Good Practice for combating Unsolicited Bulk Email

Richard Clayton,
Demon Internet.
18th May 1999

Version 1.02

7th March 2000
Document: ripe-206
Updates:

Contents

Contents Top

Introduction

Unsolicited Bulk Email (UBE) is a widespread problem on the Internet. It is sometimes called "junk email" or "spam". Because of the volumes involved and the indiscriminate nature of its sending, there can be few email users who do not have first hand experience of receiving UBE, often in significant quantity.

The sending of UBE is considered to be unacceptable behaviour because:

- it interferes with the operation of the Internet.

  There have been instances of systems collapsing from the sheer bulk of email that has been sent. Senders have arranged for delivery failures to be reported to third parties, causing significant problems to their operations. Besides these gross failures, UBE, by its presence alone, degrades email systems for everyone, delaying and blocking legitimate traffic. These effects can be seen far beyond the Internet, across all the systems that carry email.

- it creates unwanted traffic for the recipients.

  In most cases, users must pay for their connection, so they are funding the reception of something that was not wanted in the first place.

- it creates support overheads for ISPs.

  ISPs must deal not only with the complaints from their own customers who have received unwanted email, but also with the reports submitted by others, demanding precipitate action, when their own customers have sent the UBE.

Furthermore:

- In its commercial form UBE usually promotes goods of dubious provenance, legality or taste.

- No reputable schemes for regulating UBE exist.

- The individuals and companies sending UBE have shown no willingness to seriously co-operate with the Internet industry to reduce the impact of their activities.

- The UBE is seldom sent to those who might appreciate it. It costs the sender next to nothing to send UBE. This removes any incentive to limit its distribution. There are real fears that UBE could grow without limit and clog up the Internet, and the mailboxes of every email user on the planet.

It is resource intensive and to a large extent ineffective for ISPs to try to block UBE once it has been sent, so this BCP does not describe the limited manner in which this may be attempted. In the fight against UBE the ISP’s most practical contribution is to minimise or eliminate the sending of UBE by its customers or from its systems. The purpose of this BCP is to describe the industry s current collective opinion of the Best Practice in achieving this.

Besides being in the general interest for ISPs to adopt Best Practice, many ISPs will wish to be publicly seen to be doing what they can to combat UBE. To that end, it is expected that ISPs will wish to state formally that they have adopted the recommendations of this BCP. To assist in this, the document has been written as a "standard", using the terms MUST, SHOULD, MAY and MUST NOT as defined in RFC 2119 (see Appendix D for a summary of this).

For an ISP to be effective in combating UBE, Best Practice is as follows.

1. The ISP MUST ensure that their email systems will not relay email for unauthorised third parties.
2. The ISP MUST ensure that all email generated within their network can be traced to its source; and MUST ensure that the immediate source of email which arrives from other networks can be determined.
3. The ISP MUST ensure that all email generated within their own networks can be attributed to a particular customer or system.
4. The ISP MUST operate appropriate arrangements for the handling of reports of abuse by their customers.
5. Where abuse is proved, the ISP MUST take effective action to prevent the customer from sending further UBE. The legal basis on which services are provided to customers MUST allow such action to be taken.
6. The ISP MUST disseminate information on the action taken in regard to customers who have sent UBE.
7. The ISP MUST educate their customers on the nature of UBE, and MUST ensure that their customers have been made aware that sending UBE will be treated as unacceptable behaviour.

These seven points are expanded below.

Along with the extended explanations, this BCP lists a number of conditions that ISPs MUST impose upon their customers. It will be necessary to ensure that the contract made between ISP and customer gives the ISP the legal right to make these impositions and to withdraw services when unacceptable behaviour occurs.

To ensure fair competition between ISPs, so that no marketing advantage can be gained by failing to spell out these obligations properly, the ISP MAY use the standard clauses set out in Appendix C and MUST use these clauses or others which are at least as effective. The ISP MAY place these clauses into a more general Acceptable Use Policy (AUP) that covers other abuse issues.

The provisions of this BCP document are to be applied to all customers. However, some customers will have customers of their own. The ISP will conform to Best Practice by ensuring that such customers adopt this BCP themselves, and thereby apply Best Practice procedures in turn to their own customers.

