State of Spam & Phishing
A Monthly Report

Confidence in a connected world. symantec.

March 2010 Report #39

Scam and phishing messages in February accounted for 19 percent of all spam, which is 2 percentage points lower than in January, but nevertheless an elevated level. Spammers continued to use the earthquake in Haiti, and the recent earthquake in Chile as another vector to utilize. They also used other current high-profile events, such as recent auto recalls, to deliver spam messages. Also taking a look at international threats, this reports highlights attacks specific to Brazil, China, Russia, and India.

Symantec observed a 16 percent increase from the previous month in all phishing attacks. This was primarily due to an increase in the volume of unique URL and IP attacks. 13 percent of phishing URLs were generated using phishing toolkits, an increase of 9 percent from the previous month. A 12 percent increase was observed in non-English phishing sites from the previous month. There was a significant increase in phishing sites in Italian and French languages. The increase in Italian language phishing was attributed to a rise in attacks on three Italian banks. Phishing on one Canadian financial institution and one French bank led to the rise in attacks in French. More than 98 Web hosting services were used, which accounted for 12 percent of all phishing attacks.

The following trends are highlighted in the March 2010 report:

- Still No Sympathy From Spammers
- Affected by Recalls? Spammers Want to Know
- Will the Trend Continue?
- International Spam & Phishing Roundup
- Phishing the Brands of Online Auction Marketing Tools
- February 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	February	January	Change (% points)
Adult	1%	2%	-1
Financial	12%	11%	+1
Fraud	8%	10%	-2
Health	11%	14%	-3
Internet	33%	31%	+2
Leisure	4%	6%	-2
419 spam	7%	7%	No change
Political	<1%	<1%	No change
Products	19%	14%	+5
scams	4%	4%	No change

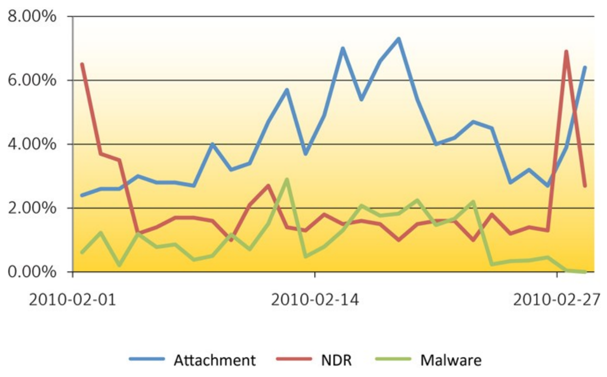
Spam URL TLD Distribution

TLD	February	January	Change (% points)
com	57.2%	68.6%	-11.4
ru	25.1%	4.9%	+20.2
org	4.9%	7.8%	-2.9
net	3.2%	Not listed	N/A

Average Spam Message Size

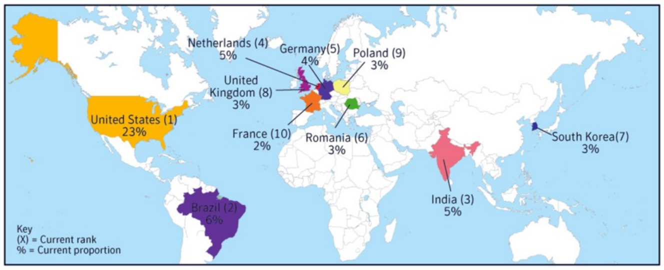
Message Size	February	January	Change (% points)
0-2kb	0.52%	0.83%	-0.31
2kb-5kb	76.53%	72.02%	+4.51
5kb-10kb	14.39%	22.58%	-8.19
10kb+	8.56%	4.57%	+3.99

