

State of Spam Report

A Monthly Report



March 2009

Report 27

The recovery plan continues in February 2009 – the spam recovery plan that is. Spam levels averaged 86% as the economy and Oscars provide fodder for spammers to use during the past month.

Highlighted in the March 2009 report:

- Economic woes bring good tidings for spammers
- Spammers give their Oscar todrum roll please... Brangelina
- Russian bride spam fills void left after Valentine's Day spam
- Spammers ask "Spring break anyone?"
- Getting "paid" to write blogs...another spam "offer"
- Spammers – the latest variety of Juris Doctorate ambulance chasers
- President Obama continues to make spammer headlines in February 2009
- Spammers go Green
- Metrics Digest

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

Economic woes bring good tidings for spammers.

U.S. President Obama and Congress continue to focus on an economic recovery package, it is clear that spammers are also working on their own unique version of a "recovery package." With economic concerns mounting across the globe and intense media coverage of the downtown, it is clear that spammers believe that economic spam is a useful vehicle — a dark cloud that for them holds a silver lining.

A search of recent job-related spam emails reveals subjects such as: "HURRY! I found you a new job...", "Free time job from home", "Job you might be interested in!", "Get the Job fast this one." and "FW: Global job vacancy- apply now" Recipients of these messages are often asked to provide personal information such as first and last name, zip code, cell phone number, home phone number, work phone number and age. With job seekers on the lookout for employment, a spam message has been observed recently which targets one of the downsides to looking for a job – the rejection letter. In the particular spam message observed, the messages states that "Unfortunately we have to inform you that your qualifications and experience does not fit the position you applied for." The URL links in the spam message point back to a legitimate site of a particular company or recruitment firm. The spam message indicates that "We have attached a copy of your application you sent for us." If human curiosity prevails and the recipient opens the attachment the user's system becomes the subject of an attack from the Hacktool.Spammer malicious virus. Hacktool.Spammer is a program that hackers use to attack mail boxes by flooding them with email. It can be programmed to send many email messages to specific addresses.

From: Internal Revenue Service
Date:
To:
Subject: Submit your Economic Stimulus Payment form [ID:
Attach: Economic Stimulus Payment Online Form.htm (144 bytes)

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a Stimulus Payment.
Please submit the Stimulus Payment form in order to process it.

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

To submit your Stimulus Payment form, please download the attached document.

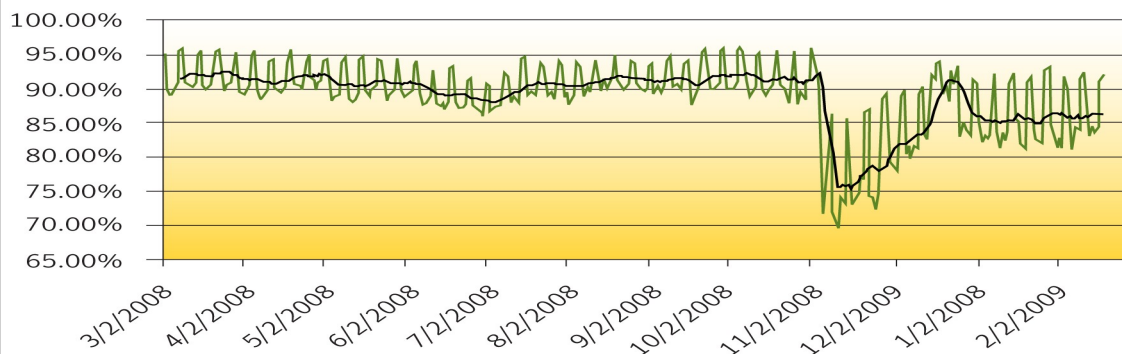
Note: If filing or preparation fees were deducted from your 2007 Refund or you received a refund anticipation loan, you will be receiving a check instead of a direct deposit.

