Good Practice in Minimising E-mail Abuse

Malcolm Hutty
Richard Clayton
Rodney Tillotson

Document ID: ripe-409
Date: June 2007
Obsoletes: ripe-206

Contents

Appendices

---

0. Introduction

Unsolicited **B**ulk **E**-mail (UBE) is a widespread problem on the Internet. It is sometimes called "junk e-mail" or "spam". Because of the volumes involved and the indiscriminate nature of its sending, there can be few e-mail 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 e-mail 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 e-mail systems for everyone, delaying and blocking legitimate traffic. These effects can be seen far beyond the Internet, across all the systems that carry e-mail.
- 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 e-mail, but also with the reports submitted by others, demanding precipitate action, when their own customers have sent the UB

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 e-mail 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 (or other use) 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 e-mail systems will not relay e-mail for unauthorised third parties.
2. The ISP MUST ensure that all e-mail generated within their network can be traced to its source; and MUST ensure that the immediate source of e-mail which arrives from other networks can be determined.
3. The ISP MUST ensure that all e-mail 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. They MUST also ensure that IP allocation entries in Regional Registries such as RIPE NCC contain appropriate abuse team e-mail addresses.
5. Where abuse is proved, the ISP MUST take effective action to prevent the customer from continuing that abuse. The legal basis on which services are provided to customers MUST allow such action to be taken.
6. The ISP MUST treat use of UBE to promote secondary services as an abuse of the provision of that secondary service.
7. The ISP MUST NOT permit customers to distribute tools, or lists of e-mail addresses, whose purpose is the sending of UBE.
8. The ISP SHOULD disseminate information on the action taken in regard to customers who have sent UBE.
9. 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. The ISP MUST inform their customers about any automated anti-spam mechanisms in operation, and MUST educate their customers about any potential harmful side-effects.

These nine 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.

1. No e-mail relaying

Discussion

Historically, e-mail systems using the SMTP protocol have been prepared to accept e-mail from anyone and then deliver it to, or towards, its true destination. This willingness to "relay" made Internet e-mail extremely robust, since minor configuration errors on one machine could be overcome by another machine with more accurate knowledge of how to deliver the e-mail. 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 e-mail programs.

Unfortunately, in recent times, the unscrupulous have been abusing the "relay" function by sending a single piece of e-mail with a long list of destinations. This can cause someone else's system to generate multiple copies of the e-mail for delivery to many different addresses. By "amplifying" e-mail 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 e-mail 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 e-mail for unauthorised people.

There are several ongoing projects on the wider Internet to identify systems that are still prepared to relay e-mail. Typically, such systems are added to blocking lists that affect the propagation of e-mail. 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 e-mail delivery for their customers, especially those on dial up 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 e-mail sent to it by unauthorised machines.

Requirements

- ISPs MUST configure their e-mail systems to prevent unauthorised e-mail relaying.
- ISPs SHOULD accept e-mail for their own customers, and they MAY make explicit private arrangements to relay e-mail for specific other systems.
- ISPs MUST prohibit their customers from running systems that will relay e-mail 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 e-mail 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 e-mail relaying does not occur.
Appendix C contains specimen contractual clauses to allow these, and other, requirements to be implemented.

2. Traceability of e-mail passing through the system

Discussion

Tracing the source of e-mail requires that all systems comply with the e-mail standards and add a "Received" header line as the e-mail passes through them. This serves to identify the machine that is adding the header and the machine from which the e-mail arrived. In principle, the oldest such line indicates the source of the e-mail. 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 e-mail will sometimes try to obscure the true origin of e-mail 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 e-mail that passes through their systems.
- ISPs MUST ensure that the identity of the machine passing them the e-mail is correctly recorded. The HELO announcement MUST NOT be treated as being valid and an IP address SHOULD be recorded.

3. Identification of the sender of e-mail

Discussion

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

With dial up 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 e-mail came from. So an accurate time must be recorded into the e-mail 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 e-mail 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, subject to local Data Protection legislation, so that they can ensure as far as possible 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 e-mail - 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 e-mail by expanding address lists and SHOULD have limiting mechanisms to ensure that the volume of e-mail passing through the server cannot be unusually high without explicit system owner knowledge.

4. Handle abuse reports

Discussion

ISPs are required to accept and process e-mailed reports about abuse by their own customers, whatever person or organisation may send the reports.

