Frequency vs. Presence of Violation

(a) Presence of violations
(b) Total traffic for 62.34.164.84.
Figure 4: Spam Delivery Rates grouped by Income
Figure 1: Histogram: Given an IP address, how many blacklisted domains use that IP address as a name server?
Figure 6: Total memory usage of traffic monitoring system.
ROC in SNARE

True positive (%) vs False positive (%)

24+ hour history
message based
packet based

tp = 70 %
fp = 0.2 %
<table>
<thead>
<tr>
<th>Statistical Highlights for 2nd Quarter 2013</th>
<th>July</th>
<th>August</th>
<th>September</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique phishing websites detected</td>
<td>49,480</td>
<td>48,758</td>
<td>45,115</td>
</tr>
<tr>
<td>Number of unique phishing e-mail reports (campaigns) received by APWG from consumers</td>
<td>61,453</td>
<td>61,792</td>
<td>56,767</td>
</tr>
<tr>
<td>Number of brands targeted by phishing campaigns</td>
<td>390</td>
<td>400</td>
<td>379</td>
</tr>
<tr>
<td>Country hosting the most phishing websites</td>
<td>USA</td>
<td>USA</td>
<td>USA</td>
</tr>
<tr>
<td>Contain some form of target name in URL</td>
<td>35.24%</td>
<td>73.51%</td>
<td>56.22%</td>
</tr>
<tr>
<td>No hostname; just IP address</td>
<td>0.15%</td>
<td>3.20%</td>
<td>1.73%</td>
</tr>
<tr>
<td>Percentage of sites not using port 80</td>
<td>0.04%</td>
<td>0.32%</td>
<td>0.86%</td>
</tr>
</tbody>
</table>
Expected Uniform Posting Pattern

\( (T \mod 3600) / 60 \)
Non-Uniform Posting Pattern

Bias towards beginning of the minute
Non-Uniform Posting Pattern

Bias towards beginning of the hour
Non-Uniform Posting Pattern

Two distinct posting processes
Non-Uniform Posting Pattern

Every 5 min., plus some organic
Hyper-Uniform Posting Pattern

Steady posting with phase drift - too uniform
Anatomy of a modern Pharma spam campaign

- Pay commission
- Spammer
- Bulk email sender
- Open proxies/botnet
- Spammer
- Spam emails
- Email recipient
- Clicks on link
- Email with link
- Other recipients
- Email target page ( disposal hosting)
- Affiliate program
- Redirects
- Commission (up to 40%)
- Viagra/pharmacy site
- VGR100
- Sale made
- Typical value $50-100
- VGR100
- VGR100
- VGR100
- VGR100
- Sildenafil citrate
- Generic pills
- Non-US supply (India, Mexico etc.)
- Patent expired
- Mere cents per pill = massive markup

Courtesy Stuart Brown
modernlifeisrubbish.co.uk
Frequently Asked Questions

How do you pay?

We pay every week on Thursday with a 2 weeks’ holdback. $50 minimum on stormpay and wires. If you require larger amounts sent at one time you can set the minimum yourself.

Payment by request is now available. Effective from 07.17.2006

Our loyal affiliates now have the chance to minimize the hold period and get the money when they need it. Even though it will be handled individually in every case the guidelines are simple.

You should have the steady sales record for the last 3 months (that is your daily average should be at least 3 sales for the above mentioned period) and your traffic source can be easily tracked. This will not apply to the commission earned during special promotions and we won’t be able to pay to PayPal earlier than scheduled. You are welcome to use Bank Wire, Epass, Egold, Webmoney and others.

What are your payment plans?

How do you know that this is “my” customer?

What should I do to join you?

What do you sell?

What if I don’t live in the USA? May I become your affiliate?

Where can I monitor the statistics of my site?

When do you ship the orders?

Can I advertise a specific product, not the whole pharmacy?

What is the commission on the refill orders?

I need help configuring my templates what do I do?

I lost my password, what do I do?

Are you accepting call centers?
What are your payment plans?

Our affiliate program offers 3 levels of RevShare.

You can choose to receive 30, 40 or 50% from sale. Prices of products increase with each new level of Revshare. You can set ANY price provided that it is higher than the base price (price of product at 30%).

For example, viagra 100mg x 10 pills, has the following prices:
- $29.95 (30%)
- $35.95 (40%)
- $49.95 (50%)

- You cannot set the price lower than $29.95
- Any price between $29.95 and $35.95 will give you Revshare of 30%
- Any price between $35.95 and $49.95 will give you Revshare of 40%
- Any price higher than $49.95 will give you Revshare of 50%

To change the price enter the new figure in "Your Price" window and click on the arrow next to it. The forecast of price per pill and your commission will be shown. Click on the Save button at the bottom of the screen to enable the new prices. (If you don’t click on the arrow the “Save” button won’t work)

You can also change all prices by setting a needed percentage in "Value", (in the upper part of interface), or by coping the prices from another Tracking id.

Please note that some products may have only one or two levels of Revshare.

How do you know that this is “my” customer?

First, your affiliate id is clearly visible in the site’s url. Our program leaves a cookie at a customer’s computer to identify him at the return. And finally the customer creates an account at our site. He is sure to remember his original login name as we offer great bonuses for the returning customers.
Are Bots & Spam the New Black Gold?

- Spam finance elements:
  - Retail-cost-to-send vs. Profit-per-response
  - Key missing element: spams-needed-per-response, i.e., conversion rate

How can we measure this? Seemingly only knowable by the spammers themselves.
Kirill Levchenko
klevchen@cs.ucsd.edu

I am a project scientist with the Systems and Networking group in the Computer Science department at the University of California, San Diego. My current research...
If we control these, we can monitor & influence these.
If we control these …

… we can monitor & influence these.