Message, Mobile and Malware Anti-Abuse Working Group

M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers

March 2015

Executive Summary

System abuse drains time and revenue for hosting and cloud providers. Providers must maintain constant vigilance to make sure systems are not compromised. Just as crucially, they must ensure that their customers are vigilant. This document categorizes types of abuse, suggests appropriate responses and reviews practices for dealing with customers and complaints. It provides current best common practices in use with the hosting, DNS and domain registration provider communities. The intended audience is anti-abuse technical operations staff and their management.

Table of Contents

1. Introduction

The Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) and the Internet Infrastructure Coalition (i2C) offer these best practices for hosting, DNS and domain registration providers in support of the M^3AAWG mission to reduce all types of messaging and other forms of network abuse. The goal of this paper is to educate providers about methods they can adopt in order to more efficiently use their resources to fight abuse.

Hosting providers must adhere to these requirements to avoid industry and regulatory actions and to avoid the risk of incurring additional regulations. Providers should also consider joining relevant coalitions and adhering to relevant self-regulatory initiatives, such as those prescribed by other industry trade associations.

Hosting providers must be in compliance with the requirements of all upstream network providers and applicable regional governments' regulations. (See Appendix 2.)

This document outlines industry best common practices. It is understood that not all hosting providers or reporting agencies will implement all of these practices due to the complexity of network infrastructures, public policy considerations, and the scalability of network platforms.

2. Types of Hosting

Hosts offer varying levels of support, equipment provision and help with abuse issues related to their customers.

Host Type	Hardware	Operating System	Software	Abuse Issues
Dedicated Hosting	Provider	Customer	Customer	Customer*
Managed Hosting	Provider	Provider	Provider	Provider or Customer
Reseller Hosting	Provider or Customer	Customer or Customer's client	Customer or Customer's client	Customer or Customer's client*
Shared Hosting	Provider	Provider	Provider	Provider and Customer
Unmanaged Hosting	Provider and Customer*	Customer	Customer	Customer*
Virtual Private Server	Provider	Provider	Customer	Customer

**Where the customer is the owner of the hardware, as it is in a hosting environment, responsibility for hardware maintenance will be shared between the hosting provider and the customer.*

The various types of hosting organizations are defined as:

- **Cloud hosting**
  This is shared hosting with redundancy. (See below.)

- **Dedicated Hosting**
  The hosting provider owns and provides the server, physical space in a facility, connectivity, electricity and physical security. The customer controls and maintains the server, OS (operating system), software, administrative and end-user access. The hosting company provides a dedicated box that only has one customer assigned to it. Usually the customer has admin-level access to the box.

- **Hosting Provider**
  Any entity which offers end users the ability to create their Web presence on hardware they do not actually own.

- **Managed Hosting**
  The hosting provider owns and provides the server, the OS and the software and/or technical support. The customer controls administrative and end-user access.

- **Reseller Hosting**
  An arrangement under which the hosting company provides space to a customer who acts as an independent hosting company. The business arrangement can be either unmanaged or dedicated hosting, as detailed above. Customers can then position themselves as hosting providers in their own right and sell services to customers. Resellers can resell to other resellers, thus adding degrees of separation that create potential latency in the abuse-handling process.

- **Shared Hosting**
  The hosting provider owns and provides server, provides physical space in facility, connectivity, electricity, physical security, and provides OS and software. The provider controls administrative access. The customer controls end-user access. Abuse issues in a shared system require the provider to point the customer in the right direction to a resolution.

- **Unmanaged Hosting**
  The hosting provider provides physical space in a facility, connectivity, electricity and physical security. The customer owns, controls and maintains the server, OS, software, administrative and end-user access.

- **Virtual Private Server (VPS)**
  An arrangement under which customers are given a virtual server environment in which they usually have admin-level control of that environment. In some cases they may also have guaranteed processes or hardware allocations. The hosting provider owns and provides the virtual server environment and the OS. The customer controls administrative and end-user access and software.

