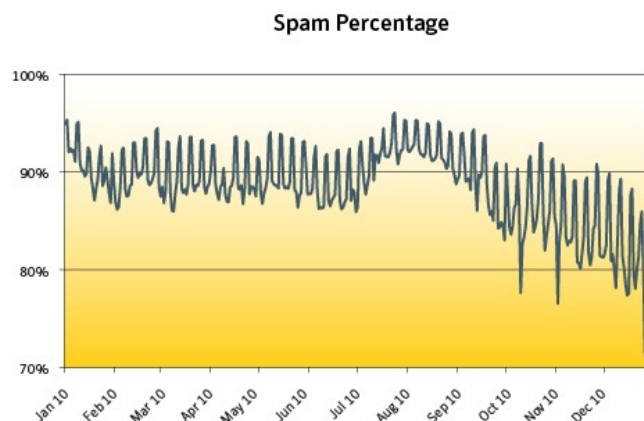


Spam made up 81.69% of all messages in December, compared with 84.31% in November. The consistent drop in spam made us wonder, did spammers take a holiday break? Global spam volume fell again in December, and made a steep drop on Christmas day. The volume has bounced back after hitting bottom on December 27. The spam percentage fell to 71% that day, which is the lowest Symantec has monitored in the last few years.



While there are no clear explanations on what caused this sudden drop, the January 2011 State of Spam & Phishing report offers a plausible scenario on why this has occurred. It also provides recent updates, including the return of the Rustock botnet and botnet volume increase.

The overall phishing landscape decreased by 15% this month. The decrease was attributed to a decline in almost all sectors of phishing. The holiday season was most likely the cause of the decrease in phishing. Phishing websites created by automated toolkits decreased by about 10%, and unique URLs decreased by 18%. Phishing websites with IP domains (i.e. domains like <http://255.255.255.255>) decreased by about 2%. Webhosting services comprised of 9% of all phishing, which was a decrease of 39% from the previous month. The number of non-English phishing sites decreased by 19%, and among non-English phishing sites, French and Portuguese were the highest in December.

The following trends are highlighted in the January 2011 report:

- Did Spammers Take a Holiday Break?
- Spammers' New Year's Resolution
- New Bait Found in Social Media Phishing
- Adult Scams Masquerade Indonesian Facebook

**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](mailto:sagar_desai@symantec.com)

### Metrics Digest

#### Global Spam Categories

Category Name	December	November	Change (% points)
Adult	<1%	2%	-2
Financial	8%	7%	+1
Fraud	4%	5%	-1
Health	4%	5%	-1
Internet	47%	43%	+4
Leisure	10%	9%	+1
419 spam	6%	9%	-3
Political	<1%	<1%	No change
Products	17%	17%	No change
scams	3%	2%	+1

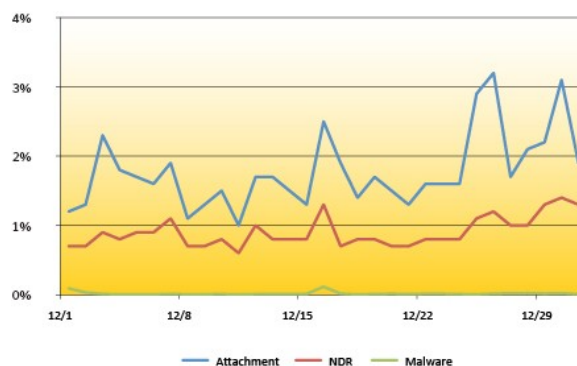
#### Spam URL TLD Distribution

TLD	December	November	Change (% points)
com	72.3%	60.6%	+11.7
ru	7.7%	23.3%	-15.6
org	7.1%	5.4%	+1.7
net	3.0%	3.3%	-0.3

#### Average Spam Message Size

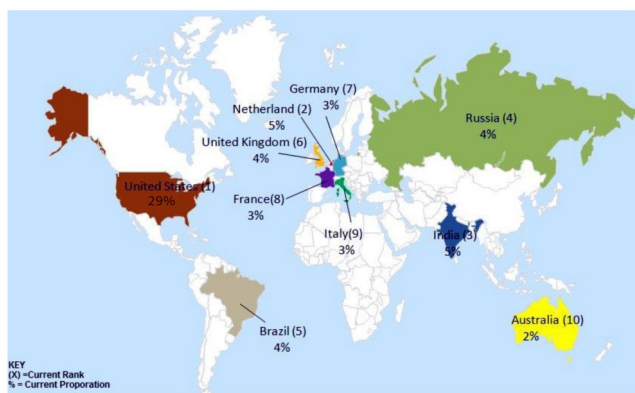
Message Size	December	November	Change (% points)
0-2kb	1.30%	2.91%	-1.61
2kb-5kb	65.41%	62.66%	+2.75
5kb-10kb	25.09%	28.31%	-3.22
10kb+	8.20%	6.12%	+2.08

