# The State of Spam

## A Monthly Report – July 2007

*Generated by Symantec Messaging and Web Security*

Confidence in a connected world.

## Monthly Spam Landscape

Spam activity in June 2007 was overall consistent with trends observed in previous months. However, the decline in image spam first reported in the Symantec State of Spam report May 2007 does continue.

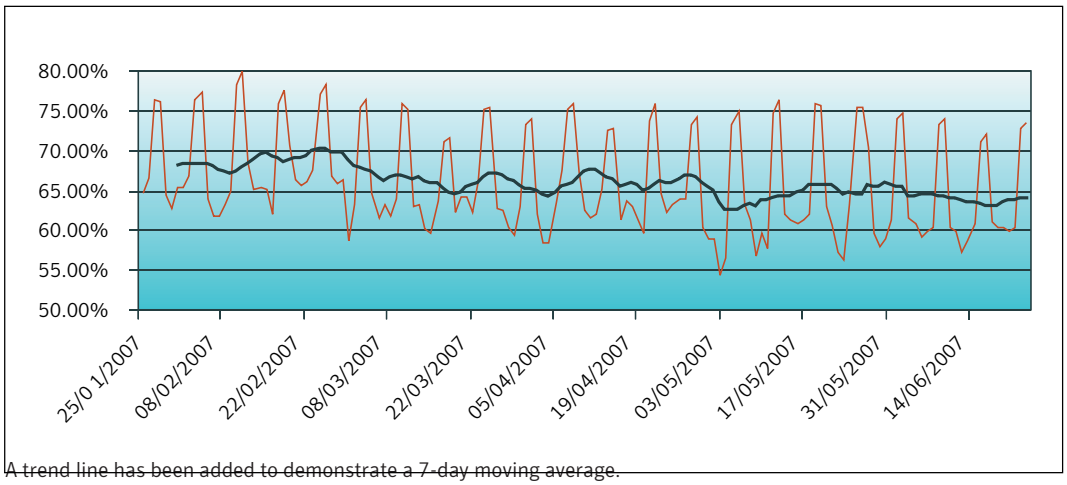
Highlights included:

- Image spam continued to decline to an average of 14.5% for the month of June, down from 27% and 37% in the months of April and March respectively. At its peak in January 2007, Symantec estimated that image spam accounted for nearly 52% of all spam. With the recent decline in image spam, Symantec has observed an increase in new spam techniques which reference spam images in different ways.
- Overall spam levels remained consistent for the month of June at the SMTP layer coming in on average around 65%.
- Scams and fraud spam combined continues to rise from 9% in March to 14% in June.
- Health spam declined from 23% in March to 13% in June
- Additional insight is provided below on the following tactics:
  - This month PDF image spam makes a splash
  - Free money anyone?
  - Current affairs used to peddle medication spam
  - As night follows day – Father's day spam follows Mother's day spam
  - DHA attacks taken to a different level
- Spam spotlight: Regional spam trends APJ