Appendix A provides a glossary of terms, but in particular, throughout this document the term "ISP" should be understood to apply not only to "top level" providers of Internet connectivity, but also to customers of such ISPs who are "recursively" applying the BCP to their own customers. Also, the term "customer" should be understood to apply not only where there is a formal contractual relationship, but also to other cases where someone may be a "user" of the ISP’s facilities.

Contents Top

1. # No email relaying

Discussion

Historically, email systems using the SMTP protocol have been prepared to accept email from anyone and then deliver it to, or towards, its true destination. This willingness to "relay" made Internet email extremely robust, since minor configuration errors on one machine could be overcome by another machine with more accurate knowledge of how to deliver the email. Furthermore, the spirit of co-operation that pervades the Internet has meant that machine owners tended not to log, let alone block, such relaying.

With the advent of the Domain Name System (DNS) and far better connectivity for all machines, this need for relaying passed away long ago. However, the functionality continues to be provided within email programs.

Unfortunately, in recent times, the unscrupulous have been abusing the "relay" function by sending a single piece of email with a long list of destinations. This can cause someone else s system to generate multiple copies of the email for delivery to many different addresses. By "amplifying" email in this way, the sender of UBE is exploiting the resources of others to do most of the work of generating the UBE. Furthermore, it is possible for the sender to use a poorly configured system to hide the true source of the email or at least to ensure that the less skilled misidentify its source.

As it is no longer required and because it is open to abuse, it is now considered quite improper for systems to be configured in such a way that they will relay email for unauthorised people.

There are several ongoing projects on the wider Internet to identify systems that are still prepared to relay email. Typically, such systems are added to blocking lists that affect the propagation of email. Even if one wished to run an "open relay" the time is approaching when few will be prepared to interwork with such a system.

It is common for ISPs to run "smarthosts", which provide SMTP email delivery for their customers, especially those on dialup connections or local networks. This avoids the necessity for these customer machines to have fully fledged delivery systems of their own. This "smarthosting" is just a form of relaying, but is of course a completely acceptable practice, provided that the smarthost is configured to refuse to relay any email sent to it by unauthorised machines.

Requirements

ISPs MUST configure their email systems to prevent unauthorised email relaying.

ISPs SHOULD accept email for their own customers, and they MAY make explicit private arrangements to relay email for specific other systems.

ISPs MUST prohibit their customers from running systems that will relay email for unauthorised people. If such a system is being run the ISP MUST take steps to remove it from the Internet until this behaviour is corrected.

The ISP SHOULD arrange to regularly check that its customers, particularly those on permanent connections, are not running open email relays. Where this is inappropriate for security reasons, or where the connection is intermittent, the ISP SHOULD ensure that the customers are told how to make this check for themselves. The ISP MAY provide tools, probably on the web, to allow customers to make their own checks.

Appendix B contains pointers to technical information about how to ensure that email relaying does not occur.

Appendix C contains specimen contractual clauses to allow these, and other, requirements to be implemented.

Contents Top

2. Traceability of email passing through the system

Discussion

Tracing the source of email requires that all systems comply with the email standards and add a "Received" header line as the email passes through them. This serves to identify the machine that is adding the header and the machine from which the email arrived. In principle, the oldest such line indicates the source of the email. In practice, this is sometimes forged, and to trace the true sender it is necessary to work through the Received lines in time order until a discontinuity is found.

The senders of email will sometimes try to obscure the true origin of email by forging the name of the source machine in the "HELO" protocol command. This type of forgery is made easy to detect by ensuring that the Received line contains not only the name, but also the IP address of the sending system, since the latter cannot be disguised.

Requirements

ISPs MUST ensure that a standards-compliant "Received" line is added to all email that passes through their systems.

ISPs MUST ensure that the identity of the machine passing them the email is correctly recorded. The HELO announcement MUST NOT be treated as being valid and an IP address SHOULD be recorded.

Contents Top

3. Identification of the sender of email

Discussion

Section 2 has the effect of ensuring that email can be traced back to an originating IP address.

With dialup access, it is common to use "dynamic IP", so that the same address will be reused for other customers. ISDN connections take only a few seconds, so in principle the same IP address can almost immediately be in use by another person entirely.

