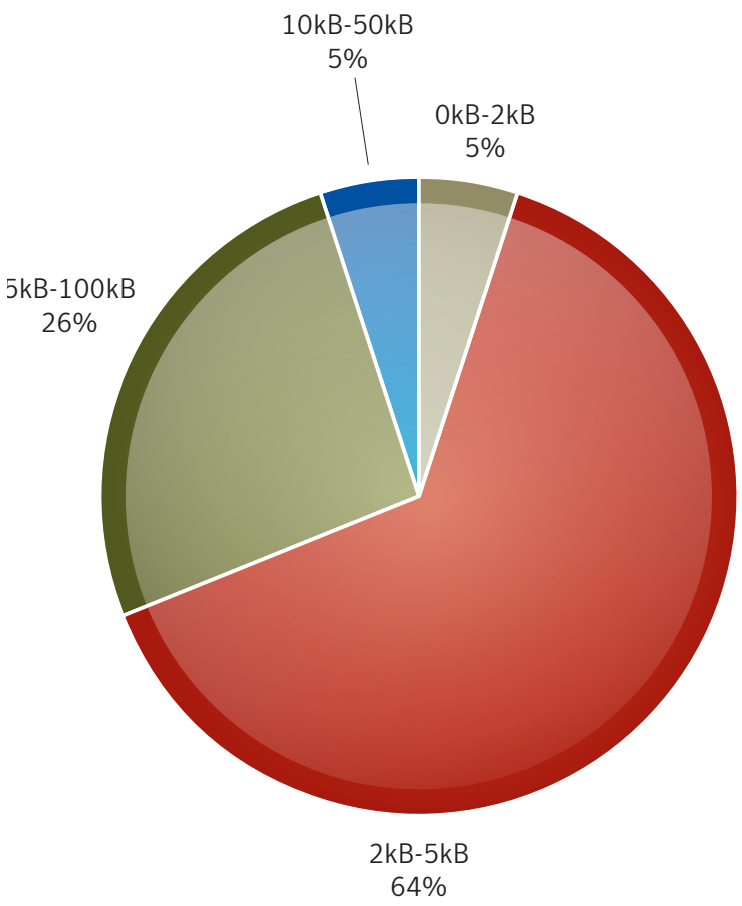
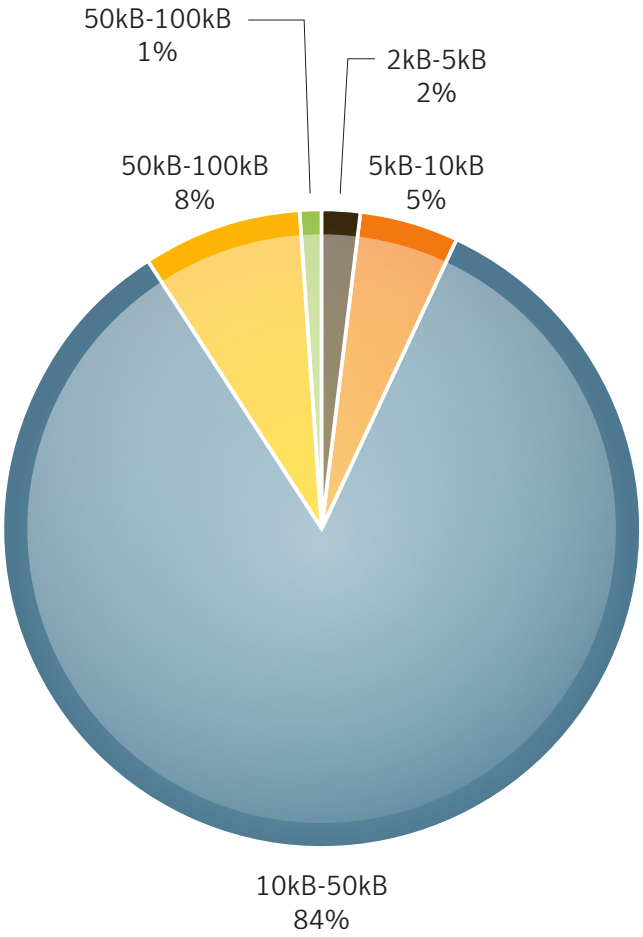