Regards,
Internal Revenue Service

Another example of economic related spam emails claimed to be from the Internal Revenue Service (IRS) and encouraged the recipient to "Submit your Economic Stimulus Payment form." Sending spam messages under the guise of the IRS is a common spam tactic used by spammers to try and obtain personal information from a recipient who may be unfamiliar with such attacks. It should be noted that as the April "tax day" in the U.S. approaches, the IRS clearly indicates on its website that it "does not initiate communication with taxpayers through email."

Another economic stimulus spam attack claims that "Economic Stimulus Grants are now available" and that in order to claim this government funding, the recipient should click on a URL link included in the spam message body. According to a "testimonial" observed on the spam URL link: "I found the grant I needed and filled out the forms and sent them in and in about two weeks I received a check in my hand for \$100,000. I'm telling everyone I know about you all and what you have done for me!" Email users should be aware of this type of ruse during this difficult economic period to avoid letting spammers collect personal information that may be used in the future to prey on unsuspecting individuals and infect machines with malicious content.

Spam Percentage



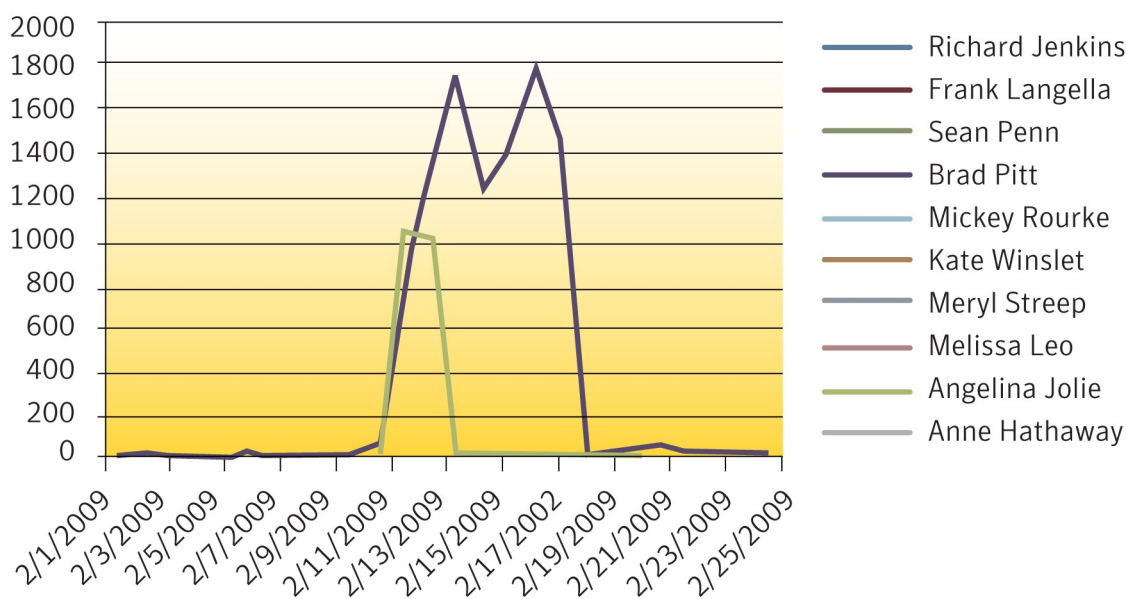
Starting in the March 2009 State of Spam report, the method used to calculate spam percentage has been modified. Previous reports have included the following statement: This metric represents SMTP layer filtering and does not include the volumes of email detected at the network layer. The model now used to calculate spam percentage factors in network layer blocking, and as a results represents a more accurate view into the actual spam percentage on the Internet.

Spammers give their Oscar todrum roll please... Brangelina

During February Symantec analyzed spam messages with a particular interest in the names of individuals nominated for an Oscar for best actor or actress in a leading role. Spam subject lines were tracked and our findings concluded that although an Oscar nomination can mean big bucks and recognition in the world of big budget films, studios and pop culture, it doesn't carry so much weight in the world of spam finance.

Of the ten actors nominated, only three appeared in spam subject lines in February. Anne Hathaway received an honorable mention with one spam message. The rest of the spam went to Brad Pitt and Angelina Jolie. The remaining seven actors or actresses in this category had no spam messages associated with them – an award that regardless of the outcome of the Oscars is worth mentioning. If the spammers could have voted for the awards, it is clear that the results would have turned out much differently.

