

**Consumer
Reports®**

WEBWATCH

LOOK BEFORE YOU CLICK

E-Crime Workshop
Wednesday, March 4, 2009
ICANN Mexico

“Registrants” vs. “Users”

Have you ever registered a domain name?

- Yes 14%
- No 86%

WebWatch survey statistically representative of NY State, May/June 2008, 2000+, four regions

WHOIS: Little known

Have you ever used WHOIS database to find the name of a Web site's registered owner?

- Yes, and I found the information I was looking for: 6%
- Yes, but I could not find the information: 2%
- No, but I was aware I could do this: 8%
- No, and I was not aware this was possible: 68%

WebWatch survey statistically representative of NY State, May/June 2008, 2000+, four regions

Fraud a Risk to Internet's Reputation

- 24 percent (NY) report malware infection
- 27 percent (NY) download less frequently
- Most (NY) consult ISP/provider for help (19%)
- 64 percent (NY) received pharmacy spam
- 45 percent (NY) 419 solicitation
- 59 percent (NY) winning lottery notice
- \$8.5B in losses, victim % 1 in 6 (CR), 2008:
- \$2.9B, viruses
- \$3.6B, spyware
- \$2B, phishing

Crime in the Open

<http://www.glavmed.com/index.php>

“GlavMed is a BEST way to convert your pharmacy traffic into real money. Forget about miserable sums you're getting sending your visitors to PPC pharmacy results. You're losing at least half of YOUR money converting traffic like this. GlavMed offers you a possibility to eliminate any agents and sell most popular pharmacy products directly. It means 30-40% revenue share.”



'Registrar Profiling'

<http://rxaffiliateforum.com/showthread.php?t=5913>

- “Hi, Can you guys suggest some safe registrars where we can register pharma domain names?
As you know these days registrars like Directi and GoDaddy suspending domains like anything.”
- “Pharmacy Shark patrol has domains with both GoDaddy and Directi. We have only had difficulty with domains on Directi. For this reason we have moved all our health related registrations to other registrars in other countries.”
- “Can Canadian registrars considered to be safer than Directi or US registrars? EU registrars are having almost double pricing.
Can you people suggest some?”
- “namecheap.com
Because he is a reseller of ENOM not Directi and other registrars that have begun to actively combat pharmacy...”

Frustrated Consumers 'Fight Back'

- <http://www.badwhois.info/wp/?cat=12>

“...As the CEO of Godaddy, you were made aware of a serious situation in your company and as such you cannot deny knowledge of this issue... You are the registrar for the scam domains reported as having fake whois and the ICANN is extremely clear in its RAA as to what should happen under these circumstances.

Please go and read these documents:

<http://www.icann.org/en/registrars/ra-agreement-17may01.htm>

<http://www.icann.org/announcements/advisory-10may02.htm>

<http://www.icann.org/announcements/advisory-03apr03.htm>

I have also tried resolving this via ICANN, however it seems they never really looked into the matter since I have had no reply again from them. As such, I have made other parties aware of this issue. I trust you will be in Mexico? This issue might be used to show how registrars willfully breach the RAA, endangering the public in the process.” (excerpts indicated by ...)

What We Tell People (You May Not Like It!)

- Don't use sites in .info, .biz, .ro, .ru, .cn domains
- Use WHOIS to investigate Web sites
- Don't do business with sites using private proxy registration

DNS and E-crime: No Myth

“We believe that malicious code using the DNS to enable propagation of worms and establishment of large botnets is likely to continue, even increase, in the short term.”

ICANN Blog Post February 14 by Greg Rattray

(<http://blog.icann.org/2009/02/conflicker-dns-security-and-what-icann-is-doing-about-it/>)

Resources and Help

- <http://blog.consumerwebwatch.org>
- <http://www.badwarebusters.org>