Spam Attack Vectors



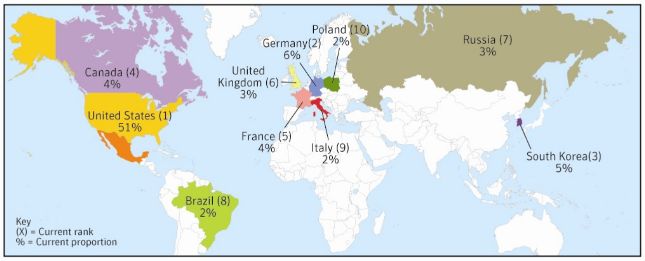
Metrics Digest

Spam Regions of Origin



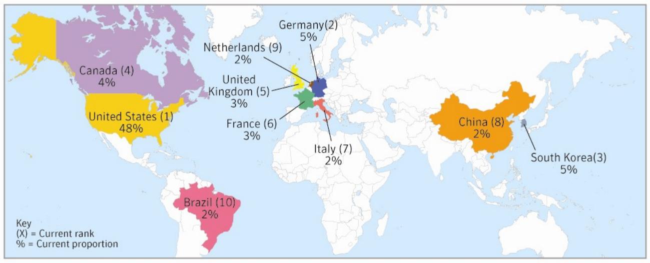
Country	February	January	Change (% points)
United States	23%	24%	-1
Brazil	6%	6%	No change
India	5%	5%	No change
Netherlands	5%	5%	No change
Germany	4%	5%	-1
Romania	3%	3%	No change
South Korea	3%	3%	No change
United Kingdom	3%	2%	+1
Poland	3%	3%	No change
France	2%	Not listed	N/A

Geo-Location of Phishing Lures



Country	February	January	Change (% points)
United States	51%	52%	-1
Germany	6%	6%	No Change
South Korea	5%	4%	+1
Canada	4%	4%	No Change
France	4%	4%	No Change
United Kingdom	3%	3%	No Change
Russia	3%	3%	No Change
Brazil	2%	3%	-1
Italy	2%	2%	No Change
Poland	2%	1%	+1

Geo-Location of Phishing Hosts

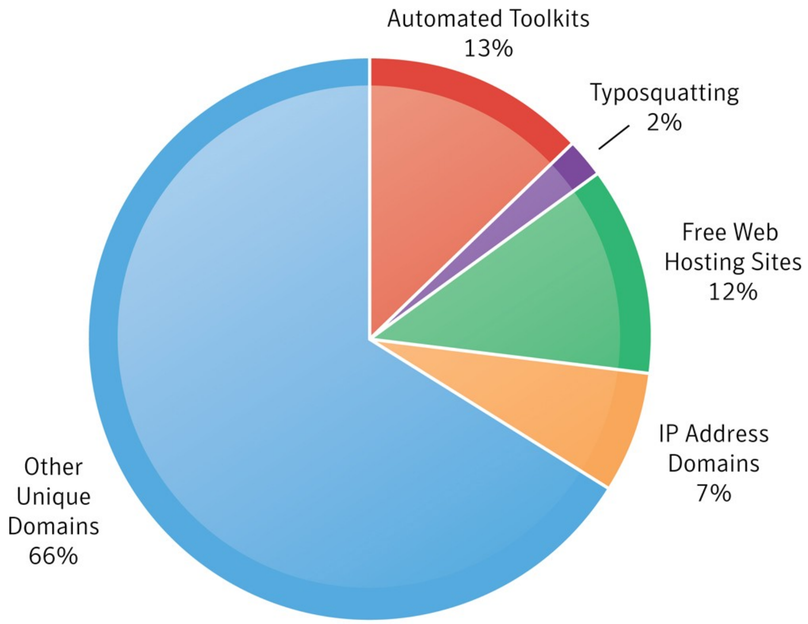


Country	February	January	Change (% points)
United States	48%	49%	-1
Germany	5%	6%	-1
South Korea	5%	3%	+2
Canada	4%	4%	No Change
United Kingdom	3%	3%	No Change
France	3%	3%	No Change
Italy	2%	2%	No Change
China	2%	2%	No Change
Netherlands	2%	Not listed	N/A
Brazil	2%	Not listed	N/A

