



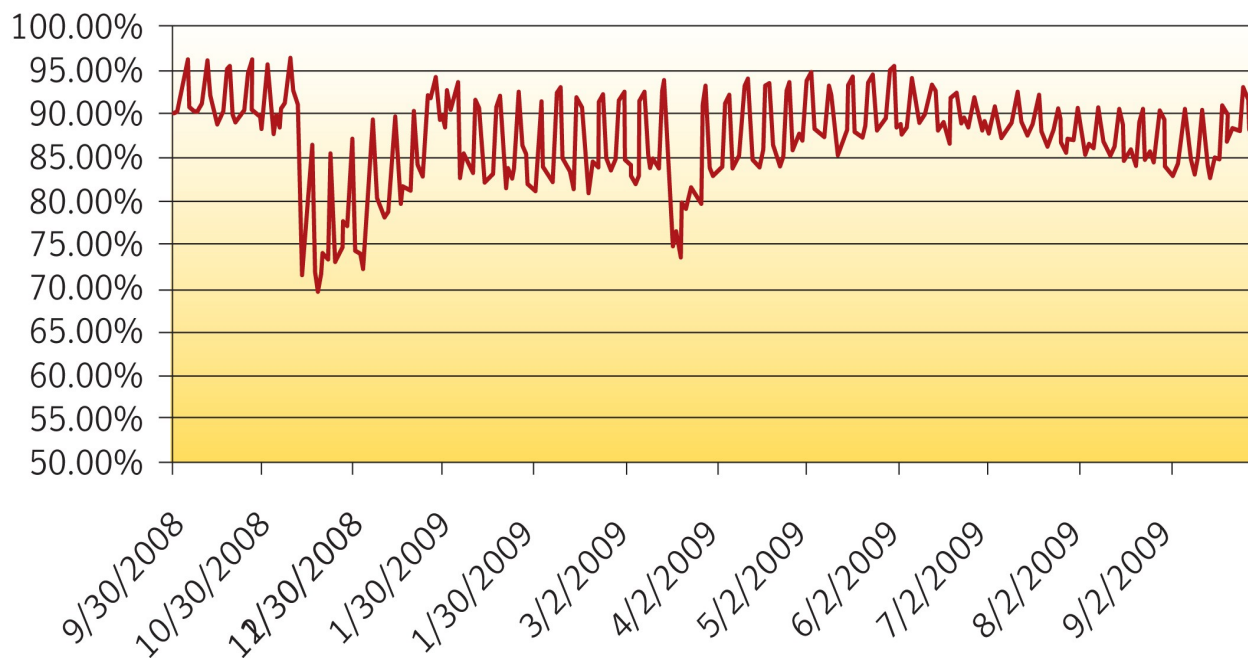
During the month of September 2009, spam averaged slightly over 86 percent of all email messages. Notable this month is that the percentage of spam containing malware has increased, reaching up to 4.5 percent of all spam at one point. When compared to August 2009, we observed a nine fold increase in spam containing malware during September. The spam types that experienced the greatest change during the past month were Internet spam which increased by three percent again this month, and averages at 32 percent of all spam, and financial spam which decreased 3 percent to account for 17 percent of all spam.

The following trends are highlighted in the October 2009 report:

- **Spam Spotlight : Implications of the Increasing Malicious Spam September 2009: Spam Subject Line Analysis**
- **Holiday Spam Campaigns Diversify**
- **Russian Spammers Dialing to Work Three Days A Week**
- **Career Opportunities @ Spammers.EDU**

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

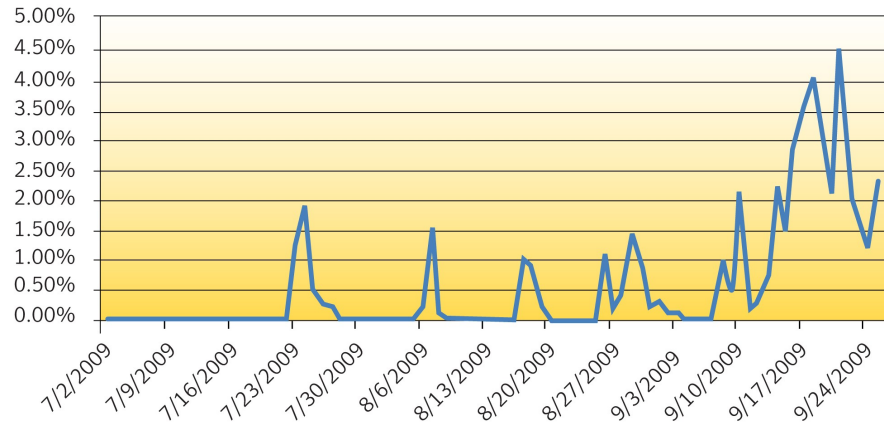
Dermot Harnett
Editor
Antispam Engineering

Cory Edwards
PR Contact
cory_edwards@symantec.com

Spam Spotlight: Implications of the Increasing Malicious Spam

Recent data suggests that the percentage of spam containing malware has increased. In September 2009, an average of 1.3 percent of all spam messages contained malware. When compared with August 2009, this equates to a nine fold increase in the number of messages containing malware month on month. The number of messages containing malware actually hit a peak of 4.5 percent of all spam at one point during September.

