



July 2009 Spam Report

McAfee Avert Labs Discovers and Discusses
Key Spam Trends

Key Findings

Governments around the world could improve their national and international business prospects by aggressively combating illegal Internet activities.

Spammers understand their "customers," regardless of the country their victims reside in, and tailor the message to suit the audience. They also protect themselves by aiming at users in other countries, thus diminishing the interest of local governments in putting a stop to their actions.

Table of Contents

Spam's Effect on International Commerce	3
Conclusion	4
Top Subjects by Domain	4
Conclusion	11

Spam’s Effect on International Commerce

Spam has a long-term effect on international commerce. It can occur when administrators decide to block a sender’s IP based entirely on geolocation—the “from” domain—or by not allowing foreign languages or URLs into their domain. Actions such as these generally stem from foreign-language spams reaching executive decision makers who then demand an administrator respond to specific language-based criteria. These sorts of policy decisions are unlikely to be regularly reviewed, and represent a digital bias against certain languages or countries that could affect legitimate communications.

The long-term economic interests of countries that don’t regulate questionable hosting providers and domain registrars can suffer significantly because of these short-sighted policies. The enormous prevalence of Chinese and Russian URLs in pharmacy spam mails causes people to want to block every incoming email from these countries, just to be safe. From a business perspective, the institutions providing the domain registrations for spammers cripple the opportunities for legitimate domains; they are branded guilty by association and are often blocked along with the rest.

The providers of these spam services make no attempt to hide their position. One spam written in Russian (see Figure 1) directs the recipient to a website where they advertise the ability to send hundreds of millions of spam messages to your choice of more than 150 million email addresses spread across various countries.



Figure 1: Advertisement for Russian-language spam

Though protected from criminal prosecution by the laws and bureaucracy of their host nations, these sites are not unknown or anonymous entities to spam researchers. The overwhelming evidence of bad behavior can far outweigh a legitimate “mom and pop” shop trying to set up a low-cost website through a local hosting provider. We feel it is in the best long-term interest of sovereign nations to police hosting companies located inside their borders rather than allow them to operate so openly.

Conclusion

Today's worldwide economic issues pose enough problems for the average business trying to stay afloat. We all rely heavily on our governments to protect us and provide an environment that is conducive to legitimate business practices. Until government regulators, together with local and international law enforcement, start cracking down on illegal Internet activities, it will be extremely difficult for companies to win business in international marketplaces.

Corporations should also review policy decisions that are based on reactions to spam. One-shot policies often ignore the continuing evolution of spam over the long term; as spam changes, security effectiveness can erode and actually create a situation in which a company actually has less security and suffers from more false-positives. For example, blocking all incoming email from a particular foreign language without determining whether the email is from friend or foe may stop a business from getting its next big sale, partner, or opportunity.

Top Subjects by Domain

The following subject lists provide data for a cross-sectional study of spam traffic—based on business and country domains—for one complete day in June. These lists are ranked from highest volume to lowest volume of the most common subjects we saw. You'll see a few misspellings among these subjects. Looks like spammers are still missing a reliable spell-checker.

.COM

1. Hello
2. Hi
3. RE: DISCOUNT 80% OFF on Pfizer !
4. Replica Watches
5. Undelivered Mail Returned to Sender
6. Delivery Status Notification (Failure)
7. Returned mail: see transcript for details
8. Exquisite Replica
9. Aloha
10. failure notice
11. Hey
12. Cheers
13. Watches
14. Complete registration here
15. Subcribed on daily news?

The “.com” domain name is most common among companies in Western countries, and we'll use it as the baseline against which we'll compare other domains.

Only one of the top subjects currently involves pharmaceuticals. It's interesting that three of the top 15 subjects mention watches or replicas, as opposed to only one pitching Viagra.

Quite a few of the top 10 spam subjects are delivery-status notifications; they represent spam that has been “bounced back” to a forged From address.

Everything else, including the one-word greetings, are all currently associated with “Canadian pharmacy” spams on Chinese URLs.

.ORG

1. Delivery Status Notification (Delay)
2. Delivery Status Notification (Failure)
3. failure notice
4. Undelivered Mail Returned to Sender
5. Hello
6. Hi
7. Returned mail: see transcript for details
8. RE: DISCOUNT 80% OFF on Pfizer !
9. Replica Watches
10. Exquisite Replica
11. Mail delivery failed: returning message to sender
12. Hey
13. Watches
14. Cheers
15. You have received an Greeting eCard

We were surprised to see that there are more bounce backs associated with the “.org” domain than there are with the .com domain. Whereas our baseline, .com, has no delivery-status messages until the fifth message subject, the .org world fills up the top four positions with status notifications.

