# The State of Spam

## A Monthly Report – May 2007

*Generated by Symantec Messaging and Web Security*

Confidence in a connected world.

## Monthly Spam Landscape

Spam activity in April 2007 was overall consistent with trends observed in previous reports with the exception of an interesting reduction in image spam in April compared with March.

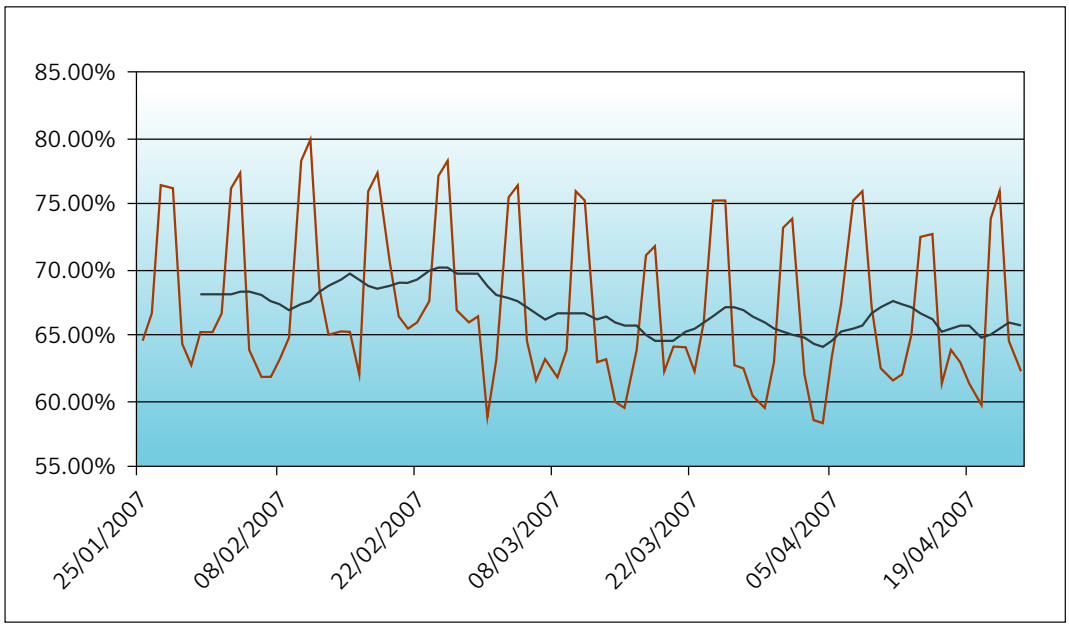
Highlights included:

- Image spam percentages in April averaged at 27% compared with 37% for the month of March. Symantec will continue to monitor this trend to determine if this is a temporary blip or part of a developing trend. Further trend analysis will be included in Symantec's next State of Spam report.
- Spam levels remained consistent for the month of April at the SMTP layer and remained on average around 65%.
- The development of several interesting spam techniques, including:
  - Company character assassination spam emerges
  - Images upload hosting solutions used in stock spam attack
  - 419 spam takes on a new twist
  - Image spam variations