Viruses as a Percentage of Spam



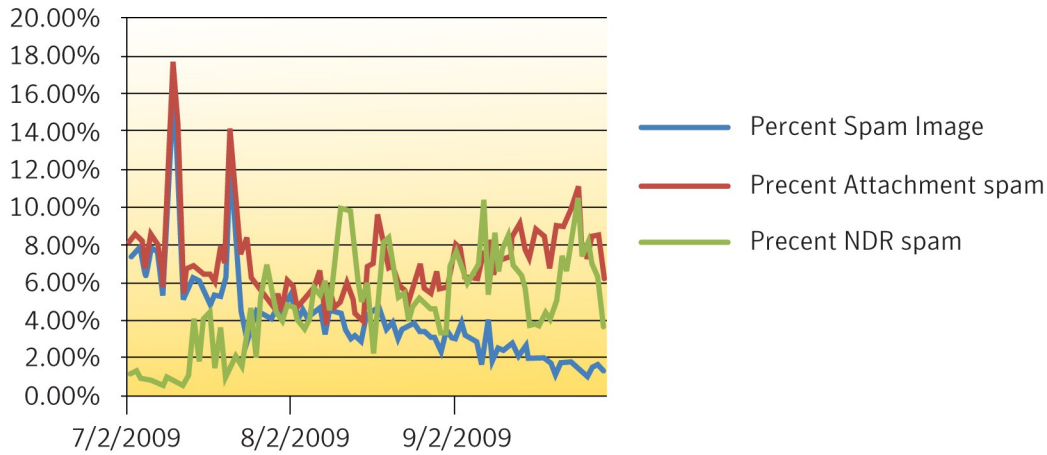
While the single digit increase may seem relatively small at first, the consequences of this rise is quite significant when you consider that 86.39 percent of all email messages in September 2009 were spam. Additional implications include :

- An increase in attached malware contributed to an increase in the average spam message size. From the spam attack vectors chart below an increase in attachment spam can be observed in September 2009. Also, in September, spam messages with a size greater than 10k increased by 5 percent while spam messages that had an average size between 0-2k dropped by 7 percent. Larger messages cause a significant burden on IT resources and can delay the delivery of legitimate messages from reaching their intended users.

Message Size	September	August	Change
0-2k	3.43%	10.24%	-7%
2k- 5k	55.19%	59.39%	-4%
5k-10k	28.21%	22.77%	5%
10k+	13%	8%	5%

Spam Spotlight: Implications of the Increasing Malicious Spam

Spam Attack Vectors



- Over the past year, a number of ISPs have been taken offline for hosting botnet activity. For example, at approximately 21:30 GMT on November 11, 2008, multiple upstream network providers shut down access to McColo.com hosted systems, based on abuse complaints. One of the results of this action was a quick and dramatic decrease in spam sent worldwide. While spam levels have recovered, the distribution of malware and the possible infection of some machines enables a shift in botnet activity to take place as various botnets fight for position.

September 2009: Spam Subject Line Analysis

#	Total Spam: September 2009 Top Subject Lines	No of Days	Total Spam: August 2009 Top Subject Lines	No of Days
1	Notice of Underreported Income	20	Delivery Status Notification (Failure)	31
2	Delivery Status Notification (Failure)	30	Delivery Status Notification	31
3	failure notice	30	Re: Order status	31
4	Undelivered Mail Returned to Sender	30	Your order	31
5	Thank you for setting the order No.475456	17	RE: Message	31
6	Returned mail: see transcript for details	30	Return Mail	31
7	Gain 3Inches	27	no-reply	31
8	Delivery Status Notification	30	new mail	31
9	Your order	22	Return mail	31
10	RE: Message	20	Undelivered Mail Returned to Sender	31

In the September 2009 report, the top subject lines used by spammers were dominated by subjects that included Delivery Status Notification (Failure), Return Mail and Undelivered Mail Returned to Sender. The prominence of these subject lines corresponded with an increase in NDR bounce spam. While NDR bounce spam continues to average at 6.14 percent of all spam in September 2009, which is an increase of 0.4 percent from August 2009, it is the emergence of malware related subject lines including “Notice of Underreported Income” and “Thank you for setting the order No.475456” that is significant. Two notable malware related attacks highlighted in the September 2009 Top Subject Lines are outlined below.

