The State of Spam

A Monthly Report – July 2008

Generated by Symantec Messaging and Web Security

Confidence in a connected world.

Doug Bowers
Executive Editor
Antispam Engineering

Dermot Harnett
Editor
Antispam Engineering

Joseph Long
Security Response Lead
Symantec Security Response

Cory Edwards
PR Contact
cory_edwards@symantec.com

Monthly Spam Landscape

"Two years from now, spam will be solved," said Bill Gates in 2004. As Bill Gates left his day job at Microsoft on June 27th, it's interesting to reflect on the spam landscape as it continues today. Since that two year mark in 2006, spam levels have steadily climbed from 56% to its present state of 80% of all email. While antispam filters have become more sophisticated in the last year, and spam threats have emerged and dissipated, it is clear that spammers are not giving up the spam fight. The Symantec July 2008 State of Spam Report notes the following trends:

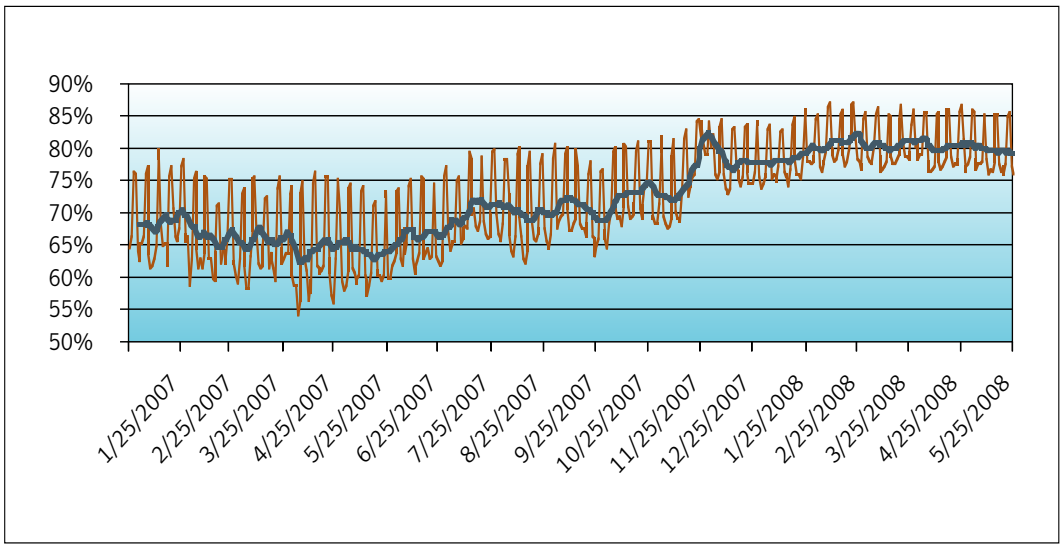
- **Hacked personal email account used to scam contacts**
- **Spammers simplify email harvesting technique**
- **Japanese adult dating spam takes a new twist**
- **China earthquake tragedy used to spread viruses**
- **Olympics related lottery scam emerges**
- **Spam targeting Japanese mobile phone market**
- **Bogus news events lure innocent victims**

Percentages of E-mail Identified as Spam

Defined:

Worldwide Internet Mail Gateway Spam Percentage represents the number of messages that were processed and classified as spam versus the total number of messages processed when scanned at the mail gateway. This metric represents SMTP layer filtering and does not include the volumes of e-mail detected at the network layer.

