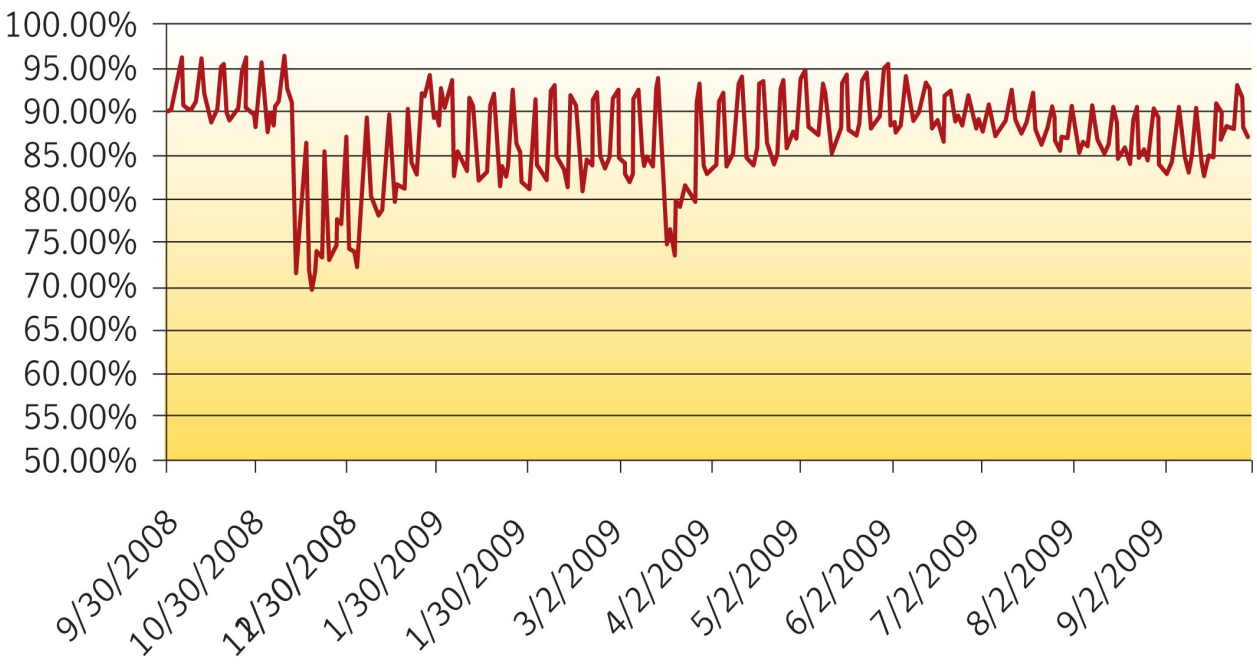
In October 2009, spam volumes made up 87 percent of all email messages. The most notable highlight this month is the growth of spam originating from APJ (23 percent) and South America (22 percent), with a corresponding decline in spam originating from EMEA (28 percent) and North America (20 percent). With respect to spam categories, Internet spam increased by 7 percent and now accounts for 39 percent of all spam messages. This category includes degree spam, which this month dominates the top 50 spam subject lines.

The following trends are highlighted in the November 2009 report:

- **EMEA's Position as the King of Spam is Threatened by New Princes**
- **Malware as A Percentage of Spam Continues to Increase**
- **Users of Social Networking Websites Face Malware and Phishing Attacks**
- **October 2009: Spam Subject Line Analysis**
- **Instant Degrees Dominate Spam Subject Lines in October 2009**
- **One Holiday spam Campaign Makes Way for Another**

Spam Percentage: The model used to calculate spam percentage now factors in network layer blocking in addition to SMTP layer filtering, and as a result represents a more accurate view into the actual spam percentage on the Internet.

Spam Percentage



Dylan Morss
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

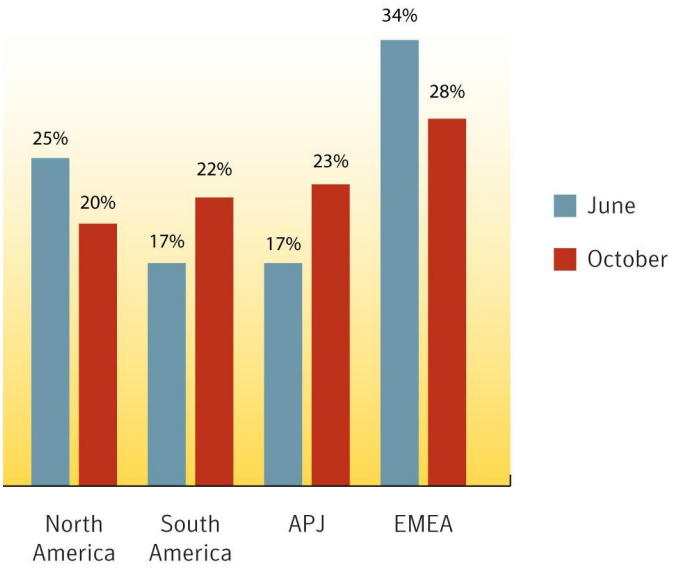
EMEA's Position as the King of Spam is Threatened by New Princes