The greeting ecard spam points to a URL that downloads an executable file and infects the computer. This same malware-delivering spam strain is global, but we find it interesting that this strain doesn't enter into the top 15 spam subjects in the .com domain.

The .org suffix also has three of the top 15 message subjects selling fake watches. This matches what we see with the .com suffix. These subjects do not make the top 15 of any other domain suffix. They occur elsewhere, but seem to be sent proportionally more to domains without country codes.

.US

1. Returned mail: see transcript for details
2. RE: DISCOUNT 80% OFF on Pfizer !
3. Hi
4. Hello
5. failure notice
6. Delivery Status Notification (Failure)
7. Undelivered Mail Returned to Sender
8. Subscription status
9. Empty package from you
10. Can't find your photos
11. Got invite for you
12. Coupons for us
13. Copy it and send
14. Your work scheme
15. Mail delivery: failure

Based on the assumption that a United States–centric mail flow would dominate the .com recipients, we find it interesting to see the differences with the “.us” domain. Delivery-status messages take the top spot for emails containing spam, and the rest of the content is pharmacy spam.

The fake Rolex spam messages don’t make the list, even though replica-watch spam is globally one of the top spam subjects. The dominance of replica-watch spam in .com and .org domains is far greater than in any other domain, which could be indicative of the time or method used to harvest or generate these email addresses.

.AU

1. Message (1) from St. George
2. RE: DISCOUNT 80% OFF on Pfizer !
3. View this text
4. Group training for us
5. Naked Rihanna in bath
6. File transport blocked
7. Still have honor?
8. Court decision
9. Full copy of subj
10. Photos of the place
11. Can’t call you
12. Cell number changed
13. I have two complaints
14. Tried doing this?
15. Interesting feature

“St. George” is an Australian bank. This phishing scam occurs only in Australia, and was the top spam subject in the most recent month. The rest of these subjects are from Chinese newsletter pharmacy emails pointing to Chinese and Russian URLs from a Chinese registrar.

.UK

1. RE: DISCOUNT 80% OFF on Pfizer !
2. Salute, man!
3. All songs zipped
4. Photo gallery
5. Court decision
6. Photos of the place
7. Group these photos together
8. New .pdf variant
9. I’m locked in room
10. Can’t call you
11. Corporate meeting
12. Your house switched off
13. What’s with bar?
14. Add this to work
15. Wondering about slow speed?

Pills, pills, pills. The “.uk” list pure pharmacy spam from top to bottom.

This list also contains no “undeliverable” bounced messages. Given that United Kingdom spam is also in English, we might assume that techniques that work in the U.S. country code would also work in .uk. However, that’s not the case, so we imagine that U.K. email addresses have been left out of the forged From addresses through some conscious action by spammers. We don’t really know whether someone

chose one country code over another. Perhaps an algorithm merely appended .com or .org to the end of a randomly generated string, but the practice stands in stark contrast to spam behavior in the .us world.

.CN

1. RE: DISCOUNT 80% OFF on Pfizer !
2. 代理业务！
3. 】【eHs【工厂安全管\$理实务|训练132
4. Part time job offer (work with us.)
5. 専門家も驚愕 レプリカブランド
6. 解决问题，就是这么简单！
7. <¥40超值换购>樱桃鲜果美白★最大可省¥110！
8. 最后一天报名参加中小企业终端防护在线会
9. 民营企|业的股|权激|励模|式
10. 3a)绩c效反|馈流|程&程cn
11. urgent
12. 經典氣密隔音窗!!許您一個寧靜的夜晚
13. 来自 people.com.cn 的退信
14. Transfer Proposal
15. 克服演讲焦虑的好方法

The People's Republic of China also sees a lot of pharmacy spam, and it is their top subject. However, the Pfizer spam is a different variety than the other pharmacy spam subjects, which tend to dominate our spam quarantines. The Pfizer spam is generally shorter and commonly takes advantage of Yahoo or MSN groups for the linking URL. The URLs that those Yahoo pages point to appear similar to the "Chinese newsletter" pharmacy spam that covers the rest of the world, but the IP address is not in flux and the registrar is not of Chinese origin.

The pharmacy spam that we don't see here passes itself off as a newsletter (or newsletter-like) email that directs you toward a Chinese or Russian URL. All these URLs are registered with a Chinese registrar but apparently do not make up as significant a part of the Chinese mail flow as they do everywhere else.

"Urgent" and "transfer proposal" are both confidence scams, generally from free email websites (such as Gmail, MSN, or Yahoo). These emails work only when the recipients communicate in the same language.