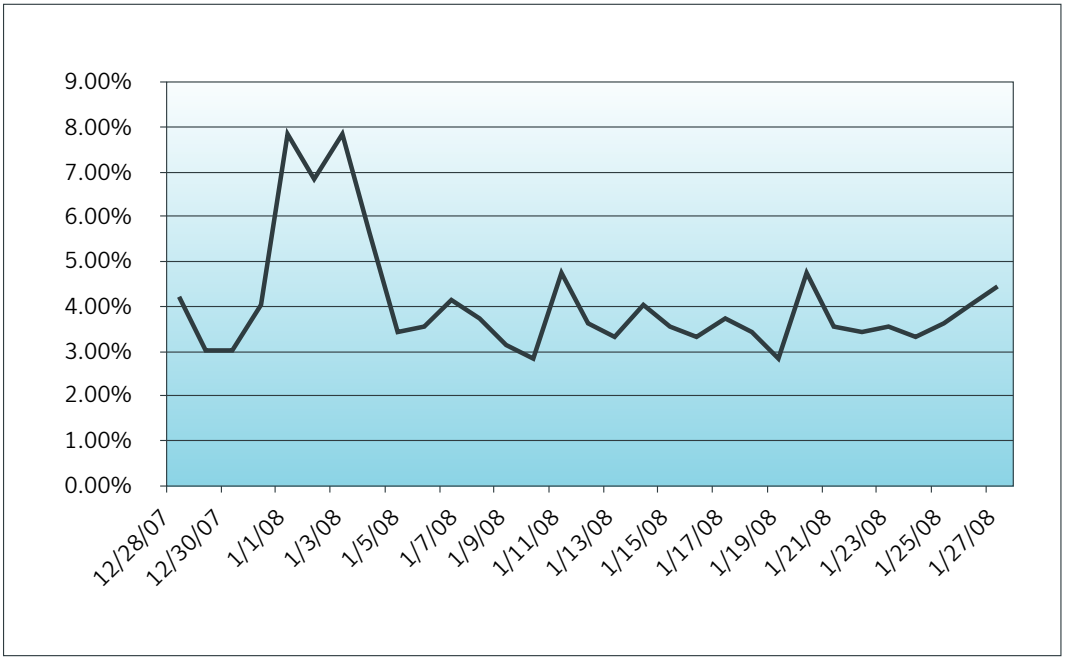


