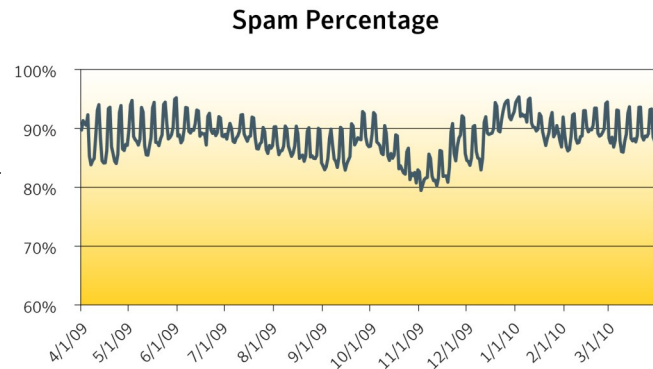


Scam and phishing messages in March accounted for 17 percent of all spam, which is 2 percentage points lower than in February. After the tragic earthquakes in Haiti and in Chile, there were no additional natural disasters for spammers to take advantage of. Instead, spammers continued to focus on seasonal and calendar events

such as Easter holiday to deliver spam messages. With respect to spam message size, there was a sizeable increase in spam messages between 5kb and 10kb (up over 10 percentage points), which correlates to an increase in attachment spam. Overall, spam made up 89.34 percent of all messages in March, compared with 89.99 percent in February.



Symantec observed a 3 percent decrease from the previous month in all phishing attacks. This was primarily due to a decrease in volume of attacks generated from automated toolkits. 9 percent of phishing URLs were generated using automated phishing toolkits, a decrease of 35 percent from the previous month. However, there was an increase in the volume of unique URL and IP attacks. Unique URLs increased by 1.5 percent and IP attacks increased by nearly 4 percent from the previous month. A 9 percent decrease was observed in non-English phishing sites from the previous month. The decrease was due to a fall in the number of phishing attacks in French and Italian. There was a slight increase in the number of attacks in Chinese that was primarily in the e-commerce sector. More than 95 Web hosting services were used, which accounted for 12 percent of all phishing attacks.

The following trends are highlighted in the April 2010 report:

- Spam as Economic Indicator
- Mass Phishing of Retail Electronic Payment Brands
- Phishing of Indian Job Sites
- Will the Trend Continue?
- Easter, and Other Holidays
- March 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	March	February	Change (% points)
Adult	1%	1%	No change
Financial	12%	12%	No change
Fraud	7%	8%	-1
Health	12%	11%	+1
Internet	34%	33%	+1
Leisure	5%	4%	+1
419 spam	6%	7%	-1
Political	<1%	<1%	No change
Products	18%	19%	-1
scams	4%	4%	No change

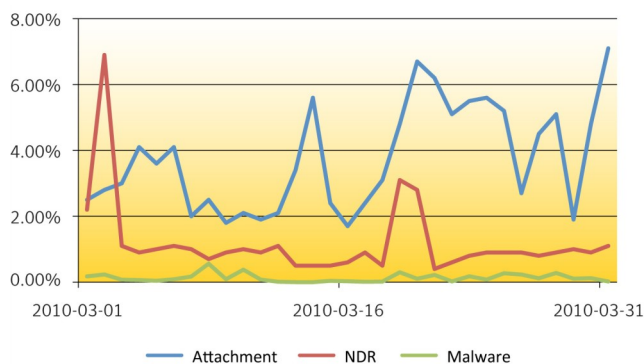
Spam URL TLD Distribution

TLD	March	February	Change (% points)
com	47.0%	57.2%	-10.2
ru	29.8%	25.1%	+4.7
net	10.4%	3.2%	+7.2
cn	4.1%	Not listed	N/A

Average Spam Message Size

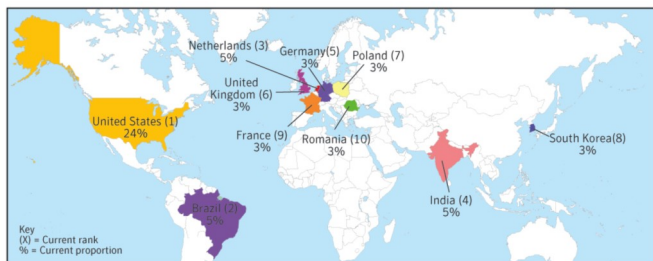
Message Size	March	February	Change (% points)
0-2kb	0.34%	0.52%	-0.18
2kb-5kb	63.63%	76.53%	-12.9
5kb-10kb	25.02%	14.39%	+10.63
10kb+	11.01%	8.56%	+2.45