## 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.



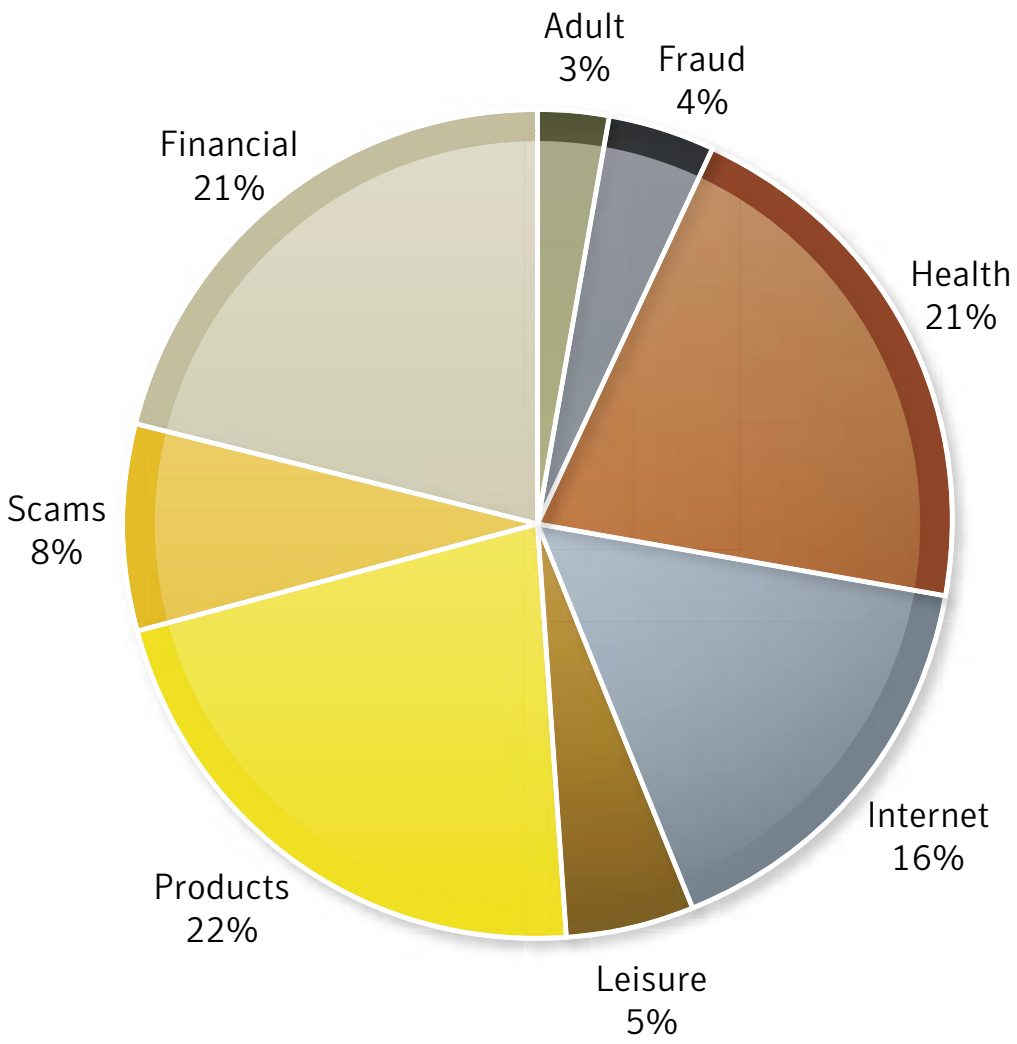

A trend line has been added to demonstrate a 7-day moving average.