Oscar Nominees in Spam



In addition to the names of these actors and actresses, some additional words related to the Academy Awards and celebrity interests were tracked and the top twenty subject lines seen in February were then extracted. This is a continuation of the usual spam types of weight loss, replica watches, male enhancement spam and of course some spam trying to get folks to download malicious code.

The top 20 Oscar related subject lines:

Angelina Jolie leaked home video
 Brad Pitt uses this
 Acai Berry Supreme Used by Oprah Winfrey and Brad Pitt For Weight Loss
 Doctors and Celebrities endorse Vital Acai!
 Acai_Weight Loss Diet is the Fat Loss Secret Diet For Celebrities From
 Even the celebrities use it
 Even celebrities use our products to lose weight
 Even famous movie stars would give up everything for a bigger tool.
 Look like the celebrities
 Doctors and Celebrities endorse Anatrium!
 Look like Brad Pitt
 CLEANSE LIKE THE CELEBRITIES
 Celebrities secret diet plan
 Celebrities Secret to Health, Energy and Beauty
 RE: Celebrities are swearing by it
 Celebrities love designer watches, you also can get one but much cheaper.
 Celebrities Love the Acai Berry, Flush out up to 20 pounds
 Celebrities Love the Acai Berry!
 You are not Brad Pitt but you have Viagra! It's better!
 Buy Brad Pitt's Tag Heuer watch here

Russian Bride Spam Helps Fill the Void After Valentine's Day

Following closely on the heels of Valentine's Day spam, a new wave of Russian bride spam has emerged. During the final analysis on Valentine's Day-related spam, it emerged that as the holiday approached there was a 700 percent increase in spam messages with a Valentine's Day theme. The biggest increases by percentage were seen in the phrases "February 14" with a 200 percent increase, Valentine's Day with a 500 percent increase, and last but certainly not least, the term "Valentine" experienced a 9,000 percent increase as Valentine's Day came and went for another year.

Russian bride spam has been around for a number of years now. With previous Russian bride spam examples, the recipient was encouraged to communicate over email with a prospective bride. However, the problem with this method was that the recipient who availed of this "offer" could not be confident that they were speaking with a prospective bride instead of a middle aged man who was trying to scam the recipient. In recent Russian spam messages, live video streaming has been suggested as a way to overcome this "issue". According to the spam email "Adding Live Video Streaming to your Live Chat session is just like going on a date - you will be able to make eye contact, see body language and pick up other cues that are important in helping you decide whether a particular woman could truly be your dream Russian woman!"

From: Russian Brides
Date:
To:
Subject: Beautiful Russian Women Are Waiting to Meet You.

Dream Marriage
Turning Dreams Into Reality

Beautiful Russian Women Are Waiting to Meet You.

Clicking on a link in the message encourages a recipient to start a "free trial " but beware these spam messages are often used to scam money from unsuspecting individuals and the trial may ultimately turn out to very costly.

Spammers ask, “Spring break anyone?”

With the constant talk of the dismal economic climate and general doom and gloom in February 2009, spammers remind us that Spring is here and are suggesting various vacation “offers” to lighten the mood. Spammers have advertised vacation offers in Mexico (Cancun in particular), Lake Tahoe, Arizona, South Carolina and multiple timeshares with the subject lines including

Looking for savings on a Mexico vacation? Book online
 4 Days & 3 Nights Confirmation
 Visit Cancun With A 3 Night Free Stay - No Purchases Required
 Need a Vacation - Get great travel deals sent right to your inbox
 Mind, Body, Spirit - Come to Sedona Arizona On Us
 Experience North Lake Tahoe With Complimentary Accommodations
 Escape to the Outer Banks for Breathtaking Beauty and the perfect family getaway
 Don't just dream of the Sand and Sun, experience its beauty

From:

Date:

To: Subscriber

Subject: Experience 3 Nights in Beautiful Cancun - Free

[Enjoy a complimentary 3 Night stay at](#)