September 2009: Spam Subject Line Analysis

- A legitimate IRS settlement offering U.S. taxpayers' holding accounts in foreign banks the opportunity to fully disclose and pay their back taxes, interest and penalties ended September 23rd 2009. Spammers used this opportunity to send fake IRS email notifications with the subject line "Notice of Underreported Income" to recipients and, using a fraudulent URL link, encouraged them to "download and execute" their IRS statement. The executable download "tax-statement.exe," is detected as malware by Symantec.

From: Internal Revenue Service
Date:
To:
Subject: Notice of Underreported Income


Taxpayer ID: mutqgaksen-00000174073547US
Tax Type: INCOME TAX
Issue: Unreported/Underreported Income (Fraud Application)

Please review your tax statement on Internal Revenue Service (IRS) website (click on the link below):

[review tax statement for taxpayer id: mutqgaksen-00000174073547US](#)

Internal Revenue Service

- In the second example which contained the subject line "Thank you for setting the order No.475456," the spam email messages promised undelivered parcels and cash for collection. Depending on whether the delivery is for cash or a parcel, the message may differ slightly. The malware samples observed so far in this campaign have been detected by our antivirus products as Packed.Generic.243.

From:
Date:
To:
Subject: Thank you for setting the order No.475456
Attach:  nz.zip (0 bytes)

Dear Customer!

Thank you for ordering at our online store.

Your order: A1133651A, was sent at your address.

The tracking number of your postal parcel is indicated in the document attached to this letter.

Please, print out the postal label for receiving the parcel.

Internet Store.

Holiday Spam Campaigns Diversify

In August 2009 it was revealed that spam campaigns targeting end of year holidays such as Christmas had begun in earnest. Overshadowed by the economic downturn and with pressure continuing on consumer spending, the emergence of Christmas-themed spam campaigns in August were not unexpected. While Christmas and Halloween spam continues, two recent holiday-themed spam campaigns show the diversification of spam campaigns today.

- The Diwali “Festival of Lights” in October is celebrated across India and a large portion of the Indian population goes out shopping and looking for holiday deals. In this example, the spam message selling database CDs of contacts (name, email address, age, phone), ‘Diwali’ is inserted to make it look enticing for recipients. As shown in the following sample message, recipients are offered a database CD of 57,000 Indian companies (SMEs).

From:
Date:
To:
Subject: Diwali Offer for Databases in India

Dear Customers,

Now you can get Database CD of 57,000 indian companies (SMEs) with following details:

Company Name / Contact Person / Designation / Phone No. / Fax No. / Mobile / Address. etc..

for just Rs. 999/-

Apart from above All India HNI/SME Database available.
Call now for more details.

In order to purchase, call
or email at
(Offer for a limited time period only)

- Chinese Mid-Autumn festival, also known as the Moon Festival is one of the major holidays celebrated in China. It occurs August 15 of the Chinese lunar calendar - that is October 3 on the western calendar this year. During this festival, families will gather to admire the bright full moon and eat mooncakes. It is a cultural tradition for friends and family members to send mooncakes and reunite for the holiday. While not unexpected, spammers have been capitalizing on this holiday in recent weeks by sending out mooncakes and gifts promotions to mark the day .



Russian Spammers Dialing to Work Three Days A Week

In January 2009, an increase in Russian spam offering various local trade services was observed. Rather than redirecting email recipients to malicious websites, the call to action for these messages was to insert telephone and ICQ numbers into the advertisements located in the message body of the spam email. Recently a new vector of this attack has emerged where spammers have inserted obfuscated phone numbers into the message header. The obfuscation has included inserted certain symbols [+*^] between the numbers found in the subject line header.

From: Гарнак Б.П.
Date:
To:
Subject: Уведомляем - Обновлено базы Высочайшая отдача -7*916 446*09-76

Докладываем - Обновлено базы
Отдача с рассылок выше

From: Вульф С.М.
Date:
To:
Subject: Уведомляем - Обновлено базы Отдача с рассылок выше -7 916+446+09 76

Уведомляем - Свежие базы
Высочайшая отдача

Translation:

Subject: highest response rate from Updated databases 7916.....