Internet E-mail Spam Percentage



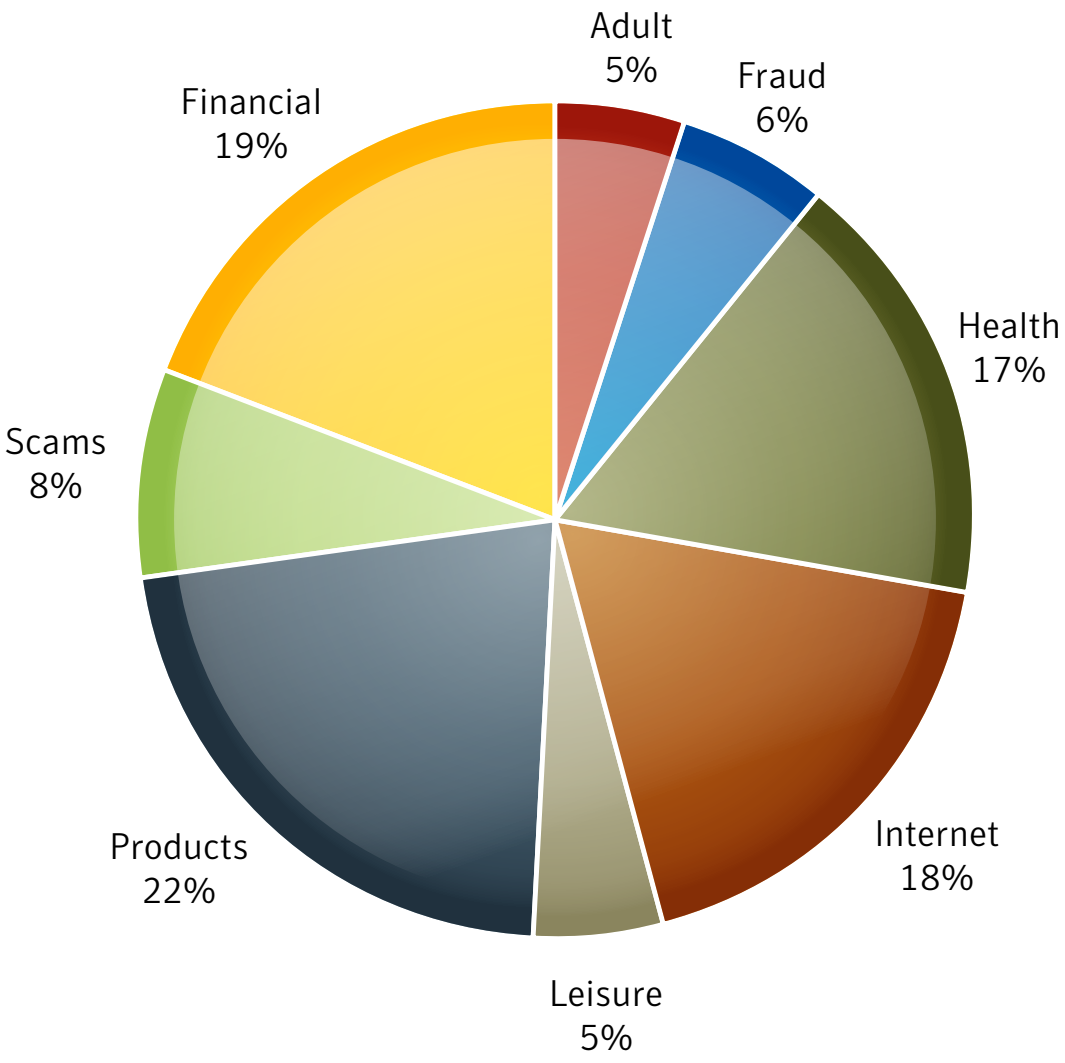
A trend line has been added to demonstrate a 7-day moving average.

Global Spam Categories

Defined:

Spam category data is collected from classifications on messages passing through the Symantec Probe Network.

Global Spam Categories Last 30 Days



Category Definitions

- **Products E-mail attacks** offering or advertising general goods and services. **Examples: devices, investigation services, clothing, makeup**

- **Adult E-mail 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**

- **Financial E-mail attacks** that contain references or offers related to money, the stock market or other financial "opportunities." **Examples: investments, credit reports, real estate, loans**

- **Scams E-mail attacks** recognized as fraudulent, intentionally misguiding, or known to result in fraudulent activity on the part of the sender. **Examples: Nigerian investment, pyramid schemes, chain letters**

- **Health E-mail attacks** offering or advertising health-related products and services. **Examples: pharmaceuticals, medical treatments, herbal remedies**