However, the combination of IP address and time of connection will uniquely identify where the email came from. So an accurate time must be recorded into the email header Received line. The combination of this time with other access logs, held by the originating ISP, will serve to identify the sender.

The above description has only skimmed the surface of a complex topic. The LINX Best Current Practice document on "Traceability" (see Appendix B) can be consulted for further information and advice.

Requirements

ISPs MUST ensure that they keep accurate time on their email systems.

Dynamic IP addresses can be reused in very short order. ISPs SHOULD be using time stamps based on NTP, or an equivalent protocol that regularly checks the time against standard values and which can provide sub-second accuracy.

ISPs MUST keep other logs for a reasonable period so that they can ensure that they are able to translate a given dynamic IP address, in use at a given time, to a particular customer who can be held accountable for any abuse.

Exception

An exception to sections (2) and (3) arises in the case of a system run to deliberately hide the source of email - often called an "anon server". "Anon servers" are used to preserve anonymity where, for example, someone seeks help from a group supporting victims of abuse or wishes to express political views in a country that may punish dissent.

ISPs or their customers MAY run anon servers where this is explicitly intended to be the function of the service being provided. They MUST NOT allow their standard service to provide anonymity by failing to comply with this BCP.

However an anon server SHOULD NOT be capable of 'amplification' of email by expanding address lists and SHOULD have limiting mechanisms to ensure that the volume of email passing through the server cannot be unusually high without explicit system owner knowledge.

Contents Top

4. Handle abuse reports

Discussion

ISPs are required to accept and process any reports of abuse by their customers.

If a customer posts UBE then complaints are likely to be made to the ISP. These complaints have, by convention, generally been sent to the "postmaster" mailbox. More recently it has become desirable to direct such email to a specialist "abuse" mailbox. This practice was first fully documented in RFC2142.

When a complaint is received, it is wise to promptly acknowledge it, perhaps merely with a standard message that describes the local policies and procedures.

It is desirable to run a "ticketing" system that allows incident reports to be tracked. This will assist in combining reports and in collating further correspondence that may arrive from the original complainant.

It is also desirable to reply to people who submit complaints to explain what action is eventually decided upon. Sometimes, especially when a large number of reports are being received, this is not very practical. The standard message described above can usefully explain that this may happen, and it may be possible to direct people to a web site where any action taken by the ISP will be recorded (see section 6 below).

Requirements

The ISP MUST accept reports to an address of the form abuse@domain where domain is the domain used by its customers, or in the case where the customer's domain is a subdomain of a generic domain, the abuse address must work in the generic domain.

i.e. where customers have addresses like:

> customer@isp.com

the abuse address to be supported is:

> abuse@isp.com

where customers have addresses like:

> email@customer.isp.com

the abuse address to be supported is:

> abuse@isp.com

If it wishes, the ISP MAY accept reports submitted to other abuse addresses as well (e.g. abuse@isp.net), but it MUST NOT require the report to be resubmitted to another address before acting upon it.

The ISP SHOULD document the existence of these addresses on the corporate web site, and

SHOULD indicate the type of information that is required to make an abuse report useful.

The ISP MUST acknowledge the receipt of abuse reports and SHOULD use a ticketing system to allow tracking of such reports.

Contents Top

5. Act upon reports of abuse

Discussion

There is no acceptable excuse for the sending of unsolicited bulk email.

Apart from people pleading ignorance of the unacceptable nature of UBE, which is covered in the Requirements section below, the most likely explanation will be a claim that the email was in fact solicited.

In determining whether to accept this explanation the ISP must look at how the email addresses were acquired. Data Protection legislation will normally require that information is processed "fairly and lawfully". In particular, the ISP should look for positive answers to all the following questions:

- Were people aware that their email address was being collected?
- Is the email being sent obviously connected to the collection of the address?
- Was there a way of "opting out" from receiving email?
- Is there a way for the recipient of the email to revoke their previous permission?

(UK Data Protection legislation implements Directive 97/66/EC; legislation in other EU countries will be similar. The UK Data Protection Registrar offers Guidelines explaining the Data Protection Principles, and the questions above follow these guidelines.)