3. Types of Abuse

Below is a list of the types of abuse most commonly seen at hosting and cloud service providers. The list does not purport to be complete and will invariably change over time.

- **Spam (outbound)**
  Spam is any email sent to end users that the receiver has specified they did not want to receive. Providers should ensure that customers are following the M³AAWG Sender Best Current Practices.[1] Hosting providers will also want to subscribe to as many relevant Feedback Loop reports as it is possible to process. (See more about Feedback Loops in Section 5 below.)

- **Spamvertising (hosted redirect and payloads)**
  Spamvertising occurs when a hosting provider's end user engages a third party to advertise its Web presence. Most spam complaints are caused by end users sending emails to potential customers that tout some overhyped product or service. Spamvertising is done via a third party. Providers who receive one of these complaints are most likely in the loop either as the sender of the email or the host of the site being advertised.

- **Phishing outbound (hosting and inbound for client credentials)**
  Phishing happens primarily when an end-user account has been compromised, almost always as a result of outdated scripts run by end users. A phishing site is a fraudulent site purporting to be a legitimate company, like Bank of America or PayPal, that directs the individual to enter confidential information. The phishers then have everything they need to rob the individual who has just been scammed.

- **Hacked or defaced pages (hosted client-side)**
  While phishing complaints will often fall into this category, not all hacked accounts will be used for phishing. Some may simply be defaced and the end users' data corrupted or destroyed. Frequently hackers will also inject malicious code or upload bots that are set to cause additional problems. Third parties and law enforcement agencies analyze these events and provide information about how to repair hacked sites. Most accounts are compromised due to end users' out-of-date CMS (Content Management System) installations such as Joomla or WordPress.

- **Child sexual abuse material (hosted client-side)**
  For appropriate handling of these issues, see the M³AAWG Disposition of Child Sexual Abuse Materials Best Common Practices
  (https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Disposition_CAM-2015-02.pdf).

- **Copyright and trademark/intellectual property issues (hosted client-side)**
  For online U.S. copyright law, see
  http://www.copyright.gov/reports/studies/dmca/dmca_executive.html.
  Other copyright regimes apply in other jurisdictions.

- **Distributed denial of service and other outbound hostile traffic (hosted amplification, redirect, botnet C&C hosts)**

- **Malicious signups (whack-a-mole/multi-account, multi-platform)**

[1] https://www.m3aawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf

4. Prevention

Vet customers before they cause problems.

Hosting providers are at the mercy of their clients' worst practices. Providers must have some type of vetting process to proactively identify malicious clients before they undertake abusive activities. A sound vetting process prior to provisioning will help the provider determine the difference between the truly bad actors and the customer who simply needs some guidance on proper online conduct. Vetting of clients is integral to maintaining a good reputation, decreasing costs and decreasing online abuse.[2]

Require customers to keep software updated.

Failure to maintain up-to-date software and hardware or firmware in the environment is one of the primary causes of abuse in the hosting space. Customer agreements should specify that customers will make a best effort to keep their systems up to date. This includes:

- OS/installs
- Plugins
- Content Management Systems (CMS)
- Themes
- Hardware/Firmware

Agreements should specify that out-of-date software may violate the prevailing contract with customers, as it can cause risks to the security both of their own environment and that of others. Where possible, customers should have automatic software updates enabled for their environment.

Prevent abusers from becoming customers.

Stopping parties intent upon abusive activities before they even get into a host's system must be given high priority when developing a prevention plan. The practices below will aid in preventing fraudulent accounts from gaining entrance to hosting systems.

- Institute preauthorization of new accounts.
- Personally contact accounts that are deemed suspicious.
- Keep records of previously terminated fraud accounts.
- Put limits on new accounts that require credible customer need to be raised.
- If possible, institute a fraud scoring system and automatically reject prospective accounts that fall below the specified threshold.
- Provide sales teams with specific questions and specific red flag statements made by prospective accounts to help identify potential fraud.

---

[2] The M³AAWG Sender Committee "Vetting Best Common Practices" may be of some use in this regard. https://www.m3aawg.org/sites/maawg/files/news/MAAWG_Vetting_BCP_2011-11.pdf

Train customer-facing staff in security awareness.