In the February 2008 State of Spam Report , Europe was crowned the new king of spam as approximately 44 percent of all spam claimed to originate there, versus 35.1 percent which claimed to originate from North America. In October 2009, it seems that EMEA's position has been threatened by the Asia Pacific and Japan (APJ) region and South America.
In October 2009 we monitored the following:

- The EMEA region continues to retain the mantle as primary region of origin for spam at 28 percent. This is a six percent decrease from June 2009.
- APJ and South America have now passed North America with 23 percent, and 22 percent respectively of all spam originating from these regions.

Twenty percent of all spam now originates from North America —a five percent decrease since June 2009.

Region of Origin



	October	June	Difference
North America	20%	25%	-5%
South America	22%	17%	5%
APJ	23%	17%	6%
EMEA	28%	34%	-6%

This sizeable increase in spam appearing from South America and the APJ region is significant, but not altogether surprising when you consider the massive growth of Internet connections in these regions during the past few years. Other factors at play here include:

EMEA's Position as the King of Spam is Threatened by New Princes

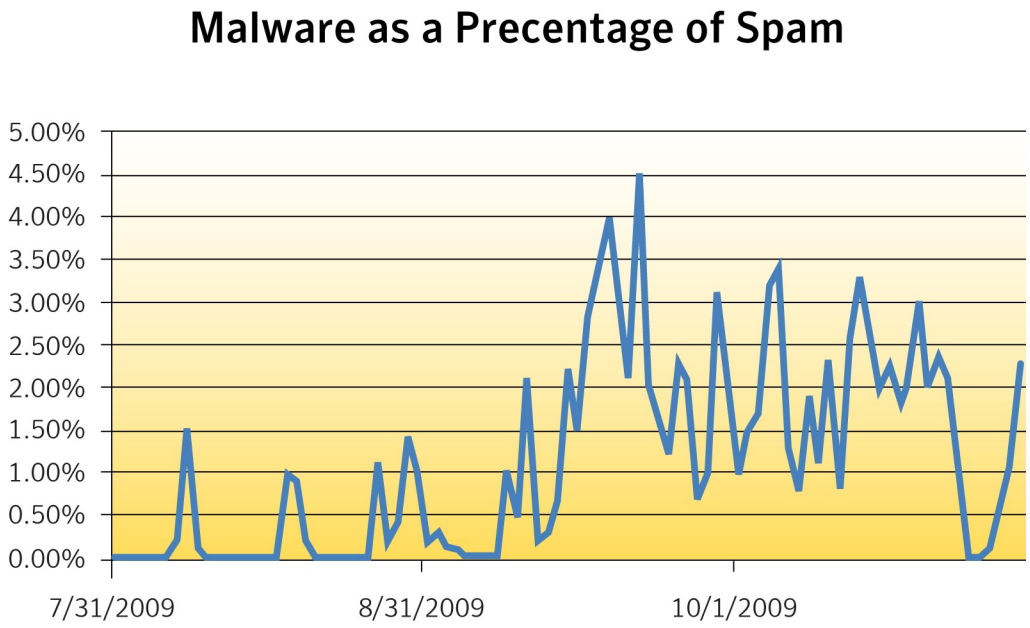
- Spam levels have increased dramatically since February 2008. In that month's report, spam levels reached 78.5 percent of all email traffic during January 2008. This contrasts sharply with what was observed in October 2009 as spam levels hit a maximum of 93 percent, and averaged at 87 percent of all email messages.
- Distribution networks are becoming more dynamic as additional broadband connected targets are coming online every day. Distribution paths are also getting more complicated with spammers now sending messages directly from infected machines, routing through compromised relays and continuing to use webmail/SMTP Auth abuse.
- Botnets continue to jockey for position after shutdowns such as McColo. The number of botnets is set to grow as hackers target developing IT infrastructures in certain regions such as APJ and South America.
- When the country ranking for origin of spam for June 2009 is compared with October 2009, it can be seen that countries such as India, Taiwan, Thailand and Chile have increased several places. Vietnam jumped 13 spot and is now the third most spamming country.

