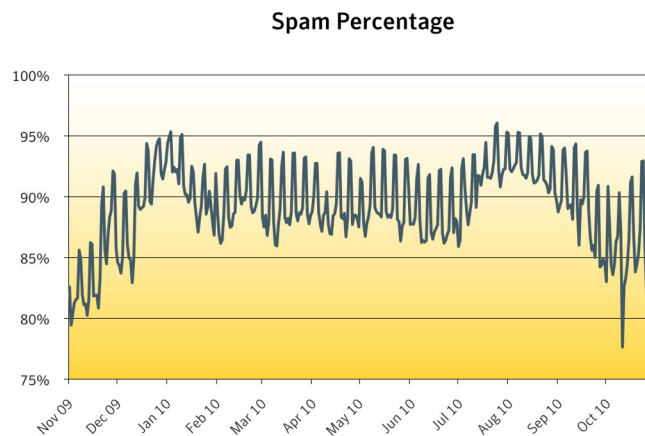


Overall, spam made up 86.61 percent of all messages in October, compared with 89.40 percent in September.

With respect to spam categories, the leisure category doubled to 12 percent in October, compared to 6 percent in September. This is reflected in the “October 2010: Spam Subject Line Analysis” section as there were several leisure type spam subject lines listed in the ranking. While this surge in the leisure category was surprising, the most unusual movement was seen in the political category. This category, which has historically been under 1 percent of all spam, increased to 1.4 percent. This can be attributed to November 2010 elections.



The overall phishing landscape increased by 0.3 percent this month, and was primarily due to an increase in automated toolkit attacks. Phishing websites created by automated toolkits increased by 41 percent, and unique URLs decreased by 10 percent. Phishing websites with IP domains (i.e. domains like <http://255.255.255.255>) increased significantly by about 58 percent and webhosting services comprised 14 percent of all phishing, an increase of 24 percent from the previous month. In addition, the number of non-English phishing sites increased by 10 percent. Among non-English phishing sites, French and Italian continued to be higher in October.

The following trends are highlighted in the November 2010 report:

- Phishing Social Media
- Spam Volume Continues to Drop
- The Holidays Arrive Early!
- 8-Part Russian Image Spam
- Phishing a Bank with an Offer of Mobile Phone Airtime
- Filing Deadline Extension Triggers More Fake Offers of Tax Refunds
- October 2010: Spam Subject Line Analysis

Dylan Morss
Executive Editor
Antispam Engineering

David Cowings
Executive Editor
Security Response

Eric Park
Editor
Antispam Engineering

Mathew Maniyara
Editor
Security Response

Sagar Desai
PR contact
sagar_desai@symantec.com

Metrics Digest

Global Spam Categories

Category Name	October	September	Change (% points)
Adult	3%	1%	+2
Financial	11%	10%	+1
Fraud	4%	3%	+1
Health	8%	12%	-4
Internet	37%	42%	-5
Leisure	12%	6%	+6
419 spam	7%	6%	+1
Political	1%	<1%	+1
Products	13%	16%	-3
scams	4%	3%	+1

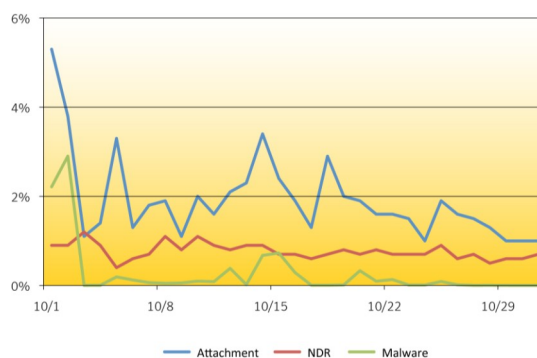
Spam URL TLD Distribution

TLD	October	September	Change (% points)
com	53.7%	60.0%	-6.3
ru	31.9%	23.2%	+8.7
org	6.6%	4.8%	+1.8
net	2.5%	Not listed	N/A