Spam Attack Vectors



Metrics Digest

Spam Regions of Origin



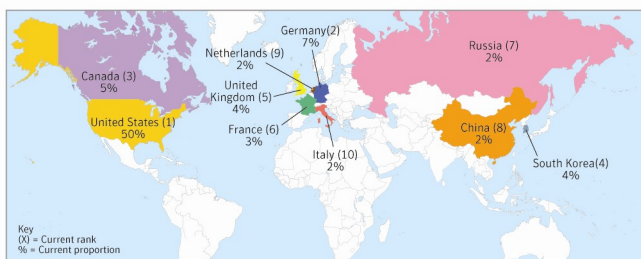
Country	March	February	Change (% points)
United States	24%	23%	+1
Brazil	5%	6%	-1
Netherlands	5%	5%	No change
India	5%	5%	No change
Germany	3%	4%	-1
United Kingdom	3%	3%	No change
Poland	3%	3%	No change
South Korea	3%	3%	No change
France	3%	2%	+1
Romania	3%	3%	No change

Geo-Location of Phishing Lures



Country	March	February	Change (% points)
United States	52%	51%	2
Canada	7%	4%	3
Germany	5%	6%	-1
France	4%	4%	No Change
South Korea	4%	5%	-1
Brazil	3%	2%	1
United Kingdom	3%	3%	No Change
Russia	3%	3%	No Change
China	2%	Not Listed	N/A
Italy	1%	2%	-1