- **Fraud E-mail 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**

- **Leisure E-mail attacks** offering or advertising prizes, awards, or discounted leisure activities. **Examples: vacation offers, online casinos, games**

- **Internet E-mail attacks** specifically offering or advertising Internet or computer-related goods and services. **Examples: web hosting, web design, spamware**

- **Political 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 party, elections, donations**

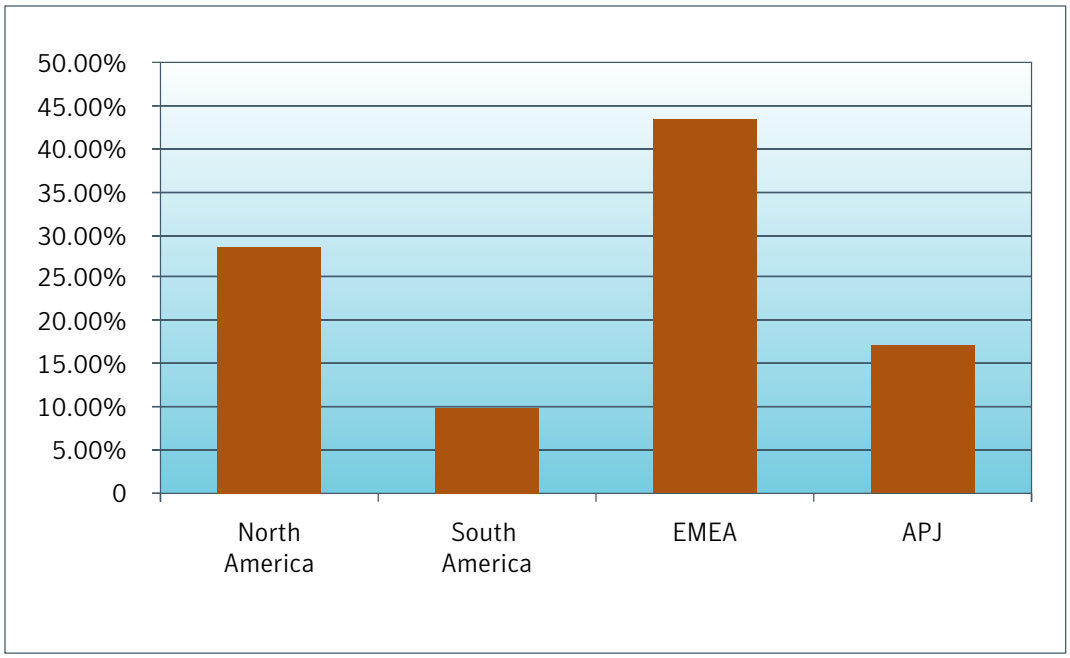
- **Spiritual E-mail attacks** with information pertaining to religious or spiritual evangelization and/or services. **Examples: psychics, astrology, organized religion, outreach**

- **Other** E-mails attacks not pertaining to any other category.

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.



Hacked Personal Email Account Used to Scam Contacts

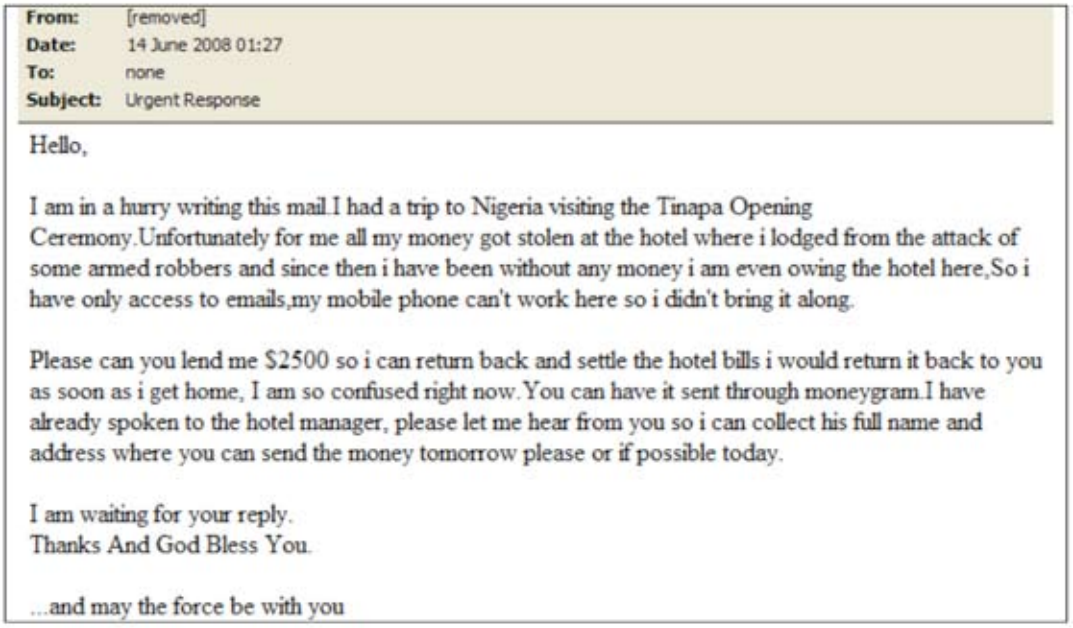
At first glance, the email below looks like a typical 419 scam.