Average Spam Message Size

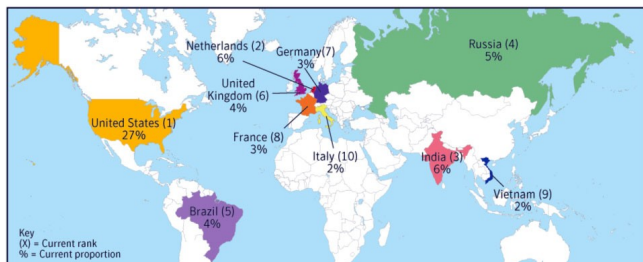
Message Size	October	September	Change (% points)
0-2kb	2.61%	11.15%	-8.54
2kb-5kb	68.00%	57.97%	+10.03
5kb-10kb	23.53%	22.88%	+0.65
10kb+	5.86%	8.00%	-2.14

Spam Attack Vectors



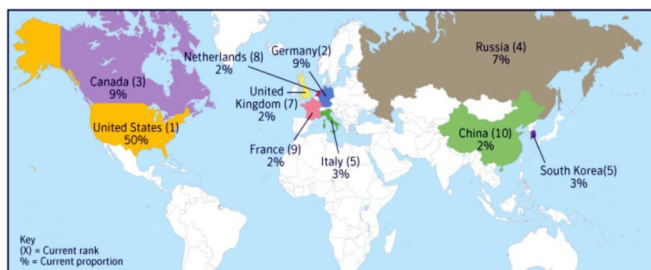
Metrics Digest

Spam Regions of Origin



Country	October	September	Change (% points)
United States	27%	23%	+4
Netherlands	6%	5%	+1
India	6%	6%	No change
Russia	5%	3%	+2
Brazil	4%	5%	-1
United Kingdom	4%	4%	No change
Germany	3%	4%	-1
France	3%	3%	No change
Vietnam	2%	3%	-1
Italy	2%	3%	-1

Geo-Location of Phishing Lures



Country	October	September	Change (% points)
United States	50%	56%	-6
Germany	9%	8%	+1
Canada	9%	5%	+4
Russia	7%	5%	+2
Italy	3%	3%	No Change
South Korea	3%	2%	+1
United Kingdom	2%	2%	No Change
Netherlands	2%	3%	-1
France	2%	2%	No Change
China	2%	1%	+1

Geo-Location of Phishing Hosts

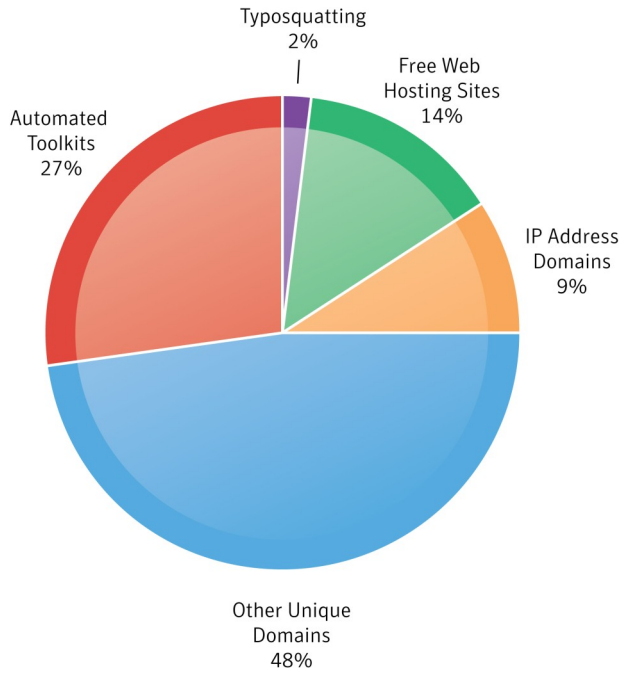


Country	October	September	Change (% points)
United States	50%	51%	-1
Canada	12%	11%	+1
Germany	7%	6%	+1
South Korea	3%	3%	No Change
Russia	3%	2%	+1
China	2%	2%	No Change
Italy	2%	2%	No Change
France	2%	3%	-1
Netherlands	2%	2%	No Change
United Kingdom	2%	3%	-1