Country	Rank June 2009	Rank October 2009
United States	1	1
Brazil	2	2
Vietnam	16	3
India	6	4
Poland	4	5
Korea [South]	3	6
China	7	7
Argentina	9	8
Colombia	10	9
Taiwan	22	10
Romania	11	11
Russia	8	12
Italy	13	13
Thailand	23	14
Germany	15	15
Chile	19	16
United Kingdom	18	17
Spain	12	18
Ukraine	20	19
Czech Republic	17	20

- Finally, it should be noted that the nature of spam and its distribution on the Internet presents challenges in identifying the location of the people sending the messages. Many spammers redirect attention away from their actual geographic location.

Malware as A Percentage of Spam Continues to Increase

In October 2009, an average of 1.9 percent of all spam messages contained malware. This equates to a 0.6 percent increase from September 2009 when the number of messages containing malware hit a maximum of 4.5 percent of all spam.



As reported in the October 2009 State of Spam Report, this increase in malware is significant when you consider that 87 percent of all email messages in October 2009 were spam and the increased message size of spam emails email that have attached malware may also be significant.

Message Size	October	September	Change
0-2k	1.83%	3.43%	-2%
2k-5k	50.62%	55.19%	-5%
5k-10k	37.82%	28.21%	10%
10k+	10%	13%	-3%

Malware as A Percentage of Spam Continues to Increase

One of the more interesting spam emails that had malware attached to it was masquerading as a notification from Facebook that the recipient's password has been reset. The message contained an attached zip file containing a malicious exe file. Symantec detects the exe files as Trojan.Bredolab. This variant of Bredolab connects to a Russian domain and the infected machine is most likely becoming part of a Bredolab botnet.


The Facebook Team
To:
Facebook_Password_7a343.zip (23.8 KB)

Facebook Password Reset Confirmation.

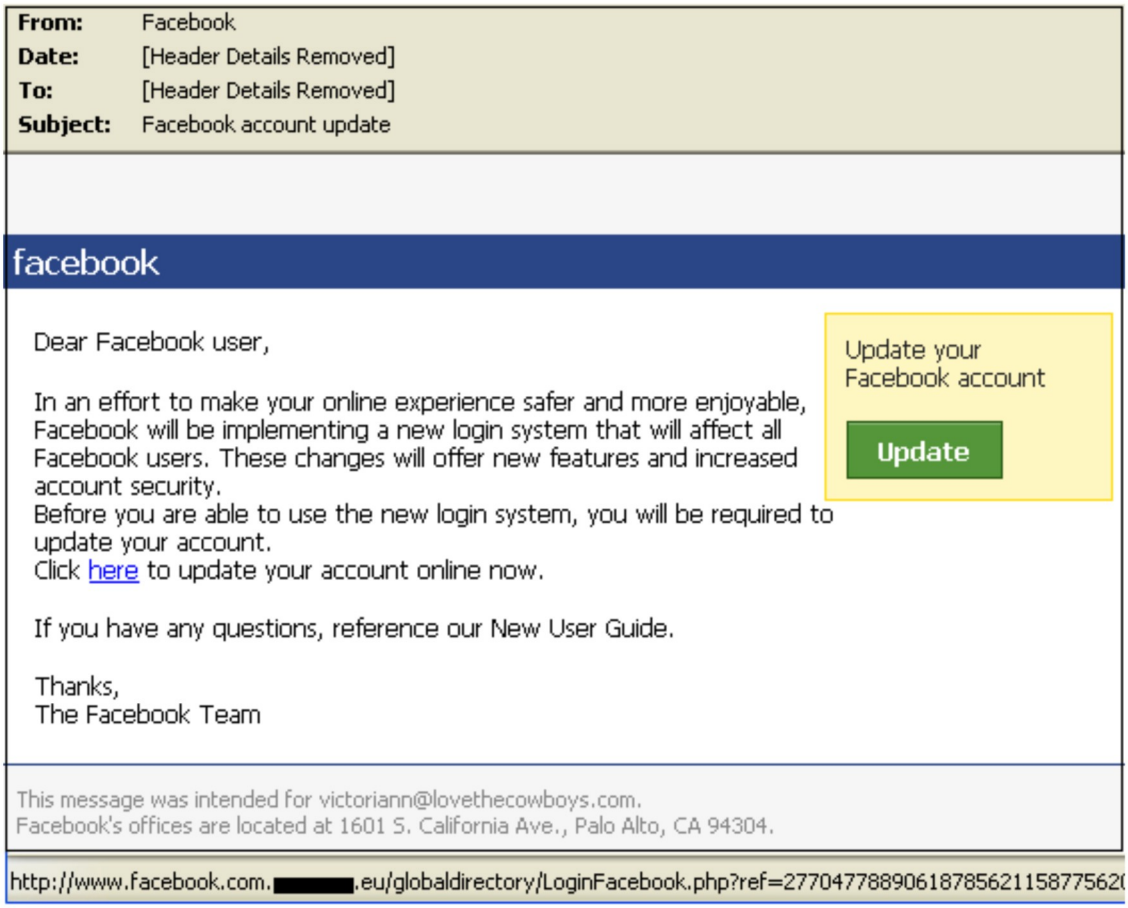
Hey ,

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

Thanks,
The Facebook Team

Users of Social Networking Websites Face Malware and Phishing Attacks

In addition to the malware related spam attack targeting Facebook in October, Symantec has observed a phishing attack targeting Facebook. The messages look like an official Facebook invite or password reset confirmation mail.