The twist is that the email came from a user's hacked webmail account and was sent to his personal list of contacts. Friends and colleagues received the request for assistance and were urged to respond via email only. As the hacker took over the user's account, the real owner would not have known about the email if the recipients fell for the scam. As a further stamp of authentication, the auto-signature typically used by the account owner was included at the end of the message.

As a result, the account owner was quickly notified by a friend via telephone of the scam, and immediately contacted the webmail service providers to get his account access back. This proved to be difficult because the hacker had changed the account details such as password, address and secret question,

The scam did not stop there – once the hacker had access to the email account, he was able to get the account owner's online auction site password emailed to the account. The hacker then began bidding on a number of laptops being sold in the UK and instructed that the laptops be sent to Nigeria.

It is important to note that this scam was not isolated to one particular web mail provider or organization. This scam also serves as a timely reminder that users should always keep passwords secure and never share them with anyone. Also, be wary of "account expiry" notifications that try to entice users to provide their account details unwittingly to a third party. More information on password security can be found at http://www.symantec.com/norton/products/library/article.jsp?aid=password_secure.



From: [removed]
Date: 14 June 2008 01:27
To: none
Subject: Urgent Response

Hello,

I am in a hurry writing this mail.I had a trip to Nigeria visiting the Tinapa Opening Ceremony.Unfortunately for me all my money got stolen at the hotel where i lodged from the attack of some armed robbers and since then i have been without any money i am even owing the hotel here,So i have only access to emails,my mobile phone can't work here so i didn't bring it along.

Please can you lend me $2500 so i can return back and settle the hotel bills i would return it back to you as soon as i get home, I am so confused right now.You can have it sent through moneygram.I have already spoken to the hotel manager, please let me hear from you so i can collect his full name and address where you can send the money tomorrow please or if possible today.

I am waiting for your reply.
Thanks And God Bless You.

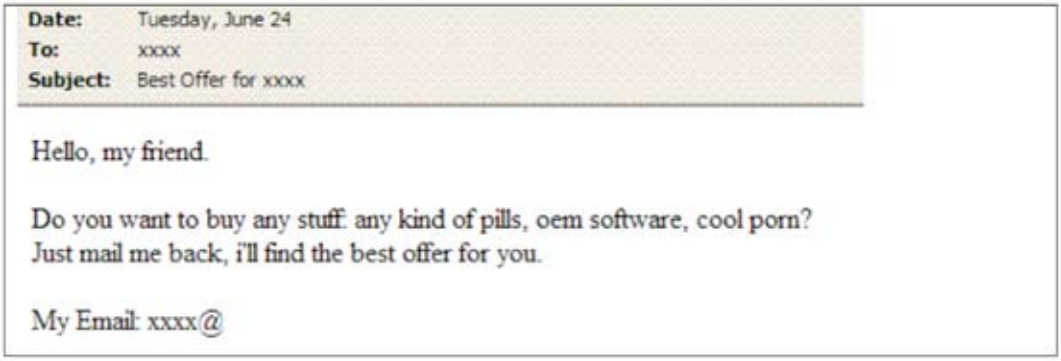
...and may the force be with you

Spammers Simplify Email Harvesting Technique

There are many different ways that spammers try to obtain email addresses. Tactics include:

- Using spambots which crawl the internet looking for email addresses
- Bombarding an email server with email addresses and storing the addresses that do not bounce
- Buying lists of email addresses from other spammers

In June 2008, Symantec observed that certain spammers tried to simplify their email harvesting techniques. Starting with a list of email addresses obtained through suspicious means, the spammer tried to send a message to people who are interested in receiving certain offers such as, "Do you want to buy any stuff: any kind of pills, oem software, cool porn? Just mail me back, i'll find the best offer for you."



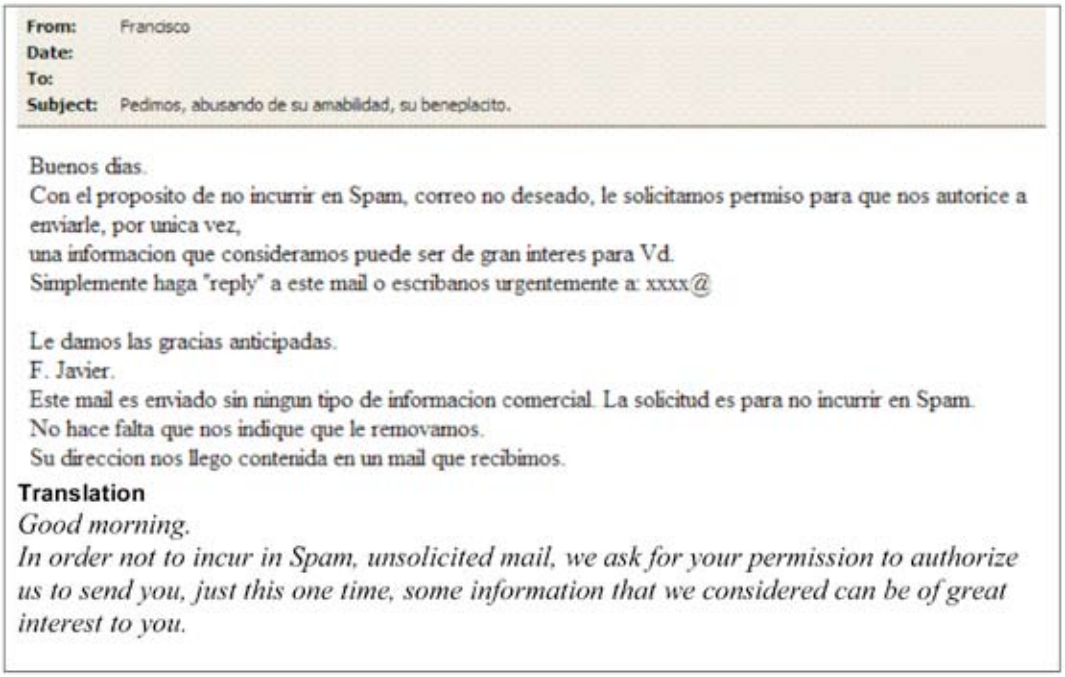
Date: Tuesday, June 24
To: xxxx
Subject: Best Offer for xxxx

Hello, my friend.

Do you want to buy any stuff: any kind of pills, oem software, cool porn?
Just mail me back, i'll find the best offer for you.

My Email: xxxx@

The list of email addresses that may be compiled would be very useful for the spammer. Not only are these people interested in buying the kind of products that the spammer is offering, but it's a bona fide opt-in list, one that the spammer can now send messages to freely without concern that he will be sending to spamtraps, or that the message will be blocked by spam filters.



From: Francisco
Date:
To:
Subject: Pedimos, abusando de su amabilidad, su beneplacito.