Customer-facing teams such as support, sales and marketing do not face the majority of daily challenges that are the norm for the abuse or security teams. Training provides these teams with knowledge of when to tell a customer or prospect that their practices do not abide by the terms and Acceptable Use Policy of the system they are on or where they are trying to provision an environment. Making efforts to target clients who will be a good fit for the hosting company is another way to preserve the safety of the hosting environment. Overall, a training program for customer-facing teams can reduce the number of problematic customers and provide them with advice about what to tell customers to fix when they encounter an issue.[3]

Prevent abuse at the network edge.

1. Consider hardware-based intrusion detection systems (IDS).

At the highest levels, M³AAWG recommends exploring Intrusion Detection Protection measures on networks. These systems help prepare for and deal with attacks.

2. Use software-based security scans and firewalls.

Automated and configurable web application security and penetration testing tools can be used to mimic real-world hacking techniques and attack. This enables companies to analyze complex Web applications and services for security vulnerabilities. At a minimum, a hardware- or software-based firewall is required for every network. It is also common to protect individual networks and computers with additional software-layer firewalls.[4]

3. Promote the use of Web application firewalls.

Hosting providers should encourage use of Web application firewalls (WAF) such as ModSecurity for their hosted clients. Managed providers should also consider managing a core set of WAF rules on their client servers.[5]

4. Use tiered-rights allocation for valued customers.

Access to the provider's network should be limited for new accounts. Seasoned, trusted accounts should be granted progressively wider access as their tenure and reputation within the system increases.
Reduced access restrictions can include, for example, limits to:

- API access
- server creation
- new domain creation
- bandwidth increases

Access privileges should not be granted to the majority of customers. They can be reserved for customers that are:

- proactive against any potential abuse
- have been hosted for an extended period of time (over 12 months)
- are responsive to your company's requests

[3] See M³AAWG Abuse Desk Common Practices document for more information: http://www.maawg.org/sites/maawg/files/news/MAAWG_Abuse_Desk_Common_Practices.pdf

[4] NIST Guidelines on Firewalls and Firewall Policy http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

[5] ModSecurity is an open source, cross-platform WAF. https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual

As with any privileges, these rights must be revoked in circumstances where customers previously in good standing commit multiple abuses or become non-responsive to company inquiries.

5. Contract with customers to protect security.

Hosting providers must require their clients to maintain a secure environment on their network and within the services they offer and the resources they consume from the provider. These requirements must be communicated to the client prior to provisioning and must form part of the contractual obligations. Clients must have a contractual obligation to notify the provider of breaches and issues.

Clients should be encouraged to back up their data regularly and to maintain those backups securely. Backups allow a client to return a server to a previous "known good state" in the case of an intrusion.

6. Maximize customer contact; protect customer identity.

Hosting providers should maintain updated and multiple avenues for client contact, such as email addresses, telephone numbers, chat accounts and customer portals that allow notification.

For the provider's protection and security, the vetting process should include the provision of a complete client identity. Furthermore, customer identity profiles should be used as part of the security of ongoing communications between the provider and the client.

The following methods are used by various providers. Clients may also suggest authentication methods of their own:

- Unique passphrases
- PINs
- Last four digits of credit card used for payment
- Individuals must be listed by account owner as approved points of contact

7. Strengthen customer passwords.

Hosting providers must require complex passwords[6] and should offer two-factor authentication. Passwords should be set to expire at regular, and relatively short, intervals.
Hosting providers should maintain a password/policy history for each client.

8. Use best practices on IPv6 networks.

IPv6 provides so many addresses that there is no need—and no reason—to share a single IP address among multiple customers. The best practice is to assign each customer a separate /64 of address space. Even on the smallest physically shared systems, each customer and each website should have a unique address. This makes it easier to track the source of abuse, makes it possible for recipients of abuse to block the offending customer without blocking everyone else on the same host, and may make it easier to suspend and renew service when required.