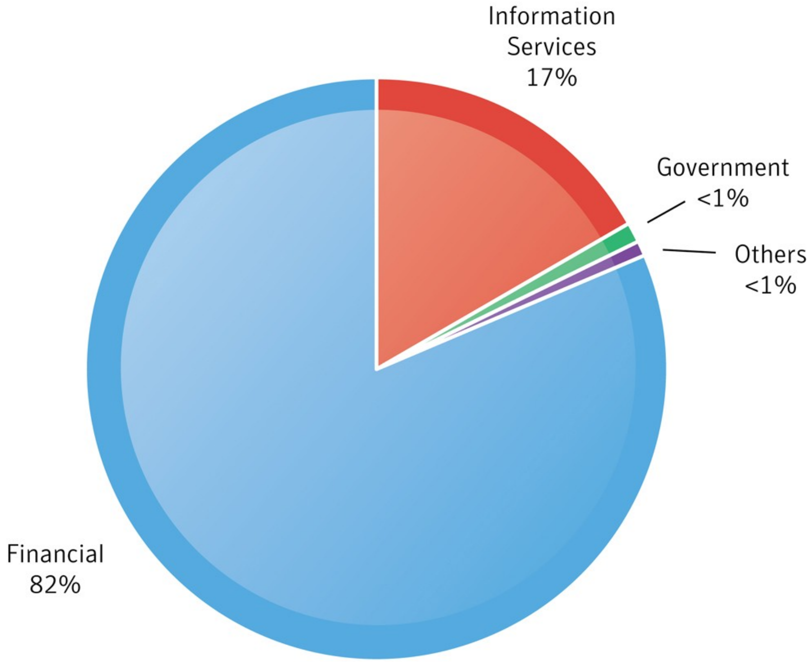
Metrics Digest

Phishing Tactic Distribution

Overall Statistics

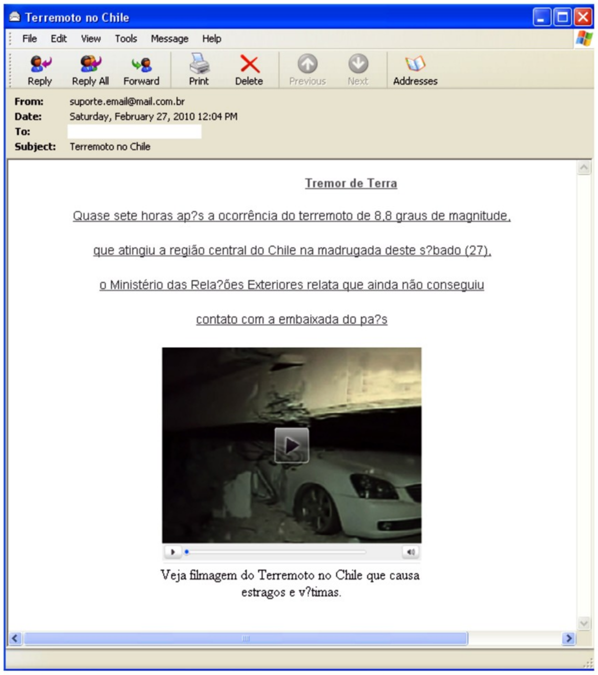


Phishing Target Sectors



Still No Sympathy From Spammers

On February 27th, a strong earthquake with a magnitude of 8.8 occurred off the coast of Chile. As Symantec noted in last month's report with the Haiti earthquake, spammers continue to leverage these tragic events for their benefit. The example below downloads malware when the user clicks on the link to view the video.



From: suporte.email@mail.com.br
Date: Saturday, February 27, 2010 12:04 PM
To:
Subject: Terremoto no Chile

Tremor de Terra

Quase sete horas ap?s a ocorrência do terremoto de 8,8 graus de magnitude,

que atingiu a região central do Chile na madrugada deste s?bado (27),

o Ministério das Rela?ões Exteriores relata que ainda não conseguiu

contato com a embaixada do pa?s

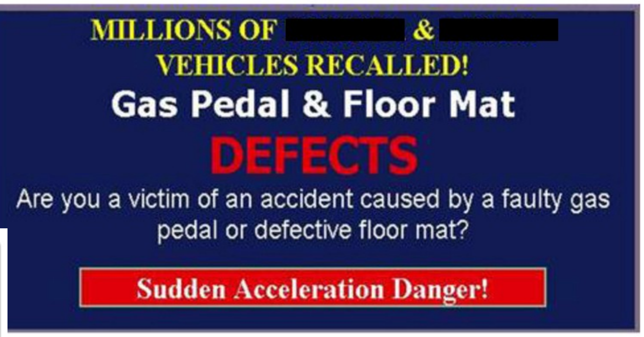
Veja filmagem do Terremoto no Chile que causa estragos e v?timas.