Buenos dias.
Con el proposito de no incurrir en Spam, correo no deseado, le solicitamos permiso para que nos autorice a enviarle, por unica vez,
una informacion que consideramos puede ser de gran interes para Vd.
Simplemente haga "reply" a este mail o escribanos urgentemente a: xxxx@

Le damos las gracias anticipadas.
F. Javier.
Este mail es enviado sin ningun tipo de informacion comercial. La solicitud es para no incurrir en Spam.
No hace falta que nos indique que le removamos.
Su direccion nos llego contenida en un mail que recibimos.

Translation

Good morning.
In order not to incur in Spam, unsolicited mail, we ask for your permission to authorize us to send you, just this one time, some information that we considered can be of great interest to you.

Simply send us a "reply" to this mail or email us back urgently to: xxx@

We thank you in advance.
F. Javier.

This mail is sent without any commercial information. The request is to not incur in Spam. It is not necessary that you indicate us to remove you. Your direction arrived to us contained in a mail that we received.

Japanese Adult Dating Spam Takes A New Twist

In the past, Japanese adult dating spam contained a URL link in the body of the email promoting a particular dating site. In a recent example observed by Symantec, the adult dating spam message did not contain a URL link. Instead, the spammer provided the recipients with two keywords asking them to search for their site on the Internet.

あなたのお住まいの街に、
どんな女性(男性)がいるのでしょうか。

同級生、
いつもすれ違うあの人、
電車、バスでいつも見かけるあの女性(男性)、
普通に暮らしていると一生巡りあわないだろう女性(男性)、

都道府県・市区町村と検索プロフを入力して下さい。
あなたの未来がちょっとだけ動き出します。

Mail body translation:

Do you know what kind of single men and women live in your town?

They might just be a stranger that you meet everyday on the train or bus.
The one you may never ever get familiar with, if you continue the life you live now.

Please enter [都道府県・市区町村(the state and city you live in)] and [検索プロフ(your profile)].
Your future may change since after.

China Earthquake Tragedy Used to Spread Viruses
Symantec has discovered an attack where the spammer is using the earthquake tragedy in China to spread a virus. The subject lines of the infected email appear as news headlines, hoping to entice the reader to open the email. There is even one subject informing users that the China Olympic Games are threatened because of the earthquake.

Sample subjects:
Subject: The most powerful quake hits China
Subject: Countless victims of earthquake in China
Subject: Death toll in China is growing
Subject: Recent earthquake in china took a heavy toll
Subject: Recent china earthquake kills million
Subject: China is paralyzed by new earthquake
Subject: Death toll in China exceeds 1000000
Subject: A new powerful disaster in China
Subject: A new deadly catastrophe in China
Subject: 2008 Olympic Games are under the threat

In the infected messages, a single line message with a URL is observed.

Deadly catastrophe in Chinese capital http:// xxx.cn/
Death toll in China is growing http://xxx.cn/
China is paralyzed by new earthquake http:// xxx.cn/
The list of Chinese victims is growing http:// xxx.cn/
2008 Olympic Games are under the threat http:// xxx.cn/
The most powerful quake hits China http:// xxx.cn/
Recent earthquake in china took a heavy toll http:// xxx.cn/

When the user opens the URL, the following image is displayed:

The user may be lured into playing the video, which in turn opens an executable file. This executable file has been detected as Trojan.Peacom.D by Symantec AntiVirus software. Trojan. Peacomm.D is a Trojan horse that gathers system information and email addresses from the compromised computer. The Peacomm family of Trojans are also commonly known as the “Storm” Trojan. Similar attempts have been made in the past using high profile news events to spread viruses via email. Users should be aware of such attempts, and avoid opening emails and clicking on suspicious links.

Olympics Related Lottery Scam Emerges

During June 2008, Symantec observed message scams claiming to originate from the Beijing Olympic Committee. The fraudulent messages purport to declare the winners of the lottery for an Olympic promotion.

The Subject and From Headers

From: BEIJING OLYMPIC LOTTERY BOARD
Reply-To: BEIJING OLYMPIC LOTTERY BOARD
Subject: BEIJING 2008 OLYMPIC COMMITTEE

The Message Body has a small note informing the recipient about the mail and instructs them to open the attachment for further details. It says:

To: Winner of Olympic Lottery Promotion.
See attachment for details .
Congratulations!!!.