[Cancun!](#)



4 Days 3 Nights In Beautiful Cancun Mexico for FREE!*
 Brought to you by Resorts!


Click Here to Register! No Purchase Required


While the promise of a “free” vacation may be appealing, it is important to remember a few facts about these offers. The offer came from a spammer who may use personal information such as credit card details provided by an unsuspecting end-user for their own ulterior motives. This spam message provided “a disclaimer” stating that the traveler would be responsible for all applicable incidental, hotel taxes and transportation costs. As the economic crunch continues consumers should be reminded that “there is no such thing as a free lunch” or a free vacation.

Getting “paid” to write blogs...another spam “offer”

From Martha Stewart to Anna Kournikova – even the White House has one – blogs and microblogs are all the rage with the ability for self-publishing for the world to read. Symantec’s spam blog has recently published myriad posts documenting the ever-changing spam landscape. Symantec’s spam blog talks about recent spam attacks such as Russian bride spam, spam attacks targeting job seekers and even Turkish language spam so it is fitting that a recent spam message observed by Symantec related to getting “paid” to write blogs should be discussed here.

The spam message indicated that “Freelance Writers were Needed” and “Post in Blogs” in order to get paid 12 - 50 per hour. The spammer noted, “Just write one or two short, simple articles or blog posts every day and you’ll be bringing in several hundred dollars of cold hard cash per-week, almost effortlessly!” Sounds good right? But then the catch... “That’s right. As soon as you log-in to our exclusive, members-only area ... For only \$2.95 you will have unlimited access.” Getting in requires personal contact information and credit card details. The site lures recipients into a false sense of security putting two security logos to tout the supposed reliability of dealing with this site.

Address  https://www.



*** mandatory fields**

Contact Information

First Name *

Last Name *

Email *

Phone Number *

Billing Address

Street Address *

City *

State *

ZIP Code *

Country *

Payment Information

Payment Method *

Card Number * (Numbers Only)

Expiration Date *

3 Digit Security code * What is This

Order Summary

Order Total **\$2.95**

100% SECURE Guaranteed Secure Transaction

HACKER SECURE VERIFIED SITE

So the question is who gets “paid” in this instance – the answer is simple, spammers who may lure another unsuspecting individual into their “exclusive, members-only area.”

Spammers – the latest variety of Juris Doctorate ambulance chasers

In the legal realm – certain spammers have from time to time occupied the defendants' chair. In a recent spam attack it seems that a spammer wishes to change this legal position and become the "pied piper" in some class action lawsuits.

Avandia was first approved by the FDA in 1999 to treat type 2 or adult onset diabetes. In February 2009, a spam message relating to this drug was reported. The message comes with the following subject line, "Have You Taken AVANDIA? Important Lawsuit Information." The spam message indicates that "If you or someone you know has taken Avandia you or that someone or their family may be entitled to monetary damages." A URL link is available for the recipient to click on to "Begin Your Free Review Form".

From: AVANDIA Lawsuit Info
Date:
To:
Subject: Have You Taken AVANDIA? Important Lawsuit Information

AVANDIA Lawsuit Info

Have You Taken AVANDIA? Important Lawsuit Information

The U.S. Food and Drug Administration (FDA) is aware of a potential safety issue related to Avandia (rosiglitazone), a drug approved to treat type 2 diabetes.

Safety data from controlled clinical trials have shown that there is a potentially significant increase in the risk of heart attack and heart-related deaths in patients taking Avandia.

Avandia (rosiglitazone) is manufactured by drug maker GlaxoSmithKline, and is one of the most popular pharmaceuticals for the treatment of Type 2 Diabetes

Another recent vector to this spam attack asked "Were you effected by a Natural Disaster?" The spam attacks claims that "Currently, a class action lawsuit is taking place in New Orleans to help those residents who lost a home, business, or loved one to recover compensation for their losses. Even if you were not a victim of Hurricane Katrina, you may be eligible to file a similar claim".

From: Natural Disaster
Date:
To:
Subject: Were you effected by a Natural Disaster?