The effect of these tests is that posting articles to Usenet or the mere visiting of a web site does NOT make the subsequent sending of bulk email "solicited". Nor does it make it likely that acquiring lists of email addresses from a third party will mean that a customer has acquired any ability to send solicited email to those addresses.

Clearly, where someone has explicitly signed up for a mailing list the email that arrives is solicited. However, in the real world some mailing lists are dormant for long periods and the people who join them can have poor memories. When email does arrive it may be reported to the mailing list owner s ISP as being unsolicited. Since the same software can be used to send genuine requested mailing list email and UBE, the ISP will have to apply the tests given above to distinguish the two cases.

Mailing list owners can demonstrate that they are behaving responsibly by keeping good records. Ideally they would be able to produce a copy of the "subscribe" email for the list and would have checked it out at the time by "mailback" confirmation techniques to ensure that a third party had not maliciously requested the subscription. It is of course vital that the recipient of the unwanted email can unsubscribe from the list. Modern mailing list software packages automate all these procedures.

As discussed at the start of this document, ISPs may have customers large enough to apply this BCP on their own account, and manage their own customers or users. In these cases the ISP may depend on their customer to deal with the sender of UBE, and need not apply the sanctions discussed below, such as disconnecting these large customers from the Internet. However, the ISP remains accountable to the wider community, which will expect the ISP to be reasonably assured that their customer will indeed take suitable action in the ISP’s stead.

Requirements

The ISP MUST act upon proven cases of sending UBE and MUST ensure that the contracts with their customers enable them to act effectively.

The ISP MUST ensure that the alleged abuser is NOT informed of the identity of those who are reporting the abuse, except with their explicit permission.

The ISP MAY immediately terminate the customer’s account.

However, since ignorance of what is acceptable will remain a popular explanation for abuse, and it may be hard to determine if this was actually the case, the ISP MAY operate a "two strike" policy and allow a customer to continue to operate their account after a "first offence".

If a "two strike" policy is applied, the ISP SHOULD, on the "first offence" take special steps to educate their customer as to what is acceptable behaviour and it MAY require the customer to sign a specific undertaking not to re-offend before allowing them to access the Internet again.

If a "second offence" occurs within six months the ISP MUST terminate the customers account and all services connected with it. The loss of the sender’s connection to the Internet from a particular email address is an important sanction in combating UBE.

Many people cannot be bothered to report abuse, because they believe reports will not be effective. So an ISP cannot expect to see a large number of corroborating reports. Therefore just two reports which give identical messages MUST be considered to be evidence of bulk sending.

If the ISP receives a single report of abuse it MAY conclude that there is insufficient evidence that the email was sent in bulk. It SHOULD, however, inform the customer of the reported incident and SHOULD take the opportunity to remind the customer of the unacceptability of bulk email sending and the sanctions available to combat it.

The ISP MUST consider the possibility of collusion and forgery, and that reports of abuse may have been faked. It MUST allow the customer the opportunity to establish their innocence, and MUST act reasonably "on the balance of probability" in establishing whether abuse did in fact take place.

The ISP may find that the customer claims that the email was in fact solicited. The ISP MUST NOT accept this claim unless the email address was obtained and processed "fairly and lawfully".

If the email was sent out through mailing list software the ISP MUST consider the likelihood that the email was solicited but this fact has been forgotten. However, the ISP SHOULD encourage mailing list owners to keep records of subscription requests and to validate their authenticity. The ISP MUST ensure that it is straightforward for people to remove themselves from mailing lists run by their customers.

Where the sender of UBE is not directly a customer of the ISP, then the ISP MAY delegate the responsibility to enforce this BCP to the customer, provided that the ISP takes reasonable steps to ensure that the customer will do so.

Contents Top

6. Disseminate information on action taken against customers

Discussion

There are a number of advantages to making public any action taken against customers who have sent UBE.

If the report is timely, it may serve to prevent further reports of abuse from other recipients of the UBE. This will reduce the ISP s workload.

An ISP which reports the action it takes will improve its standing in the community, since people look favourably upon ISPs which take a tough line on the senders of UBE. The ISP will also demonstrate to potential abusers that there is a real risk of being detected and sanctions being imposed.

However, when publishing information about the action that has been taken it is vital to be accurate and matter of fact, for otherwise there is a risk of an action for defamation.