Image Spam



Percent of Total Spam that Contains an Attachment



Google Search Abuse by Spammers Continues

First reported in the Symantec State of Spam in November 2007, Spammers continue to exploit Google's search operators for its own means. This month Symantec has observed the introduction of the spam domain directly into the "Search String". The URL provided in the spam mail looks like a "Search String" but it when clicked upon it opens up the spam domain mentioned at the end of the URL rather than opening any search results. The TLDs associated with the Google domain are also changing.

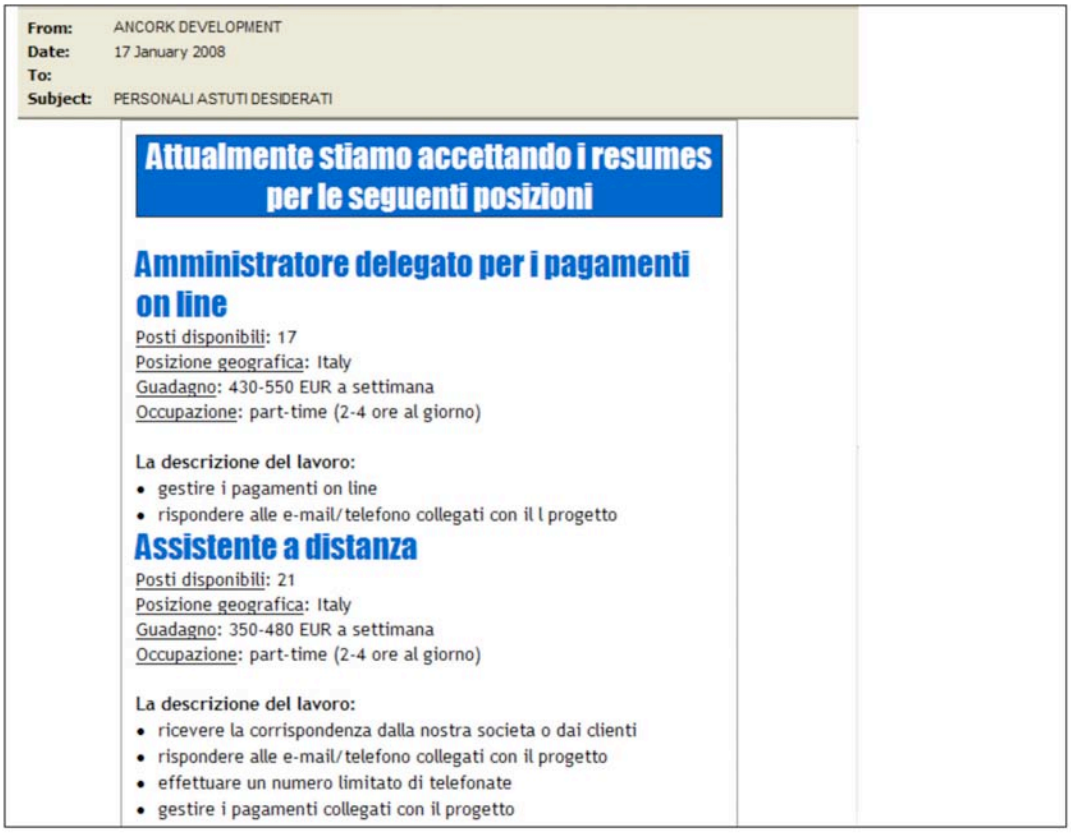
Resumes Accepted for Money Laundering

One of the most persistent Italian spam attacks in recent months has been this work from home job offer. The email states that "We are currently accepting resumes for the following positions" which are:

- Administrative Agents for Online Payments
- Remote Support Agent

For either position they write that you will only need to work 2-4 hours per day and can earn up to €550 a week. This could be quite a tempting offer as the current economic situation in Italy means it can be quite difficult to find employment, especially outside the major cities. The only requirement for this scam is that the applicant must live somewhere in Italy. Why is this? When cybercriminals succeed in obtaining bank details via phishing attacks or other scams, they often need to have access to a legitimate bank account in Europe, America etc. in order to make the transaction less suspicious and traceable. Anyone who fills out the simple email form is at risk in becoming involved in the world of "reciclaggio di denaro sporco" – literally recycling dirty money, or money laundering.

This particular attack is easily blocked by several of Symantec's filtering technologies, with only the subject and from line changing infrequently. At least 650,000 of these messages were blocked in January 2008 alone.



From: ANCORK DEVELOPMENT
Date: 17 January 2008
To:
Subject: PERSONALI ASTUTI DESIDERATI

Attualmente stiamo accettando i resumes per le seguenti posizioni

Amministratore delegato per i pagamenti on line

Posti disponibili: 17
Posizione geografica: Italy
Guadagno: 430-550 EUR a settimana
Occupazione: part-time (2-4 ore al giorno)

La descrizione del lavoro:
- gestire i pagamenti on line
- rispondere alle e-mail/telefono collegati con il l progetto