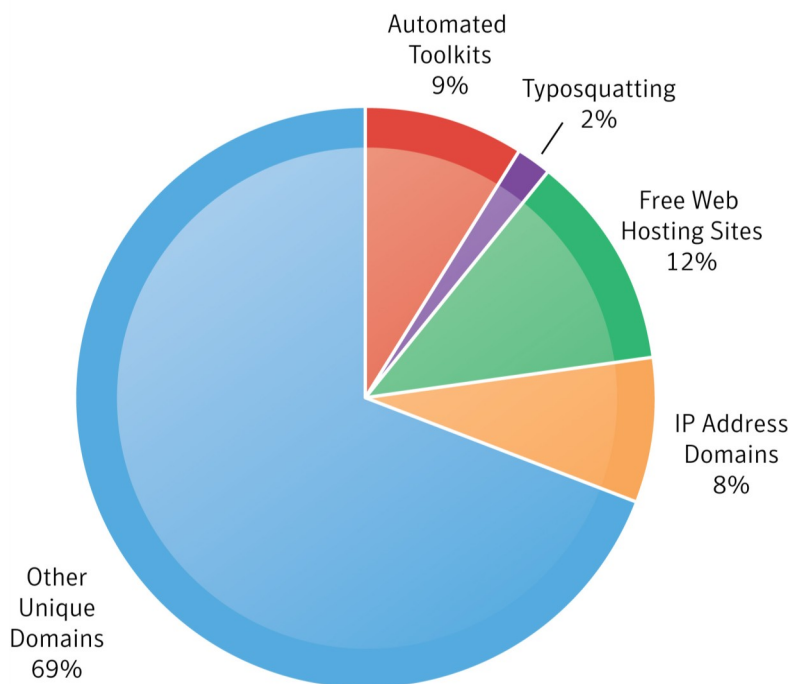
Geo-Location of Phishing Hosts



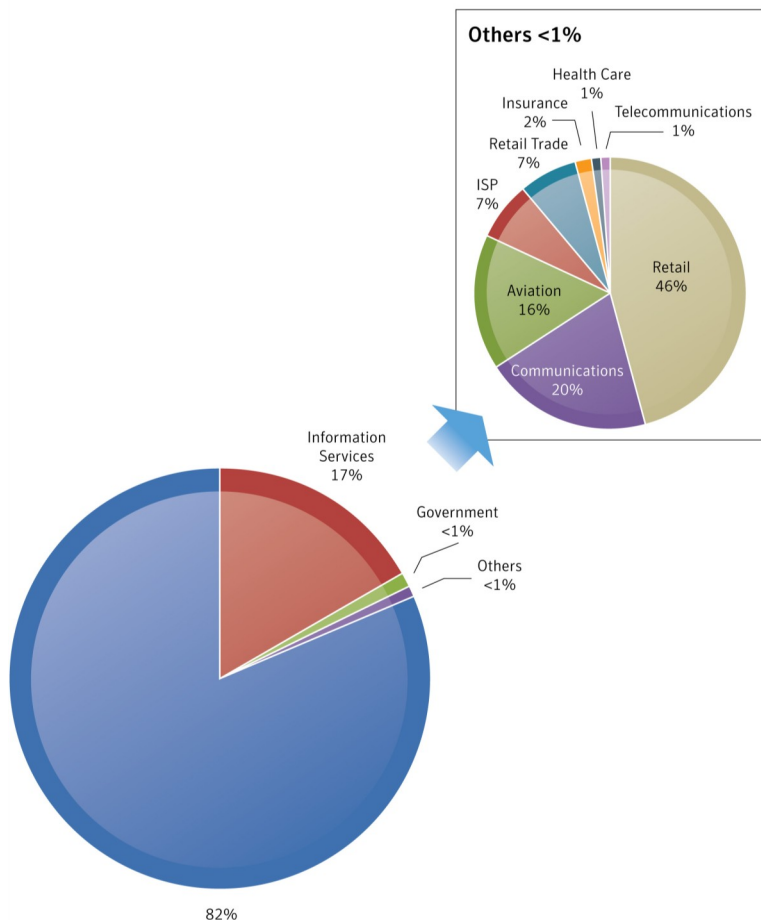
Country	March	February	Change (% points)
United States	50%	48%	2
Germany	7%	5%	2
Canada	5%	4%	1
South Korea	4%	5%	-1
United Kingdom	4%	3%	1
France	3%	3%	No Change
Russia	2%	Not listed	N/A
China	2%	2%	No Change
Netherlands	2%	2%	No Change
Italy	2%	2%	No Change

Metrics Digest

Phishing Tactic Distribution



Phishing Target Sectors



Spam as Economic Indicator

According to the National Bureau of Economic Research, the United States has been in a recession since December 2007. Looking through its Global Intelligence Network, Symantec found that this recession certainly kept the spammers busy at adapting to current events.

- **October 2007** : Spammers Feed Off Housing Crisis
- **January 2008** : As Oil Prices Hike, Spammers Strike:
- **February 2008** : Rising gas prices lead spammers to bio-fuel
- **June 2008** : Economic Climate Helps Fuel Spam Climate
- **August 2008** : Gas prices and foreclosures remain a focus
- **September 2008** : Job Seekers: Beware of Bogus Recruiting Ads bearing Viruses
- **November 2008**: Economic bailout package & FDIC guarantee get the attention of some spammers
- **January 2009**: Spammers Use the Recession to Enter Your Inbox
- **March 2009**: Economic woes bring good tidings for spammers.
- **April 2009**: Spammers Rethink Their Mortgage Strategy
- **March 2010**: Job offer spam signaling an upturn in the economy??

While the United States consumer sentiment remained unchanged in March 2010, top ten subject lines containing economic keywords show that spammers have an optimistic view of the economy with job offer spam among their top spam subject lines.

