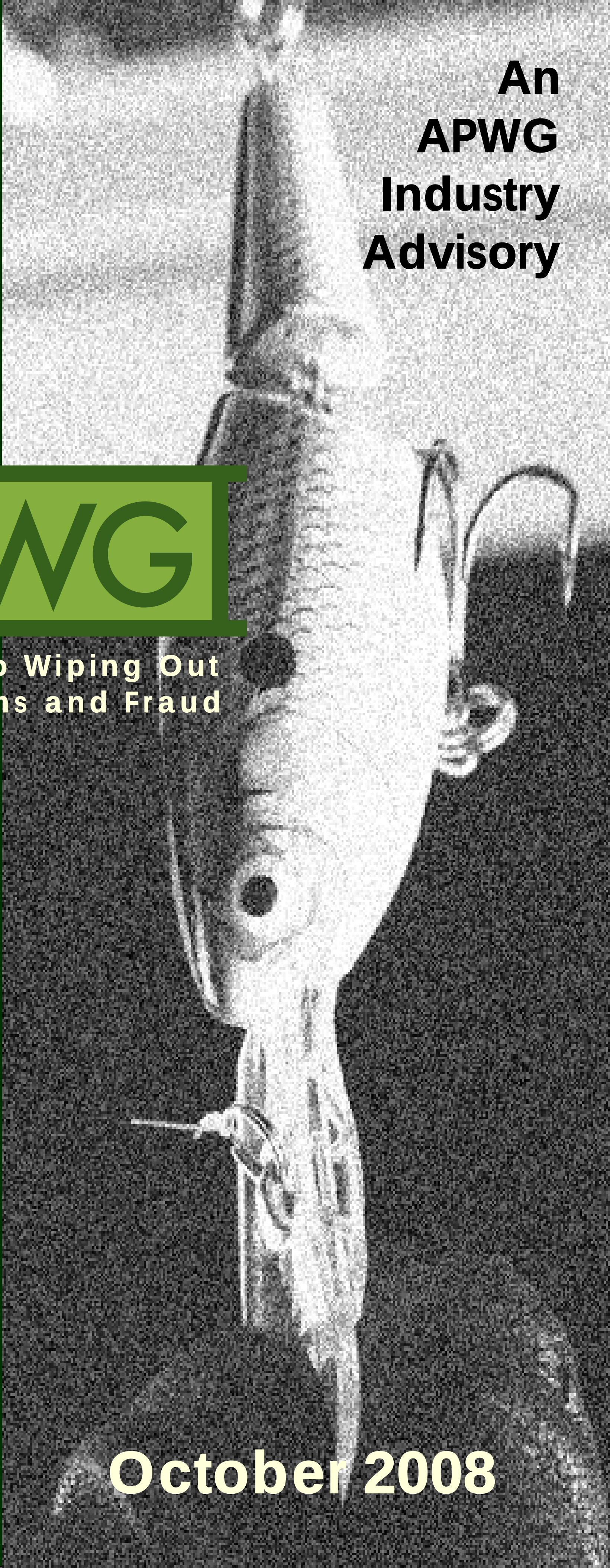
Anti-Phishing Best Practices Recommendations for Registrars

An
APWG
Industry
Advisory



APWG

Committed to Wiping Out
Internet Scams and Fraud

October 2008

Correspondent Authors Contact Data:

Dmitri Alperovitch, Secure Computing: dmitri_alperovitch@securecomputing.com
Ryan MacFarlane, FBI: rmac@jacketnet.com

Disclaimer: PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this message as a public service, based upon aggregated professional experience and personal opinion. These recommendations are not a complete list of steps that may be taken to avoid harm from phishing. We offer no warranty as to the completeness, accuracy, or pertinence of these recommendations with respect to any particular registrar's operation, or with respect to any particular form of criminal attack. Please see the APWG website — http://www.apwg.org — for more information.

