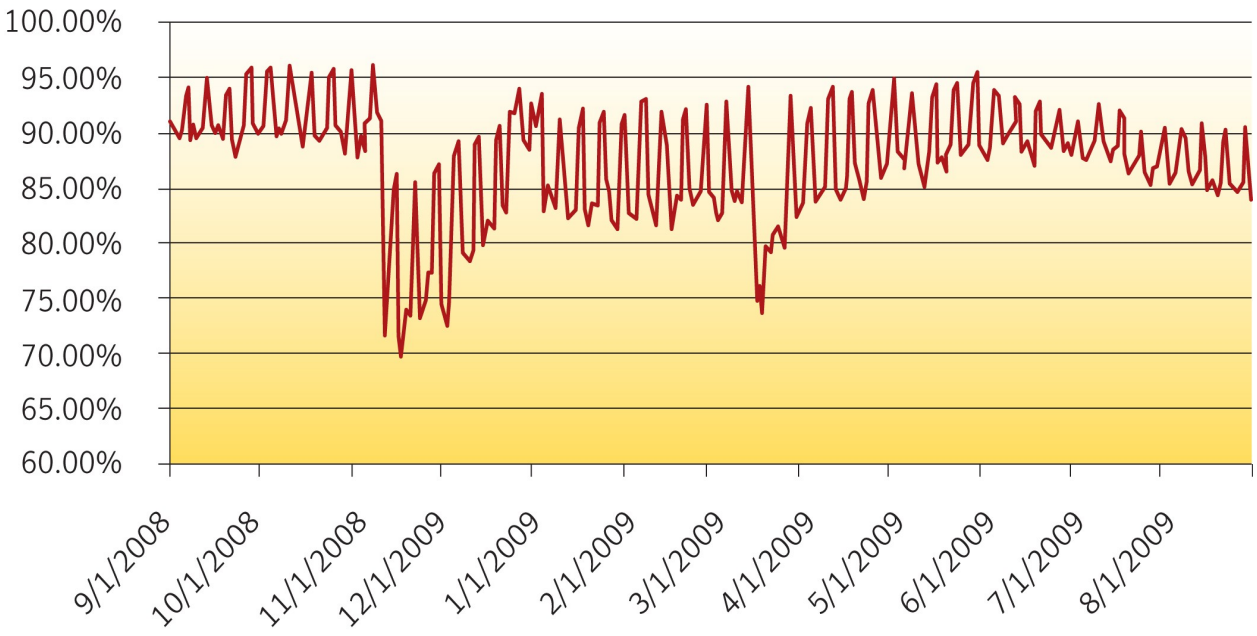
Overall spam volumes averaged at 87 percent of all email messages in August 2009. Health spam decreased again this month and averaged at 6.73 percent, while over 29 percent of spam is Internet related spam. Holiday spam campaigns have begun leveraging Halloween and Christmas, following closely after Labor Day-related spam.

The following trends are highlighted in the September 2009 report:

- **Holiday Spam Campaigns Begin in Earnest**
- **Spoofing Around the URLs**
- **Image Spam Gaining Weight**
- **August 2009: Spam Subject Line Analysis**
- **Checklist: Protecting your business, your employees and your customers**

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

Holiday Spam Campaigns Begin in Earnest

This year economists predict that there will be more pressure than ever for retailers to get an early start on what is expected to be a very difficult holiday season, overshadowed by the economic downturn and pressures on consumer spending. At the end of August 2009, two major retailers in the U.S. launched Christmas clubs. A Christmas Club is a savings program where a set amount of money is deposited into a special savings account, and the money is received back at the end of the year for Christmas shopping. Weak spending during the holiday season in 2008 brought sales to levels not seen since the 1980s.

Total holiday sales in 2008 were down two -to -four percent. With back to school campaigns now over the holiday campaigns starting, it is not surprising that spammers have followed suit with campaigns for Halloween and Christmas. Some of the holiday related spam subject lines include:

- Hello Halloween + Summer Sale, $3.99 and under!
- Labor Day Sale
- Sign Up for Our Halloween Workshop for Party Plans, Pumpkins, Decorations, and More!
- Biggest deal this Halloween
- Halloween discount
- It's new improved crazy Christmas
- Halloween great offers
- It's new improved crazy Christmas
- Halloween Already? Yes! Special Florida family coupons from Extreme Halloween

Labor Day which occurred in the U.S. on September 7, 2009 also did not escape the attention of spammers.

From: Get Ready For Labor Day
Date:
To:
Subject: Who can lend you Labor Day cash?