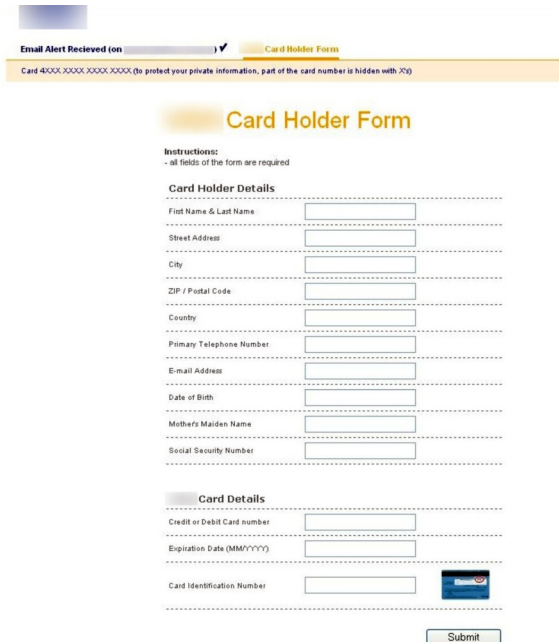
1. Get the Job fast this one
2. Job seekers in USA
3. Finance Manager vacancy
4. FW: Global job vacancy
5. Job position REF83782 USA only
6. Finance ManagerUSA postion
7. Get a diploma for a better job
8. Need a job ?
9. RE: Your Job is at stake
10. Looking good does not have to bankrupt you

Mass Phishing of Retail Electronic Payment Brands

Symantec observed a mass phishing attack on two major brands that provide retail electronic payment services for banks across the globe. Phishers initiated a massive attack that made up 4.4 percent of all unique phishing websites. (Fraudsters developed the phishing websites in non-English languages as well, with French being the most utilized.) The phishing websites were targeted toward customers by spam mails containing the subject “your XXX card 4XXX XXXX XXXX XXXX: possible fraudulent transaction ID.”

There were two distinct types of phishing websites observed in the attack:

1. The first type was created using automated phishing toolkits. The most common TLD utilized was ‘.cz’, which represents the Czech Republic. In this case, customers are asked to enter their sensitive information into a “Card Holder Form” page to complete the fake verification process.



2. The second type of attack consisted of URLs with IP domains (for example, an URL like <http://255.255.255.255/index.html>). The IPs were hosted on US-based servers. The URLs were found to be very long, usually with more than 700 characters. In these attacks, the page asked for sensitive information, but the credit or debit card number was auto-assigned.

Advanced verification.

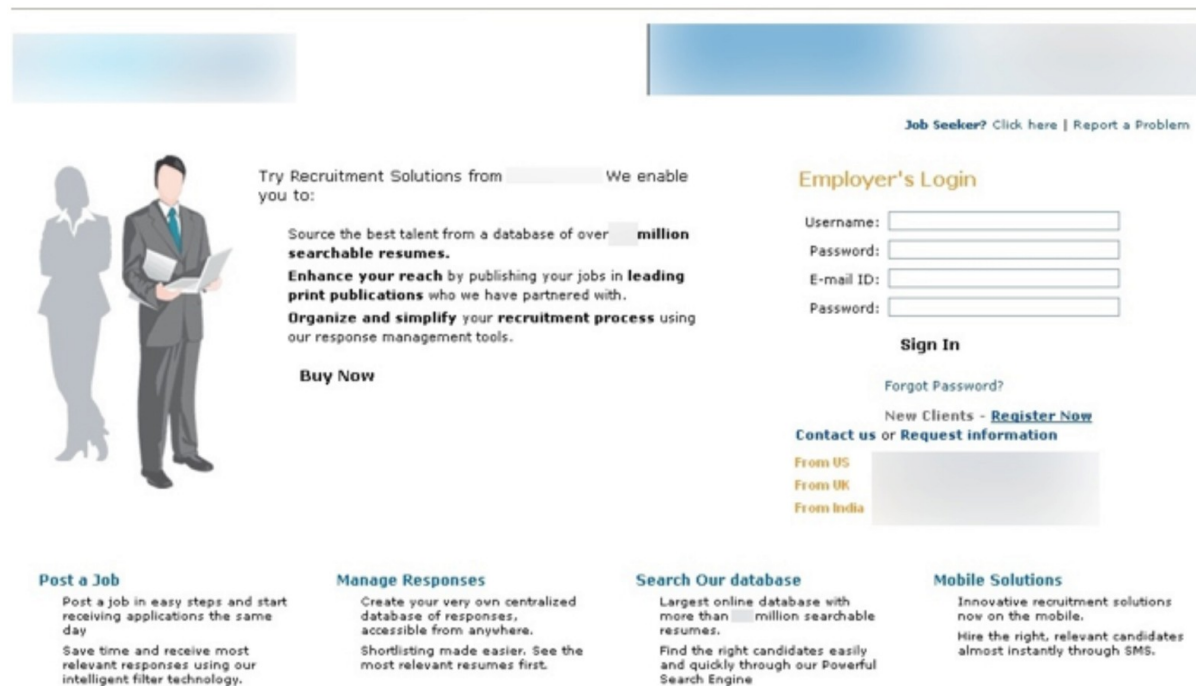
For security reasons please provide information requested below.