## 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.



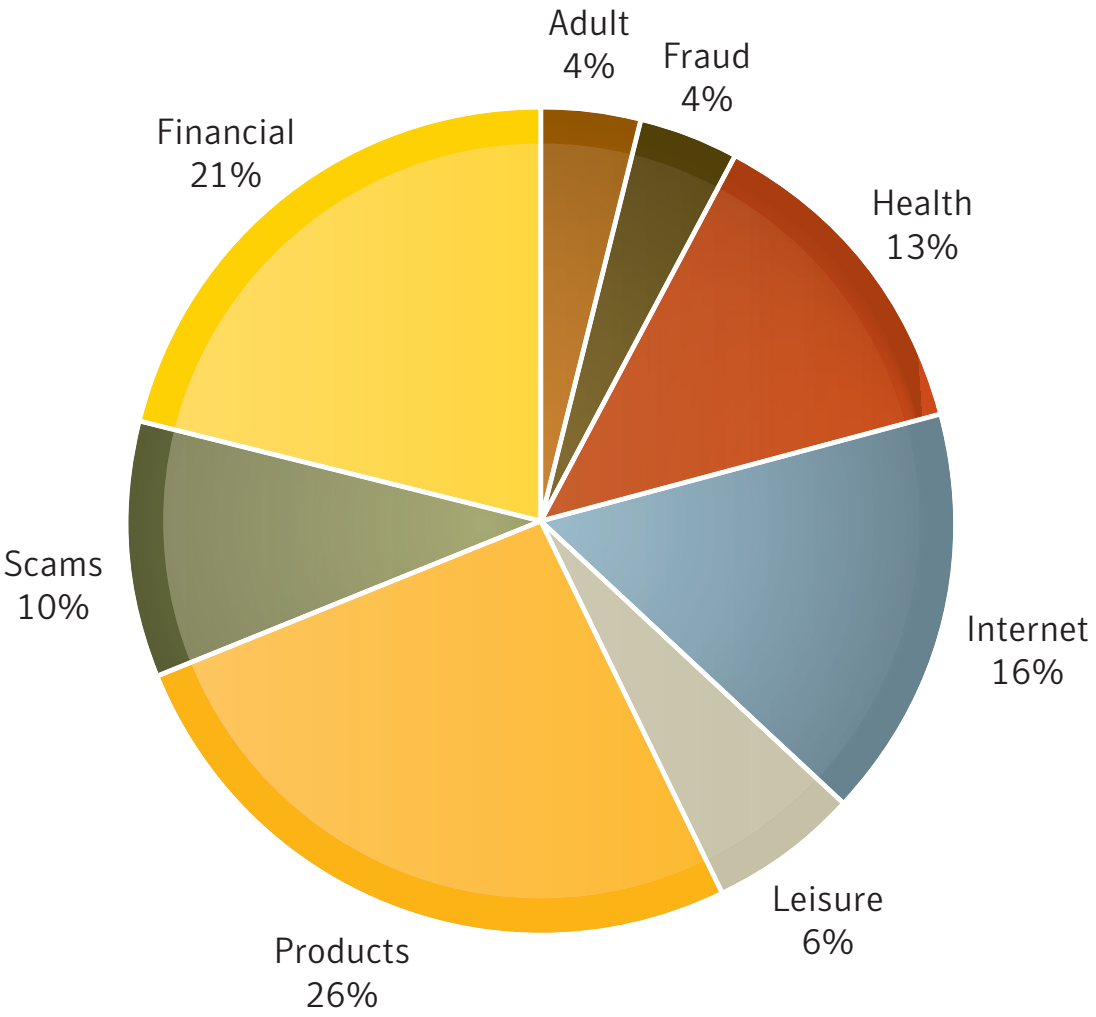

A trend line has been added to demonstrate a 7-day moving average.

## Global Spam Categories

**Defined**:

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

**Global Spam Categories (90 Days)**



## 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**

- **Political Messages** advertising a political candidate's campaign, offers to donate money to a political party or political cause, offers for products related to a political figure/campaign, etc. **Examples: political party, elections, donations**

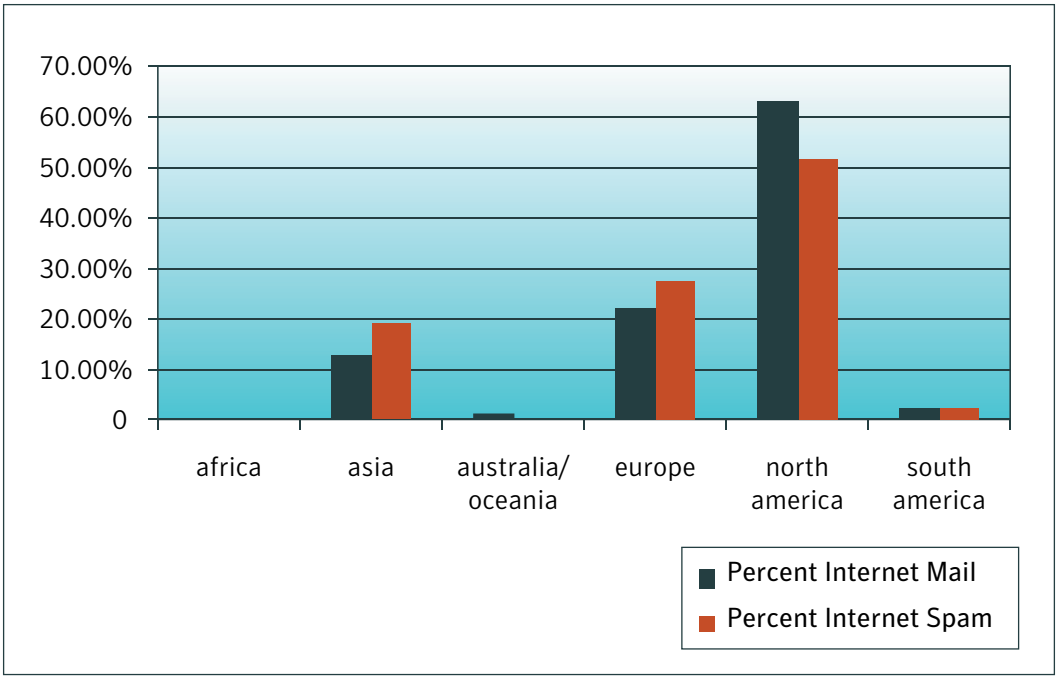
- **Spiritual Email attacks** with information pertaining to religious or spiritual evangelization and/or services. **Examples: psychics, astrology, organized religion, outreach**