In both of these examples, a form asking a number of personal questions is offered to the individual who may be eligible to join the lawsuit. Collecting personal information for their own benefit from a person with a specific illness or a person who has undergone a severe personal trauma is yet another avenue that spammers seem willing to explore at this time.

President Obama continues to make spammer headlines in February 2009

During February 2009 spammers continued their attempts to leverage newly elected president Barack Obama through spam messages focused on the bailout, a Barack Obama Inaugural Dollar and a Presidential fleece blanket.

Subject lines included:

Get your piece of history today

Fluffy Fleece Inaugural Presidential Blankets

Barack Obama Limited Edition Barack Obama inaugural fleece blanket

Bailout-News: -Obama endorses Loan-Modification

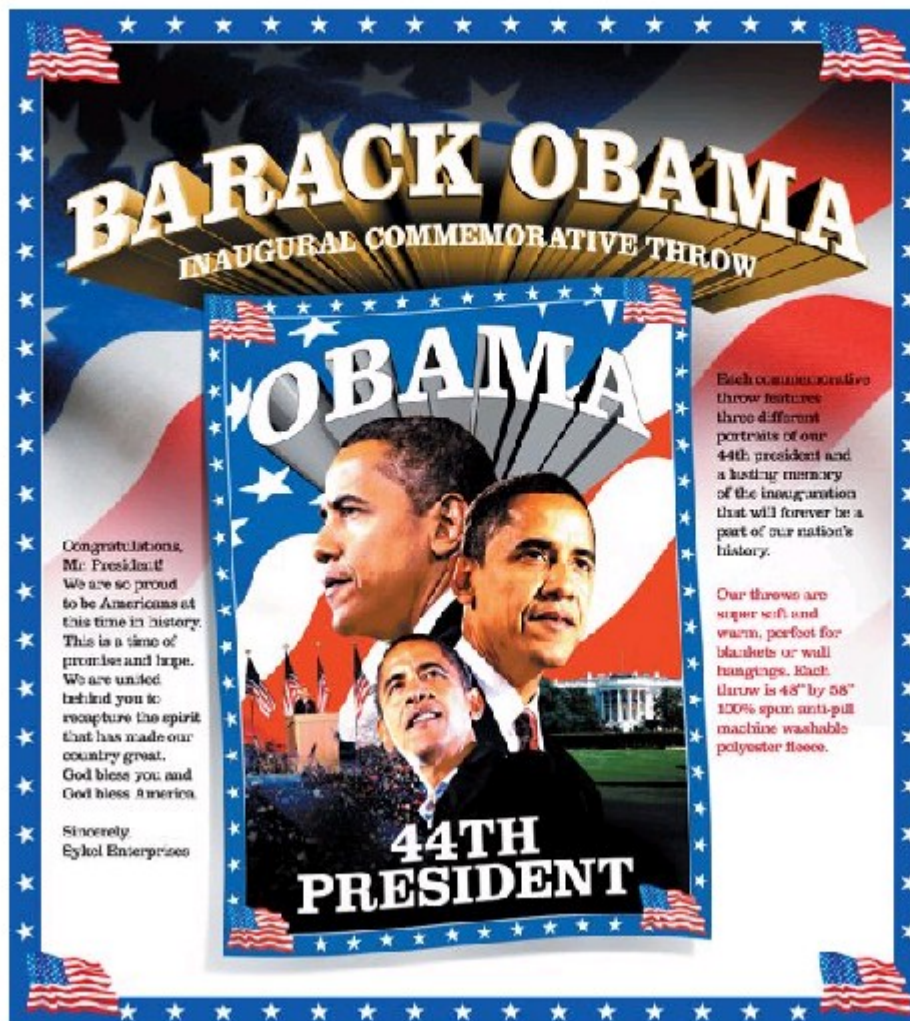
Fluffy Fleece Inaugural Presidential Blankets

From: Fluffy Obama Blankets

Date:

To: Subscriber

Subject: Fluffy Fleece Inaugural Presidential Blankets



Spammers Go Green

Everyone is talking green these days and it's not just with St. Patrick's Day around the corner on March 17th. The Obama administration has recently reiterated its efforts to create, "21st century jobs that improve energy efficiency and utilize renewable resources." With the renewed attention to environmental responsibility, spammers seem to be inspired and have decided on contribute with green spam.