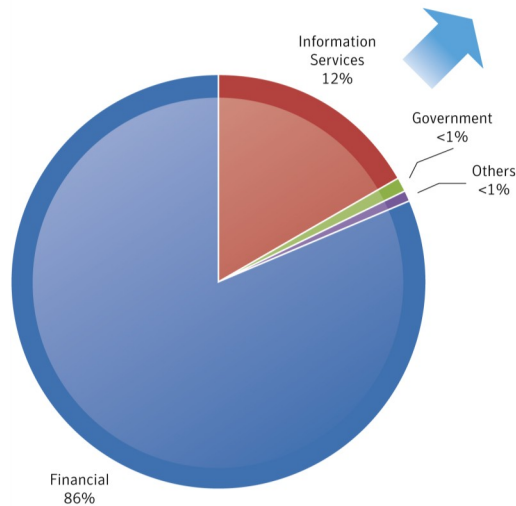
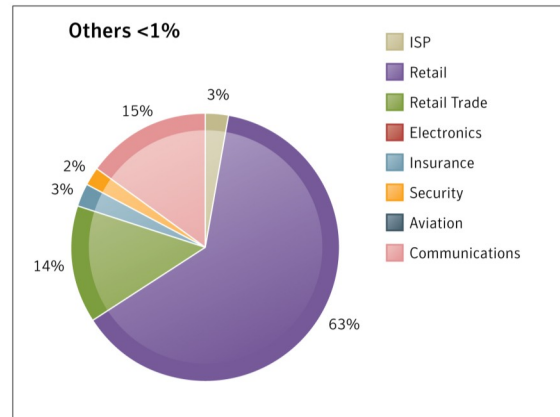
Metrics Digest

Phishing Tactic Distribution

Overall Statistics



Phishing Target Sectors



Phishing Social Media

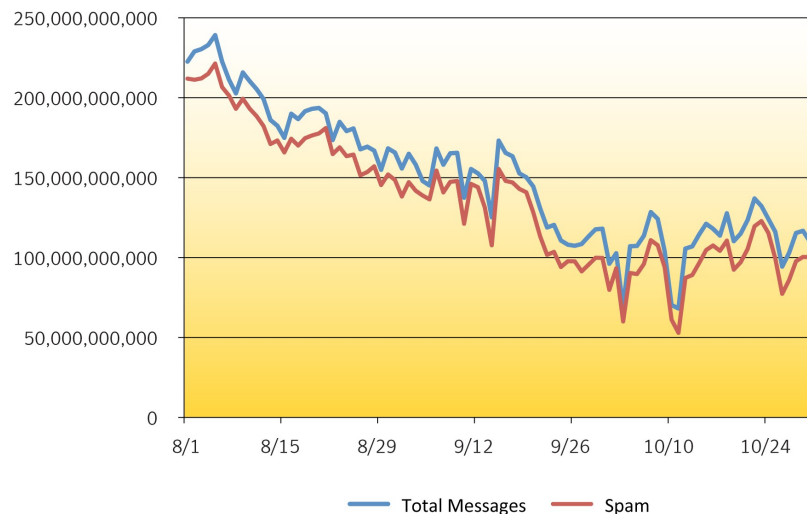
In October 2010, phishing on social media comprised about four percent of the overall phishing landscape. The number of phishing sites on social media increased significantly by about 80 percent compared to the previous month. As in the previous month, the majority of the phishing websites spoofed two brands. Phishing on these two brands combined comprised nearly 98 percent of all phishing on social media.

Phishers are known to use different kinds of bait to lure end-users in to giving away their confidential information. In October, a common type of bait observed was phishing sites that claimed to be from the security service of the social networking brand. The end-users were prompted to provide their login credentials to continue to access the social networking site.