- **Other Emails attacks** not pertaining to any other category.

## Regions of Origin

**Defined**:

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

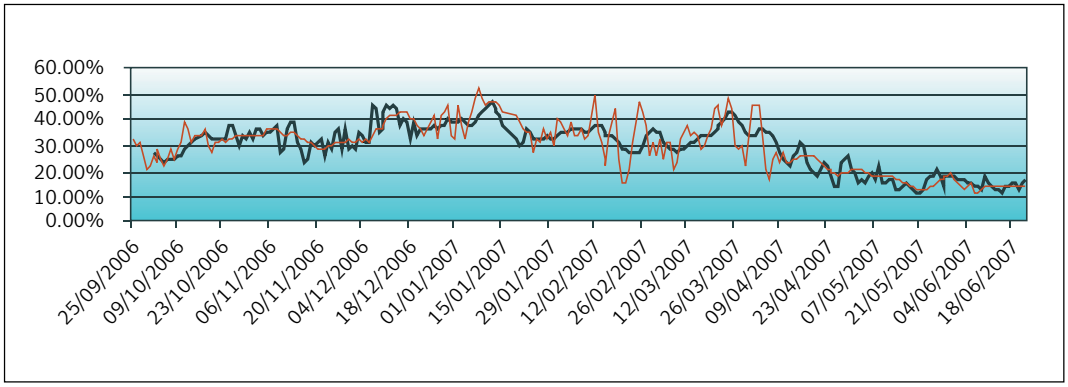


# Percent Image Spam

**Defined**:

The total number of image spam messages observed as a percentage of all spam observed.