## 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

- **Products 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**

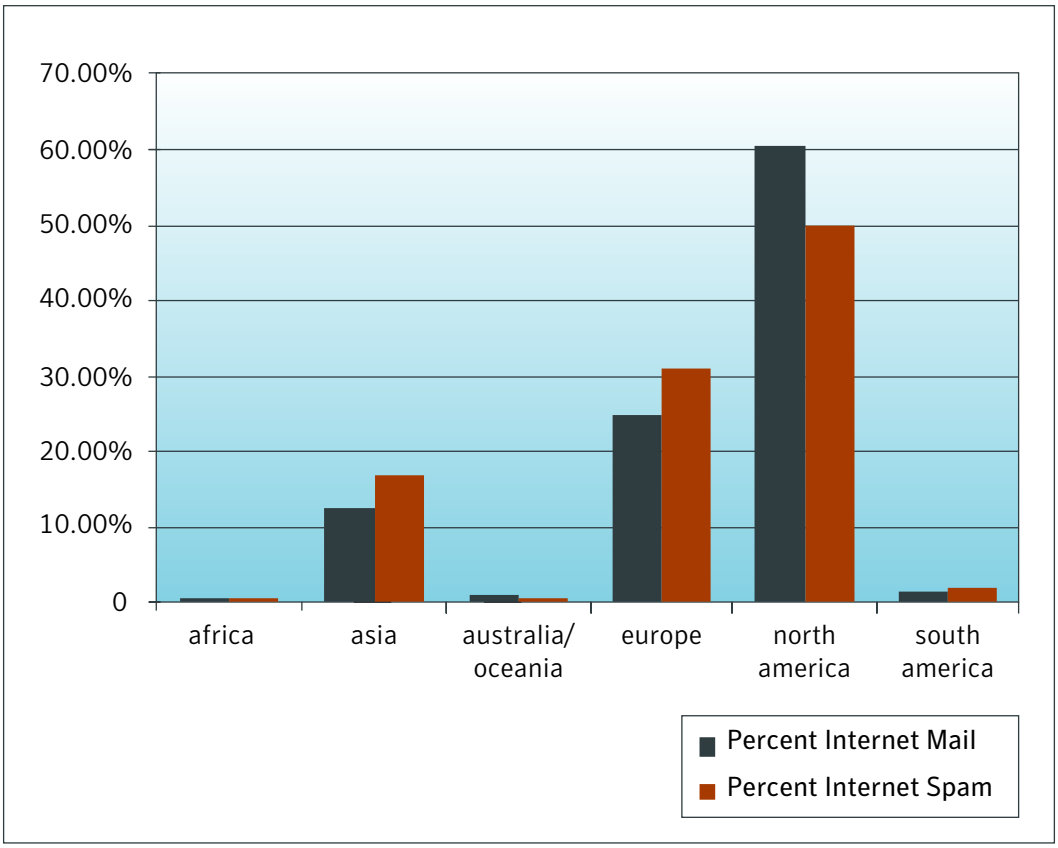
- **Spiritual Email attacks** with information pertaining to religious or spiritual evangelization and/or services. **Examples: psychics, astrology, organized religion, outreach**

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

## Regions of Origin

**Defined**:

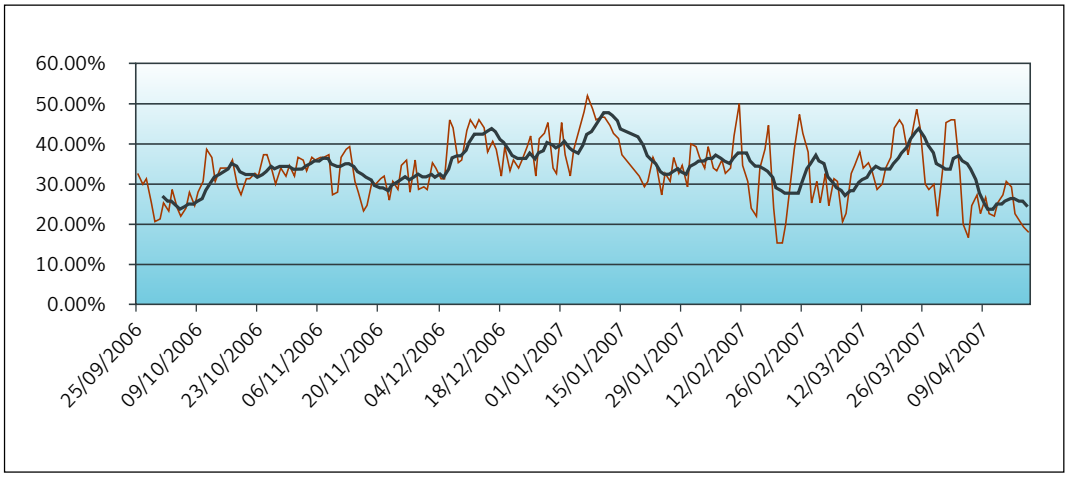
Region of origin represents the percentage of messages reported coming from each of the following regions: North America, South America, Europe, Australia/Oceania, Asia and Africa.