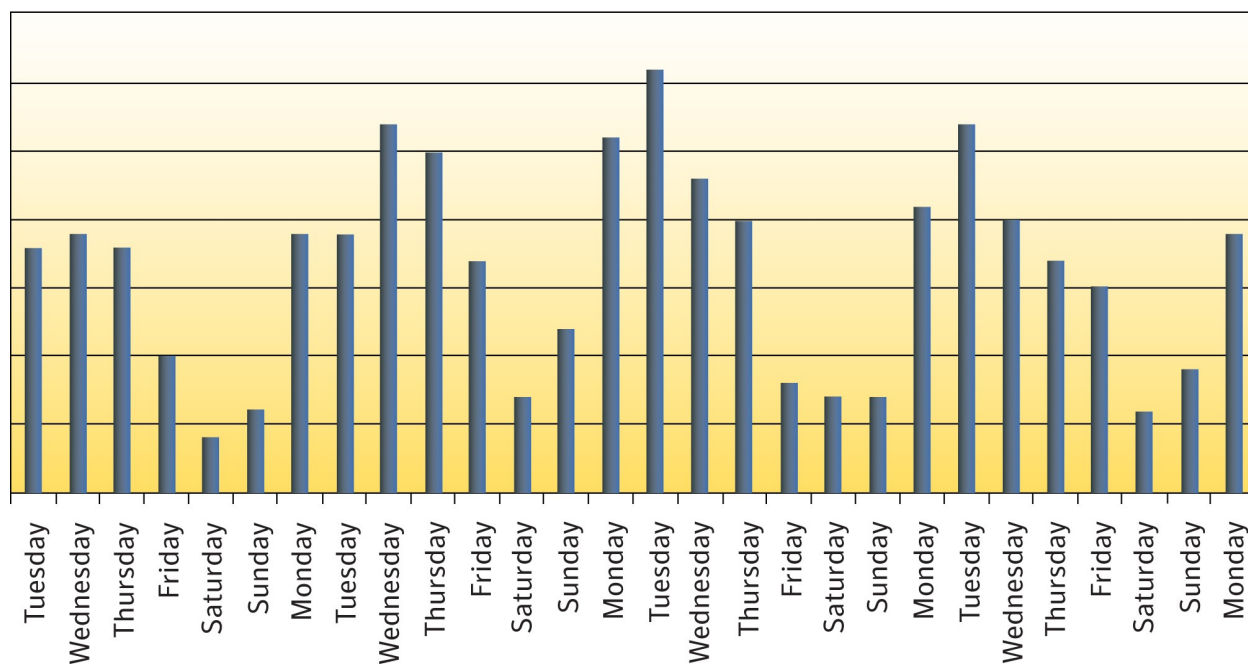
**Alert - Newest Databases
Highest response rate**



Russian Spammers Dialing to Work Three Days A Week

As this new Russian spam vector emerged, Russian spam volume was also examined and showed fluctuations with peaks on the first few days of the week, specifically on Mondays, Tuesdays, and Wednesdays. It declined on the remaining days of the week. This fluctuation in Russian spam volume can also be observed in July and August.

Russian Spam Volume September 2009





Career Opportunities @ Spammers.EDU

Online degree spam has been around for some time now with the emphasis generally placed on securing a degree within a few days. As many colleges reopened for another semester in August and September, and with the economic downturn forcing others to focus on alternate career opportunities, these degree spam messages are now focused on directing recipients to specific degree courses.

The top five “degrees” advertised through spam are:

1. Police Officer
2. Federal Agent
3. Nursing
4. Culinary Art
5. Teacher

It is interesting to note that this list is dominated by careers which are generally stable in the current economic environment and also careers, such as nursing, where shortages often occur. Other degree options provided and promoted after the above top five are: Crime Scene Investigation (CSI), Ultrasound Technician, Pharmacy Technician, Radiology, Photography, Paralegal and Medical Billing.

In addition to the degrees offered, certain terminology is consistently used in this type of spam message. The text shown in bold below is often exchanged in both the Subject and From header.

1. From header: Frequently, this header will indicate an urgency along with certain obfuscation patterns.

Examples:

+++NURSES NEEDED+++
TEACHERS NEEDED
POLICE OFFICERS NEEDED

Photography Schools
CULINARY TRAINING

2. Subject header: This header encourages a recipient to pursue a particular career.

Examples:

Become a CSI !!!
Become a Ultrasound Technician
Become a Teacher
Become a Chef !!n