It is also necessary to comply with Data Protection legislation. This may not apply to companies - so their full name and address can be published; but with individuals it would almost certainly be necessary to avoid exact identification unless contractual steps had been taken to allow this information to be released when abuse had occurred.

The sort of report which would cause no problems would be along the lines of "On <date> we terminated the account known as <hostname@isp.com> because of its use in sending Unsolicited Bulk Email. Further reports of abuse by this account are unnecessary."

In addition to any public reporting, an ISP will wish to take such steps as are possible to disseminate information about abuse within its own organisation. It is not good practice to allow terminated accounts to be reopened, or the same individual, detectable by name, address or perhaps credit card, to immediately open a new account to replace the previous one.

Requirements

ISPs MAY announce the action that they have taken in dealing with the sending of UBE.

If announcements are made, ISPs MUST avoid defamation or contravention of the Data Protection Act.

Even if individual reports are not given, ISPs SHOULD publish overview statistical information.

ISPs SHOULD ensure that individuals whose accounts have been terminated for sending UBE are not immediately able to open a new account, since there is clearly a risk of continuing abuse.

Contents Top

7. Education

Discussion

ISPs need to take steps to educate their customers in acceptable email behaviour. It is recognised that ISPs may have difficulty in doing this because their marketing departments wish to play up the advantages of the Internet and downplay negative issues.

Many reports of abuse that are received by ISPs do not contain vital information that will allow action to be taken. Customers forget, for example, to include full header information, which is needed to properly identify the sender. Customers can also let their feelings run away with them and heap abuse on the abuse handling personnel.

It is the responsibility of everyone to try and improve this situation so that fewer inadequate or objectionable reports are sent, and less time is wasted dealing with such reports and less frustration is experienced by all concerned.

Requirements

ISPs MUST ensure that documentation is available to customers that explains the nature of UBE and that sending it is considered to be unacceptable.

ISPs MUST help to educate customers in the information that it is necessary to include in abuse reports, and the way such reports should be written.

Contents Top

APPENDIX A: Glossary

AUP

Acceptable Use Policy
: An extension to the contract between ISP and customer that sets out what the customer may and (mainly) may not do whilst using the ISP s services.

BCP

Best Current Practice
: A description of the best practice presently known to the industry.

DNS

Domain Name System
: The distributed system that provides a translation service between names and IP addresses. It is described in RFC1035.

HELO

Hello
: A command within the SMTP email protocol, used to announce the name of a remote machine.

IP

Internet Protocol
: A basic protocol for exchanging packets between machines on the Internet. Other protocols are layered upon this to provide services for users. It is described in RFC791 and RFC1122.

ISP

Internet Service Provider
: ISP is used in this document as a generic term to describe companies and organisations that provide Internet access to others. It is also used to describe customers of ISPs who have adopted this BCP and are applying it to their own customers in the ISPs stead.

LINX

London Internet Exchange
: The LINX is a totally neutral, not for profit partnership between ISPs. It operates the major UK Internet exchange point. As well as its core activity of facilitating the efficient movement of Internet traffic it is involved in non-core activities of general interest to its members. One such activity on "content regulation" has, as part of its work, generated this document.
See: http://www.linx.net/

NTP

Network Time Protocol
: A protocol for obtaining an accurate measurement of the current time described in RFC1119 and RFC1305.

RFC

Request for Comments
: The RFCs are a series of notes, started in 1969, about the Internet (originally the ARPANET). The notes discuss many aspects of computing and computer communication focusing in networking

protocols, procedures, programs, and concepts, but also including meeting notes, opinion, and sometimes humour. The Internet standards are documented within the RFC documents.
See: http://www.rfc-editor.org/

SMTP

Simple Mail Transfer Protocol
: The email transfer protocol. It is documented in RFC821 and RFC1123.

UBE

Unsolicited Bulk Email
: UBE is email that has been sent in large amounts without any explicit requests for it being made. It is sometimes called "junk email" or "spam". At present it usually contains advertising material for commercial ventures of dubious propriety.

UCE

Unsolicited Commercial Email
: Some discussion of UBE distinguishes unsolicited email that is commercial in nature from non-commercial material. This document treats UBE as unacceptable per se, avoiding the need for value judgements on what may or may not be "commercial".