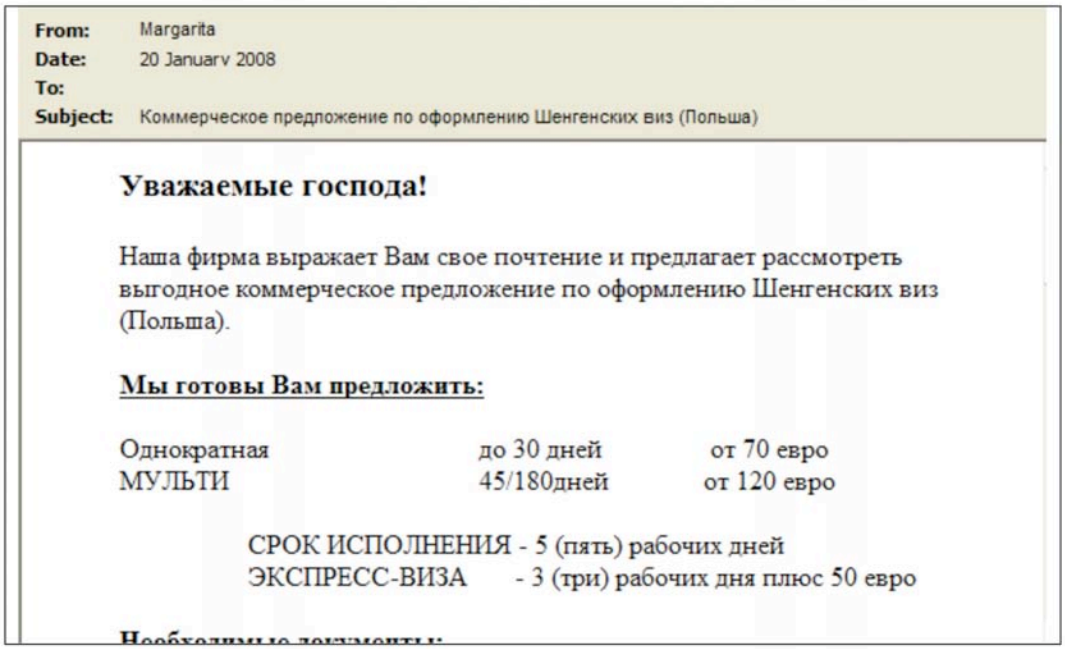
Assistente a distanza

Posti disponibili: 21
Posizione geografica: Italy
Guadagno: 350-480 EUR a settimana
Occupazione: part-time (2-4 ore al giorno)

La descrizione del lavoro:
- ricevere la corrispondenza dalla nostra societa o dai clienti
- rispondere alle e-mail/telefono collegati con il progetto
- effettuare un numero limitato di telefonate
- gestire i pagamenti collegati con il progetto

Spammers Offer Quick-fix Solution to Visa Problems in Europe

A recent political move to tighten restrictions on visas has resulted in the emergence of visa spam. Before signing up to the Schengen agreement in Dec 2007 Poland was a popular destination for many Russians and Ukrainians because it was relatively easy to obtain a visa. Visa spams offer recipients a way to skip the red tape. In the following example a company in Moscow promotes a quick and easy solution to get visas to Poland and other EU countries.



From: Margarita
Date: 20 January 2008
To:
Subject: Коммерческое предложение по оформлению Шенгенских виз (Польша)

Уважаемые господа!

Наша фирма выражает Вам свое почтение и предлагает рассмотреть выгодное коммерческое предложение по оформлению Шенгенских виз (Польша).

Мы готовы Вам предложить:

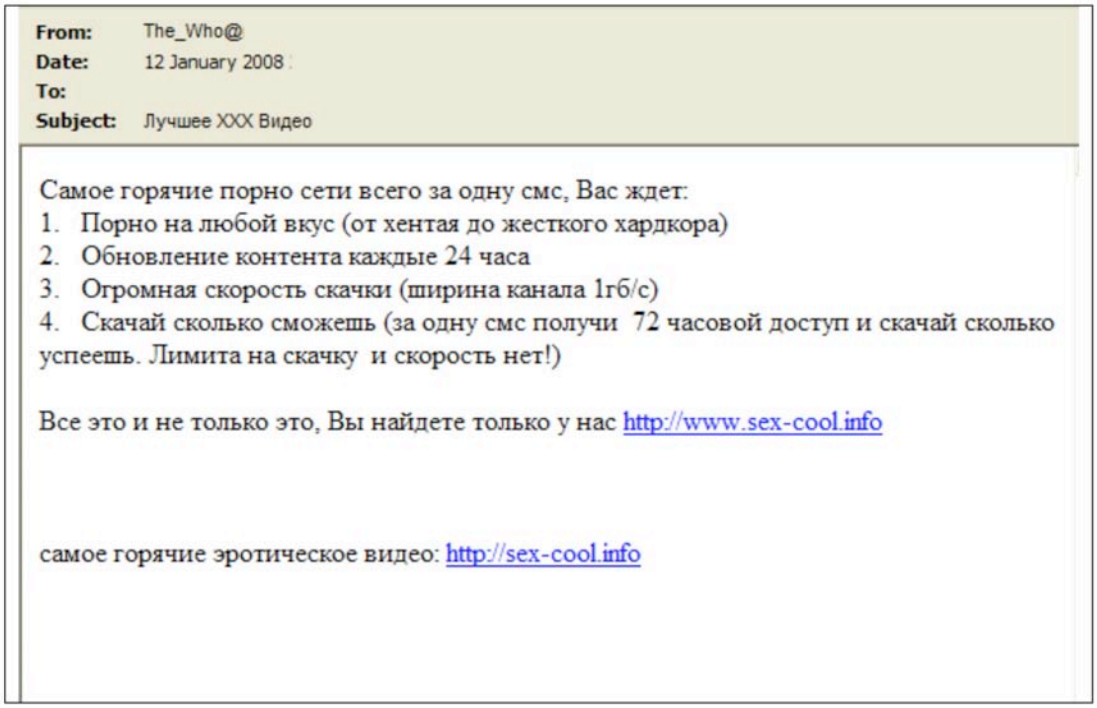
Однократная	до 30 дней	от 70 евро
МУЛЬТИ	45/180дней	от 120 евро

СРОК ИСПОЛНЕНИЯ - 5 (пять) рабочих дней
ЭКСПРЕСС-ВИЗА - 3 (три) рабочих дня плюс 50 евро

Необходимые документы:

Russian Spam Offers Porn Site Access Via SMS Message

Russian porn spam has been around for some time now. Russian porn spam typically contains an image and a spam URL link. Symantec has recently observed a new trend in Russian porn spam. The spam email contains the spammer's website and faked sender information, which is a noticeable feature of all Russian spam. However, unlike typical Russian spam instead of a regular registration service online, the email asks recipients to text their registration information via SMS before they can proceed further. Users must comply in order to receive subsequent pornographic services. The spammer claims that by registering through this SMS service the user will receive endless pornographic materials in the future. For every SMS sent by the user they will be charged $4.75USD. In effect the recipient is paying the spammer to receive personal information.



From: The_Who@
Date: 12 January 2008
To:
Subject: Лучшее XXX Видео

Самое горячие порно сети всего за одну смс, Вас ждет:
1. Порно на любой вкус (от хентая до жесткого хардкора)
2. Обновление контента каждые 24 часа
3. Огромная скорость скачки (ширина канала 1гб/с)
4. Скачай сколько сможешь (за одну смс получи 72 часовой доступ и скачай сколько успеешь. Лимита на скачку и скорость нет!)

Все это и не только это, Вы найдете только у нас http://www.sex-cool.info

самое горячие эротическое видео: http://sex-cool.info

Bizarre Spams

Over the course of many years, Symantec has seen spam products that range from the extreme to the downright bizarre. This month Symantec would like to highlight just a couple of these products.