Some noteworthy statistics of phishing on social media for October 2010:

- About 89 free webhosting services were used to host nearly 81 percent of all the phishing on social media.
- The highest occurrence of Top Level Domains (TLDs) in phishing sites on social media were .com, .net and .org which comprised of 74%, 6%, and 1% respectively.
- Among the country code TLDs (ccTLDs), Brazilian was evaluated to be the highest.
- Among the non-English social media phishing sites, Portuguese, Italian, and Spanish continued to be the highest. Other languages observed were Indonesian, Russian, Albanian, and Turkish.

Spam Volume Continues to Drop

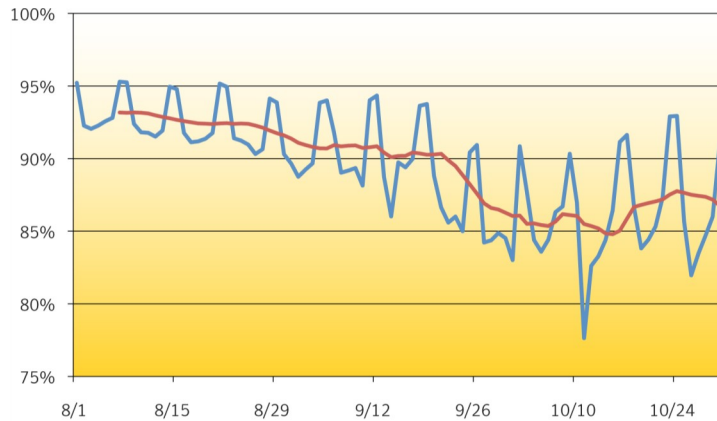


Last month's report highlighted a sharp decrease in global spam volume. While daily figures above show some signs of stabilization, monthly figures suggest otherwise. In October, global spam volume was down 22.5 percent month-over-month. Compared to August, volume was down over 47 percent.

Spam Volume Continues to Drop (continued)

In addition to events highlighted in last month's report (Zeus ring takedown and spamit.com shutdown), Netherlands recently have taken down several servers associated with Bredolab botnet.

Historically, lower spam volume translates into lower spam percentage. This is primarily due to the volume of legitimate mail being fairly constant. More spam added to the legitimate mail leads to higher overall spam percentage. October was no exception to this as the overall spam percentage was 86.6 percent, the lowest since September 2009.



The Holidays Arrive Early!

Though consumers may be keeping a conservative hold on their wallets, spammers have already started their holiday spam campaign blitz. Symantec has observed a variety of spam using the holiday angle including: replica, online pharmacy, and even the 419-type Nigerian scam. With the holidays just around the corner, we expect spammers to pick up the volume of holiday spam.

From: [REDACTED]
Date: [REDACTED]
To: [REDACTED]
Subject: Product availability

THE CLOCK IS TICKING

...Christmas is coming

Orders prior to November 5th will ensure product availability, 15% instant rebates and complimentary express postage.
All 2010 and 2011 product models are currently available.

Our full product line is handcrafted to ensure 100% accurate details.
We do not use any parts/materials manufactured in China.

ONLINE MALL:

[http://www.\[REDACTED\]](http://www.[REDACTED])

*Product pictures on website are of actual products

[REDACTED] est 2004

From: [REDACTED]
Date: [REDACTED]
To: [REDACTED]
Subject: Be [REDACTED] this Christmas

Simply the best option for men... [REDACTED] at the same time... See the results!
Gain Strength and Power
Burn Off Excess Fat
Boost Energy Levels

[CLICK HERE](#)

From: [REDACTED]
Date: [REDACTED]
To: none
Subject: CHRISTMAS OFFER !!!!

New for CHRISTMAX 2010! from the hottest fashion to the latest electricals, we've got it all.

To Get Started, Please Click below.