#### Spam Attack Vectors



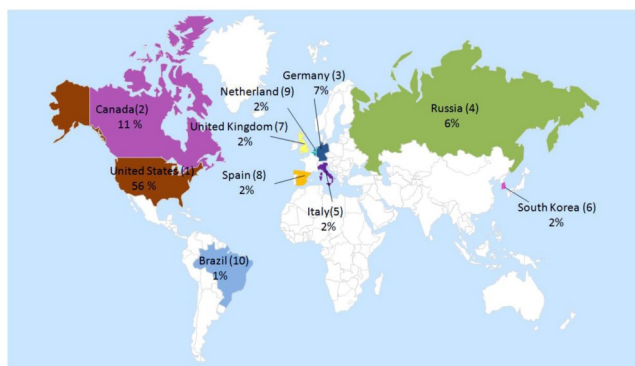
### Metrics Digest

#### Spam Regions of Origin



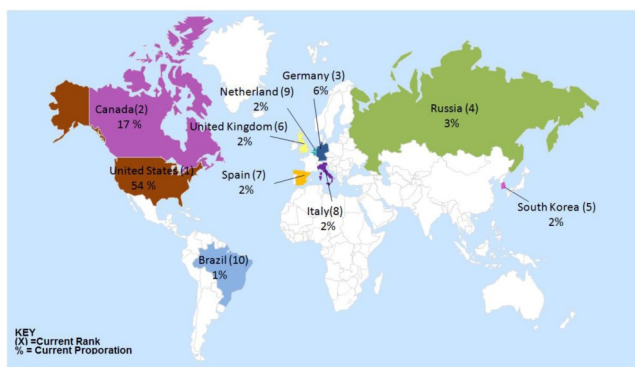
Country	December	November	Change (% points)
United States	29%	27%	+2
Netherlands	5%	5%	No change
India	5%	5%	No change
Russia	4%	4%	No change
Brazil	4%	4%	No change
United Kingdom	4%	4%	No change
Germany	3%	3%	No change
France	3%	3%	No change
Italy	3%	Not listed	N/A
Australia	2%	3%	-1

#### Geo-Location of Phishing Lures



Country	December	November	Change (% points)
United States	56%	51%	+5
Canada	11%	11%	No Change
Germany	7%	8%	-1
Russia	6%	9%	-3
Italy	2%	2%	No Change
South Korea	2%	3%	-1
United Kingdom	2%	1%	+1
Spain	2%	Not listed	N/A
Netherlands	2%	2%	No Change
Brazil	1%	Not listed	N/A