**Internet Email – Percent Image Spam**



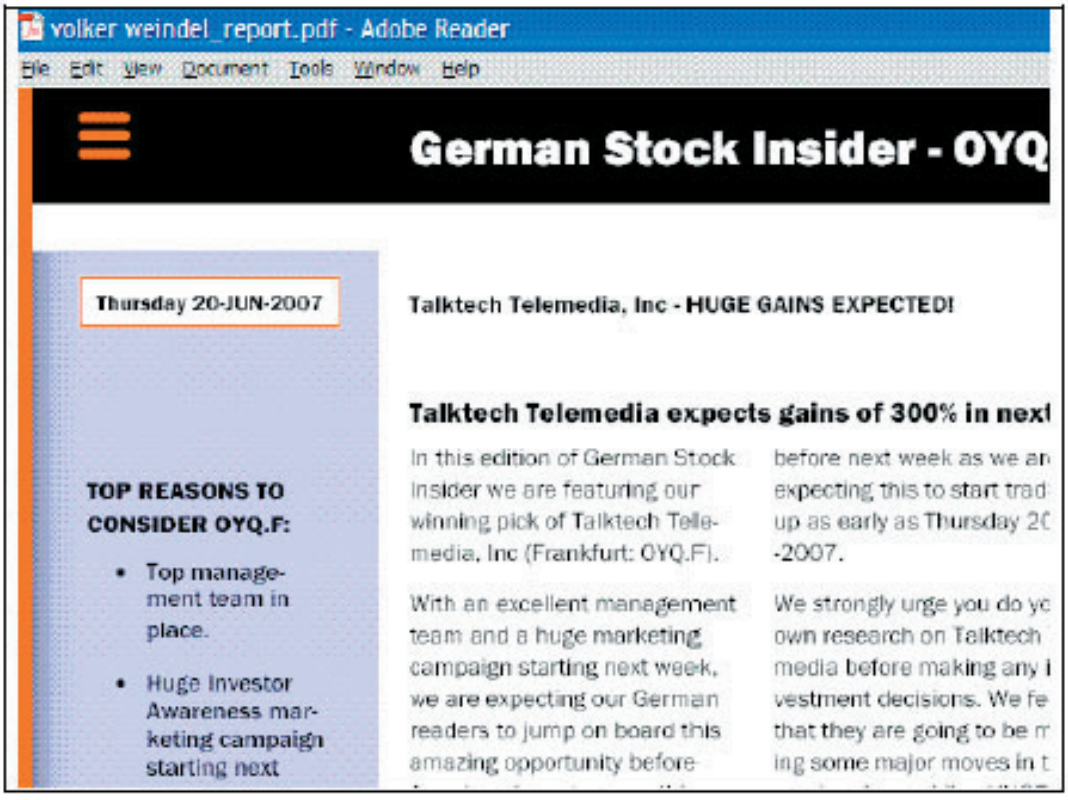

A trend line has been added to demonstrate a 7-day moving average.

## Additional Insights

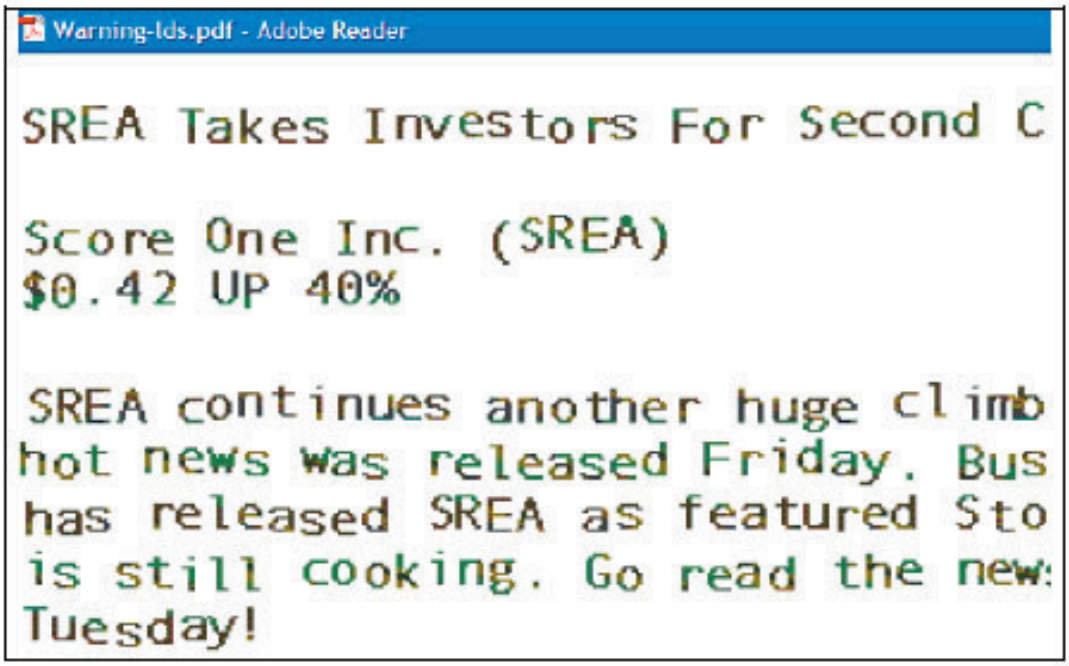
**Image spammers continue to try out new techniques – This month: PDF image spam**

As first reported in the May release of this report, image spam as we know it has declined considerably over the past few months. However, image spammers have not gone away.

- In May, Symantec reported that image spammers were using legitimate image upload hosting solutions for stock spam attacks.
- In June, Symantec reported an increase in spam which used links and embedded URLs to reference images contained in spam.
- In July, Symantec reports the emergence of PDF image spam. Symantec has observed at least two variants of PDF image spam. The first variant is a spam email which has a PDF attached purporting to be a legitimate stock newsletter. This newsletter does not follow the normal rules of images typically used in spam. For example, the newsletter looks professional and does not contain any noise or distortions which would normally be associated with image spam.