9. Security is paramount.

Hosting providers must maintain strong internal security practices and systems. All the recommended measures above are pointless if bad actors can guess the passwords the provider's staff uses. Hosting providers should follow PCI Compliance Standards.[7]

---

[6] Krebs on Security, Passwords Do's and Don'ts, http://krebsonsecurity.com/password-dos-and-donts/ ; US CERT security tip ST04-002, https://www.us-cert.gov/ncas/tips/ST04-002

[7] https://www.pcisecuritystandards.org/documents/Prioritized_Approach_for_PCI_DSS_v3_.pdf

5. Detection and Identification

M³AAWG recommends the following practices to prevent intrusion and detect abusive activity:

1. Use confidential client identifiers.

Hosting companies should create a unique identifier for each specific customer. This identifier must be apparent only to the hosting company and be unintelligible to outside parties. This maintains the privacy of the customer's identity yet gives the hosting company a simple, effective way to identify customers.

2. Establish role accounts for domains.[8]

RFC-specified role and common practice email accounts must be set up for every domain and client domain provisioned on a network.

	HOSTING PROVIDER	CLIENT WITH EMAIL
postmaster@	X	X
abuse@	X	X
hostmaster@	X	X
noc@	X	
legal@[9]/copyright	X	

3. Maintain accurate SWIP and IP WHOIS records.

Hosting companies should maintain clear and accurate entries with their Regional Internet Registry (RIR) for IP space allocation, including sub-allocations greater than a /27 to clients. These WHOIS listings should include functional role accounts for abuse reporting.

4. Set up internal telemetry that reports on the state of the network.

- Network self-scans
- Traffic analysis
- Outbound spam filter monitoring

5. Make community abuse reporting straightforward.

Hosting providers must provide facilities for members of the community at large to submit reports about abuse they perceive emanating from the network in question. Providers must then acknowledge the submission of these reports and take action as appropriate.

Hosting providers should maintain redundant communication channels to account for failure of any given channel.

- Email
- Telephone
- Instant message (chat)
- Ticketing systems (See Appendix 4)
- Website status reports
- Social media presence

---

[8] https://www.ietf.org/rfc/rfc2142.txt

[9] This is determined by a company-specific submission to their local copyright office.

Reporting channels should be monitored constantly. Issues should be dealt with according to the Complaint Priorities for System Abuse chart in Remediation, Section 6, below. Failure to address abuse reports can result in widespread propagation of an issue, incurring negative consequences for providers and their end-user clients.

6. Respond promptly to complaints.

Individual submissions should have an auto-acknowledgement (AUTO-ACK) message with enough specificity to be discrete from other submissions the complainant has made. They should include the original complaint, an original ticket number, and any other information that will assure the user that the complaint has been received and is being acted upon.

- A "quiet" submission address may also be maintained for bulk submissions and those individuals who prefer no such acknowledgement.
- APIs also may be maintained for bulk submissions.

See also the section on Remediation in Section 6 below.

7. Consider designating trusted reporters.

Complaint submitters may be determined to be of high quality or high priority. These sources may be both internal and external. Provision should be made for a priority lane-style service while maintaining specified priority levels.

For example, a contact at a widely-used DNSBL (Domain Name System Blacklist) may be designated an appropriate priority reporter, although a spam complaint from that source would obviously remain less significant than a DDoS issue happening simultaneously.

8. Set up Feedback Loops (FBLs) and automated reports.

Consuming FBL Data
Signing up for FBLs helps providers avoid DNSBL listings, limits reputation damage, and allows staff to proactively deal with abusive and abused (compromised) clients. For more information about available FBLs, see:

- Word to the Wise, Industry News and Analysis Blog, ISP Information, http://blog.wordtothewise.com/isp-information/

The authors also recommend reviewing the following two documents:

- IETF RFC 6449: Complaint Feedback Loop Operational Recommendations[10]
- M^{3}AAWG Feedback Reporting Recommendations[11]

Set up an FBL for providers with inbound messaging infrastructure.
Providers may wish to publish their own FBL, as some in the industry have done, as a way of reporting and thus reducing abusive traffic.