#### Geo-Location of Phishing Hosts

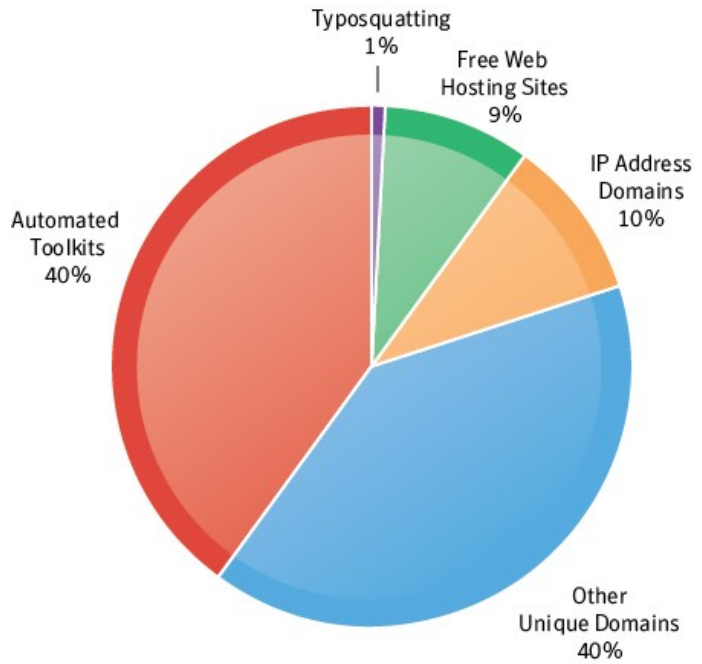


Country	December	November	Change (% points)
United States	54%	51%	+3
Canada	17%	13%	+4
Germany	6%	6%	No Change
Russia	3%	4%	-1
South Korea	2%	4%	-2
United Kingdom	2%	2%	No Change
Spain	2%	Not listed	N/A
Italy	2%	2%	No Change
Netherlands	2%	2%	No Change
Brazil	1%	3%	-2

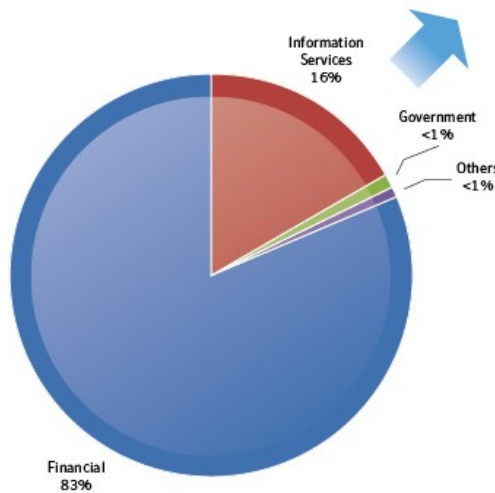
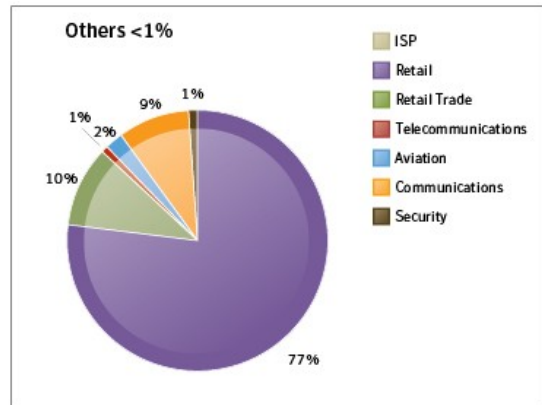
### Metrics Digest