Checklist: Protecting your business, your employees and your customers

Do

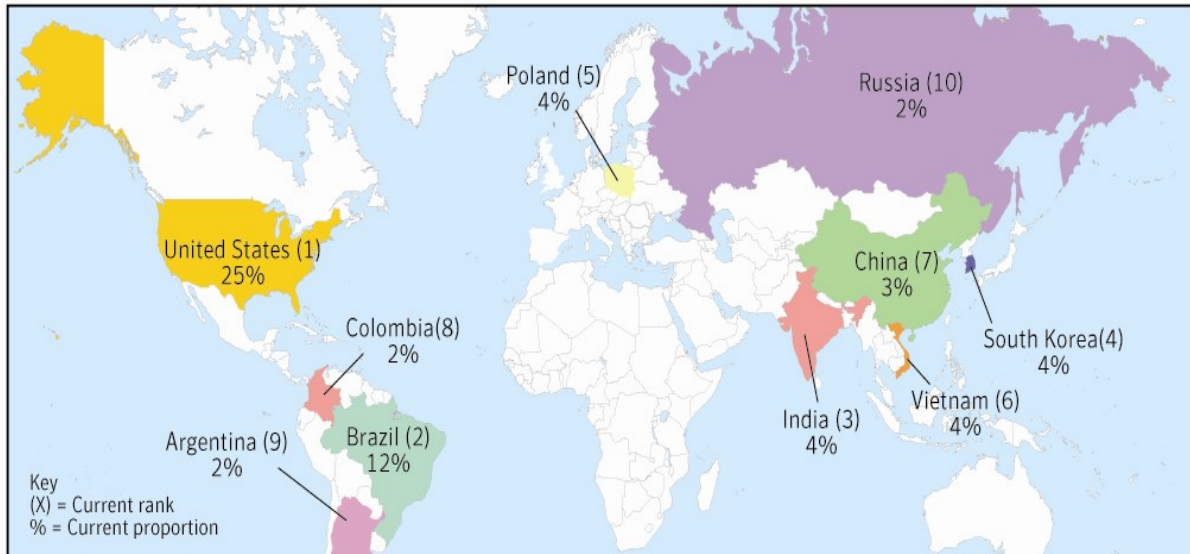
- Unsubscribe from legitimate mailings that you no longer want to receive. When signing up to receive mail, verify what additional items you are opting into at the same time. Deselect items you do not want to receive.
- Be selective about the Web sites where you register your email address.
- Avoid publishing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



Metrics Digest: URL TLD Distribution

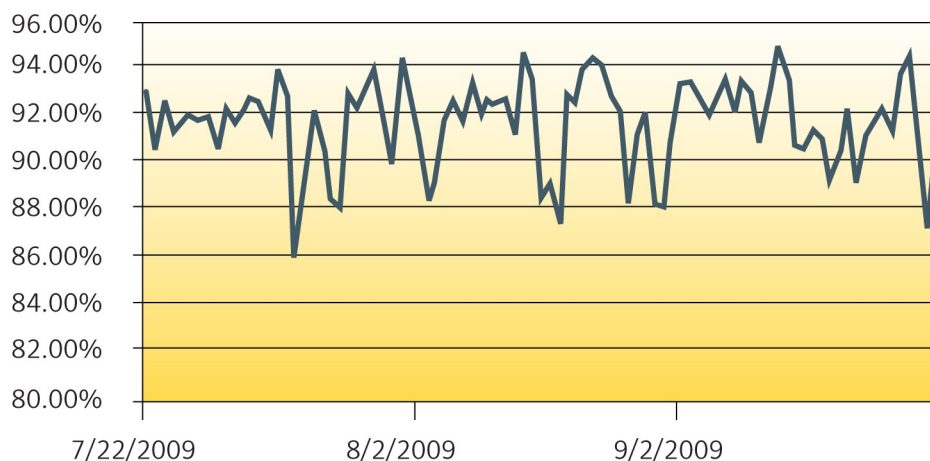
TLD	September	August	Change
com	43%	45%	-2%
cn	48%	46%	2%
net	2%	3%	-1%
org	4%	2%	2%
Other	3%	4%	-1%

Metrics Digest: Average Spam Message Size

Message Size	September	August	Change
0-2k	3.43%	10.24%	-7%
2k- 5k	55.19%	59.39%	-4%
5k-10k	28.21%	22.77%	5%
10k+	13%	8%	5%

Metrics Digest: Percent URL Spam

Percent URL Spam





Metrics Digest: Global Spam Categories:

Category Name	September	August	Change
adult	1.50%	1.80%	0%
financial	17.10%	19.68%	-3%
fraud	6.60%	6.55%	0%
health	6.90%	6.73%	0%
internet	32.30%	29.30%	3%
leisure	3.10%	4.16%	-1%
419 spam	9.70%	9.23%	0%
political	<1%	<1%	No Change
products	19.60%	18.30%	1%
scams	2.70%	3.84%	-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 misleading, 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*