Principal Investigators:
Dmitri Alperovitch, SecureComputing
Ryan MacFarlane, FBI

Contributing Researchers:
Jon Nevett, Network Solutions
Mike Rodenbaugh, Rodenbaugh Law
Pat Cain, The Cooper-Cain Group and APWG
Rod Rasmussen, Internet Identity

Summary

The purpose of this document is to provide a set of recommendations to the domain registrar community that can substantially reduce the risk and impact of phishing on consumers and business worldwide. The recommendations focus on 3 areas where registrars can be of assistance:

1. **Evidence Preservation for Investigative Purposes**: As registrars are in direct contact with the criminals as they are registering fraudulent domains (typically through the registration process on the registrar's website), they may have the ability to acquire key important evidence that can be later used by law enforcement to identify and prosecute the phishers. This document enumerates the type of evidence that can be collected during the domain registration process by the registrar that would be helpful to law enforcement. We encourage registrars to collect and store as much of this evidence as is feasible in their circumstances to achieve the best chances of law enforcement catching the criminals. Increasing the risk for these criminals of capture, prosecution, and incarceration should have a significant deterrence impact and eventually result in a reduction of these types of crimes.

2. **Proactive Fraud Screening:** With a bias towards not impacting legitimate customers, anything that registrars can do to complicate the domain registration process in order to frustrate the phishers and limit their ability to perform fraudulent domain registrations on a large scale is highly beneficial. This document suggests some lightweight processes registrars can put in place to identify fraudulent activity before the domain registration takes effect. The harder it is for the criminals to commit these frauds, the more likely it is that they will move off to something else that requires less effort on their part.

3. **Phishing Domain Takedown:** Once a phishing site goes live and is promoted by the phisher, it is imperative that it be taken down as quickly as possible in order to limit its impact and the number of potential victims. As part of the takedown process, anti-phishing organizations typically contact both the hosting provider of the phishing website, as well as the registrar or registry responsible for a *fraudulent* domain registration. This document contains best practices that registrars can use to process the takedown requests in the most optimized fashion and limit the victim's financial losses.[1]

[1] Please note that in the context of this guide, phishing domain take-downs refers only to domains that were registered solely for fraudulent or criminal purposes. Such procedures do *not* apply to those cases where the web site of a legitimate domain is compromised and used by criminals to attack or compromise other computers

Organizing Principles

The measures described in this document reinforce a set of principles commonly practiced in the anti-phishing community. These principles include:

- Phishing is a security risk to consumers; it hurts consumer confidence in the Internet and damages the reputation of the domain registration system.
- Protecting against phishing protects consumers, protects the security of the Internet, and reduces financial loss to the registrar, registry, and ISP.
- Taking steps to protect consumers against phishing is equivalent to protecting the registrar's, registry's, or ISP's brand from the damage caused by phishing.
- Organizations that are part of the infrastructure of the internet (ISPs, registrars, registries, etc.) should take reasonable steps to protect against phishing in order to fulfill their obligations to protect the stability and security of the Internet.

Background

Phishing is a global and growing criminal problem that victimizes hundreds of businesses and millions of consumers worldwide. Phishing refers to social engineering techniques designed to fool users into disclosing sensitive personal information to web sites impersonating known brands and specially registered domains used to serve malware designed to compromise the computers that connect to these domains and then steal a range of sensitive information from them. In both cases these attacks are mostly conducted for illicit financial gain/fraud.

Many things can be done to improve defenses against phishing, ranging from consumer education and fraud detection techniques to more advanced login authentication and fast phish site takedowns. In this document, we will address the part of the problem that can be addressed by the ICANN community and present specific recommendations for domain name registrars about what they can do to assist in this effort.

The members of the APWG include brand owners who are being phished; vendors that specialize in phish site takedown and other anti-phishing technologies; ISPs; domain registration providers; academic researchers; and law enforcement. This wide range of experience puts the APWG — as a collective whole — at the very forefront of expertise on issues surrounding the relationship of domain name registrations and their impact on the "phishing" problem.