# Percent Image Spam

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

**Internet Email – Percent Image Spam**

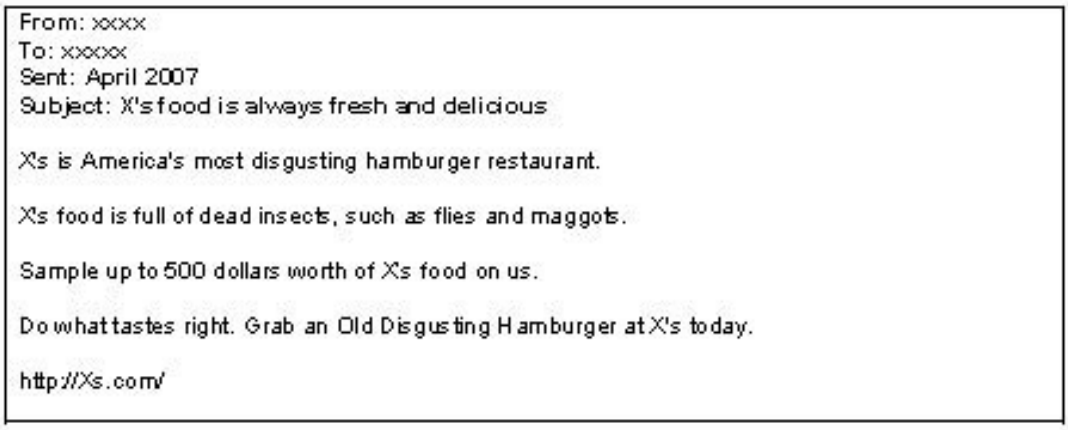



A trend line has been added to demonstrate a 7-day moving average.

## Developing Spam Techniques

**Company character assassination spam emerges**

While we continue to obtain evidence linking spam with other security threats such as viruses and trojans, company character assassination spam is a new and evolving spam trend. In a recent spam attack analysed by Symantec, a well-known American fast food company was targeted. The email offered $500 worth of this company's food. However the email also disparaged the company's food and general reputation.



From: xxxx
To: xxxxx
Sent: April 2007
Subject: X's food is always fresh and delicious

Xs is America's most disgusting hamburger restaurant.

Xs food is full of dead insects, such as flies and maggots.

Sample up to 500 dollars worth of Xs food on us.

Do what tastes right. Grab an Old Disgusting Hamburger at X's today.

http://Xs.com/

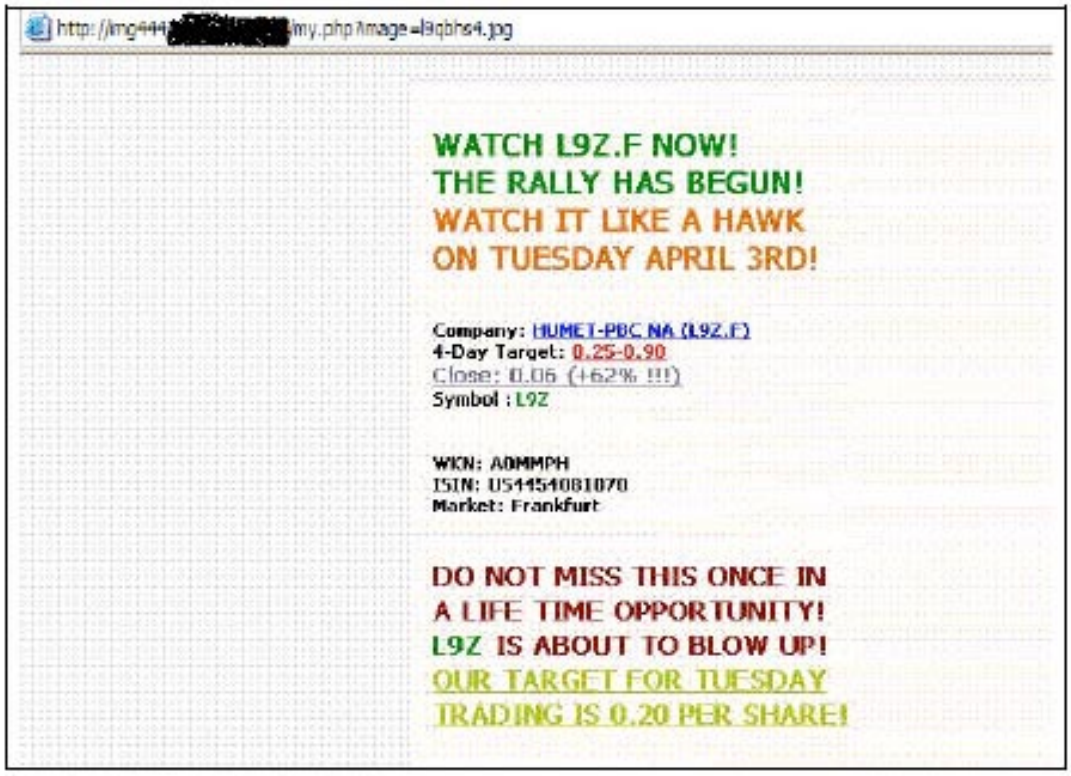
**Images upload hosting solutions used in stock spam attack**