[https://www.\[REDACTED\]](https://www.[REDACTED])

Hurry while offer last

[REDACTED] Online Department

8-Part Russian Image Spam

Symantec has observed spammers sending out Russian spam messages being sent with 8 mime parts, with 6 of the parts being images. This particular spammer in the example below is going to great lengths to improve delivery. Taking it one step further, other spammers are also randomizing the sizes of the image parts as well as the zoom level of the image that is being split. All of these efforts may render non-premium antispam filters ineffective.

1: **обслуживание клиентов и претензиями**

Москва

ний!

Ваши продажи и репутация напрямую зависят от качества обслуживания клиентов. Пройдя наш тренинг, Вы сможете построить

2: **Первоклассное обслуживание клиентов и претензиями**

22 23 ноября | г. Москва

2 дня практических занятий!

Ваши продажи и репутация напрямую зависят от качества обслуживания клиентов. Пройдя наш тренинг, Вы сможете построить

3: **Вы сможете повысить уровень сервиса своей компании и увеличить количество постоянных и новых клиентов!**

8 (495) 229 30 11

4: **Вы сможете построить компанию, приобрести лояльных постоянных и новых клиентов!**

Действуют скидки!
Материалы входят в стоимость регистрации на семинар:

5: **Пройдя наш тренинг, Вы сможете повысить уровень сервиса своей компании и увеличить количество постоянных и новых клиентов!**

Осталось 5 мест!
Стоимость: 17 900 р. Действуют скидки!
Ресторанное питание и материалы входят в стоимость
Подробности и регистрация на семинар:

6: **Первоклассное обслуживание клиентов и претензиями.**

Ресторанное питание и материалы входят в стоимость

From: [REDACTED]
Date: [REDACTED]
To: [REDACTED]
Subject: [REDACTED]

Первоклассное обслуживание клиентов и претензиями.

22 23 ноября | г. Москва
2 дня практических занятий!

Ваши продажи и репутация напрямую зависят от качества обслуживания клиентов. Пройдя наш тренинг, Вы сможете построить компанию, приобрести лояльных постоянных и новых клиентов!

Осталось 5 мест!
Стоимость: 17 900 р. Действуют скидки!
Ресторанное питание и материалы входят в стоимость
Подробности и регистрация на семинар:

These six image parts add up to a complete one in actual email:



Phishing a Bank with an Offer of Mobile Phone Airtime

In October 2010, a phishing site of a bank was observed that used fake offers of mobile phone airtime as bait. A similar trend was reported earlier in the phishing of a social networking site. To read more on the trend, please refer to “[Fraudsters Offering Free Mobile Phone Airtime](#)”.

In this particular attack, the phishing site spoofed the login page of a popular Italian bank. Upon entering the login credentials, the phishing page requested that the customer choose from a list of four mobile service providers. After the service provider was selected, the page requested the customer’s mobile phone number and the amount of airtime to recharge. The phishing page claimed that 40 Euros would be given as a bonus in addition to the amount selected for recharge. This fake offer of a bonus is the bait used by fraudsters in the hopes of tempting customers to give away their sensitive information.



RICARICA CELLULARI

Scegli il gestore di telefonia mobile

RICARICA CELLULARI

Scegli il gestore di telefonia mobile

Seleziona il numero da ricaricare

Seleziona l'importo della ricarica

RICARICA CELLULARI

Scegli il gestore di telefonia mobile

Seleziona il numero da ricaricare

Inserisci il prefisso inserisci il numero [avanti](#)

Seleziona l'importo della ricarica

10 € * Saranno accreditati altri 40 € sotto forma di bonus. [continua](#)