Domain name registrars are not simply bystanders in this fight. They are also among the thousands of organizations that are routinely victimized by the organized criminal enterprises involved in phishing fraud. Since these criminal individuals and organizations nearly always use stolen credit and debit cards acquired from their prior phishing attacks to register new domains, registrars are the ones that absorb the cost of the charge backs for these fraudulent domain registrations. They also suffer from the increase in indirect support and abuse department costs that are associated with processing the growing number of requests from individuals and organizations are tracking phishing sites and attempting to take them down.

Another troubling trend emerged in July 2007, when phishers began targeting domain name registrars themselves. This means that registrars now also need to be cognizant of the fact that their customers are becoming victims of phishing and that legitimately registered domains, including those that may be owned by financial institutions, are being compromised by phishers.

It is our belief that registrars that implement some or all of the recommendations offered in this document will not only do their part in combating this global crime problem, but in the process will also help to reduce their own losses and costs, as well as improve the protection of their customers.

A final note —we understand that registrars are cost-constrained. Our purpose with this document is to give registrars options for hardening their systems against phishers. While we hope that every registrar will implement a majority of these recommendations, it is understood that individual registrars will have to evaluate which of the prescribed best practices make the most business sense.

Top 5 Most Consequential Recommendations

1. *Timely response to domain takedown requests by shutdown authorities and/or law enforcement*

Phishing sites typically do most of their damage and steal the majority of credentials and financial account data from their victims in the first hours of the phishing operation. Thus, it is absolutely critical that the domain be terminated as quickly as possible once the registrar/registry is notified and has confirmed the criminal activity associated with that domain. In addition, keep in mind that it is not usually law enforcement that will be contacting you about shutting down a phishing domain. Instead, the brand owner themselves or third party anti-phishing providers will likely be first to initiate contact.

Having procedures in place with regard to handling phish domain termination can go a long way toward handling an event in a timely and cost-effective manner. For example:

- Identify the company internal team that addresses phishing inquiries and provide them with procedures and guidance policies (if possible, this should be a 24x7 team since phishing inquiries can arrive at any time)

- Specify the evidence required to verify that a site is being used for phishing. This may include having your team perform an independent verification of the organization reporting the phish site or investigate whether the site is being used for malicious purposes. (The APWG is working on a process to accredit phish site takedown providers. Once that process is in place, registrars can use it to confirm an organization has been accredited to identify phishing sites.)

- Outline the steps to take to shut down the domain

- Outline the procedure for evidence collection, evidence storage, and contacting law enforcement

2. *Proactively use available data to identify and shut down malicious domains*

There are numerous sources that can provide information to help in identifying malicious activity. The APWG can provide a daily feed to registrars listing all of the phishing URLs identified by the APWG community for cross reference. Entities such as the SORBS Dynamic User and Host List can provide networks associated to dial-up, DSL, and cable networks that are more likely to be abused. The Composite Block List (XBL) may indicate fraud. Optimally, a registrar would check against this information at DNS set-up or modification time; however, periodic scanning should return good results.

3. *Share fraudulent domain registration information with law-enforcement*

Whenever action is taken to shut down a fraudulent domain registration, appropriate law enforcement authorities should be notified and all available information about the deceptive registration should be shared with them. Such information includes re-gistrant IP addresses used during registration or modification of the domain record, credit card information, name, address, e-mail, company name, and all other available data. There is more detail about what to store in the "Other Recommendations" section below.

4. *Protect your customers from being phished*

ICANN's Security and Stability Advisory Committee has written a document on how registrar customers can be targeted for phishing. This document gives an overview of the problem, how the problem can impact the security of the Internet, and ways to protect against its occurrence.

See this document http://www.icann.org/committees/security/sac028.pdf for more information.