The Phishing of Indian Job Sites

Despite the global economic slowdown, India witnessed a high number of new jobs in the country during the first quarter of 2010. With the job market looking positive, job sites seem to have benefited with more users accessing their websites.

Below is a screenshot of a phishing website that takes advantage of the brand of a popular Indian job site:



[Job Seeker?](#) [Click here](#) | [Report a Problem](#)

Try Recruitment Solutions from [redacted] We enable you to:

Source the best talent from a database of over [redacted] million searchable resumes.

Enhance your reach by publishing your jobs in leading print publications who we have partnered with.

Organize and simplify your recruitment process using our response management tools.

Buy Now

Employer's Login

Username:

Password:

E-mail ID:

Password:

Sign In

[Forgot Password?](#)

New Clients - [Register Now](#)

Contact us or Request information

[From US](#)

[From UK](#)

[From India](#)

Post a Job

Post a job in easy steps and start receiving applications the same day

Save time and receive most relevant responses using our intelligent filter technology.

Manage Responses

Create your very own centralized database of responses, accessible from anywhere.

Shortlisting made easier. See the most relevant resumes first.

Search Our database

Largest online database with more than [redacted] million searchable resumes.

Find the right candidates easily and quickly through our Powerful Search Engine

Mobile Solutions

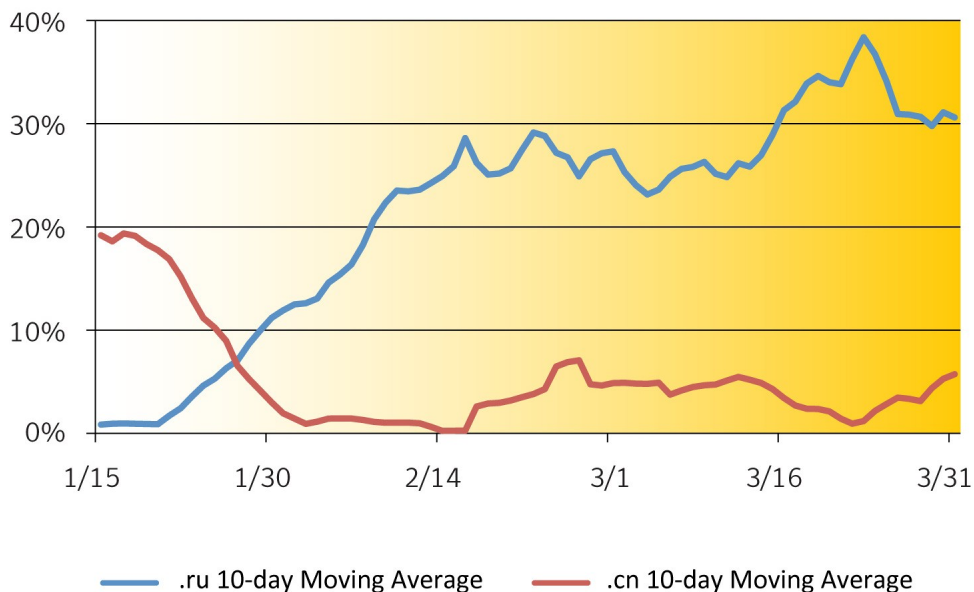
Innovative recruitment solutions now on the mobile.

Hire the right, relevant candidates almost instantly through SMS.

The increased number of candidates seeking jobs in India has led to the launch of phishing attacks on Indian job sites. The phishing page in the above example is asking for potential employers' login credentials. The phishing website was created on servers located in the Netherlands. The credentials consist of a username and password as well as the employer's email ID and password. After stealing these credentials, fraudsters send targeted spam messages to the employers. The spam message states that the employer is required to pay an amount to upgrade or continue his access of particular recruitment solutions. The link provided to make the payment leads to a phishing page that asks for confidential information such as credit card numbers, pin number, etc. Attackers also masquerade as the employer to send spam containing fake job opportunities to job seeking candidates—an action that means the attackers are always seeking financial gain.