Contents Top

APPENDIX B: References and Resources

[Note: the publisher of this document is not responsible for the content of third party sites, does not necessarily endorse their contents and of course these links may not remain accurate forever]

There are many sites on the Internet that discuss unsolicited email in general. Some of the more interesting ones are:

- CIAC I-005c: Email spamming countermeasures

  http://ciac.llnl.gov/ciac/bulletins/i-005c.shtml

- "Fight Spam on the Internet"

  http://spam.abuse.net/

- Coalition against Unsolicited Commercial Email

  http://www.cauce.org/

- The European Coalition against Unsolicited Commercial Email http://www.euro.cauce.org/

There is almost certainly a discussion of the prevention of unauthorised email relaying on the home site of all mail handling software. For example:

- Sendmail

  http://www.sendmail.org/antispam.html

- Exim

  http://www.exim.org/howto/relay.html

- Qmail

  http://qmail-docs.surfdirect.com.au/docs/qmail-antirelay.html

- Exchange Server

  http://support.microsoft.com/support/kb/articles/q196/6/26.asp

For a comprehensive survey of pointers to information about email server software see the MAPS Transport Security Initiative

http://maps.vix.com/tsi/

There are also generic products that can be used with many systems to control relaying. For a commercial example see:

http://www.mailshield.com/

To test if your system allows unauthorised relaying use:

http://maps.vix.com/tsi/ar-test.html

LINX Best Current Practice "Traceability"

http://www.linx.net/noncore/bcp/traceability-bcp.html

All published RFCs are available from:

http://www.ietf.org/rfc/

Contents Top

APPENDIX C: Specimen clauses

The following are clauses that ISPs may use in their Terms and Conditions and elsewhere to support the enforcement of sanctions against senders of UBE, as required to conform to this BCP. In these model clauses the ISP is referred to as "We" and the customer as "You". ISPs may wish to replace these by other defined terms from their own paperwork.

General clause to allow action to be taken

> From time to time We publish Acceptable Use Policies ("AUPs") for the various services We provide. As a condition of Your use of a service, You are required to abide by the then current AUP for that service. If You do not do so, then We have the right at our sole discretion to suspend or terminate your account without notice or refund, to make an additional charge for the misuse, or to block access to the relevant part of the service.

General clause to permit scanning

> We may, at our discretion, run manual or automatic systems to determine Your compliance with our AUPs (e.g. scanning for "open mail relays"). You are deemed to have granted permission for this limited intrusion onto Your network or machine.

An AUP clause to disallow sending of bulk email

> You may not use your account to send Unsolicited Bulk Email. You must have explicit permission from all destination addresses before you send an email in any quantity.
>
> You may not assume that you have been granted permission by passive actions such as the posting of an article to Usenet or a visit made to Your web site.
>
> Where You have acquired explicit permission, either on a web site or through some other relationship You should keep a record of this permission and must cease sending email when requested to stop.

An AUP clause banning unauthorised mail relaying

> You must ensure that you do not further the sending of Unsolicited Bulk Email by others. This applies to both material that originates on Your system and also third party material that might pass through it.
>
> This includes but is not limited to a prohibition on running an "open mail relay", viz a machine which accepts mail from unauthorised or unknown senders and forwards it onward to a destination outside of Your machine or network. If Your machine does relay mail, on an authorised basis, then it must record its passing through your system by means of an appropriate "Received" line.
>
> As an exception to the ban on relaying and the necessity for a "Received" line, You may run an "anonymous" relay service provided that You monitor it in such a way as to detect unauthorised or excessive use.

Contents Top

APPENDIX D: Key words in requirements

This is a summary of the contents of RFC2119 "Key words for use in RFCs to Indicate Requirement Levels". Readers are encouraged to consult the full document for guidance.

MUST

This word means that the definition is an absolute requirement.

MUST NOT

This phrase means that the definition is an absolute prohibition.

SHOULD

This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT

This phrase means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY

This word means that an item is truly optional.

Contents Top

The original LINX version of this document has certain references specific to the UK, and is available at http://www.linx.net/noncore/bcp/ube-bcp.html

---