To protect from such malware threats as well as other types of scam and phishing attempts using these earthquakes as cover, Symantec suggests that users:

- Avoid clicking on suspicious links in e-mail or instant messages as these may be links to spoofed, or fake, Web sites.
- Never fill out forms in messages that ask for personal or financial information or passwords. A reputable charitable organization is unlikely to ask for your personal details via e-mail. When in doubt, contact the organization 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).

Affected by Recalls? Spammers Want to Know

There has been several recalls from multiple automobile manufacturers recently. Due to a very large number of vehicles involved in this round of recalls, there has been widespread interest in developments regarding this event. In these examples, spammers trick the user to give up personal information by pretending to be a legal industry representative.

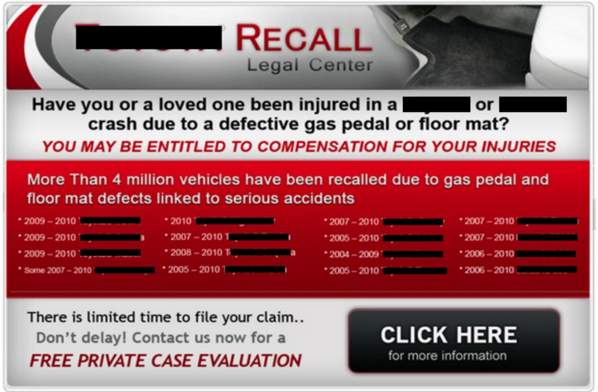


MILLIONS OF [redacted] & [redacted] VEHICLES RECALLED!

Gas Pedal & Floor Mat DEFECTS

Are you a victim of an accident caused by a faulty gas pedal or defective floor mat?

Sudden Acceleration Danger!



[redacted] RECALL
Legal Center

Have you or a loved one been injured in a [redacted] or [redacted] crash due to a defective gas pedal or floor mat?

YOU MAY BE ENTITLED TO COMPENSATION FOR YOUR INJURIES

More Than 4 million vehicles have been recalled due to gas pedal and floor mat defects linked to serious accidents

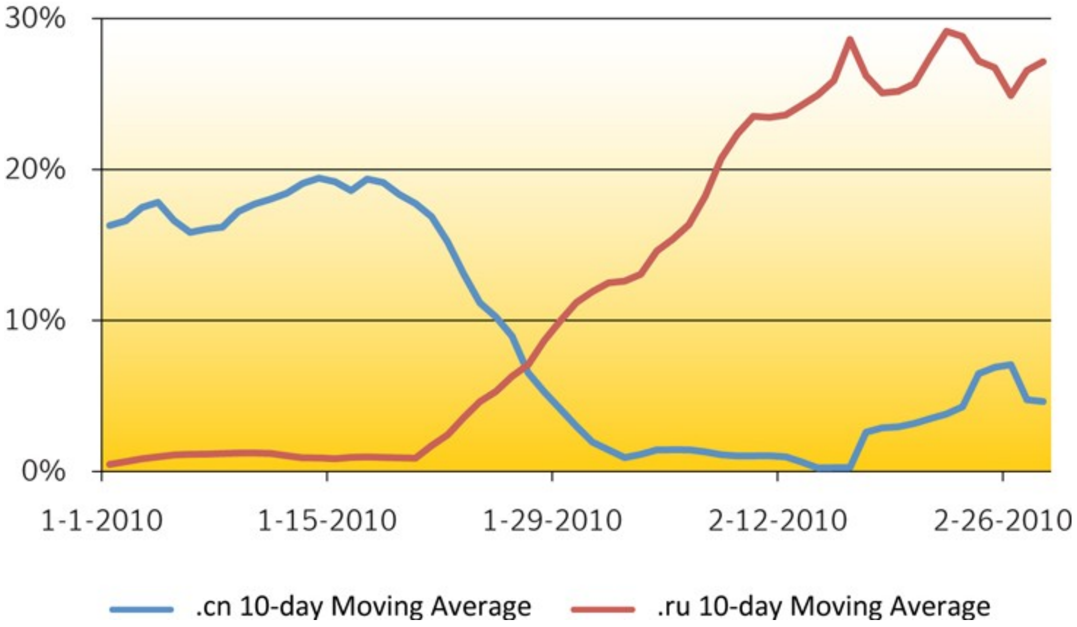
- 2009 – 2010 [redacted]
- 2009 – 2010 [redacted]
- 2009 – 2010 [redacted]
- Some 2007 – 2010 [redacted]
- 2010 [redacted]
- 2007 – 2010 [redacted]
- 2008 – 2010 [redacted]
- 2005 – 2010 [redacted]
- 2007 – 2010 [redacted]
- 2005 – 2010 [redacted]
- 2004 – 2009 [redacted]
- 2005 – 2010 [redacted]
- 2007 – 2010 [redacted]
- 2007 – 2010 [redacted]
- 2006 – 2010 [redacted]
- 2006 – 2010 [redacted]