5. *Prohibit/minimize use of fast-flux domains*

Fast-Flux domains, domains for which either the base IP address (A record) or name server address (NS record), or both (known as double-flux), are changed numerous times during the day, are now increasingly being used by criminal phishing, spam, and botnet gangs to ensure the resiliency of their sites and make it increasingly difficult for takedown authorities to remove or restrict access to illegitimate sites.

This problem can be addressed partially by both registries and registrars by preventing or making it much more difficult to frequently change the NS record of a domain registration. There is very little, if any, legitimate need to change the NS record for a domain more than few times a month and any such action should trigger immediate red flags and possible investigation of the domain for illegal activity.

See this document http://spamtrackers.eu/wiki/index.php?title=Fast-flux for a full explanation of fast-flux domains.

Other Recommendations

Protect your customers from phishing of their registrar information

ICANN's Security and Stability Advisory committee has released an advisory on how phishers can impersonate registrars in an attempt to take control of a registrant's account at the registrar. The advisory gives an overview of the techniques used by the phishers, the implications of this behavior, and best practices to protect registrants.

The advisory can be found here: http://icann.org/committees/security/sac028.pdf

1) Investigate domain registrations/name servers related to known criminal activity

Whenever action is taken to shut down a fraudulent domain registration, action should be taken to identify and shut down other fraudulent registrations that had been submitted by the same registrant (same name, IP, email, address, credit card information, etc.). In addition, name servers that are found to be associated only with fraudulent registrations should be added to a local blacklist and any existing or new registration that uses such fraudulent NS record should be terminated.

2) DNS Registration

a) *Practices/Services for common abuses*

Use a "Registrar Lock" on registrations that are deemed to be suspicious enough to warrant further investigation. Such measures would make it impracticable to use stolen credit cards to register domains and would also introduce time into the criminal cycle for those that would use the DNS for malicious purposes.

i) Scan for providers of so-called bulletproof domain name hosting and de-accredit anyone found to be offering those sorts of services (particularly if the service involves knowingly accepting bogus WHOIS data).

b) *Data collection*

Collect and store as many of the technical details of the registration as possible. This information has multiple uses, including registration scoring, validation, takedown resolution, investigation, etc. This data includes:

(1) Source IP address

(2) HTTP Request Headers
 (a) From
 (b) Accept

(c) Accept-Encoding
(d) Accept-Language
(e) User-Agent
(f) Referrer
(g) Authorization
(h) Charge-To
(i) If-Modified-Since
(j) Pragma

(3) The time it takes to fill out each step of the registration process (to identify automated form-filling scripts)

(4) Collect and store the following data from your registrants:
(a) First Name:
(b) Last Name:
(c) E-mail Address:
(d) Alternate E-mail address
(e) Company Name:
(f) Position:
(g) Address 1:
(h) Address 2:
(i) City:
(j) Country:
(k) State:
(l) Enter State:
(m) Zip:
(n) Phone Number:
(o) Additional Phone:
(p) Fax:
(q) Alternative Contact First Name:
(r) Alternative Contact Last Name:
(s) Alternative Contact E-mail:
(t) Alternative Contact Phone:

Use this information for the account, *not* for the WHOIS information; have a separate form for the WHOIS information that is pre-populated with this information. Explain that this WHOIS information will be used by external parties to contact that person in event of malicious activity or other issues with the domain.

(5) Collect data specifically for public WHOIS records, and don't automatically allow initial registration information to become public WHOIS information. Provide education regarding WHOIS information and how to protect registrants from malicious use of data by providing users with a "best practice" example that facilitates contact, yet reduces privacy concerns such as social engineering.

(6) Collect data on all additional add-on services purchased during the registration process.

c) *Data validation/scoring*

This section describes several data variables that can be used to determine whether or not a particular registration is suspicious. The goal of enumerating these variables is to give the registrar several indicators for what may constitute a suspicious domain. The registrar will need to determine its own internal policy about which indicators trigger the need for further verification of the registrant or denial of the registration request.

i) Data Validation

(1) Domain Name

(a) Screen/score all registrations for "unusual" domain name registration practices, such as registering hundreds of domains at a time, registering domains which are unusually long or complex, include an obvious series of numbers tied to a random word (baddomain01, baddomain02, baddomain03).