If the cursor is placed over the update button in the message, the phishing URL can be observed. The user may then be redirected to a Facebook look-alike phishing site where they are asked to enter their password to complete the update procedure. Unfortunately, the user's password will be stolen if they try to login on this page.

These attacks can be identified by the subject lines listed below:

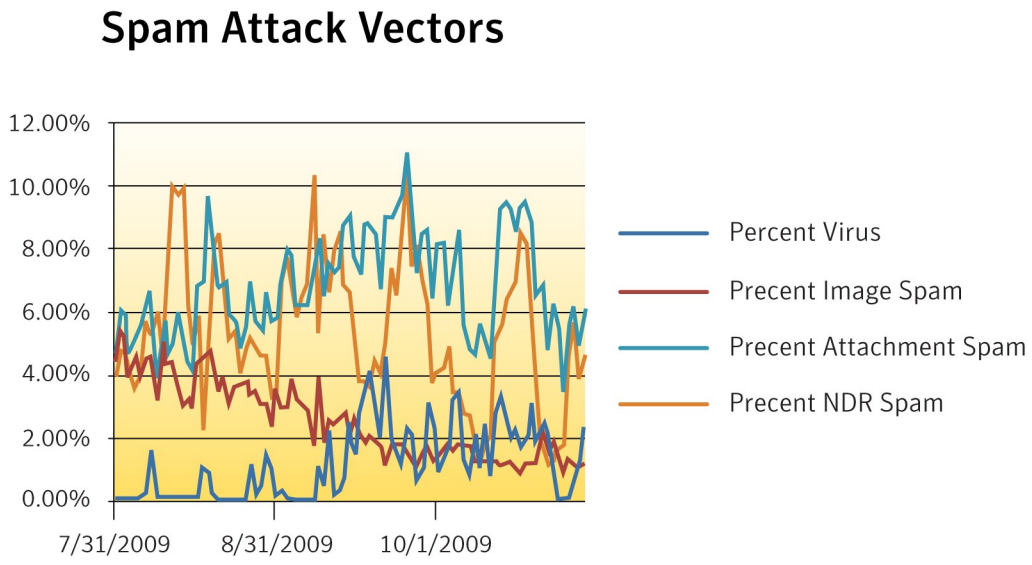
Facebook account update
New login system
Facebook Update tool

As spammers continue to hide behind the reputation of legitimate senders, social networking sites which have a large user base will continue to be targets of malicious and phishing emails.

October 2009: Spam Subject Line Analysis

In the October 2009 State of Spam Report , the top ten subject lines used by spammers were dominated by a mixture of malware related attacks and NDR bounce spam subject lines. NDR bounce spam averaged at 4.54 percent of all spam while spam messages containing malware averaged at 1.9 percent of all spam messages.