20 €

25 €

50 €

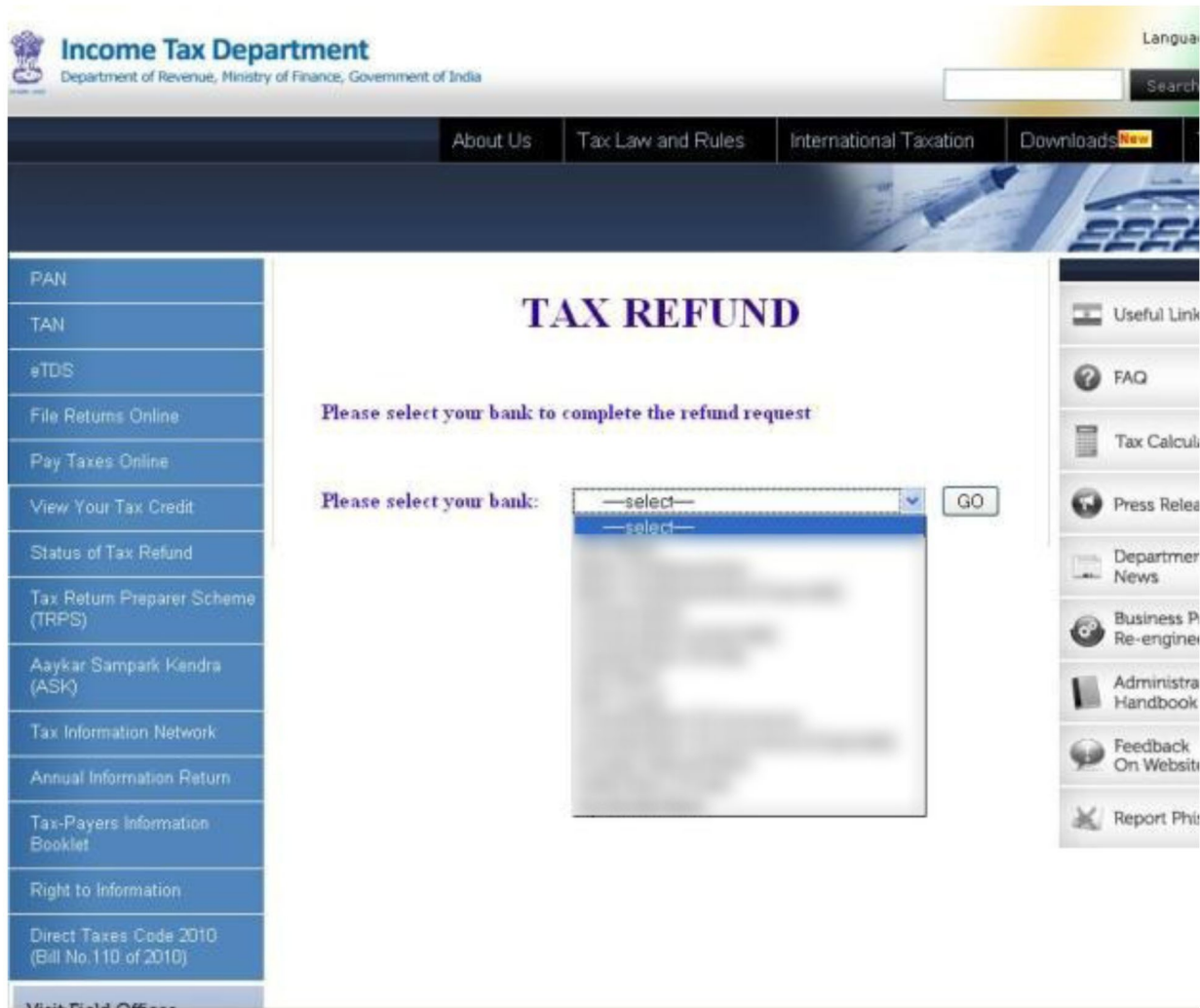
Finally, the phishing page displayed a summary of the data provided by the customer. The phishing page further requested a password of the customer’s mobile device in order to complete the transaction. After the password is entered, a message is displayed that the recharge will be delivered within 24 hours. The customer is then redirected to the legitimate bank’s website. Fraudsters are yet again looking for means by which they can steal banking credentials for financial gain.

The phishing site was hosted on servers based in the USA. The domain name of the phishing site was a typosquat of the bank, so customers may have entered the phishing site from typographical errors made while typing the legitimate website address.