(b) Screen/score all registrations for patterns known to be associated with phishing (bank, secure, PayPal, eBay, etc.)

Reviewing all domain names proposed for registration against known sites that are often the subject of phishing type attacks will ensure registrars do not inadvertently aid in the provisioning of illegitimate content in online scams.

(2) Technical Data

(a) Examine IP addresses used to register domain names.
(i) Cross validate the IP address against blacklists such as the Spamhaus XBL, as well as other proxy lists.

1. Cross validate the geo-location of the IP address against the provided address and credit card billing address. In the case that the geo-location does not match, this can be used as one of many indicators that the registration is suspicious.

2. Rank IP blocks and validate against them, such as those from large ISP pools versus companies, as done by Gmail, Earthlink, and other ISPs using the Spamhaus Policy Block List (SPBL)

(b) E-mail Address
(i) When possible, verify that registration e-mail addresses are valid.

1. Confirmation of email addresses information will ensure that you and any takedown authority will be able to contact the registrant to ensure illegitimate content is removed at the earliest opportunity

2. This will also assist registrars that may inadvertently host illegitimate content in avoiding potential liability associated with any financial loss suffered as a result of the illegitimate content, e.g., financial institutions seeking damages from registrars due to extended delays in removing illegitimate content

(ii) Rank e-mails by corresponding domain, with free e-mail addresses typically ranked lower. Keep track of frequently abused providers by domain and rank accordingly. Use these rankings as a potential indicator of suspicious activity.

(c) Name Servers
Name servers should be specified as both fully qualified domain names (FQDN) *and* as IP addresses; i.e., do not allow FQDN's alone.

(i) This can reduce the use of fast flux name servers.

(ii) Tying FQDN to specific IPs will ensure illegitimate domains cannot be associated with botnets and thus allow the timely removal of illegitimate content.

(d) Time
Record the time span it takes to fill out forms within the new domain registration process. Very short sessions to fill out forms can be indicative of an automated registration process and thus suspicious registrations.

(3) Billing Data

(a) Validate and store credit card information based on best practices within the payment card industry (PCI standards).

(4) Contact Data

(a) Validate that data is being provided by a human. Use some anti-automatic form submission technology (such as dynamic imaging) to ensure registrations are done by humans, and share this technology with your resellers.

(b) Automate validation of contact addresses, ensuring that they are valid and deliverable, via GPS/Map data. The benefits of this practice include:
(i) Reduction of bogus WHOIS data

(ii) Allows Law Enforcement Agencies (LEAs) to ensure enforcement activities are targeted against those responsible for illegitimate web content. This ensures that LEA's efforts are not wasted when dealing with fictitious information.

(iii) The retention of IP, date/time, and payment information relating to registrant assists LEAs in ensuring they are dealing with the correct individuals when actions are undertaken to identify and/or prosecute persons responsible for illegitimate web content.

(c) Validate current address WHOIS data and correlate with in-house fraudulent data for domain contact information and registrant's IP address.

(d) Phone Numbers

(i) Confirm that point of contact phone numbers are valid using an automated system. This will help to reduce bogus WHOIS data.

(ii) Cross validate the phone number area code with the provided address and credit card billing address and score appropriately.

3) Data Scoring

Based on the data collected in the beginning of this section, the registrar can identify registrations that are likely fraudulent in nature. Development of the scoring model would include the following steps:

a) Track registration details associated with abused domain names and develop a scoring model that assigns penalty points for data that often occurs with domain registrations that are later deemed to be fraudulent.

b) Implement Predictive Analysis, Bayesian Classification, Decision Trees, and/or other technology to leverage data collected during the registration process when combined with actual fraud data.

i) Data mining allows registrars to understand complex business issues beyond fraud, such as how to effectively market to each individual customer, targeted services, etc., and can be funded as business development.

ii) Use scoring to determine the next step, overall time, or level of validation required in the registration process. For example, registrations that score poorly could require additional validation or scrutiny before becoming active. Implementing this type of protection allows the registrar protection from fraudulent registrations without adversely impacting legitimate customers.