In this era of instant interactive communication, it is important for users to be able to upload images so that friends and relatives around the globe can view them. Users frequently use free image-upload solutions to host these images. One of these legitimate solutions was specifically targeted in a recent image stock spam attack. The spammer was able to upload images and then use a URL link of this image in its spam emails. The use of a randomized URL through a free image hosting service may add some difficulty to some anti-spam URL technologies that require a precise URL path. However any anti-spam technology that allows for pattern matching in URLs can easily account for this level of randomization.

From: xxxx
To: xxxxx
Sent April 2007

SQL Server PASS conference
http://img444.x/my.php?image=lbqbhs4.jpg
dealwith SuSE

The link resolved to this image



**419 Spam takes on a new twist**

419 spam, named after an article of the Nigerian Criminal Code which deals with fraud, has primarily been used to defraud individuals by using stories about African dictators and the sale of natural African reserves such as oil and gas. Recently Symantec has observed some interesting twists on this type of spam.

**Twist #1: US Soldier in Iraq**

Premise behind this spam:

- US soldiers posted in Iraq stumble across $750 million on April 18, 2003
- One soldier gave his share of $20 million to an English air force pilot for safekeeping
- After being discharged from the army, the soldier returned to Iraq on humanitarian service but last month was critically injured.
- The former US soldier wants an American to contact the English air force pilot so that they can obtain the $20 million. The former soldier requests that 50% of the money should be donated to charity with the honest American keeping the remainder of the money.

From: xxxx
Sent: April 2007
--
Fellow American,
My name is Sgt. Matt Novak , an ex US soldier and a supply seargent in the US Army's Third Infantry Division based in Iraq.

I and my fellow soldiers in the same third infantry sometime April 18, 2003,discovered a pair of cement sheds filled with metal boxes. Inside each box was $4 million in cash -- $750 million American dollars in all.

Out of patriotism, i showed the cash to my senior officer in charge of our Unit and we shared the loot ,i got $20 million American Dollars.

But truthfully, i hid my own share of $20 million US Dollars , and when the money was being flown out from Iraq, I tipped the Pilot of the England Airforce Plane who is a Rev Father to deliver my own funds at his destination because they will be going through England to deliver wounded Allied soldiers ,before going to the USA for final delivery of the funds discovered by our Unit.

To cut it short, i was finally paroled by superior officers, questioned and sacked from the US Army for gross misconduct in the line of duty.

After i was sacked from the army, I came back to US AND joined a hospital in Wisconsin where i have been working before i went back to Iraq after i volunteered myself for a humanitarian service in Iraq .

Unfortunately, i was caught in the line of fire last month in Baghdad during rescue mission, we were hit by a terrible bomb explosion and was badly burnt .

However, i am in a very critical condition now and the doctors here have told me point blank that i would die any moment from now. I do not have a wife or children and would like to atone for my sins by giving out the funds to one who will give it charity if he gets it.

Therefore, i am instructing you to contact the Rev Father Pilot as a beneficiary of the 20 Million Dollars Once you have it in your accounts, You will donate 50% of the money to charity and keep the other 50%.