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

Some ISPs are developing specialised reporting systems that, for example, allow complaints to be entered into a form on a website. There are many advantages to such systems in that they ensure that reports are complete and they can boost productivity, allowing prompt and efficient handling of the reports. However, they have disadvantages in that they can only be used online and at present there are no standard conventions for their layout or their location. Therefore, although ISPs may wish to encourage their use and to develop other automated submission systems for third-party sites that collate reports from many people, it is not appropriate, at present, to see them as entirely replacing e-mail reports.

It is often "obvious" which ISP is responsible for particular IP addresses and hence which "abuse" mailbox to use. However, in some cases it may be necessary to consult the appropriate Regional Registry (such as RIPE NCC) in order to determine IP address ownership. It has therefore become standard practice to document within registry entries the explicit abuse@isp e-mail address to be used. It is important that complaints continue to be accepted at the "obvious" address even though the registry entry may indicate that another address is to be preferred. At present, registry entries can only record abuse mailbox details by means of comment fields, which inhibits automatic processing, but a formally specified system may be introduced in the future.

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 website where any action taken by the ISP will be recorded (see Section 6 below).

Requirements

- Where ISPs have many customers whose domain names are structured in a hierarchy linked to the ISP name (as in the examples below) then 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 e-mail@customer.isp.com
      the abuse address to be supported is abuse@isp.com
- Where ISPs have customers who use their own domain names, not immediately linkable to the ISP, then the ISP MUST still accept abuse reports sent to the ISP
    - For example, where customers of isp.com use their own domains, such as customer@example.com
      the abuse address to be supported is abuse@isp.com
- The ISP MUST document the appropriate "abuse@" address within the Regional Registry information for each IP address block delegated to them
- 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
- If it wishes, the ISP MAY accept reports submitted via other media such as web forms and MAY encourage this so as to improve the accuracy of reports and to improve productivity in dealing with reports, but an ISP MUST NOT refuse to accept reports by e-mail to the appropriate "abuse@" address
- The ISP SHOULD document the existence of their "abuse@" addresses on their corporate website, 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

5. Act upon reports of abuse

Discussion

There is no acceptable excuse for the sending of unsolicited bulk e-mail.

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 e-mail was in fact solicited.

In determining whether to accept this explanation the ISP must look at how the e-mail 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 e-mail address was being collected?
- Is the e-mail being sent obviously connected to the collection of the address?
- Was there a way of "opting out" from receiving e-mail?
- Is there a way for the recipient of the e-mail to revoke their previous permission?

All EU countries have legislation implementing EC Directive 2002/58/EC and its forerunners 95/46/EC and 97/66/EC; in most cases the questions above will reflect the primary concerns of the legislation.

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

Clearly, where someone has explicitly signed up for a mailing list the e-mail 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 e-mail 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 e-mail 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" e-mail 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 e-mail can unsubscribe from the list. Modern mailing list software packages automate all these procedures. There is a great deal more about this topic in the LINX Best Current Practice document on "Operating Mailing Lists" (see Appendix B).

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 strikes' policy and allow a customer to continue to operate their account after a "first offence".
- If a 'two strikes' 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 origination of UBE by the customer occurs within six months the ISP MUST terminate the customer's account and all services connected with it. The loss of the sender's connection to the Internet from a particular e-mail 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 e-mail 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 e-mail 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 e-mail was in fact solicited. The ISP MUST NOT accept this claim unless the e-mail address was obtained and processed "fairly and lawfully".
- If the e-mail was sent out through mailing list software the ISP MUST consider the likelihood that the e-mail 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 its own customer, provided that the ISP takes reasonable steps to ensure that the customer will do so.

6. Deny use of UBE for promotion

Discussion

Improvements in filtering technology have led many senders of UBE to move much of the content of their message from the e-mail to a website or other medium, and to direct their recipients towards that secondary source. Traffic coming to such websites provides the incentive for senders to keep sending UBE, and much UBE would not exist or would be more readily controlled but for the existence of these websites.

It is not acceptable to use UBE to promote websites or other secondary services, nor is it acceptable to use such services to promote or reap the benefits of sending UBE. Accordingly, use of UBE to promote a website or other service must be treated as an abuse not only of the e-mail service used to send the UBE, but also as infringing the conditions of use of the website or other service promoted by the UBE. The expectation should be that promoting websites via UBE will result in them being shut down.

The unacceptability of using UBE for promotion and the necessity of taking action against websites is not affected by there being more than one ISP involved. Each ISP is expected to take effective action against their particular customer.

In some cases a franchise system is in operation and a central, legitimately operated, website is promoted by UBE sent by a franchisee without the knowledge or permission of the central website owner. In such circumstance UBE will only be eliminated if the website owner takes firm action to disenfranchise the UBE sender and to ensure that they do not profit from their abuse. ISPs providing services to such websites must satisfy themselves that appropriate control mechanisms are in place before concluding it would be unfair to suspend the website and letting it remain operational.