There is limited time to file your claim..
Don't delay! Contact us now for a
FREE PRIVATE CASE EVALUATION

Will the Trend Continue?

In the previous month’s report, Symantec highlighted a sharp decline in spam containing .cn URLs. This was due to the China Internet Network Information Center (CNNIC)’s action to tighten registration of .cn domains. Although spam messages containing .cn URL crept up a little bit towards the end of February, the effect of CNNIC’s new policy is clearly shown in the graph below.

However, Symantec researchers have noticed a strong inverse relationship between .cn and .ru URLs as spam messages with .ru domains have increased dramatically. Spammers may have just found themselves a refuge after getting pushed out by CNNIC.

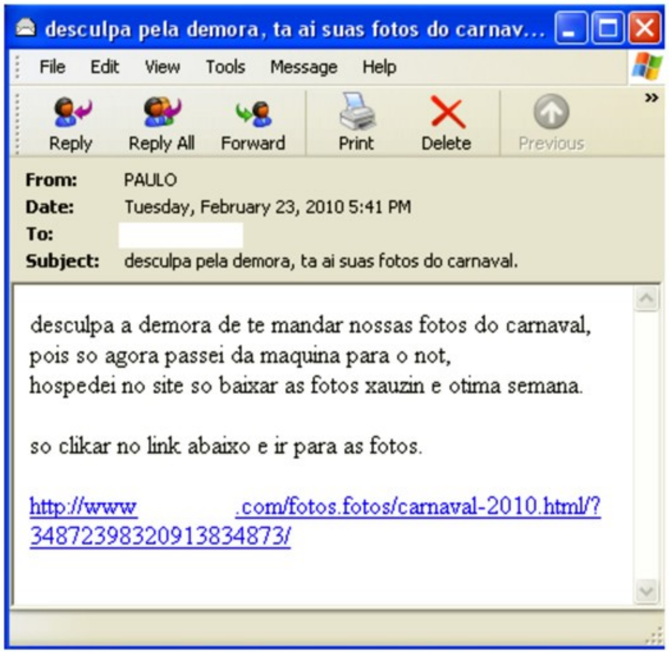


Unlike last month when EMEA region recorded 7.9 percentage point increase month-over-month, the geographical breakdown of origin of spam remained fairly flat in February.

Region	February	January	Change (% points)
North America	23.5%	24.6%	-1.1
Latin America	13.7%	13.9%	-0.2
APJ	19.6%	19.2%	+0.4
EMEA	43.2%	42.3%	+0.9

International Spam & Phishing Roundup

Spammers delivered malware by luring the user with pictures of the Rio Carnival.