Spoofing Around the URLs

For the purpose of evading antispam filters, spammers often use obfuscation techniques, misuse brand names and other tactics to try and make it more difficult for content filtering to identify spam messages. Recently, Symantec has observed a spam attack where homograph spoofing is used so that the spoofed domain name partially or completely resembles the reputable brand domain name. Before discussing this trend, terms like IDN, Punycode and Homograph Spoofing will be introduced.

IDN

An Internationalized Domain Name (IDN) is a domain name that contains one or more non-ASCII characters. Such domain names could contain characters from non-Latin scripts such as Arabic, Chinese or Devnagari.
Example:
The domain ëxample.com uses “ë” which is a Cyrillic character.

Punycode

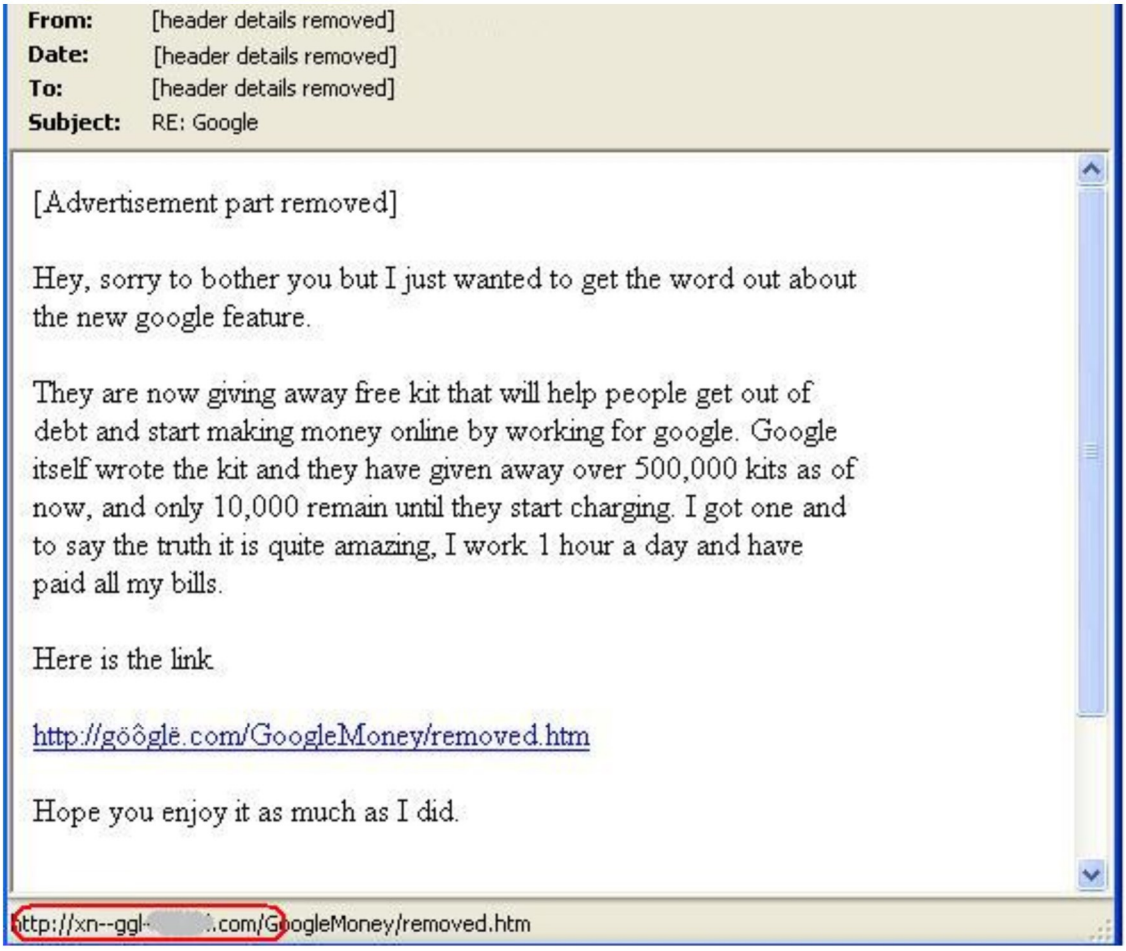
Punycode is syntax designed for encoding IDN in applications such that these domain names (non-ASCII part) may be represented in the ASCII character set. Using Punycode non-ASCII, characters are converted into ASCII character set. This provides unique and reversible identification of the domain. Punycode converted names are prefixed with “xn--”.
Example:
Punycode for ëxample.com is http://www.xn--xample-ouf.com/

Homograph Spoofing

This is spoofing of characters by exploiting the fact that in multilingual computer systems, many different characters may have nearly (or wholly) indistinguishable glyphs.
Example:
The domain ëxample.com (Russian) resembles closely example.com (Latin)

In the spam example below , a spammer is offering free money making kits. A URL is provided in the message which directs users to a registration form where a user’s personal information is harvested. When analyzed closely, it was found that the domain in the URL is scripted using IDN. This spoofed domain resembles google.com. The URL and Punycode is as shown in the below image.