In some cases websites are promoted by third parties who misrepresent the nature of the e-mail they will send, so that UBE is sent on behalf of the website owner. In such circumstances the website owner will look to their service contract with the third party for recompense for the significant damage that will have been done to their reputation. Provided that the ISP is satisfied that the problem will not recur it would clearly be unreasonable to suspend the website.

Requirements

- ISPs MUST treat use of UBE to promote a website or other service as an abuse of that other service, as well as an abuse of e-mail service provision.
- The ISP MUST act upon proven cases of using UBE to promote a website or other service hosted by the ISP whether or not the UBE originated on the ISP's network, and MUST ensure that the contracts with their customers enable them to act effectively.

- Where the promotion by UBE is authorised by or within the reasonable control of the customer who owns the website or other service, the ISP MUST treat this as abuse by the customer.
- Where UBE has been sent to promote a website or other service the ISP MAY immediately terminate that service. However, since ignorance of what is acceptable will remain a popular explanation for abuse and since it may be hard to determine if this was actually the case, the ISP MAY operate a 'two strikes' policy and allow a customer to continue to operate their system after a "first offence".

If a 'two strikes' policy is applied:

- The ISP SHOULD take special steps to educate their customer as to what is acceptable behaviour;
- it MAY require the customer to sign a specific undertaking not to re-offend or permit a re-offence before allowing them to access the Internet again;
- it SHOULD also take steps to ensure their customer explicitly informs the actual sender of the UBE that they do not authorise the sending of UBE, and instructs the sender to desist;
- it MAY require that the customer provide proof they have given such instruction before allowing them to access the Internet again.

- The ISP MUST ensure that where UBE is being sent to promote their customer's services by the customer's franchisees (or by entities in other similar relationships) the customer has adequate safeguards in their franchise arrangements and is acting promptly to prevent the sender of the UBE from profiting from their activity. The ISP MUST ensure that their contracts with their customers enable them to act effectively in such situations.
- The ISP may find that the customer claims that e-mail promoting their website was not sent by them or with their authority, or that it was sent maliciously in an attempt to persuade the ISP to take action against the customer.

- The ISP MUST consider the possibility that this might be true, and MUST act reasonably "on the balance of probability" in establishing whether abuse did in fact take place.
- The ISP MUST consider the possibility that the UBE was sent under the authority of the customer but without the customer's direct knowledge.

7. Prohibit the distribution of UBE tools and address lists by customers

Discussion

Some businesses promote the sending of UBE by making available programs for bulk e-mail sending or e-mail address harvesting, and may also sell their own lists of e-mail addresses. Since using these products is unacceptable, the community considers the

promotion of these products, usually on the web, as also being unacceptable. Although the major league senders of UBE use their own systems, the ability to obtain "kits" for sending UBE encourages others to attempt to use them and so there is a real benefit in suppressing these kits.

Of course many products have entirely legitimate uses in handling mailing lists run on an opt-in basis and there is no question of preventing these products being promoted. However, legitimate products do not provide methods for hiding the source of e-mail or for seeking out and using third party machines.

Similarly, there are a few legitimate sellers of address lists, although such lists are unusual because of the necessity of complying with Data Protection principles. It is regrettable to note that many alleged "opt-in" lists turn out to be incorrectly described.

Requirements

- ISPs MUST NOT permit customers to advertise or distribute tools or lists of e-mail addresses whose primary purpose is the sending of UBE, and must ensure that their contracts with their customers, for all services but especially websites, reflect this prohibition. Where customers are found to have breached this prohibition, ISPs MUST take effective action to ensure that their customer does not distribute this type of material in the future.
- When considering a customer advertising or distributing tools for the sending of UBE the ISP MUST consider whether the tool has legitimate uses, but MUST also consider if it has special features which would only be appropriately used when sending UBE. Consideration MUST also be given to the general nature of any advertising material to assess whether it acts effectively to discourage the use of "dual purpose" tools for sending UBE.
- When considering a customer advertising or distributing lists of e-mail addresses, the ISP MUST consider whether their collection and likely use would conform to Data Protection principles and legislation

8. 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 <username@isp.com> because of its use in sending Unsolicited Bulk e-mail. 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 Data Protection legislation
- 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

9. Education

Discussion

ISPs need to take steps to educate their customers in acceptable e-mail 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.