The attachment informs the repicient that she has won a lottery from randomly selected email addresses. In order to claim the prize, the user has to contact the courier company below via email. Personal information is also requested. As the leadup to the Summer Olympics in Bejjing continues, it is expected more fraud and spam messages will emerge.

BEIJING 2008 OLYMPIC LOTTERY PROMOTION

BEIJING 2008

LOTTERY WINNING NOTIFICATION

Dear Sir / Madam,

We are pleased to inform you today of the result of the winners of the BEIJING 2008 OLYMPIC LOTTERY PROMOTION, held on Monday 16TH of June, 2008. Email addresses were selected randomly from official worldwide Company's, internet data web through online email addresses search engine with the aid of Google prominent search, which consequently won you the online sweepstakes in the 2nd category, in Europe, America region etc. Lucky numbers: 4-33-34-38-39-49 (bonus no.23) Your E-mail address has won the sum of CNY7, 200,000.00 ($960,000.00 USD) in cash credited to file IPL/4249859609/WP1. The Game will commence on the 8 of August, 2008.

You are to contact our affiliate courier company through E-mail with the contact information provided below for the delivery of your Winning Certificate and winning Cheque of CNY7, 200,000.00 ($960,000.00 USD).

WORLDWIDE EXPRESS MAIL SERVICE (EMS)
Email: ems_courier_service@ubbi.com
Web: http://www.ems.coop/site/Main.php
Country: Beijing, China.

VERIFICATION FORM TO AUTHENTICATE YOUR EMAIL

Full Name.....
Delivery Address.....
Sex.....Age.....
Occupation.....
Tel.....Fax..... (If any)
Country.....
E-mail.....
Winning Number.....

Congratulations once more from all members and staffs of this Beijing 2008 Olympic Committee. Thank you for being part of our online promotional lottery program.

Spam Targeting Japanese Mobile Phone Market

Spam messages that target mobile devices are not new, but they regained prominence in the last month. Sending emails from mobile devices is very popular in some countries, especially in Japan, so it's not surprising that users would become targets for spammers. Porn, product and adult dating spam targeted towards mobile devices have all been observed. The format of these mobile spam messages are very similar to messages targeted towards other electronic devices. There are some differences however. In the example below, the Japanese adult dating spam message contains information about the service it offers to prospective users and provides a link for the mobile user to access. The URL page is designed with a specified width and height allowing it to be more visible on a small screen such as a mobile device. As people spend more time using mobile devices to check email, the growth of these types of mobile spam messages is expected to continue.


■新着サイトのご案内■
完全無料のコミュニティサイト！フリーメールでのエントリーも可能！！

今すぐクリック！
http://********.net/kura/starm/
※ご利用は無料です。

Translation
Introducing new website
Community site for completely free of charg!
Can register with your free email account!!

Click Now!
http://********.net/kura/starm/
Available free of charge

Bogus News Events Lure Innocent Victims

As antispam filters continue to become more sophisticated, spammers techniques are evolving. However, some spammers return to techniques they have deployed in the past. One technique they have used, and continue to use, is sending bogus news headlines as subject lines for their spam emails to try and entice recipients to open the message. Some of the bogus news headlines observed recently in spam subject lines include:

Subject: White House hit by lightning, catches fire
Subject: Lastest! Obama quits presidential race
Subject: Egypt Giza pyramids rocked by massive earthquake
Subject: Great Wall of China damaged by earthquake
Subject: Oprah found sleeping the streets
Subject: Stonehenge damaged by massive earthquake
Subject: Donald Trump missing, feared kidnapped
Subject: Eiffel Tower suffers structural damage, collapse possible

By opening these messages, the user is invariably presented with a link directing them to a spam offer.. Using eye catching and often absurd subject lines is a quick ploy by spammers to catch the recipient's attention and play on their curiosity. Be warned, as the old proverb says "curiosity killed the cat" but in this case, curiosity could perhaps make you an unwitting target for a spammer.