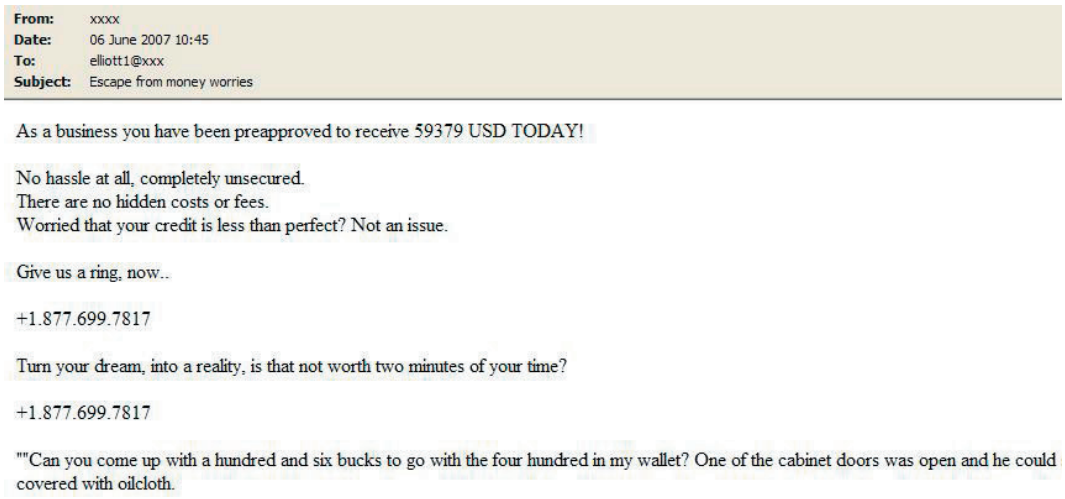


In the second variant, the PDF attached to the email contained a stock spam image. This approach is very similar to image spam attacks focusing on stocks. The goal is to evade AntiSpam filters which depend on being able to "read" the text of a message. This variant of PDF image spam was targeted to over 30 million end users between the 17th June and 27th of June 2007.



### Free money anyone?

Another interesting spam attack observed this month was an attack which claimed to offer free money to a business, “hassle-free.” The recipient was directed to call a number to turn this “dream into a reality”. This spam email was targeted to over 32 million end users between the 7th June and 27th of June 2007



**From:** xxxx
**Date:** 06 June 2007 10:45
**To:** elliott1@xxx
**Subject:** Escape from money worries

As a business you have been preapproved to receive 59379 USD TODAY!

No hassle at all, completely unsecured.
There are no hidden costs or fees.
Worried that your credit is less than perfect? Not an issue.

Give us a ring, now..

+1.877.699.7817

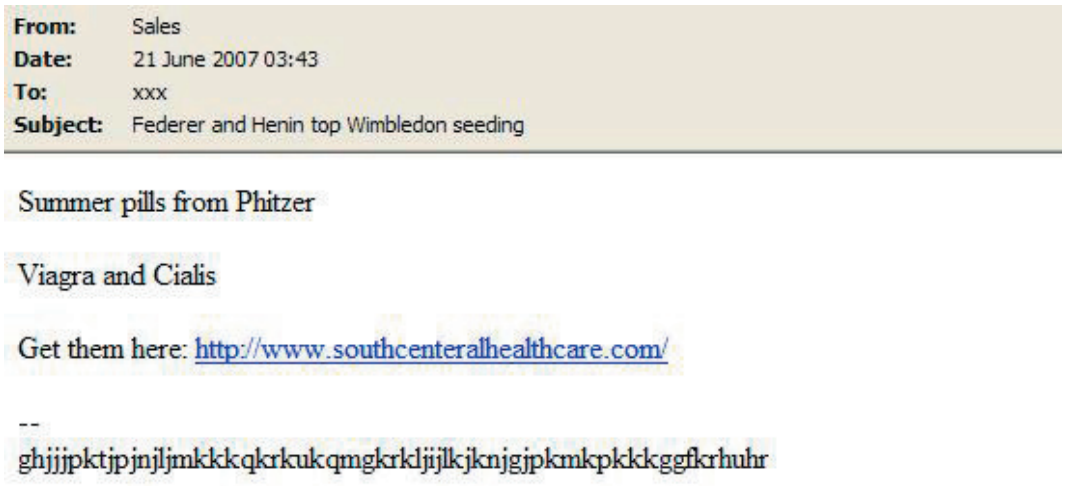
Turn your dream, into a reality, is that not worth two minutes of your time?