### Phishing Tactic Distribution

### Overall Statistics



### Phishing Target Sectors

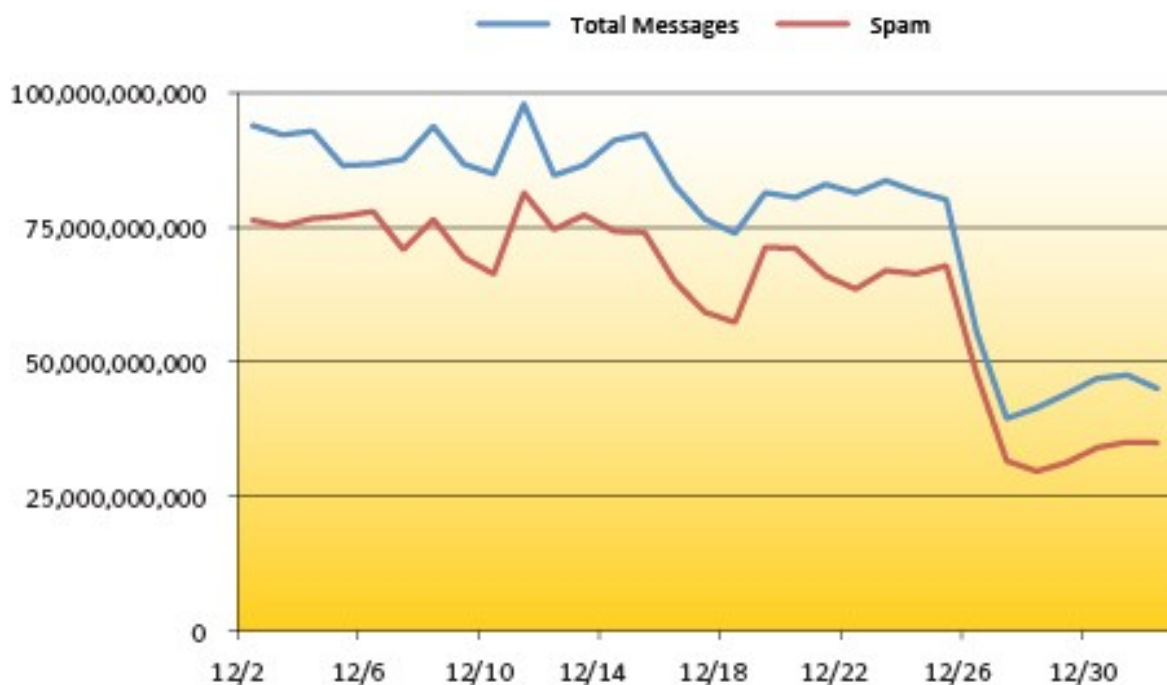


### Did Spammers Take a Holiday Break?

Symantec has been monitoring the steep decline in spam for several months. This trend continued in December with the global spam volume falling 19.98% month-over-month. From the most recent peak in August, the drop represents a staggering 65.03% decline in spam.

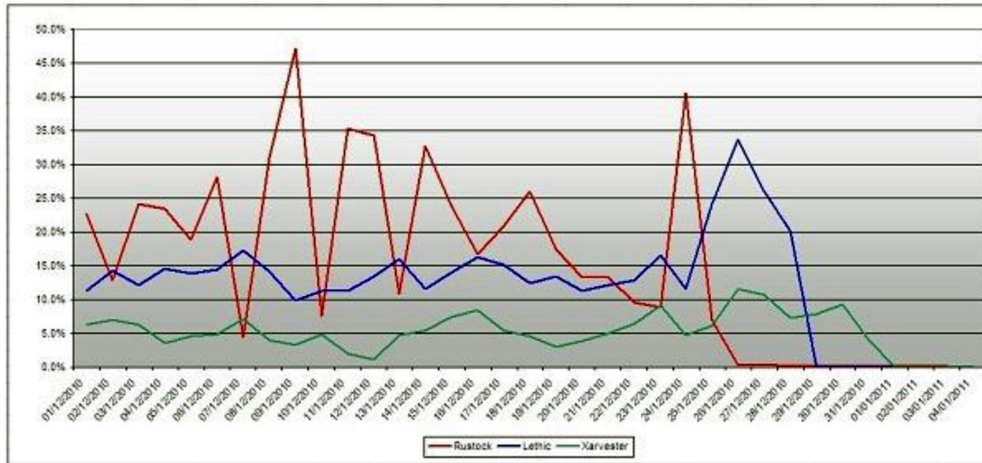


While the month-over-month numbers represented another significant drop, the more astonishing drop was monitored on Christmas day. Here is the volume chart for the month of December:



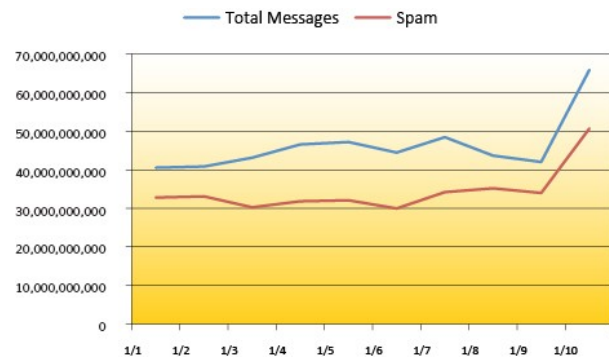
### Did Spammers Take a Holiday Break? (continued)

What caused such a big drop? We have a potential answer. According to MessageLabs, there was a huge reduction in output from the Rustock botnet, which was by far the most dominant spam botnet in 2010. Since December 25, the Rustock botnet has basically disappeared as the amount of spam from the botnet has fallen below 0.5% of spam worldwide. In addition to the decline in the Rustock botnet activity, MessageLabs also pointed out that two other major botnets disappeared off the spam map. The Lethic botnet has been quiet since December 28, and the Xarvester botnet went silent on December 31. The chart below shows relative botnet spam volumes:



While the drop in spam is good news, it does not mean that spam has completely disappeared. During this lull in spam messages, where did the spammers turn? Symantec observed increasing use of freeweb domains and URL shorteners in spam messages. The .ru URLs, which have remained a favorite, saw an over 15 percentage point decline month-over-month. The .com URLs increased, in part due to .ru URL's decline, but it did not go up enough to make up the loss volume of .ru URLs. This suggests that the remaining slack may have been picked up by freeweb domains and URL shorteners.