Automated reports
Automated reports should be made in accordance with RFC 5965[12] and RFC 6650.[13]

[10] https://tools.ietf.org/html/rfc6449
[11] https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Feedback_Reporting_Recommendation_BP-2014-02.pdf

6. Remediation

Remediation priorities provide hosting companies and customers with guidelines to resolve issues. Recommendations regarding the priority of complaints must also take into account the severity and seriousness of the abuse and the scope of a given issue. Additionally, the source of the report and the severity of the damage to the reputation of the hosting company and of the customer must be taken into account. A massive spam campaign may be of higher priority than a C&C presence for a dormant botnet. There must be a case-by-case assessment of issues that may alter the priority level for a given provider or a given customer.

Complaint Priorities for System Abuse	***Priority Level***
• Child exploitation[14] • Offensive or harmful content • Data theft from the corporation	***Critical*** **P0**
• Botnet C&C • DDoS • Data theft on network • Data theft from network	***High*** **P1**
• Malware drops • Phish data drops • Phish hosting • Dictionary/bruteforce attacks • Data theft as client	***Medium*** **P2**
• Spam • Control panel • SSH forwarding • Spamvertising on network • Spamvertising support network, hacking/cracking • Remote file injection	***Low*** **P3**
• Web defacement • Exploitable services • Port scanning • Comment spamming	***Very Low*** **P4**
• Copyrights and trademark issues.	*

**Copyright and trademark issues vary in priority as a function of the location of the issue and the hosting provider. For example, in North America, these tend to be P1 or P2 due to DMCA Safe Harbor requirements. In Europe, where no such legal requirement exists, these may be of lower priority.*

---

[12] https://tools.ietf.org/html/rfc5965

[13] http://tools.ietf.org/html/rfc6650

[14] M³AAWG Disposition of Child Sexual Abuse Materials Best Common Practices, https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Disposition_CAM-2015-02.pdf

Respond swiftly to high-profile/high-priority issues.

The majority of complaints received by any hosting company only require an acknowledgement of receipt. Some cases, however, such as high profile complaints, takedown requests and blacklist removal, require an additional response. The customer or reporting agency should be contacted initially to communicate that the issue is being addressed. They should be contacted again when the issue is resolved. Only if there are lingering or exceptional issues should multiple communications be necessary.

Communicate proactively when industry or company-wide events occur.

In the event of a serious compromise or vulnerability that could put multiple clients or a specific group of clients at risk, a communication plan should be developed to make them aware of the issue and provide general instructions on how to resolve the issue. These communications must be sent in a timely manner. Additionally, the support staff should be made aware of the issue and have proper instructions on resolving the matter with customers who need assistance.

Deal effectively with problem customers.

1. Confirm the validity of the complaint.

2. Notify the customer of a compromise. Include any vetted instructions to the customer that will assist in the resolution of the issue.

3. Provide the customer with the pertinent Terms and Conditions and/or any applicable government regulations that may have been breached and caused the notification of violation or suspension of service. By doing this, the agreement with the customer is intact. Notification of the customer protects the hosting company from potential customer or outside complainant issues that could result in litigation.

4. Grant time to the customer to remediate the issue or—if an agreement is in place—allow time for the provider to remediate the issue themselves.

5. Confirm that the complaint has been resolved.

6. Close the incident. If necessary, notify the reporting party that the issue has been resolved.

Suspend service to non-responsive customers.

If a customer has been compromised or is engaging in actions that compromise the hosting provider's network and does not take action to resolve the issue, the provider must have the ability to remove services or shut them down short of termination. This can take the form of a suspended webpage that requires the owner to contact the hosting provider or the ability to turn off key aspects of the hosting environment. For example, repeat spam offenders may have their ability to send email discontinued for some period of time.

Terminate non-responsive customers.

When a non-responsive customer continues to generate abuse on a provider's network, the relationship must be terminated to protect the provider and its customers.