+1.877.699.7817

""Can you come up with a hundred and six bucks to go with the four hundred in my wallet? One of the cabinet doors was open and he could covered with oilcloth.

### Current affairs used to peddle medical spam

Wimbledon 2007 started June 25th and the spammer used this event to lure a recipient into a medical spam email with a Subject: Federer and Henin top Wimbledon seeding.



**From:** Sales
**Date:** 21 June 2007 03:43
**To:** xxx
**Subject:** Federer and Henin top Wimbledon seeding

Summer pills from Phitzer

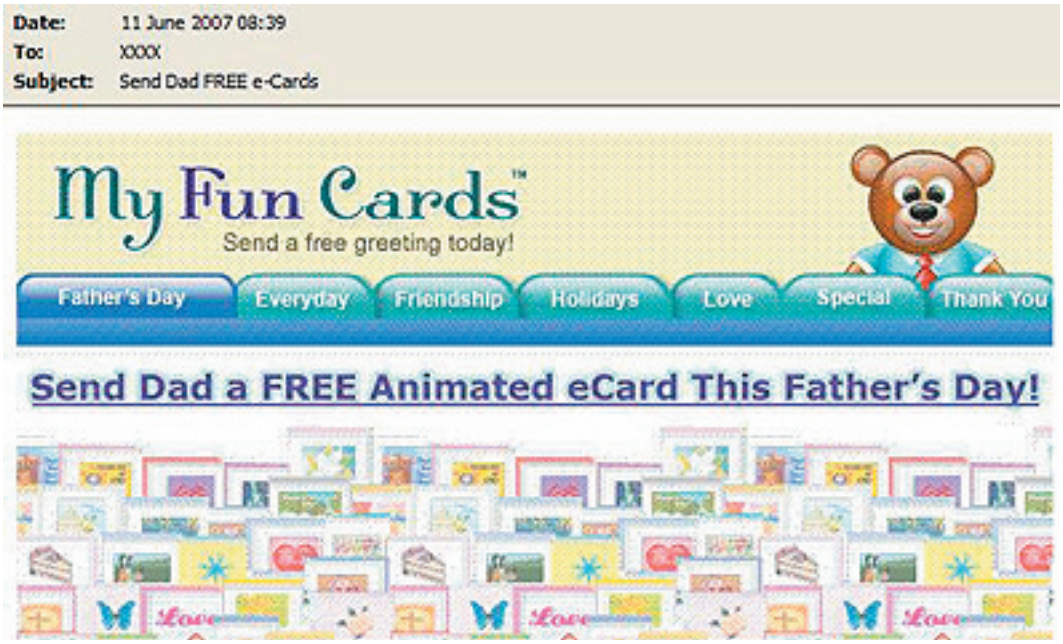
Viagra and Cialis

Get them here: http://www.southcenteralhealthcare.com/

--
ghjjjpktjpjnjljmkkkqkrkukqmgkrkljijlkjknjgjpkmkpkkkggfkrhuhr

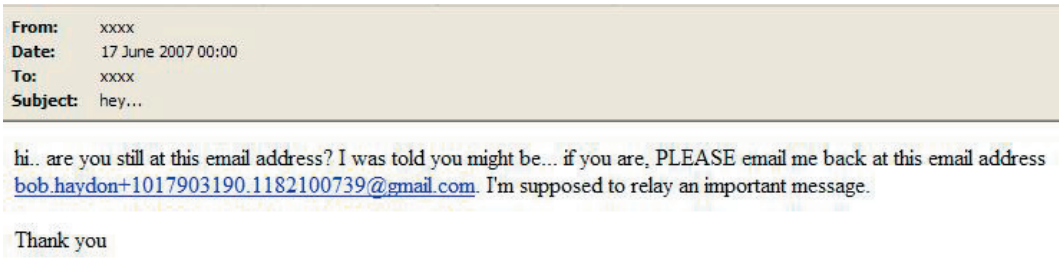
### As night follows day – Father's day spam follows Mother's day spam

Like Mother's Day, Father's day is celebrated on different days around the globe. Father's too were not forgotten by spammers this year, with spammers suggesting gift cards, online greeting cards and even cigars for the fathers out there.