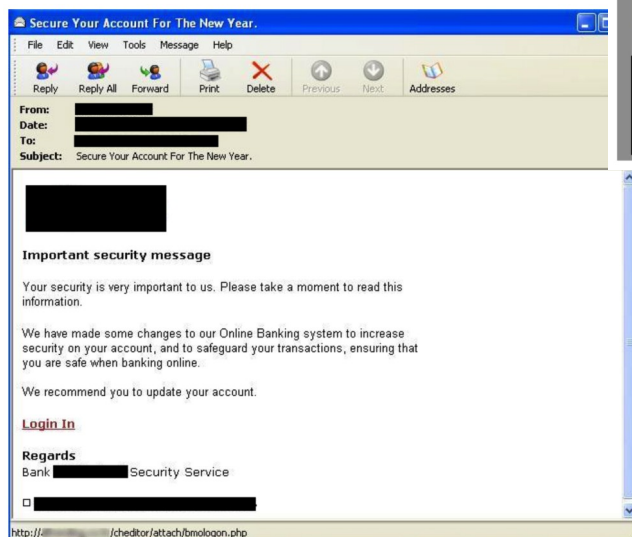
However, spammers' holiday breaks were short. On January 10<sup>th</sup>, Symantec observed an uptick in spam volume as well as spam output from Rustock botnet. Spam volume on January 10<sup>th</sup> was up 49% compared to the previous day.



This .ru URL spam chart shows that the volume dropped around Christmas day and spiked up on January 10<sup>th</sup>. This suggests that the new spike in spam mostly consisted of .ru URL spam messages.

## Spammers' New Year's Resolution

One of the most common New Year's resolutions is to get in shape. Gyms and athletic clubs usually see much higher enrollment in January as many people sign up in the beginning of the year to follow through with their resolutions. Spammers were crafty to use getting in shape as a lure, and send out the seasonal offer.



As we pointed out in the “*Buyers Beware! Holiday Do's and Don'ts*” section in the previous month's report, Symantec has monitored a phishing attempt that includes the New Year theme.

While New Year's day has already passed at the time of this report's publication, the Chinese New Year is in February. Chinese spammers are offering gift baskets of food in the example here:

**From:** [REDACTED]  
**Date:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** 亲爱的会员123123: 春节到了, 为您精心准备的食物! 直接进入淘宝购买~省心省力~

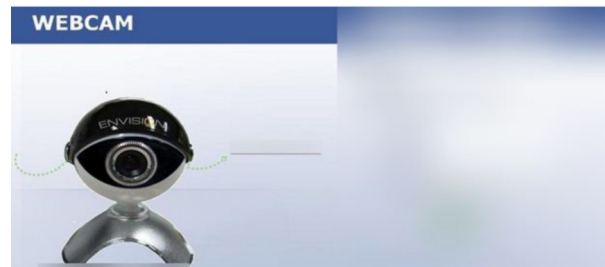
本邮件为HTML格式, 如果不能直接显示, 请[点击此处链接](#)

或者直接复制网址[http://www.\[REDACTED\].com/go/chn/tbk\\_channel/food.php?pid=mm\\_14629015\\_0\\_0&eventid=101865](http://www.[REDACTED].com/go/chn/tbk_channel/food.php?pid=mm_14629015_0_0&eventid=101865)并打开。

### New Bait Found in Social Media Phishing

In the past couple of months, Symantec observed a series of phishing websites spoofing social networking brands. These scams utilized many new bait tactics in an attempt to trick end users into giving away their confidential information.

In one particular example, the phishing website was titled “Webcam” and the phishing page contained an image of a webcam. Here, the phishing Web site gave the impression that the social networking site was providing a webcam facility for end users to interact with one another; however, the legitimate Web site does not provide any such kind of facility.



The use of fake offers of pornography in social networking scams is now frequently observed. It seems that phishers are relentlessly using pornography as bait to steal user credentials. In this second example, though pornography was the bait, phishers used a different kind of approach in the hopes of tempting end users. The phishing website claimed that the social networking brand has come up with a new edition meant for adult users. The new edition allegedly contained applications in which end users can view adult videos of known scandals taken from hidden cameras. The phishing website further claimed that the user can interact and take part in adult chat with individuals near the user’s locality. The deceptive claims did not end there. A third claim stated that users can check for updates on scandals of popular actresses. The phishing website contained a pornographic image and the look and feel of the website was created to increase the pornographic appeal.