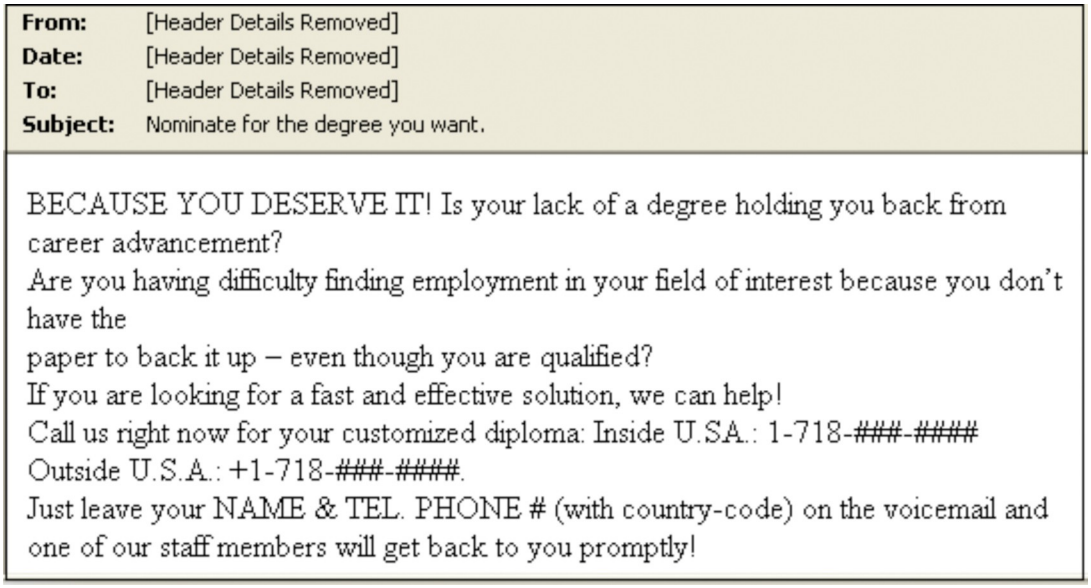
#	Total Spam: October 2009 Top Subject Lines	No. of Day	Total Spam: September 2009 Top Subject Lines	No. of Day
1	Notice of Underreported Income	19	Notice of Underreported Income	20
2	Delivery Status Notification (Failure)	31	Delivery Status Notification (Failure)	30
3	failure notice	31	failure notice	30
4	Undelivered Mail Returned to Sender	31	Undelivered Mail Returned to Sender	30
5	You've received a postcard	13	Thank you for setting the order	17
6		31	Returned mail: see transcript for	30
7	Thank you for setting the order	6	Gain 3Inches	27
8	Returned mail: see transcript for details	31	Delivery Status Notification	30
9	Hi	31	Your order	22
10	Sales Receipt from Amazon	27	RE: Message	20



Instant Degrees Dominate Spam Subject Lines in October 2009

Instant degree spam attacks have become one of the most high profile attacks observed in recent months. These messages try to entice users with degrees in policing, nursing, teaching and the culinary arts. These attacks often offer instant degrees, with no effort required – just call the number provided in the message and users may obtain a degree certificate in no time.

Sample image of these messages:



From: [Header Details Removed]
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: Nominate for the degree you want.

BECAUSE YOU DESERVE IT! Is your lack of a degree holding you back from career advancement?
Are you having difficulty finding employment in your field of interest because you don't have the
paper to back it up – even though you are qualified?
If you are looking for a fast and effective solution, we can help!
Call us right now for your customized diploma: Inside U.SA.: 1-718-###-####
Outside U.S.A.: +1-718-###-####.
Just leave your NAME & TEL. PHONE # (with country-code) on the voicemail and one of our staff members will get back to you promptly!

With the increased popularity of online education, spammers are once again tapping into a high profile market. In October 2009, degree spam dominated 22 out of the top 50 subject lines observed related to this attack.

Rank October 2009	Subject	No of Days
18	Choose the needed field.	31
19	Online diplomas here.	31
20	Get a diploma for your career.	31
21	Apply for your diploma.	31
22	Call for your diploma now.	31
23	Get a diploma for a better job.	31
24	Receive the desired degree.	31
25	Get your diploma immediately.	31
26	Nominate for the degree you want.	31
27	Bachelors, Masters or Doctorate degree.	31

One Holiday Spam Campaign Makes Way for Another

With the Halloween spam campaigns set aside for another year, it is time for the Thanksgiving, Christmas and New Year spam campaigns to take center stage. Earlier this year, Symantec reported that spam campaigns targeting end of year holidays, such as Christmas, began in August.

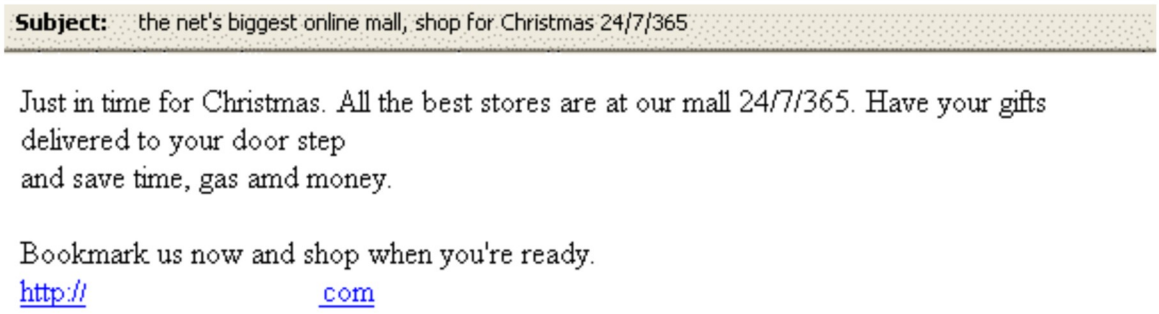
Observations from the 2008 spam holiday season included:

- As legitimate mailers sent out more and more mailings with special "deals" and "offers" (as observed in the run up to Cyber Monday and Black Friday of 2008) to try and sell their products during the difficult economic time, spammers also used subject lines that tried to draw users in by saving money.
- Similar seasonal subject lines were often used in both spam and legitimate mailings. Spammers used these subject lines to try and evade some antispam filters.
- Seasonal spam subject lines often did not use randomization or other obfuscation techniques.