Factors to take into account when deciding to terminate:

- Length of time with the hosting company
- Size of the account
- Type and number of infractions
- Time and responsiveness to resolve infractions
- Client that is abusive to customer-facing staff
- Service level of the account

After termination has been issued:

- Set timeframe for client to retrieve data
- Set clear expectation that they are no longer welcome to use the hosting company's services
- Notify support, sales and billing departments of the termination
- Verify at the end of the timeframe that the account has been removed

Fraudulent accounts are a special case.

Many of the measures detailed above DO NOT apply to accounts determined to be fraudulent. For example, fraudulent accounts should not be permitted to retrieve their data. Care must be taken to not alert miscreants to actions being taken to secure the network against their activities. [15]

Conclusion

These best common practices are provided to assist the hosting, DNS and domain registration provider communities with the necessary recommendations for maintaining ongoing vigilance to protect their systems from compromise. Implementation of these practices will benefit the entire online community by preventing abuse and can also help avoid costly and time-consuming issues for host providers.

Authors:

Neil A. Schwartzman, Executive Director, CAUCE
John R. Levine, Senior Technical Advisor, M³AAWG
Justin Lane, Terms of Service Manager, Bluehost
Matthew C. Stith, Postmaster/Anti-Abuse, Rackspace Hosting

[15] https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Compromised_User_ID_BP-2014-08.pdf

Appendix 1: Glossary of Standard Terms

Wherever possible, these terms are derived from RFC 5598.[16]

Abuse Report – A catch-all term signifying any malware, phishing or spam report.

Box – The physical hardware that is set up to run the various programs used by hosting providers and customers.

DMCA – The Digital Millennium Copyright Act of 1998 protects copyright holders from unauthorized electronic transmission. Under this act, U.S. Internet Service Providers receive notices from copyright holders who believe that the ISP's customers are infringing their copyright. See http://www.copyright.gov/reports/studies/dmca/dmca_executive.html

Email Service Provider – A company that offers services to send email at volume.

End User – A client of a customer using the services of a hosting provider.

ESP (see **Email Service Provider**)

FBL (see **Feedback Loop**)

Feedback Loop (**FBL**) – A system used by a mailbox provider to share with qualified, legitimate senders of messages copies of messages sent from an IP address belonging to that sender which the mailbox provider's end users have reported as spam. The system is provided so that senders can identify and address the problems that are causing the complaints.

Hard Bounce – A receiving MTA indicates that an email cannot be delivered to the recipient due to a permanent failure (email address no longer exists or has never existed; domain no longer exists or has never existed).

Mailbox Provider – A company that provides an email box to an end user. The company may or may not also provide end users with access to the Internet.

Messaging Abuse Complaint/Report – A messaging abuse complaint or report occurs when a recipient of a message complains about or reports a message as abuse. The most frequent vehicle for this is by clicking the "spam" button in a Web interface. It can also involve opening a ticket with a mailbox provider's support or abuse desk; sending an email complaint to a mailbox provider's support or abuse desk or to the sender of the message; or making a phone call to the mailbox provider's support or abuse desk or to the sender of the message.

Opt-in – Recipient's indication of the wish to receive messages from this sender.

Opt-out – Recipient's indication of the wish not to receive messages from this sender.

Receiving MTA – The mail transport agent that the mailbox provider is using to receive mail messages.

[16] https://tools.ietf.org/html/rfc5598

Regional Internet Registry (RIR**)** – One of five regional organizations responsible for assigning IP addresses: AfriNIC (Africa), LACNIC (Latin America), ARIN (North America and Antarctica), RIPE (Europe), and APNIC (Asia Pacific). All of these sites provide lookup tables to determine the source of an address based on the sender's IP address, if the IP address has been assigned within their geographic service area.

Sender – The source or origin of an email message. May refer to both the ESP who controls the MTA that is sending the message and the brand or company responsible for the content of the message.

Sending MTA – The mail transport agent that the sender is using to send mail messages.

Shared IP – An IP that has many different senders/brands/ESP customers all mailing from it, usually at the same time. Usually identified with the ESP that the IP belongs to, rather than one of the brands sending from that IP.