In the third example, the bait used was fake offers of hacking software. The phishing website contained modified content to help it look like an alternate version of a social networking site intended for professional hackers. There were three fake benefits of hacker tools mentioned in the phishing web page. One was an opportunity to learn new tricks in social networking with the help of toolkits. The second was that users were offered a cookie hacker which was allegedly available for download. The phisher does not mention the exact purpose of a cookie hacker but it is possibly for hacking user accounts. The final benefit was that users were encouraged to interact with other professional hackers to better understand and exploit new features in the social networking site.





### New Bait Found in Social Media Phishing (continued)

Phishers continue to use new and different forms of bait that all have a common notion - that certain key benefits are available to users if they enter their login information on the phishing site. Of course, if users fall victim to these tricks, phishers would have successfully stolen their confidential information for identity theft.

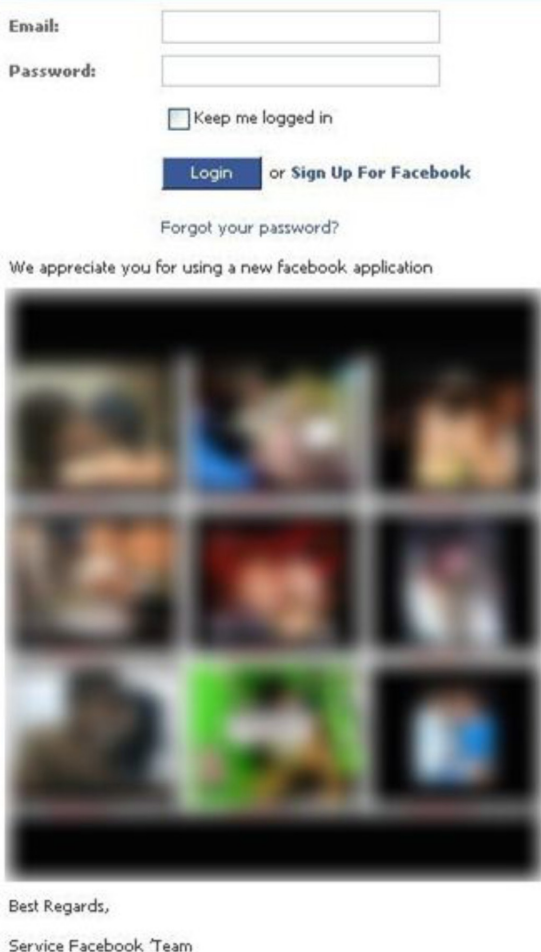
### Adult Scams Masquerade Indonesian Facebook

Facebook has become very popular in Indonesia. The country is ranked third in the most number of Facebook users. With more end users in Indonesia, phishers seemed to have gained interest in creating phishing sites that target Indonesians. Recently, Symantec observed an adult scam spoofing Facebook that targeted Indonesian end-users. The phishing Web site was hosted on a free web-hosting site.

The phishing site stated that an application in which end users can view adult videos of popular Indonesian celebrities was available. It claimed that the videos were taken from hidden cameras in hotel rooms. Users were prompted to enter their login information to gain access to the fake application. To make it look more convincing, it was claimed that the application was from Facebook's service team. The phishing page displayed a slide show of pornographic images of Indonesian celebrities. The images gave the impression that they were screenshots of the adult videos available in the fake application. The motive of displaying such pornographic images was certainly to tempt end users. On the other hand, no such adult application exists in the legitimate Facebook website.

This is a bait used by phishers in the hopes of tricking users in to giving away their confidential information. If phishers succeeded, they will have stolen information for identity theft.

Symantec notified Facebook regarding this issue, and they blocked this URL from being shared on Facebook. Facebook actively block links to sites that have been identified as malicious (i.e., phishing sites or sites that host malware) from being shared on the website and work with third parties to get the sites added to browser blacklists, and where possible, removed by the web-hosting service.



Email:

Password:

Keep me logged in

[Login](#) or [Sign Up For Facebook](#)

[Forgot your password?](#)

We appreciate you for using a new facebook application

Best Regards,  
Service Facebook Team

### 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.