We recently observed a spam attack with a message claiming that the recipient could lower their electric bill to \$0.00 per month with the possibility of even getting a power company to pay the recipient for the use of any excess energy produced. Among the reasons provided by spammer as to why this offer should be accepted is that, "You will be able to protect your pocket book during these recession times and spend money on more important things..."

The green spam "offer" included the following testimonials

"Using the HomeMadeEnergy guide me and my son have built our own wind mill."

"I'm so glad I tried your system. I made my first solar panel this weekend"

"I've decided to go with the solar system. Although it's very rainy in UK, there is enough Sun to power it up."

And

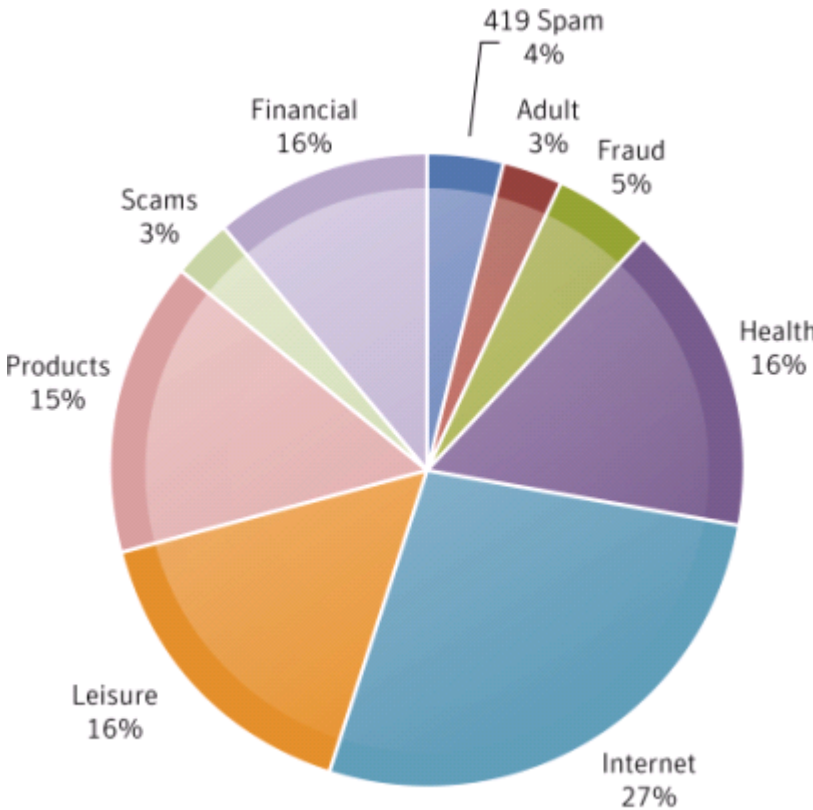
"We live in an apartment. We have an open balcony and I decided it's the best place to use a wind mill."



The spammer claimed that they would "teach you everything you need to have your own solar or wind power system for \$200 or even less." Of course your credit card and personal information is needed to help you go green.

Metrics Digest: Global Spam Categories:

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



Category Name	Jan-09	Feb-09	Change
Internet	19%	27%	8%
Health	20%	16%	-4%
Leisure	9%	16%	7%
Products	23%	15%	-8%
Financial	12%	11%	-1%
Fraud	4%	5%	1%
419 spam	3%	4%	1%
Adult	7%	3%	-4%
Scams	3%	3%	No Change
Political	<1%	<1%	No Change

Global Spam Category Definitions:

- Products** Email attacks offering or advertising general goods and services.
Examples: devices, investigation services, clothing and 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 and 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 and loans
- Scams** Email attacks recognized as fraudulent, intentionally misleading, or known to result in fraudulent activity on the part of the sender.
Examples: Pyramid schemes and chain letters
- Health** Email attacks offering or advertising health-related products and services.
Examples: pharmaceuticals, medical treatments and 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 and billing updates
- Leisure** Email attacks offering or advertising prizes, awards, or discounted leisure activities.
Examples: vacation offers, online casinos and games
- Internet** Email attacks specifically offering or advertising Internet or computer-related goods and services.
Examples: web hosting, web design and spamware
- 419 spam** is named after the section of the Nigerian penal code dealing with fraud, and refers to spam email that typically alerts an end user that they are entitled to a sum of money, by way of lottery, a retired government official, lottery, new job or a wealthy person that has passed away. This is also sometimes referred to as advance fee fraud.

Metrics Digest: Regions of Origin:

Defined:

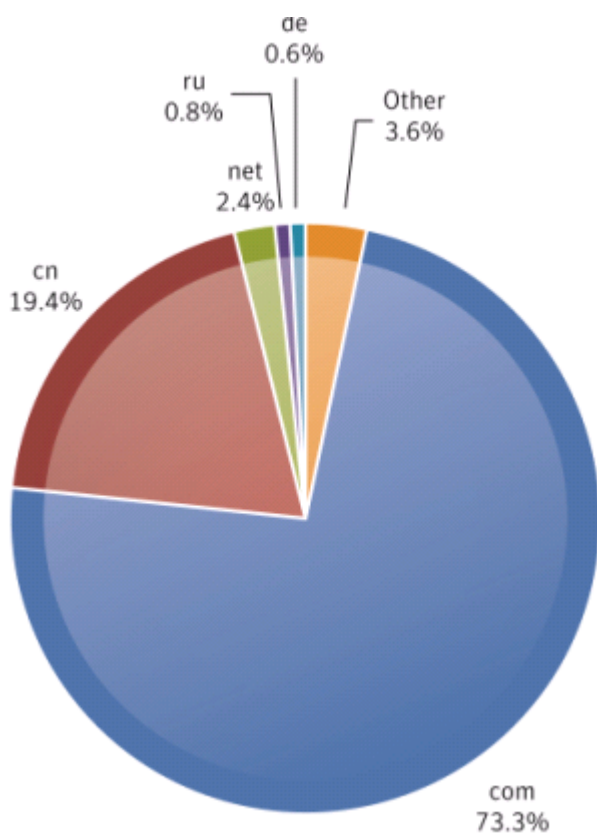
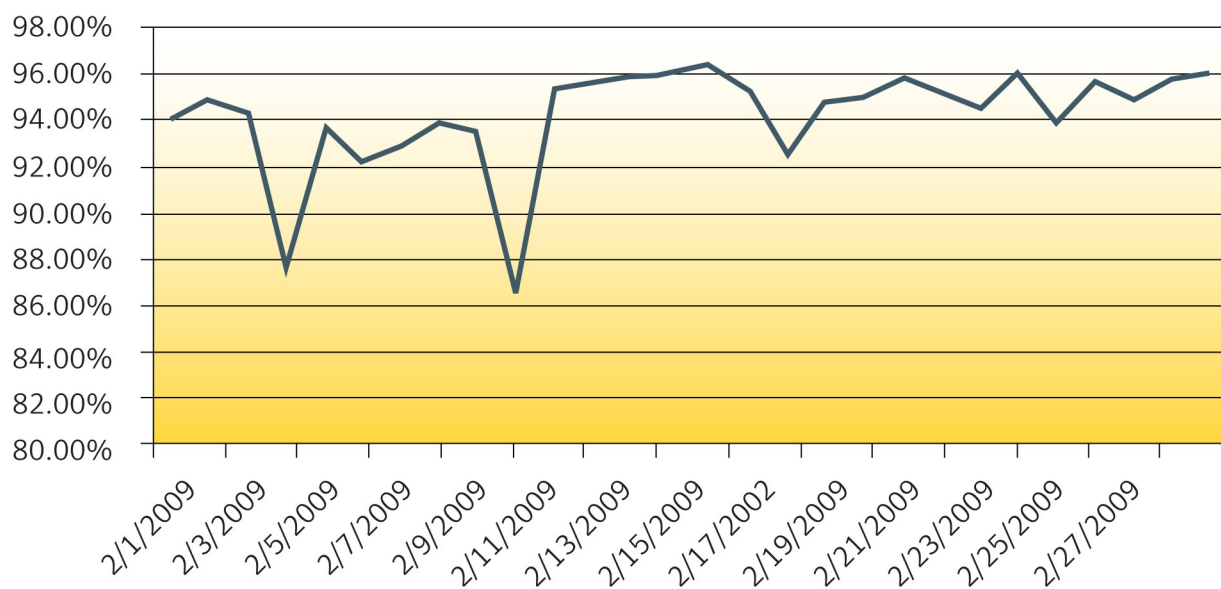
Region of origin represents the percentage of spam messages reported coming from certain regions and countries in the last 30 days.