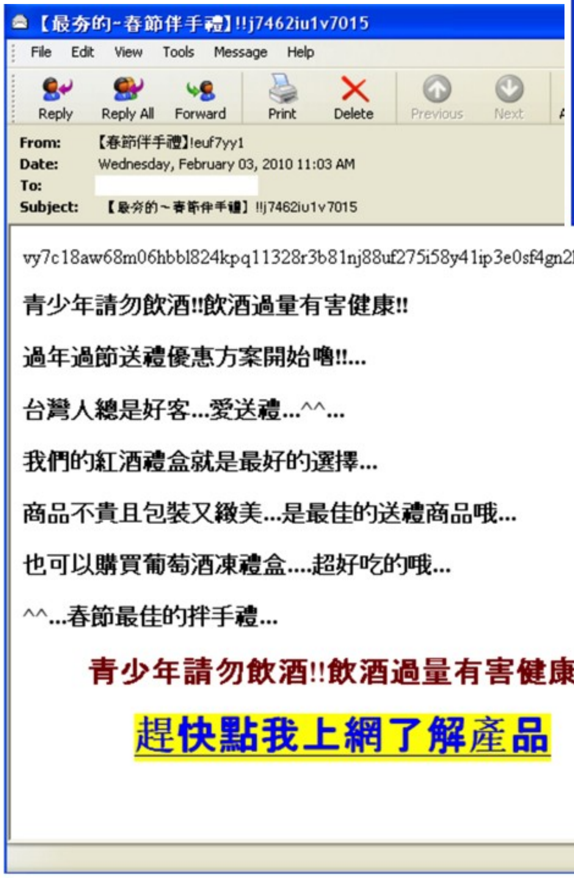

desculpa pela demora, ta ai suas fotos do carnav...
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous

From: PAULO
Date: Tuesday, February 23, 2010 5:41 PM
To:
Subject: desculpa pela demora, ta ai suas fotos do carnaval.

desculpa a demora de te mandar nossas fotos do carnaval,
pois so agora passei da maquina para o not,
hospedei no site so baixar as fotos xauzin e otima semana.

so clikar no link abaixo e ir para as fotos.

http://www .com/fotos.fotos/carnaval-2010.html/?34872398320913834873/


【最夯的~春節伴手禮】!!j7462iu1v7015
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next

From: 【春節伴手禮】!euf7yy1
Date: Wednesday, February 03, 2010 11:03 AM
To:
Subject: 【最夯的~春節伴手禮】!!j7462iu1v7015

vy7c18aw68m06hbbl824kpq11328r3b81nj88uf275i58y41ip3e0sf4gn2lolrl610t00

青少年請勿飲酒!!飲酒過量有害健康!!

過年過節送禮優惠方案開始嚕!!...

台灣人總是好客...愛送禮...^^...

我們的紅酒禮盒就是最好的選擇...

商品不貴且包裝又緻美...是最佳的送禮商品哦...

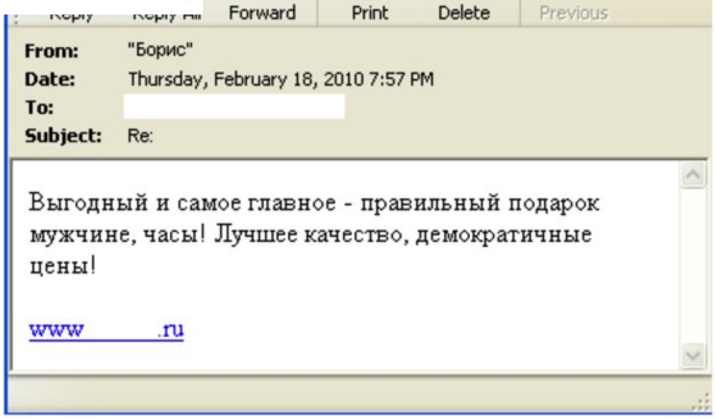
也可以購買葡萄酒凍禮盒....超好吃的哦...

^^...春節最佳的拌手禮...

青少年請勿飲酒!!飲酒過量有害健康!!

趕快點我上網了解產品

Chinese spammers sent product spam using the Chinese New Year holiday.



From: "Борис"
Date: Thursday, February 18, 2010 7:57 PM
To:
Subject: Re:

Выгодный и самое главное - правильный подарок мужчине, часы! Лучшее качество, демократичные цены!