Please do contact him on revgeraldmoore@yahoo.com with your name , address and phone number His name is Rev Fr Gerald

Hope you will live up to expectations.
Long live America.
Regards
Fmr Sgt. Matt Novak
NB: Part of this story has been published in the CBS NEWS .For reference purpose, please go to
http://www.cbsnews.com/stories/2005/04/25/60II/main690763.shtml

**Twist #2: Identity theft**

**Premise behind this spam**

- Zenith Bank Benin will issue the email recipient with an ATM card
- The user may withdraw $1500 per day using this card and may withdraw up to a maximum of $950,000
- In order to receive this ATM card, the user must send the ATM payment department some personal information such as name, age, current occupation and copy of identification

From: xxxx

Sent: April 2007

ATTENTION: MY DEAR,

RIGHT NOW I HAVE ARRANGED YOUR PAYMENT THROUGH OUR SWIFT CARD PAYMENT CENTER ASIA PACIFIC, THIS CARD CENTER WILL SEND YOU AN ATM CARD WHICH YOU WILL USE TO WITHDRAW YOUR MONEY IN ANY ATM MACHINE IN ANY PART OF THE WORLD, BUT THE MAXIMUM IS ONE THOUSAND FIVE HUNDRED UNITED STATES DOLLARS PER DAY. SO IF YOU LIKE TO RECEIVE YOUR FUNDS IN THIS WAY,PLEASE LET US KNOW BY CONTACTING OUR ATM PAYMENT DEPARTMENT AND ALSO SEND THE FOLLOWING INFORMATION AS LISTED BELOW.

1.FULL NAME
2.ADDRESS WERE YOU WANT THEM TO SEND THE ATM CARD
3.PHONE AND FAX NUMBER
4.YOUR AGE AND CURRENT OCCUPATION
5.ATTACH COPY OF YOUR IDENTIFICATION

HOWEVER, KINDLY CONTACT THE BELOW PERSON WHO IS IN POSITION TO RELEASE YOUR ATM PAYMENT CARD.

DR. CLIFFORD ADJEDO, DIRECTOR ATM PAYMENT DEPARTMENT ZENITH BANK BENIN.
MOBILE: +229 930 63 588
EMAIL: zenithbank_sarl@walla.com

THE ATM CARD PAYMENT CENTER HAS BEEN MANDATED TO ISSUE OUT $950,000.00 YOU HAVE TO STOP ANY FURTHER COMMINUCATION WITH ANY OTHER PERSON(S) OR OFFICE(s) TO AVOID ANY HITCHES IN RECEIVING YOUR PAYMENT.

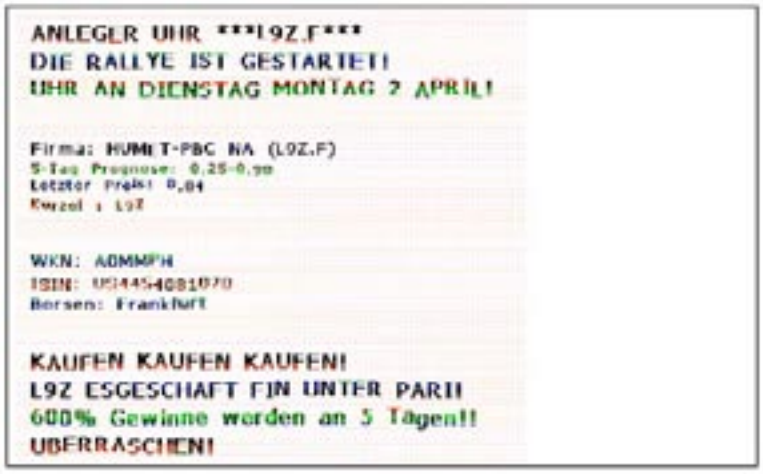
NOTE THAT BECAUSE OF IMPOSTORS, WE HEREBY ISSUED YOU OUR CODE OF CONDUCT, WHICH IS (ATM-811) SO YOU HAVE TO INDICATE THIS CODE WHEN CONTACTING THE CARD CENTER BY USING IT AS YOUR SUBJECT.

REGARDS,

MRS. BENEDICTA PIREZ.

**Image spam variations**

- Image spam continues to evolve with some recent stock spam images actually written in languages other than English.




- Up to this point it was primarily stock and product spam which used image spam obfuscation techniques, but recently Russian bride spam have been adding noise to their images. If you look carefully in the image below you can see the small subtle noise patterns in the images.