.TW

1. RE: DISCOUNT 80% OFF on Pfizer !
2. 歡樂衣整夏◇電視購物狂銷 M&J牛仔褲超值百搭單品◇bling飾品299元起 (ADV)
3. Hey
4. Hi
5. Cheers
6. Hello
7. ■■■ 強棒出擊激殺戰 ■■■ Seagate 500GB 外接硬碟\,\$1999
8. Aloha
9. 全新義大利·奢華風裝潢!! 女服務生絕對精挑細選·滿意再消費
10. 來這裡比在夜店花費還便宜! 應酬, 玩樂, 把妹, 是你最佳選擇!
11. ㄟ ★奢華風~獨家限定!!★ ㄟ HOYA雙人四件式(仿真絲蕾絲)被套床包組\,\$1499●全館滿\$1980((送)藤蓆座墊x2
12. 9週年慶★旭光8-10坪《清靜型》1對1冷氣-破盤價\$16900★獨家送:冰淇淋+沙宣吹風機
13. 6/23(二) 辦理 懲戒性解雇、經濟性解僱之審查標準及程序進行之法律問題探討 課程講座
14. Our menu
15. Outlook Setup Notification

There are some significant differences between the domains of the Republic of China (Taiwan's ".tw") and the People's Republic (.cn), particularly in the greater amount of English-language email the former

receives. In Taiwan, all the top English subjects are pharmacy spam. China and Taiwan have the Pfizer spam in common, but the rest of the "Chinese newsletter" spams appear only in .tw and not in .cn. All have Chinese or Russian domains registered with a Chinese registrar. We might assume the spammers are purposely avoiding sending their spam to a .CN site to avoid official retribution for their behavior, but the spammers apparently do not consider .tw a part of .cn.

.DE

1. Outlook Setup Notification
2. RE: DISCOUNT 80% OFF on Pfizer !
3. Information of your Transactions
4. Worldpay CARD transaction Confirmation
5. Degree in any field.
6. Masters degree with no efforts.
7. Call us for a Masters degree.
8. Real University diplomas.
9. Claim your degree.
10. Call for your diploma now.
11. Bachelors, Masters or Doctorate degree.
12. Receive a Bachelors degree.
13. Get a diploma for a better job.
14. Give us a call to get a diploma.
15. You have received an Greeting eCard

Germans receive lots of diploma spam as well as both of the top malware-carrying email strains we've seen in other countries. Unique to the German top 15, however, is the "Information of your Transactions," which is similar to other malware samples in that it links to an executable over the web. Both malware examples in their top 15 subjects as well as the popular diploma spam give the Germans a dubious double "prize."

.FR

1. RE: DISCOUNT 80% OFF on Pfizer !
2. Outlook Setup Notification
3. Aloha
4. Hey
5. Hello
6. Cheers
7. Hi
8. Mutual Benefit
9. Information of your Transactions
10. New replies to your entry
11. Worldpay CARD transaction Confirmation
12. Super Obama's pants
13. See new RHCP clip
14. Pick me after work
15. Claim your degree.

France, like the United Kingdom, doesn't see much spam with delivery-status subjects. They're not plagued solely by pharmacy spam, though. The Worldpay spam contains a zipped executable that installs malware, and we also see diploma spam.

.CA

1. RE: DISCOUNT 80% OFF on Pfizer !
2. Your work scheme
3. Did you sign it?
4. Mail delivery: failure
5. Copies of your documents
6. Our menu
7. Call on this number
8. Eminem's buttkissing interview
9. Full list of invited ones
10. Help me identify song
11. Your 3rd late arrival
12. Scandalous Aguilera's rowdy scene
13. Visit me in hospital
14. Sale in the whole network
15. Coupons for us

Canada gets a few more delivery-status messages than the .com world, but as in the United Kingdom, the Canadians are dominated by pharmacy spam. The strains leading to ".ca" domains have fewer one-word greeting subjects than most other domains.

.BR

1. Hey
2. Aloha
3. Hello
4. Hi
5. Cheers
6. RE: DISCOUNT 80% OFF on Pfizer !
7. Informativo de Segurança do Cadastramento de Computadores.
8. Award Result 2009
9. Tell me about this man
10. See new RHCP clip
11. Further letters
12. All employees' MSNs
13. All lecture notes
14. Can't call you
15. KIND ATTENTION

Brazil is dominated by pharmacy spams with one-word greetings (a strain of the Chinese newsletter spam), and also sees the Pfizer spam and a number of longer subjects for the Chinese newsletter spam. "KIND ATTENTION" is a confidence scam.