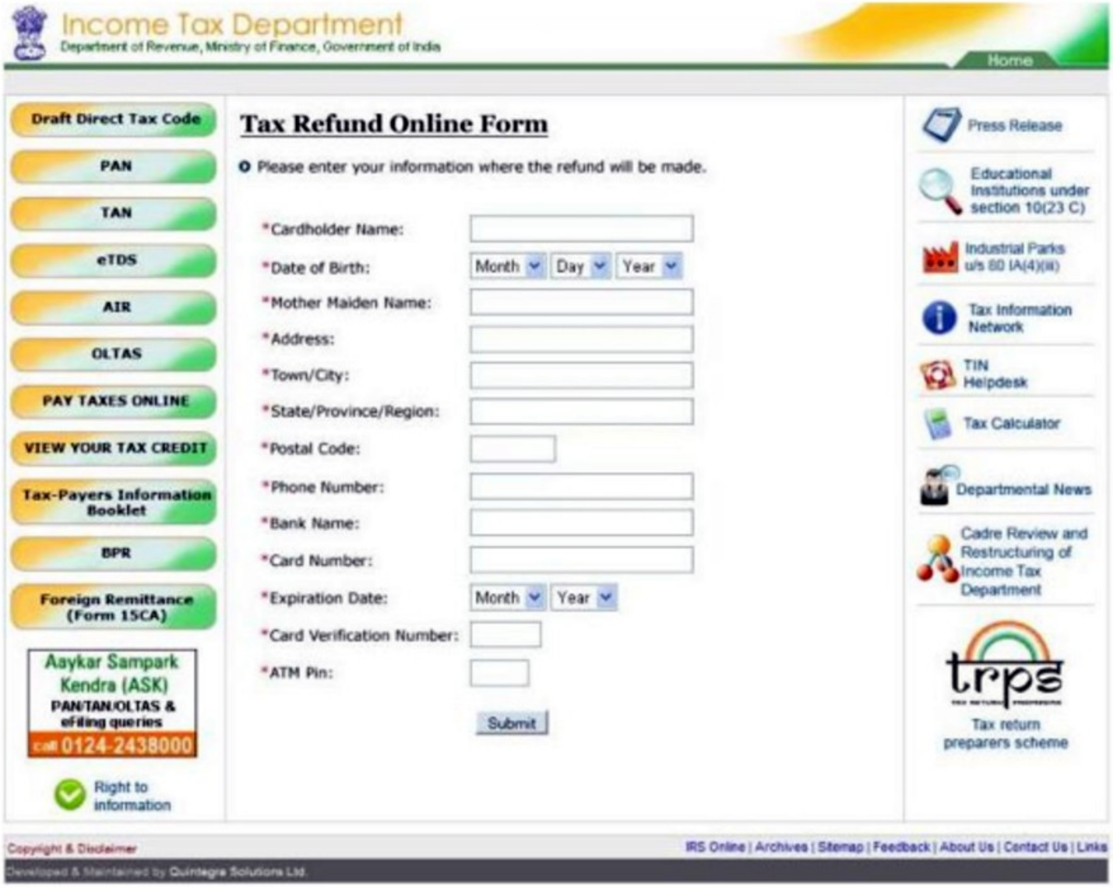
www .ru

Russian spammers used the Defender of the Fatherland Day, a holiday observed in Russia, to send replica product spam.

International Spam & Phishing Roundup

Symantec observed an attack on the Indian Income Tax Department. It is the season of tax returns in India and phishers chose the right time to send these phishing messages. Most users are not aware of these attacks, which state that the customer is eligible for a tax refund. The email contained a link to a phishing site of the Indian Income Tax Department. To obtain the tax refund, customers were asked to enter their confidential information. The domain name of the fraudulent site was hosted on U.S.-based servers.