Many ISPs now operate e-mail filtering systems that attempt to distinguish UBE from legitimate e-mail and block or redirect the UBE. Systems may also attempt to detect mass-mailing e-mail "worms" or "viruses". These systems are not perfect and will let through some UBE and some worms and can, on occasion, also disrupt the flow of items of legitimate e-mail. It is important that ISP customers are aware of whether filtering is occurring, the type of system that is deployed, and hence the likely risk of e-mail disruption.

Because reports sent to "abuse@" mailboxes are highly likely to contain copies of UBE or viruses, it is most important that this e-mail does not pass through filtering systems that discard or reject this type of e-mail.

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. This MUST include mention that it is not acceptable to promote a service provided by the ISP using UBE sent via third-party internet connection.
- 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.
- ISPs MAY use automated anti-spam mechanisms to protect customers' e-mail accounts. If such mechanisms are used, the ISP MUST inform the customer and MUST explain what risks this may or may not cause to legitimate e-mail.
- ISPs MAY provide general advice to customers about any anti-spam mechanisms available that the customer may choose to employ on their own systems. If such advice is given, the ISP MUST explain what risks this may or may not cause to legitimate e-mail.
- ISPs MUST NOT deploy automated anti-spam or anti-virus mechanisms that block or reject reports sent to their abuse mailboxes.

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 e-mail 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 the document from which this RIPE Document is derived.

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.

RIPE - Réseaux IP Européens

RIPE is a collaborative forum open to all parties whose objective is to ensure the administrative and technical coordination necessary to enable the operation of the Internet within the RIPE NCC service region.

RIPE NCC

The RIPE NCC is the Regional Internet Registry for Internet number resources in Europe, the Middle East and parts of Asia. The organisation also facilitates RIPE Meetings and RIPE Working Groups.

SMTP -Simple Mail Transfer Protocol

The e-mail transfer protocol. It is currently documented in RFC2821.

UBE - Unsolicited Bulk E-mail

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

UCE - Unsolicited Commercial E-mail

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

Appendix B: References and Resources

Notes:

1. The RIPE NCC is not responsible for the content of third-party sites, and does not necessarily endorse their contents.
2. It is recognised that the links referred to here may not be available or current at any time in the future.

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

- CIAC I-005c: e-mail spamming countermeasures
- Fight Spam on the Internet
- Coalition against Unsolicited Commercial e-mail
- The European Coalition against Unsolicited Commercial e-mail

There is almost certainly a discussion of the prevention of unauthorised e-mail relaying on the home site of all mail-handling software.
Some examples include:

- Sendmail
- Exim
- Qmail
- Exchange Server

For a comprehensive survey of pointers to information about e-mail server software, see the MAPS Transport Security Initiative

There are also generic products that can be used with many systems to control relaying.
Mailshield is a commercial example.

You can test if your system allows unauthorised relaying.

LINX Best Current Practice Documents:

- Traceability
- Operating Mailing Lists

All published RFCs are available from:
http://www.ietf.org/rfc.html

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 and promoters of UBE, as required to conform to this BCP. In these model clauses the ISP is referred to as "we"/"us" and the customer as "you"/"your". 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 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, to block access to the relevant part of the service, or to apply a combination of these measures.

An AUP clause banning unauthorised mail relaying

You must ensure that you do not further the sending of Unsolicited Bulk E-mail (UBE) 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", such as 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.

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 unsolicited bulk e-mail (UBE)

You may not use your account to send unsolicited bulk e-mail. You must have explicit permission from all destination addresses before you send an e-mail to multiple recipients.

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 website.

Where you have acquired explicit permission, either on a website or through some other relationship, you should keep a record of this permission and must cease sending e-mail when requested to stop.

An AUP clause to prohibit promotion of websites using UBE

Websites must not be advertised by you, or by another person, using techniques that would be classified as "abuse" if they were carried out using a service provided by us. This includes, but is not limited to, the sending of unsolicited bulk e-mail. Such action will be treated under this AUP as if it had been done using your account.

An AUP clause to prohibit promotion of UBE tools and address lists

You must not offer or distribute any of the following products or services:

- software for sending UBE

- lists of e-mail addresses, except where all the address owners have given their explicit permission

---

Appendix D: Definition of Normative Terms

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

The original LINX version of this document has certain references specific to the UK, and is available at:
https://www.linx.net/good/bcp/ube-bcp-v2_0.html

Version 1.0 of this document was prepared by Richard Clayton and approved by LINX Members on 18 May 1999.

Version 2.0 was prepared by Malcolm Hutty and Richard Clayton and approved by LINX Members as an authoritative statement of Best Current Practice on 17 August 2004.