### DHA attacks taken to a different level

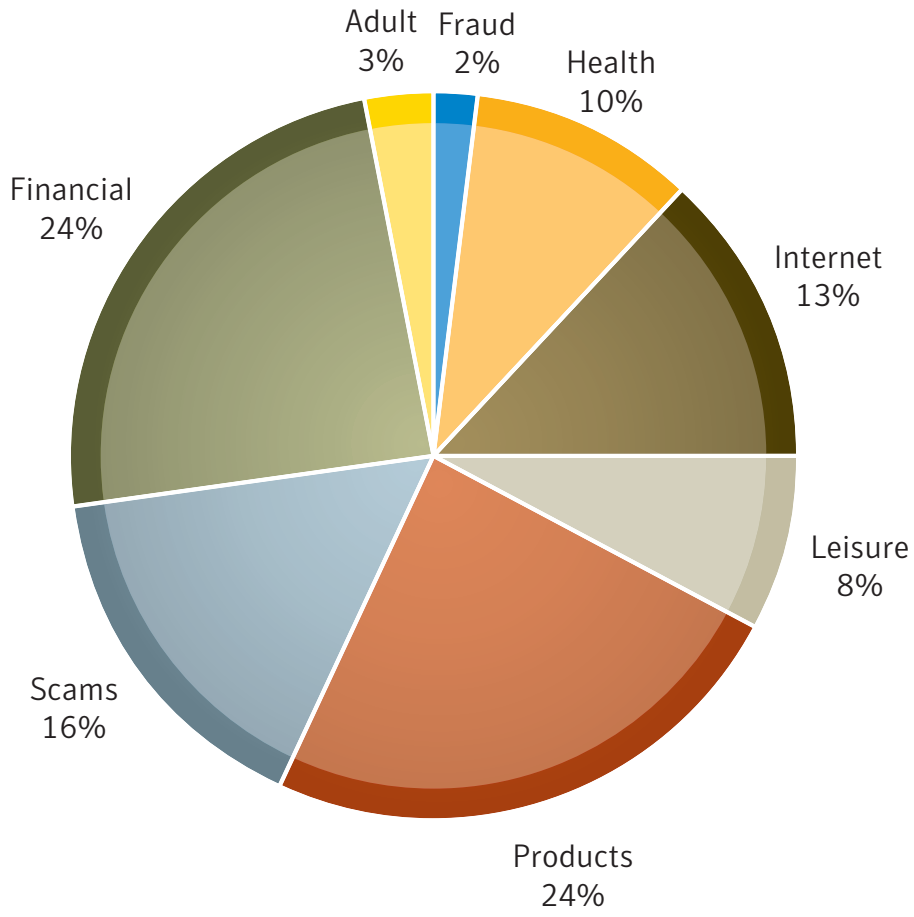
A directory harvest attack (DHA) is an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a spam database. An e-mail server generally returns a "Not found" reply message for all messages sent to a nonexistent address, but does not return a message for those sent to valid addresses. The DHA program generally creates a database of all the e-mail addresses at the server that were not returned during the attack. Symantec recently observed a simplified version of a DHA attack. Using the premise of being a causal acquaintance, the recipient was asked if they were still at that email address and if they could email the sender to receive an important message.



## Spam spotlight: Regional spam trends APJ.

APJ Spam activity in June 2007 was overall consistent with trends observed in last month's report. Scams and fraud spam continued to account for 18% of all spam attacks in the Asia Pacific and Japan (APJ) region.