Spoofing Around the URLs



The table below shows various possible spoofed variants of the domain google.com. Many of them closely resemble its Latin counterpart.

IDN	Script	Punycode
google.com	Greek	http://www.xn--ggle-0nda.com/
google.com	Cyrillic	http://www.xn--ggl-tdd6ba.com/
google.com	Portuguese	http://www.xn--ggle-55da.com/
g□□gle.com	Thai	http://www.xn--ggle-gpoa.com/

This is not the first time that spammers have lured recipients into action by hiding behind reputable brands. However, users can avoid falling victim to spoofed URLs by looking at the actual URL in the status bar or typing in the URL manually. Taking some time to do a little re-search can save your personal information from being jeopardized.

Image Spam Gaining Weight

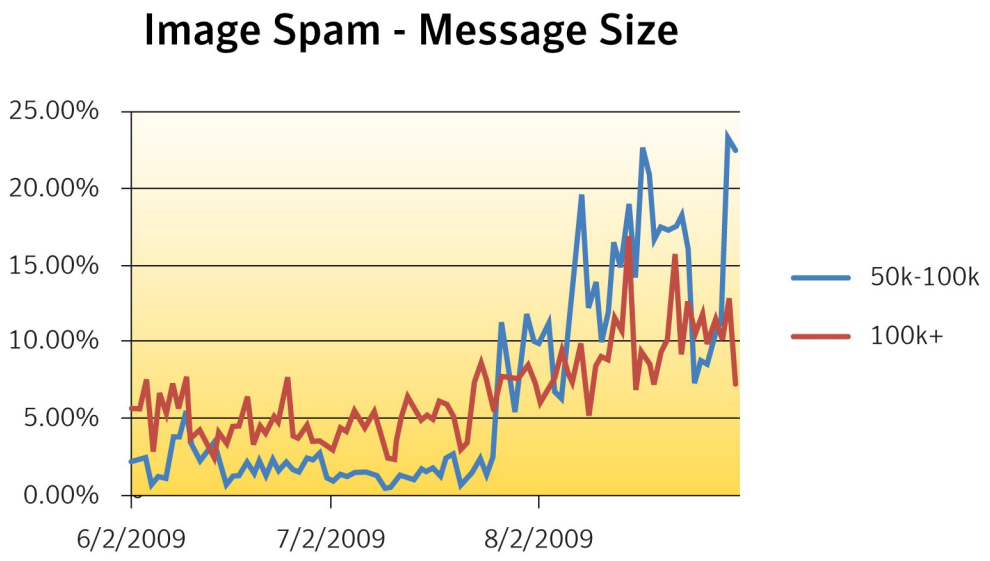
While image spam never quite went away and averaged at four percent of all spam in August 2009, image spammers continue to use various techniques to try and evade antispam filters. In August 2009, Symantec observed an increase in the average size of these messages. Similar increases in message size were also reported by Symantec in November 2008.

After monitoring the messages during the month of August the following was concluded:

- 9.3 percent of image spam had a message size greater than 100kb
- 14.43 percent of image spam had an average size of between 10kb-50kb.

In recent weeks, a variation in the approach of image spam has also been observed. Spammers are again inserting Shakespearean text in their messages. In the last 2-3 months, Symantec observed similar messages with similar attachments. However, the messages contained just a single line or no text at all in the messages. The chart below illustrates our observations. It displays image spam data collected for the last three months.