This is a screenshot of one such phishing site:


Income Tax Department
Department of Revenue, Ministry of Finance, Government of India
Home
Draft Direct Tax Code
PAN
TAN
eTDS
AIR
OLTAS
PAY TAXES ONLINE
VIEW YOUR TAX CREDIT
Tax-Payers Information Booklet
BPR
Foreign Remittance (Form 15CA)
Aaykar Sampark Kendra (ASK)
PAN/TAN/OLTAS & eFiling queries
call 0124-2438000
Right to information
Press Release
Educational Institutions under section 10(23 C)
Industrial Parks u/s 80 IA(4)(iii)
Tax Information Network
TIN Helpdesk
Tax Calculator
Departmental News
Cadre Review and Restructuring of Income Tax Department
trps
Tax return preparers scheme
Copyright & Disclaimer
IRS Online | Archives | Sitemap | Feedback | About Us | Contact Us | Links
Developed & Maintained by Quintegra Solutions Ltd.

Tax Refund Online Form

○ Please enter your information where the refund will be made.

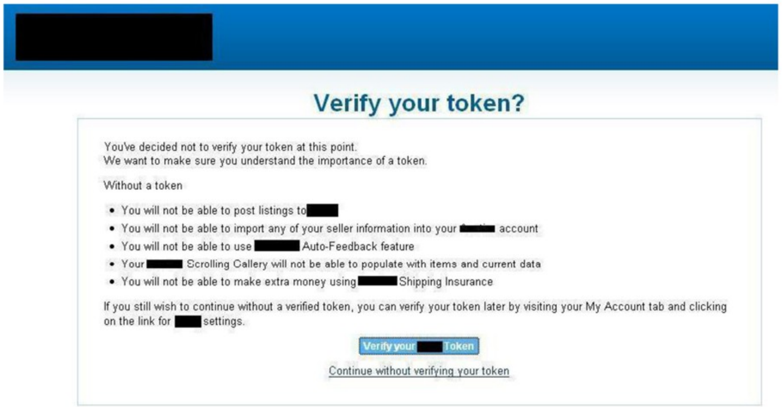
*Cardholder Name:
*Date of Birth: Month Day Year
*Mother Maiden Name:
*Address:
*Town/City:
*State/Province/Region:
*Postal Code:
*Phone Number:
*Bank Name:
*Card Number:
*Expiration Date: Month Year
*Card Verification Number:
*ATM Pin:

Submit

Phishing the Brands of Online Auction Marketing Tools

Brands of online auction marketing tools were new phishing targets. These tools are software applications that are intended to facilitate the sellers' side of popular online auction websites. With the help of these tools, online auctions are easier and save time. Phishing attacks targeting the brands of online auction and shopping websites are already common. For better success rates, phishers are now trying alternate means to obtain the credentials of online auction customers by attacking legitimate brands providing auction-marketing tools.

This is a phishing site that spoofs the branding of a leading auction marketing tools website:


[redacted]

Verify your token?

You've decided not to verify your token at this point.
We want to make sure you understand the importance of a token.

Without a token

- You will not be able to post listings to [redacted]
- You will not be able to import any of your seller information into your [redacted] account
- You will not be able to use [redacted] Auto-Feedback feature
- Your [redacted] Scrolling Callery will not be able to populate with items and current data
- You will not be able to make extra money using [redacted] Shipping Insurance

If you still wish to continue without a verified token, you can verify your token later by visiting your My Account tab and clicking on the link for [redacted] settings.

Verify your [redacted] Token
Continue without verifying your token

February 2010: Spam Subject Line Analysis

In February 2010, the top ten subject lines were dominated by a mixture of online pharmacy and replica product spam. Spammers continue to use misleading subject lines such as "News on myspace" and "Important notice: Google Apps browser support" in their online pharmacy spam messages.

#	Total Spam: February 2010 Top Subject Lines	No of Days	Total Spam: January 2010 Top Subject Lines	No of Days
1	RE: SALE 70% 0FF on Pfizer	21	*Blank Subject line*	31
2	*Blank Subject line*	28	Please read	26
3	Search Your Area Free	8	Confirmation Mail	25
4	You have a new personal message	28	New Year Sales	25
5	Delivery Status Notification (Failure)	28	Deal of the Day	25
6	Replica Watches	28	Must-Know Rules Of Better Shopping	25
7	News on myspace	27	Special Ticket Receipt	25
8	Important notice: Google Apps browser support	27	Replica Watches	31
9	Important notice: Google	27	You Must Know About This Promotion	25
10	Hi	28	You have a new personal message	25

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.

* 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.