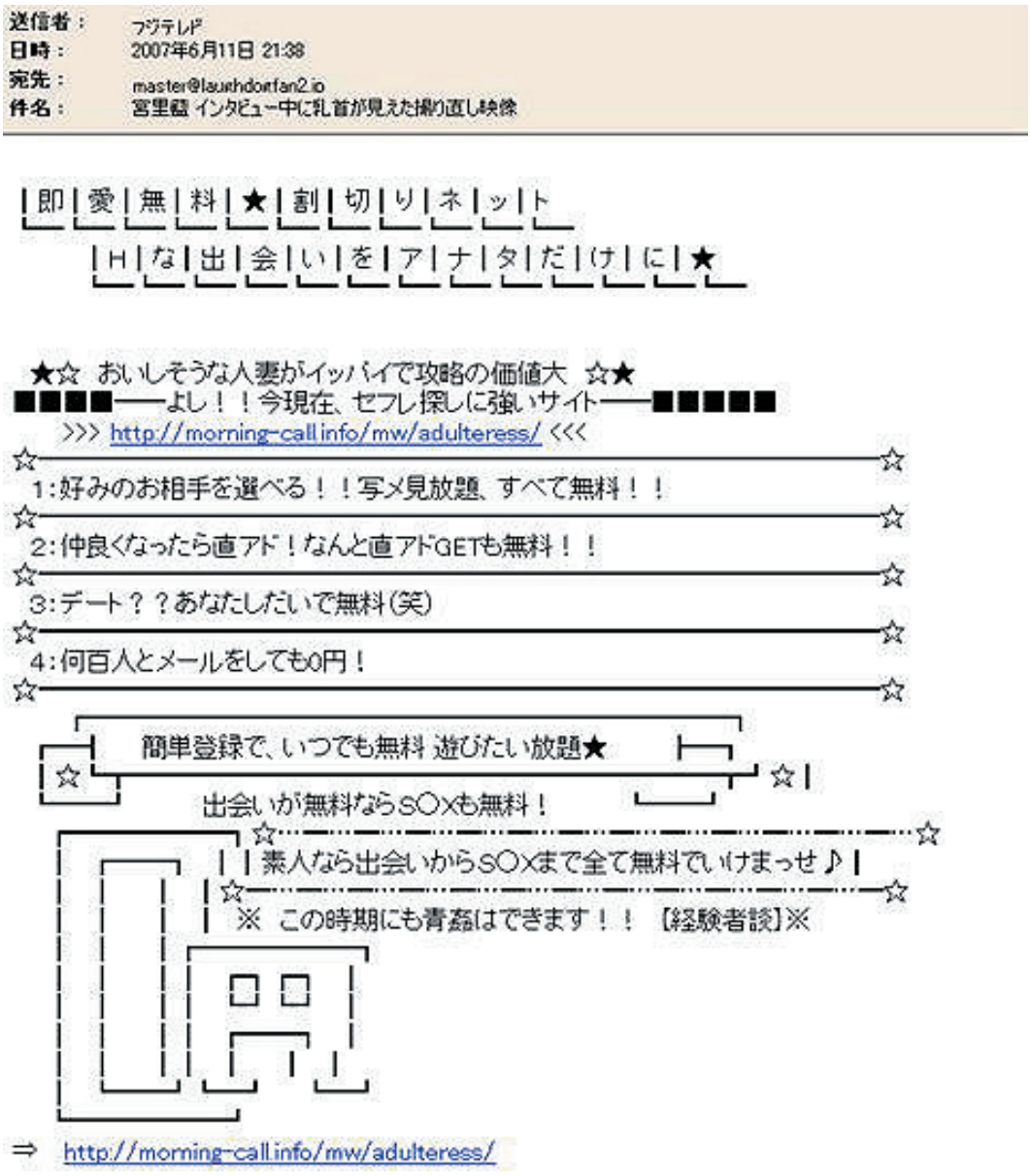
**APJ Category Count - last 90 Days**



Notable regionalized spam attacks include:.

**Rock star recognition**

One of the notable attacks this month in the APJ region is the use of famous names in subject lines to lure the recipient into opening the spam email. In the following example a famous pro-golfer's name is used in the subject line.



**Spam attacks continue to localize in order to target specific regions or countries.**

As we reported in the April Symantec monthly state of spam report, we are seen increasing amounts of spam being written to target a local region or country. The following is an example of a work at home spam written in Japanese.

送信者： biznet02@infotecsol.info
日時： 2007年6月12日 15:28
宛先： master@motorcyclefan2.jp
件名： 在宅をお考えの方へ・・・

この仕事にはセンスが必要です。
センスがなくても努力すれば、
そこら辺のアフェリエイトよりは儲かります。
センスがある方が努力をすれば本業にできます。

コンピュータが得意だと言う方は一度ご覧ください。
http://www.d-station.biz/

片手間でそれなりという方もご覧ください。
http://www.d-station.biz/

在宅ワークをお考えの方は覚悟をしてからご覧ください。
http://www.d-station.biz/
それ以外の方、お時間を取らせました。