Will the Trend Continue?

In last two reports, Symantec kept an eye on the sharp decline in spam containing .cn URLs as well as associated increase in spam messages with .ru domains. As the graph below illustrates, China Internet Network Information Center (CNNIC)'s action to tighten registration of .cn domains had a huge impact on spam messages containing .cn URLs. Unfortunately, spammers have found themselves a refuge in .ru domains as spam messages containing .ru domains increased dramatically. Spammers have either given up on finding a loophole for .cn domains or are currently happy with .ru domains.



EMEA region further solidified its status of “king” in origin of spam as it sent 44.7% of world-wide spam in March, which represents 1.5 percentage point increase.

Region	March	February	Change (% points)
North America	24.5%	23.5%	+1.0
Latin America	11.7%	13.7%	-2.0
APJ	19.1%	19.6%	-0.5
EMEA	44.7%	43.2%	+1.5

In EMEA region, top ten countries (Netherlands, Germany, United Kingdom, Poland, France, Romania, Italy, Spain, Russia, and Czech Republic) made up over 62% of the region’s volume.

Easter, and Other Holidays

After focusing on tragic events in Haiti and Chile, spammers have once again turned their attention to seasonal calendar events.

****Personalized Letter from the Easter Bunny****

Shop for Personalized Letter from the Easter Bunny.

Hand delivered by a plush 9" Easter Bunny with bendable ears, arms and hands. Personalized with child's first name, home address, city and state, and a friend or family member.

Only \$19.95

Shop Now!

[Press Here](#)

We hope you enjoyed receiving this email. Should you no longer wish to receive emails from this advertiser [visit this link](#) to unsubscribe, or mail comments to PersonalCreations 19W001 101st Street, Lemont, IL 60438

We hope you enjoyed today's offer. You may click here to unsubscribe at anytime. Our postal address is: 18766 John J Williams Highway #122, Rehoboth Beach, DE 19971

From: St. Patrick's Day
 Date: [redacted]
 To: [redacted]
 Subject: Irish luck in a tree e-card from [redacted]

Can't see the images? [Click Here](#) to visit our website.

Send Some Luck and a Bit of Irish Charm On St. Patrick's Day

Try fun ecards today and spread a little St. Patty's cheer! We've got everything you need to send fun E-cards online - it's like a whole card store at your fingertips. Just [get the easy-to-use E-card software](#) and easily share cards among your friends and colleagues by email. Even if you thought you'd be late, you can send an E-card at any time, even on St.Patrick's Day itself!

[Click Here](#)

Print and Share your card!

For more information about My Fun Cards, including our address and unsubscribe link, [click here](#).
 My Fun Cards My Fun Cards One North Lexington 9th Floor White Plains, NY 10601
 (c) 2006 My Fun Cards. All Rights Reserved.

Forward this mail to a friend:

10685-B Hazelhurst Dr., Suite 1764 Houston, TX 77043. We deal promptly with all unsubscribe requests. Your email address will be removed within 24 hours and can never be reentered into our database. We will not share your email address with any other party. If you would prefer not to receive additional emails from us, please [press this link](#).

March 2010: Spam Subject Line Analysis

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

#	Total Spam: March 2010 Top Subject Lines	No of Days	Total Spam: February 2010 Top Subject Lines	No of Days
1	Blank Subject line	31	RE: SALE 70% OFF on Pfizer	21
2	News on mspace	31	Blank Subject line	28
3	Important notice: Google Apps browser support	31	Search Your Area Free	8
4	Important notice: Google	31	You have a new personal message	28
5	You have a new personal message	31	Delivery Status Notification (Failure)	28
6	Bestsellers. 70% Discount.	12	Replica Watches	28
7	SALE 79% OFF on PFIZER!	4	News on mspace	27
8	Replica Watches	24	Important notice: Google Apps browser support	27
9	Delivery Status Notification (Failure)	31	Important notice: Google	27
10	RE: SALE 70% OFF on PFIZER!	11	Hi	28

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.