4) Acceptable Use Policy/Service Agreement

a) Amend the terms and conditions associated with domains that change name servers more than twice a week (except by agreement). If possible, this should result in scrutiny and even the suspension of the domain until a suitable explanation is provided by the registrant.

b) Address the issue of domains pointing to hacked sites hosting malicious code and what the expected response times by registrants should be to the remediation process before the service agreement has been violated and the domain is redirected or suspended at your discretion.

c) Include policy on how domains that are hosting phishing sites and/or malware are handled.

5) Domain Life-Cycle Best Practices

a) Track the IP address, date, time, and action of all account changes such as updating DNS or WHOIS information

b) Limit the ability of registrants to repeatedly change their name servers via a programmatic interface to reduce or eliminate automated name server hopping.

c) Require additional safeguards in the case of registration service providers acting as a provider of registration services for themselves.

d) Make it a priority to review wdprs.internic.net reports and, when you receive such a report, also look for similar domains sharing common name servers, common WHOIS details, etc.

e) Summarize name servers which are used for a very large number of domains, dotted quads which have a large number of name servers associated, and name servers which appear to be listed on Spamhaus Zen. Use this list to look for fraudulently registered domains.

6) Takedown Best Practices

a) Registrars Role

i) Registrars should have a dedicated abuse department that has published contact information, including both phone and e-mail, on both the registrar's website and WHOIS records.

ii) Drive towards response times in the 1-3 hours range.

iii) Establish expedited channels and contact information for law enforcement and community partners.

iv) Insure that glue records using an invalid domain are removed when that domain is found to be invalid, even if those glue records are in use in conjunction with other domains.

v) Information Sharing

It is understood that information sharing programs can be difficult to implement due to legal concerns and other policy development issues. We are hoping that registrars can use the APWG's data sharing program and other similar programs, like the phishing data shared with Internet Explorer and Microsoft by hundreds of organizations, as models on how to create a sustainable data sharing policy.

(1) Adopt a policy of publicly publishing cloaked WHOIS data if/when a private registration is found to be violating terms of service (either due to bogus data, fraudulent use, spamming, etc.). This discourages use of private WHOIS as a way of avoiding investigation.

(2) Work within the registrar community to provide a clearing house for all fraudulent DNS registrations and associated information. Benefits of publishing this data are:

(a) It can be used as a data source to validate future registrations.

(b) It is a great source of information for law enforcement.

(c) It is also a great source of data for researchers and other people addressing the phishing and malware problems.

(3) Work within the registrar and law enforcement community to establish a data exchange format for all fraudulent DNS registrations and associated information. Law enforcement needs to extend the ability to do automatic fraud reporting based on trusted relationships, as well as provide information back to the registrar community.

Example: Law Enforcement needs to have a digital intake for certain trusted partners based on established standards for registrars and organizations to easily pass information and shorten the investigation life-cycle

(4) Share information with industry partners. Some data to consider sharing include:
(a) IPs associated with fraudulent domain registrations with respectable blacklists.

(b) Full fraud reports with industry and law enforcement, such as those at the Internet Crime Complaint Center

(c) Best practices regarding accepting and managing domain registrations.

References:

Can registrars suspend domains for spam and abuse?

http://www.spamhaus.org/faq/answers.lasso?section=Generic%20Questions#127

Role Accounts & Feedback Loops

http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#119

SORBS Dynamic User and Host List

http://www.au.sorbs.net/faq/dul.shtml

The Internet Crime Complaint Center

http://www.ic3.gov/

Identity Scores

http://en.wikipedia.org/wiki/Identity_score