The top ten seasonal spam subject lines observed between October and November 2008 include the following:

1. Best Sales 2008!
2. Spend less this Christmas
3. A Really Good Gift
4. Christmas Specials
5. Christmas promo few days left
6. Gifts for Christmas
7. Holiday Luxury Gifts
8. Hot Christmas Specials
9. Most Affordable Gifts
10. Low Christmas Pricing

Examples of holiday-themed spam campaigns observed so far this year are listed below:


Subject: the net's biggest online mall, shop for Christmas 24/7/365

Just in time for Christmas. All the best stores are at our mall 24/7/365. Have your gifts delivered to your door step
and save time, gas amd money.

Bookmark us now and shop when you're ready.
http:// com

One Holiday Spam Campaign Makes Way for Another

Subject: Two months BIG discount for Christmas Day and the New Year

hi dear client friend,
how are you recently? this is www. .com feifei
feifei has a great news need to tell you -- our company is going to do discount on products for **Christmas Day and the New Year** now. below is the detailed discount info:
Time: TWO MONTH--beijing time 1st Nov to 31th Dec;
Web: (www. .com)
To: **all the old and new customers.**
Content:
$100-$200, can get 2% discount off;
$201-$500, 3% discount off,
$501-$800, 4% discount off;
$801-$1000, 5%discount off;
$1001-$2000, 6% discount off;
$2001-$3000, 7% discount off;
$3001-$4000, 8% discount off;
$4001-$5000, 9% discount off;
more than $5001, 10% discount off;
Notice: **the price is PRODUCTS price, it is not including shipping cost.**
hope have a little help for you

Subject: CHRISTMAS AND NEW YEAR IS HERE AGAIN

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

CHRISTMAS AND NEW YEAR OFFER

Dear Customer

Login to your account and grap all the new offers for the christmas and new year.

Hurry while offer last.

To Get Started,Please Click Here

Online Promotion Department
Advert Advisor

Checklist: Protecting your business, your employees and your customers

Do

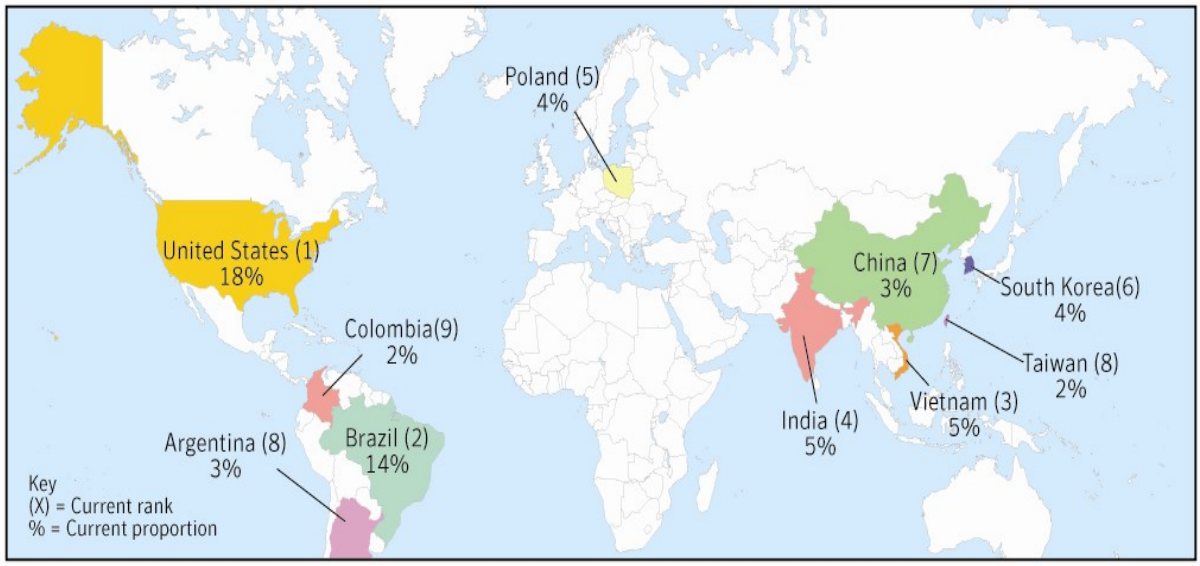
- Unsubscribe from legitimate mailings that you no longer want to receive. When signing up to receive mail, verify what additional items you are opting into at the same time. De-select items you do not want to receive.
- Be selective about the Web sites where you register your email address.
- Avoid publishing your email address on the Internet. Consider alternate options – for example, use a separate address when signing up for mailing lists, get multiple addresses for multiple purposes, or look into disposable address services.
- Using directions provided by your mail administrators report missed spam if you have an option to do so.
- Delete all spam.
- Avoid clicking on suspicious links in email or IM messages as these may be links to spoofed websites. We suggest typing web addresses directly in to the browser rather than relying upon links within your messages.
- Always be sure that your operating system is up-to-date with the latest updates, and employ a comprehensive security suite. For details on Symantec's offerings of protection visit http://www.symantec.com.
- Consider a reputable antispam solution to handle filtering across your entire organization such as Symantec Brightmail messaging security family of solutions.
- Keep up to date on recent spam trends by visiting the Symantec State of Spam site which is located here.