Country	January 2009	February 2009	Change
United States	23%	25%	+2%
Brazil	10%	9%	-1%
India	4%	5%	+1%
Russia	4%	4%	No Change
China	7%	4%	-3%
South Korea	4%	4%	No Change
Turkey	3%	4%	+1%
Taiwan	3%	2%	-1%
Romania	Not listed in top ten region/country of spam origin	2%	N/A
Poland	Not listed in top ten region/country of spam origin	2%	N/A

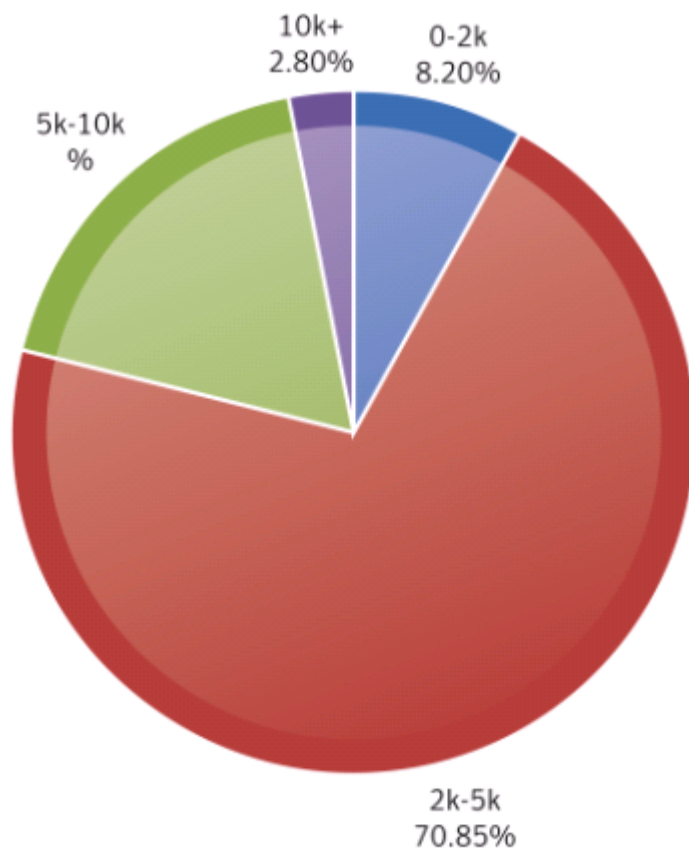
Metrics Digest: URL and spam

Percent URL Spam – February 2009



TLD	Jan-09	Feb-09	Change
com	57.64%	73.30%	16%
cn	32.19%	19.64%	-13%
net	3.45%	2.40%	-1.05%
ru	1.88%	0.80%	-1%
de	0.62%	0.60%	0%
Other	4.20%	3.60%	-0.60%

Metrics Digest: Size of Messages and spam



Message Size	January 2009	February 2009	Change
0-2k	5.41%	8.20%	3%
2k- 5k	77.88%	70.85%	-7%
5k-10k	13.98%	18.12%	4%
10k+	2.73%	2.80%	0%