Appendix 2: Legal and Other Resources

A variety of laws apply to the email industry, and it is the responsibility of each company to consult its own legal counsel to insure it is in compliance with all regional laws. The resources below include several national and international repositories of email law.

- CAUCE-Cornell University Law School Legal Information Institute: Spam Law Inbox Project, http://www.inboxproject.org
- Europa, http://europa.eu/legislation_summaries/internal_market/single_market_services/l24120_en.htm A summary of European Union data protection legislation in the electronic communications sector
- Canada's Anti-spam Law (CASL), http://fightspam.gc.ca
- CAUCE List of Official Documents Related to Canada's Anti-Spam Law http://www.cauce.org/2014/06/official-documents-related-to-canadas-anti-spam-law-casl.html
- U.S. Federal Trade Commission, "FTC Issues Final Commission Report on Protecting Consumer Privacy," http://ftc.gov/opa/2012/03/privacyframework.shtm
- Internet Infrastructure Coalition (iC2), http://www.i2coalition.com
- Anti-Phishing Working Group (APWG), http://apwg.org
- Host Exploit, http://hostexploit.com

Appendix 3: A Note about Data Security

Professionals engaged in data storage and the management of subscriber email addresses or other personally identifiable information (PII) are strongly encouraged to maintain a comprehensive security program which leverages industry standard best practices to achieve security of their environment and applications. Detailed recommendations are beyond the scope of this document. Furthermore, most countries have legal requirements with which providers must comply.

As a starting point, the authors recommend searching for more information on the Open Web Application Security Project (OWASP - https://www.owasp.org) and the computer security training organization SANS (https://www.sans.org), which provide voluminous information relating to cybersecurity and data security risks and recommendations.

Additionally, some members recommend adherence to the ISO/IEC 27002:2013 controls (http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533), found in the Access Control, Communications and Operations Management, and Information Security Incident Management domains of that international standard as a suitable basis for a comprehensive security program.

M^{3}AAWG very strongly recommends that data security be a primary consideration when developing processes for collecting and storing data. As criminals rob banks "because that's where the money is," cybercriminals look to email service providers and other online stewards of consumer data as targets to obtain email address data for nefarious uses. Similarly, do not assume that because a hosting provider's service or software stores "only" email addresses, it is unlikely to be a target. The data is valuable both to its owner (i.e., the subscriber) and to bad actors. It is absolutely crucial to ensure that data is properly kept in trust and out of the hands of criminals.

Appendix 4: Ticketing Systems

Ticketing systems are essential to maintaining proper workflow and to keeping track of current issues. No matter how hosting provider operations are organized, a ticketing system is critical. In most cases this system will not be used only by the abuse team. Providers need a system that will allow them to differentiate between their various departments and also create subgroups within those departments. Systems should apply date and timestamps to the tickets as they come in. As the number of reports grows, providers will most likely need a larger number of people looking at them. Having reports conveniently accessible in a ticketing system means that teams do not have to look in multiple places for them.

Hosting provider systems must also have a reporting interface for non-customers. This can be a simple webpage giving them the ability to report issues such as spam or phishing directly to the provider's abuse group. The system then should automatically create a ticket.

Providers will also want the ability to pull in email reports as a ticket. Subscribing to a feedback list allows providers to get those reports in their ticketing systems. Systems should be set up so that these tickets are assigned to the correct area in the provider's system. Once a feedback loop area is set up, subfolders for AOL, Comcast, Google, Spamhaus and others can be created. Distinct areas allow reports to be prioritized more easily.

Systems must be searchable. It is common to receive multiple reports at one time or another for the same issue from different sources. The ability to gather all the reports at once will allow providers to keep their teams from being buried under large numbers of duplicate tickets and waste time going over duplicate reports.

Currently, the Malware Reporting Standards team is considering adding a "reporter reputation" into the mix that would allow known good actors, like Spamhaus, to receive priority while reports from unknown parties would be rated lower. If this is adopted, hosting providers will want to adjust their ticketing systems accordingly.