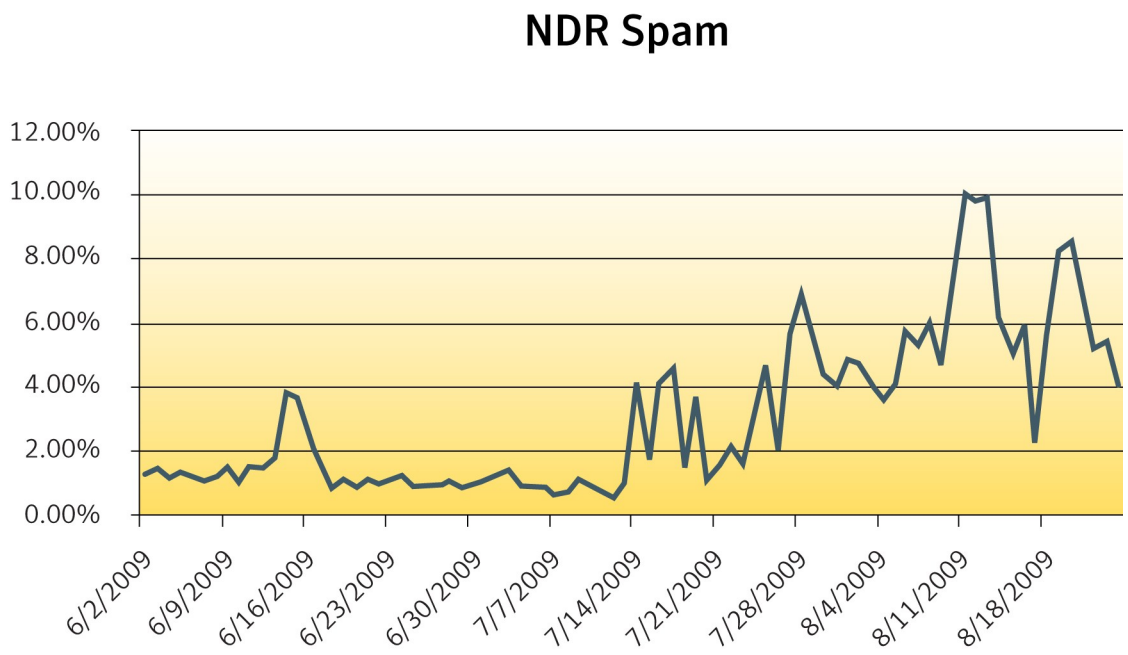
Larger messages cause a significant burden on IT resources and can delay the delivery of legitimate messages from reaching their intended users.



August 2009: Spam Subject Line Analysis

#	Total Spam: August 2009 Top Subject Lines	No of Days	Total Spam: July 2009 Top Subject Lines	No of Days
1	Delivery Status Notification (Failure)	31	You've received a greeting ecard	22
2	Delivery Status Notification	31	RE: UK Pharmacy Online Sale 80% OFF!	8
3	Re: Order status	31	You have new message!	7
4	Your order	31	Delivery Status Notification (Failure)	31
5	RE: Message	31	You have a new message!	11
6	Return Mail	31	Delivery Status Notification	31
7	no-reply	31	rxsub	10
8	new mail	31	Hey	31
9	Return mail	31	Hi	31
10	Undelivered Mail Returned to Sender	31	Aloha	31

In the August 2009 report, the top subject lines used by spammers were revealed. Spammers often use common and casual subject lines such as; *Hey* or *Hi,* in an effort to evade antispam filters and try and entice the end user into opening their spam message. In this month's report, the top subject lines are dominated by subjects that included: Delivery Status Notification (Failure), Return Mail and Undelivered Mail Returned to Sender. The prominence of these subject lines in August corresponds with an increase in NDR bounce spam which reached up to 10 percent of all spam at some points, but averaged at 5.7 percent in August 2009. Symantec defines NDR bounce messages that contain full or partial spam messages within the bounce report as spam.