Do Not

- Open unknown email attachments. These attachments could infect your computer.
- Reply to spam. Typically the sender's email address is forged, and replying may only result in more spam.
- Fill out forms in messages that ask for personal or financial information or passwords. A reputable company is unlikely to ask for your personal details via email. When in doubt, contact the company in question via an independent, trusted mechanism, such as a verified telephone number, or a known Internet address that you type into a new browser window (do not click or cut and paste from a link in the message).
- Buy products or services from spam messages.
- Open spam messages.
- Forward any virus warnings that you receive through email. These are often hoaxes.

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	October	September	Change
United States	18%	25%	-7%
Brazil	14%	12%	2%
India	5%	4%	1%
Vietnam	5%	4%	1%
South Korea	4%	4%	0%
Poland	4%	4%	0%
China	3%	3%	0%
Argentina	3%	2%	1%
Colombia	2%	2%	0%
Taiwan	2%	Not Listed	n/a

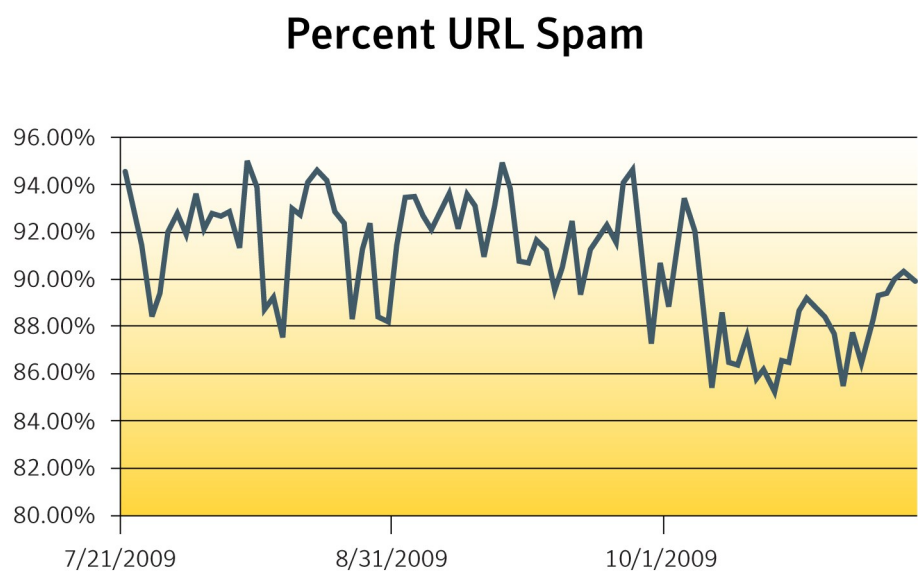
Metrics Digest: URL TLD Distribution

TLD	October	September	Change
com	43%	43%	0%
cn	47%	48%	-1%
net	3%	2%	1%
org	3%	4%	-1%
Other	3%	3%	0%