Naturally Improve Your Genes

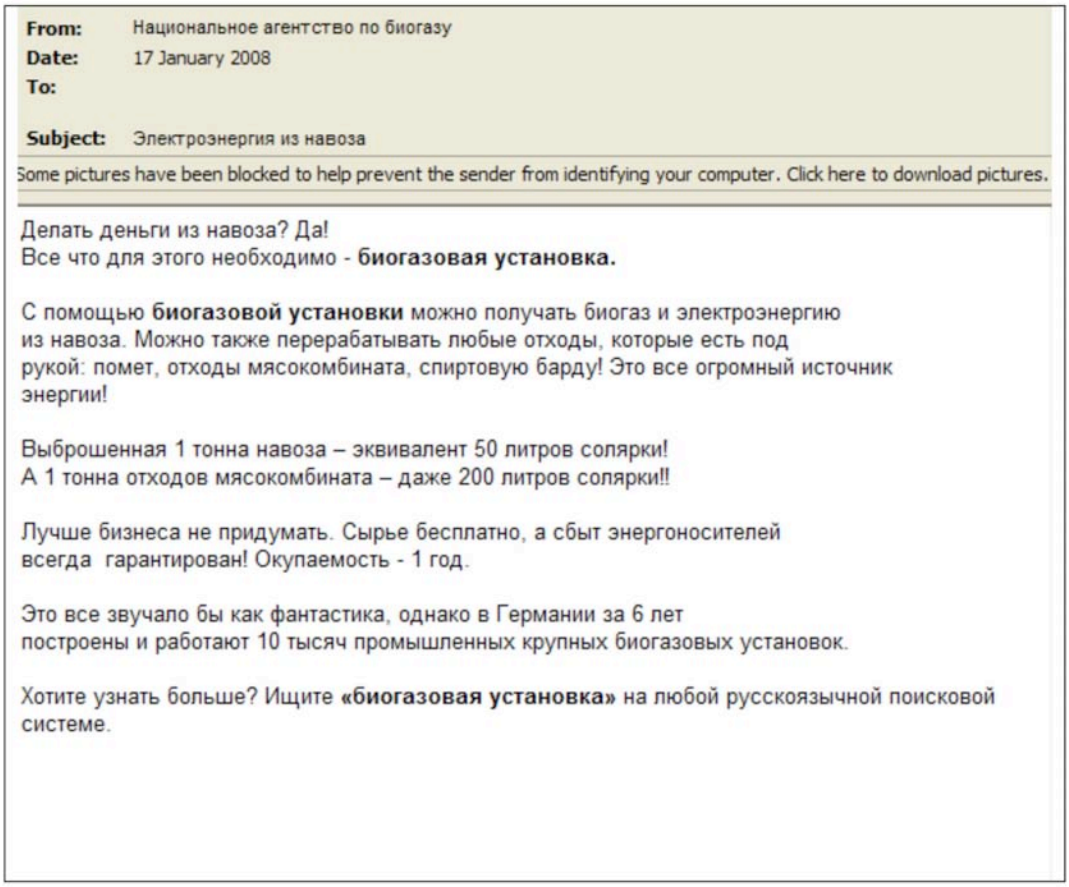
In the best tradition of quackery and Snake Oil, here it comes, the hippest, trendy medicine, with it share of (genetic) science, of course. This little jewel will cure obesity, depression, arthritis, cholesterol, even impotence! Plus, it will make you look younger! No drugs, no surgeries!

Rising Gas Prices Lead Spammers to Bio-fuel

Tired of high gas prices? Wish you had an endless supply of gas that you could sell or use? Spammers claim to have the answer to your problems. Symantec has observed some Russian spam that promotes a device that would allow the user to change manure into bio-fuel.

The hook the spammers are using to lure you into this enticing deal is based on the premise that the product buyer would be able to sell the electricity and gas made from the manure to friends and family. As the spammer claims “With 1 ton of manure equaling 50 litters of diesel fuel there is an opportunity to be had”.

The question is where to get your hands on a ton of manure and is it worth the effort?



From: Национальное агентство по биогазу
Date: 17 January 2008
To:

Subject: Электроэнергия из навоза

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

Делать деньги из навоза? Да!
Все что для этого необходимо - **биогазовая установка.**

С помощью **биогазовой установки** можно получать биогаз и электроэнергию из навоза. Можно также перерабатывать любые отходы, которые есть под рукой: помет, отходы мясокомбината, спиртовую барду! Это все огромный источник энергии!

Выброшенная 1 тонна навоза – эквивалент 50 литров солярки!
А 1 тонна отходов мясокомбината – даже 200 литров солярки!!

Лучше бизнеса не придумать. Сырье бесплатно, а сбыт энергоносителей всегда гарантирован! Окупаемость - 1 год.

Это все звучало бы как фантастика, однако в Германии за 6 лет построены и работают 10 тысяч промышленных крупных биогазовых установок.

Хотите узнать больше? Ищите **«биогазовая установка»** на любой русскоязычной поисковой системе.