.BE

1. RE: DISCOUNT 80% OFF on Pfizer !
2. Outlook Setup Notification
3. Worldpay CARD transaction Confirmation
4. Information of your Transactions
5. Call for your diploma now.
6. You have received an Greeting eCard
7. Don't miss unbelievable savings on Apple Macintosh.
8. Call us for a Masters degree.
9. Buy Soft For The Prices You Will Enjoy.
10. Nominate for the degree you want.
11. Original software of different versions at friendly prices.
12. Get a diploma for a better job.
13. Get a degree with no problems.
14. Choose the needed field.
15. You Are Sure To Find Any Soft You Need.

Belgium, like Germany, has a significant amount of diploma spam. Cheap foreign-language software spams also make the top 15. Cheap software is a global spam strain, but not often does it manage to get into the top 15 spam subjects. The Worldpay emails contain a zip file with malware and claim to be payment for an order from amazon.com. The "Outlook Setup Notification" contains a Russian URL both registered and hosted in Russia. The "Information of your Transactions" is similar to the Russian spam except that it is registered and hosted in Poland.

.CL

1. RE: DISCOUNT 80% OFF on Pfizer !
2. Hey
3. Hi
4. Hello
5. Cheers
6. Aloha
7. Outlook Setup Notification
8. Information of your Transactions
9. Worldpay CARD transaction Confirmation
10. You have received an Greeting eCard
11. We will call you back.
12. Mail could not be delivered
13. Degree in any field.
14. Apply for your diploma.
15. Diplomas for everybody.

Chile receives a mass of malware that we've seen in other top 15's; subjects #7 through #10 all try to infect the recipients. The country's top six subjects are common pharmaceutical spams, and they also get a significant amount of diploma spam.

.TR

1. Aloha
2. Hey
3. Hello
4. Hi
5. Cheers
6. Disappointed with your sexual health?
7. Anti-Crisis Sale
8. RE: DISCOUNT 80% OFF on Pfizer !
9. Why purchase from Canadian Healthcare?
10. Portatif stand
11. Altýn Örumcek web ödüllerinde Tekfen Sigorta' yý seçti
12. Sex Pharm
13. Request Approve
14. Outlook Setup Notification
15. Don't waste time waiting for the delivery of software CD.

Turkey, like Belgium, also suffers from a lot of cheap foreign-language software spam. "Outlook Setup Notification" and "Request Approve" casino spam lead to malware. Pharmaceutical spam from China fills many other spots.

.VE

1. Hi
2. Aloha
3. Cheers
4. Hello
5. Hey
6. RE: DISCOUNT 80% OFF on Pfizer !
7. Win in Fiesta
8. Show her overwhelming desire
9. Make your main part bigger
10. Be hot long action king
11. Play today in LA Casino
12. Iron hot-rod forever!
13. Her emotions will go off-scale!
14. Make your pecker your trump trotter
15. Become number one in dating fortelage

Venezuela gets a ton of the widespread newsletter pharmacy spam with Chinese and Russian URLs, but they also get a lot of lottery spam. The "Win a Fiesta" spams—along with others that include the word *casino*—are all spams that attempt to lure victims with online gambling. Click on one of these and you'll get a malware package from a Russian URL pointing to a server hosted in China.

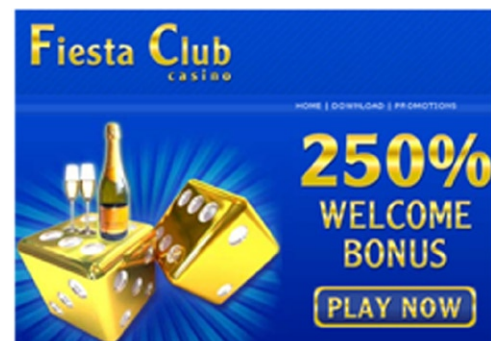


Figure 2: Online gambling spam is common in Venezuela. Most delivers malware.

Conclusion

We have seen a dominance of spam bounce-backs in the .com, .org, and .us domains compared with other countries, in which bounce-backs are insignificant. Although spam is international, it seems that spammers prefer to forge sending domains with these three to a degree out of proportion with the rest of the globe. Was that choice made maliciously, by convenience, or by slacking?

Spammers appear to understand their customers as well as or better than the average corporate marketing department. They tailor messages and products to what is most likely to appeal to a specific audience. Maybe they should give seminars on "How to Market to International Audiences."

At the same time, spammers are smart enough to avoid directing traffic to URLs in the countries in which they operate. After all, how upset can a government get if its own citizens aren't being taken advantage of?