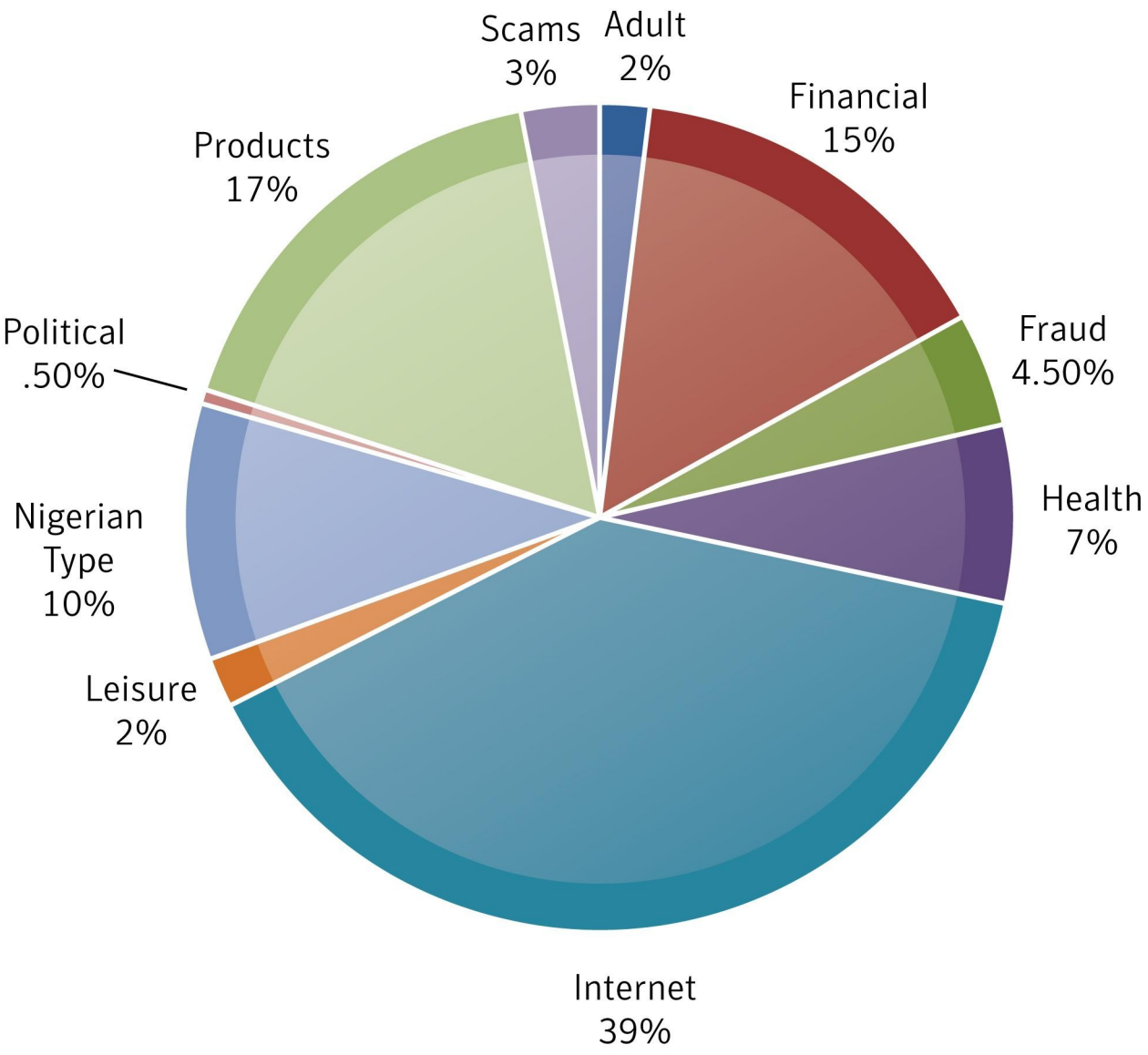
Metrics Digest: Average Spam Message Size

Message Size	October	September	Change
0-2k	1.83%	3.43%	-2%
2k-5k	50.62%	55.19%	-5%
5k-10k	37.82%	28.21%	10%
10k+	10%	13%	-3%

Metrics Digest: Percent URL Spam



Metrics Digest: Global Spam Categories: Last 30 Days



Metrics Digest: Global Spam Categories:

Category Name	October	September	Change
adult	2.00%	1.50%	1%
financial	15.00%	17.10%	-2%
fraud	4.50%	6.60%	-2%
health	7.00%	6.90%	0%
internet	39.00%	32.30%	7%
leisure	2.00%	3.10%	-1%
419 spam	10.00%	9.70%	0%
political	<1%	<1%	No Change
products	17.00%	19.60%	-3%
scams	3.00%	2.70%	0%

- **Internet Email attacks** specifically offering or advertising Internet or computer-related goods and services. *Examples: web hosting, web design, spamware*
- **Health Email attacks** offering or advertising health-related products and services. *Examples: pharmaceuticals, medical treatments, herbal remedies*
- **Leisure Email attacks** offering or advertising prizes, awards, or discounted leisure activities. Examples: vacation offers, online casinos
- **Products Email attacks** offering or advertising general goods and services. *Examples: devices, investigation services, clothing, makeup*
- **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.
- **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 E-mail address, financial information and passwords. *Examples: account notification, credit card verification, billing updates*
- **419 spam Email attacks** 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 that has passed away. This is also sometimes referred to as advance fee fraud.
- **Political Email attacks** 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*
- **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*