Filing Deadline Extension Triggers More Fake Offers of Tax Refunds

The Central Board of Direct Taxes of India extended the deadline for filing income tax for FY11 from September 30, 2010, to October 15, 2010, in view of difficulties caused by the recent floods in various parts of the country. The announcement was followed by phishing attacks spoofing the Indian Income Tax Department's website.

The phishing websites had "Tax Refund" as the title and contained a message that requested the customer to select from a list of 10 Indian banks to complete the refund request. Once a bank was selected from the list, the customer was redirected to a phishing site spoofing the login page of the selected bank. After the login credentials were entered into the phishing site, the customer was redirected back to the legitimate bank's website. In this way, phishers were targeting several banks from a single phishing website. The primary motive in these phishing attempts was financial gain. The phishing sites were hosted on servers based in Mississauga, Canada.



The screenshot shows a phishing website designed to look like the official Indian Income Tax Department website. At the top, it features the department's logo and name: "Income Tax Department, Department of Revenue, Ministry of Finance, Government of India". A search bar and language selector are visible in the top right. A navigation menu includes "About Us", "Tax Law and Rules", "International Taxation", and "Downloads".

The main content area is titled "TAX REFUND" in large, bold letters. Below the title, it says "Please select your bank to complete the refund request". There is a form with a dropdown menu labeled "Please select your bank:" and a "GO" button. The dropdown menu is open, showing a list of banks, though the text is blurred. A sidebar on the left contains a list of services: PAN, TAN, eTDS, File Returns Online, Pay Taxes Online, View Your Tax Credit, Status of Tax Refund, Tax Return Preparer Scheme (TRPS), Aaykar Sampark Kendra (ASK), Tax Information Network, Annual Information Return, Tax-Payers Information Booklet, Right to Information, and Direct Taxes Code 2010 (Bill No. 110 of 2010). A sidebar on the right contains "Useful Link", "FAQ", "Tax Calculators", "Press Release", "Department News", "Business Process Re-engineering", "Administrative Handbook", "Feedback On Website", and "Report Phishing".

October 2010: Spam Subject Line Analysis

#	Total Spam: October 2010 Top Subject Lines	No of Days	Total Spam: September 2010 Top Subject Lines	No of Days
1	Katya 21y.o, new message for you	2	<i>Blank Subject line</i>	30
2	Julia 22y.o, new message for you.	4	hello	30
3	Nikki Sent You A Message	18	Delivery Status Notification (Failure)	30
4	<i>Blank Subject line</i>	30	Get Unlimited Lovin!	9
5	Hello	28	Your wife photos attached	11
6	hi!	20	LinkedIn Messages, 9/30/2010	1
7	You have got new message(dating)	1	LinkedIn Alert	6
8	Re: CV	20	Labor Day Specials! The Official Site of AsSeenOnTV	2
9	News Alert: New #1 Online Dating Site	8	LinkedIn new messages	3
10	Undelivered Mail Returned to Sender	30	You have notifications pending	10

As mentioned in the Monthly Landscape Summary, the leisure category doubled month-over-month. Five subject lines in the ranking were related to the leisure category. Coupled with online pharmacy spam, it made malware spam messages leveraging social networks completely disappear. Going forward into the holiday season, we expect product and gift related spam subject lines to be most prevalent.

From: Notification
Date: [REDACTED]
To: [REDACTED]
Subject: You have got new message(dating)

Dear member of our D a t i n g site!
 You have **7 unread** messages from ladies.
 Please, check them [HERE](#)

Best wishes to you,
 Olga
 administrator

From: [REDACTED]
Date: [REDACTED]
To: [REDACTED]
Subject: Katya 21y.o, new message for you

My best wishes to you!
 I am Katya, 21 y.o,
 I am looking for man to have a strong family.
 And you?
I am online now, let's chat?
 my profile and new photos are [HERE](#)

Note! New free services! check info at the site!
 to unsubscribe- reply with "delete"

kisses, Administrator Elena

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.

* Spam data is based on messages passing through Symantec Probe Network.

* Phishing data is aggregated from a combination of sources including strategic partners, customers and security solutions.