Checklist: Protecting your business, your employees and your customers

Do

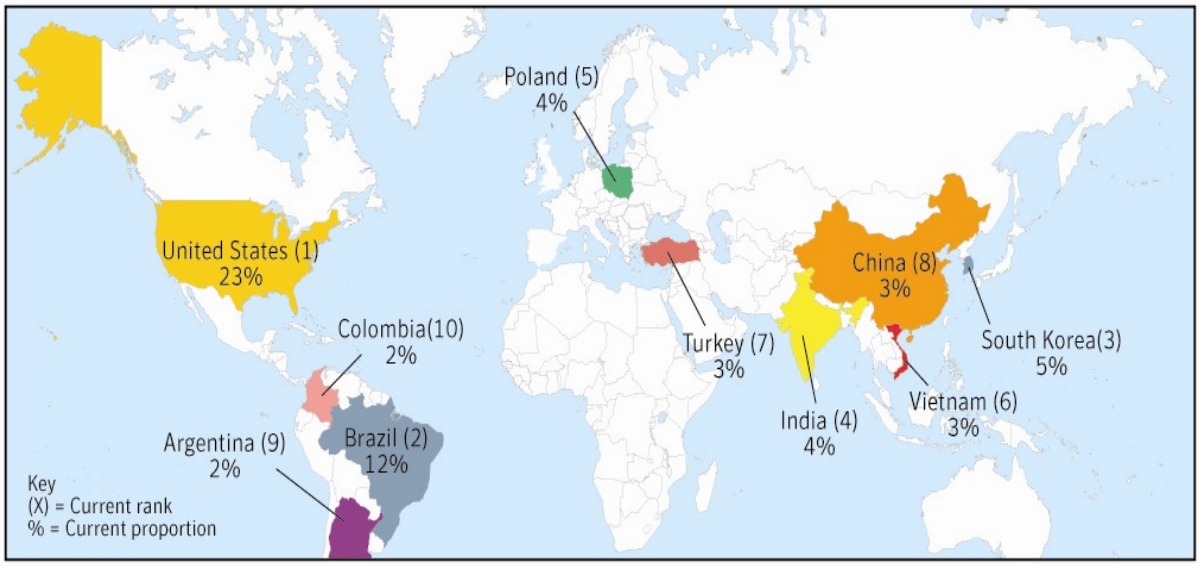
- Unsubscribe from legitimate mailings that you no longer want to receive. When signing up to receive mail, verify what additional items you are opting into at the same time. De-select items you do not want to receive.
- Be selective about the Web sites where you register your email address.
- Avoid 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	August	July	Change
United States	23%	25%	-2%
Brazil	12%	12%	0%
South Korea	5%	6%	-1%
Turkey	3%	4%	-1%
India	4%	4%	0%
Colombia	2%	Not listed	n/a
Poland	4%	4%	0%
China	3%	3%	0%
Vietnam	3%	2%	1%
Argentina	2%	2%	0%

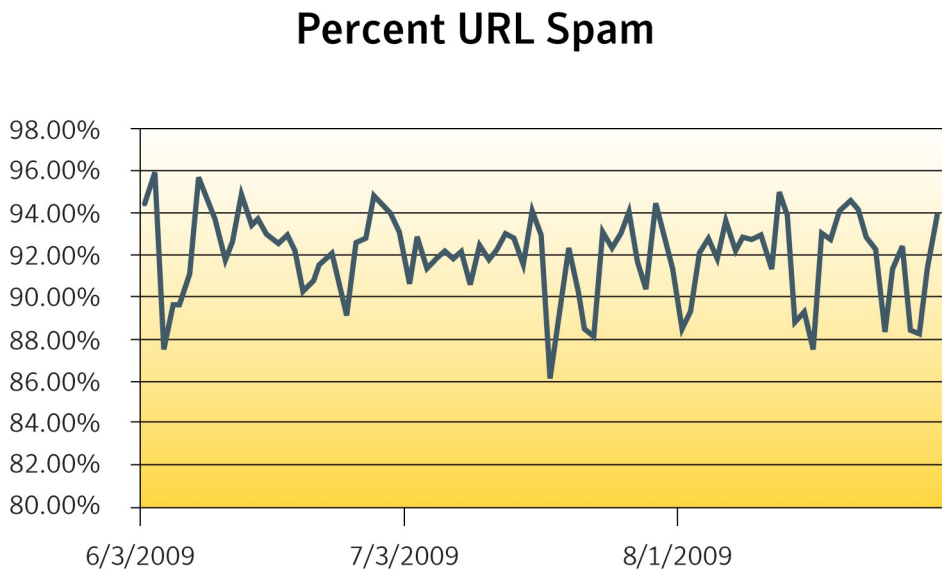
Metrics Digest: URL TLD Distribution

TLD	August	July	Change
com	45%	42%	3%
cn	46%	46%	0%
net	3%	6%	-3%
org	2%	2%	0%

Metrics Digest: Average Spam Message Size

Message Size	August	July	Change
0-2k	10.24%	6.00%	4%
2k- 5k	59.39%	55.00%	4%
5k-10k	22.77%	29.00%	-6%
10k+	8%	10%	-2%

Metrics Digest: Percent URL Spam



Metrics Digest: Global Spam Categories:

Category Name	August	July	Change
adult	1.80%	3%	-1%
financial	19.68%	16%	4%
fraud	6.55%	5%	2%
health	6.73%	11%	-4%
internet	29.30%	28%	1%
leisure	4.16%	4%	0%
419 spam	9.23%	9%	0%
political	<1%	<1%	No Change
products	18.30%	21%	-3%
scams	3.84%	3.00%	1%

- **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*