

8 Electronic Mail

8.1 Email Usage

Electronic mail or *email* is one of the most popular uses of the Internet. With access to Internet email, one can potentially correspond with any one of millions of people world-wide. Proprietary email systems can be gatewayed to Internet email, which expands the connectivity of email many fold.

In addition to one-to-one communication, email can support email address lists, so that a single individual or organization can send email to a list of addresses of individuals or organizations. Sometimes email lists have entries which point to other email lists, so that a single message can end up being delivered to thousands of people.

A variation on email lists are email-based discussion groups. Participants send email to a central mailing list server, and the messages are broadcast to the other participants. This allows subscribers, who may be in different timezones or different continents, to have useful discussions. With the appropriate software, people can subscribe or unsubscribe from the list without human intervention. These discussion list servers often provide other services such as archives of list traffic, discussion digests, and retrieval of associated files. USENET newsgroups are an elaboration of the email discussion group.

Electronic mail is increasingly critical to the normal conduct of business. Organizations need policies for email to help employees use electronic mail properly, to reduce the risk of intentional or inadvertent misuse, and to assure that official records transferred via electronic mail are properly handled. Similar to policies for appropriate use of the telephone, organizations need to define appropriate use of electronic mail.

Organizational policies are needed to establish general guidance in such areas as:

- The use of email to conduct official business
- The use of email for personal business
- Access control and confidential protection of messages
- The management and retention of email messages

8.2 Email Primer

The principle Internet email protocols (not including proprietary protocols which are tunneled or gatewayed to the Internet) are SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol) and IMAP (Internet Mail Access Protocol).

8.2.1 SMTP

SMTP is a host-to-host email protocol. An SMTP server accepts email messages from other systems and stores them for the addressees. Stored email can be read in various ways. Users with interactive accounts on the email server machine can read the email using local email applications. Users on other systems can download their email via POP or IMAP email clients.

UNIX hosts have been the most popular SMTP email platform. Some commonly used SMTP servers are Sendmail, Smail, MMDf, and PP. The most popular UNIX SMTP server is *Sendmail*, written by Brian Allman. Sendmail supports queuing of messages, rewriting of headers, aliases, email lists, etc. It is usually configured to run as a privileged process. This means that if it can be subverted somehow, an attacker can cause damage beyond deleting email.

8.2.2 POP

POP is the most popular email retrieval protocol. A POP server allows a POP client to download email that has been received via another email server. Clients can download all messages or just unread messages. It does not support deleting messages before downloaded based on message attributes like sender or subject. POP version 2 supports authenticating the user with a password, which is transmitted in the clear (not encrypted) to the server.

POP version 3 supports an additional authentication method called APOP, which hides the password. Some POP implementations support Kerberos for authentication.

8.2.3 IMAP

IMAP is a newer, and as yet, less popular email retrieval protocol.

As stated in the RFC:

IMAP4rev1 includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and clearing flags; [RFC-822] and [MIME-IMB] parsing; searching; and selective fetching of message attributes, texts, and portions thereof.

IMAP is more convenient for reading email while traveling than POP, since the messages can be left on the server, without having to keep the local list and server list of read email messages in sync.

8.2.4 MIME

MIME stands for Multipurpose Internet Mail Extensions. As stated in RFC 2045, it redefines the format of email messages to allow for:

- (1) textual message bodies in character sets other than US-ASCII,
- (2) an extensible set of different formats for non-textual message bodies,
- (3) multi-part message bodies, and
- (4) textual header information in character sets other than US-ASCII.

It can be used to support security features like digital signatures and encrypted messages. It also facilitates mailing virus-infected executables and malign active content.

Much like helper applications for World Wide Web browsers, mail readers can then be designed to automatically invoke helper applications to address certain MIME message types.

8.3 *Potential Email Problems*

8.3.1 Accidents

It is easy to have email accidents. An email message can be sent instantly with no hope of retrieval. A single keystroke or mouse-click can misroute the message. Email messages may be archived for years, so that an ill-considered remark can return to haunt the sender later. Email folders can grow until the email system crashes. Misconfigured discussion group software can send messages to the wrong groups. Errors in email lists can flood the subscribers with hundreds of error messages. Sometime errors messages will bounce back and forth between email servers, multiplying until they crash the servers.

When an organization's internal email system is connected to the Internet, the effect of accidents can be multiplied a thousandfold.

Some ways to prevent accidents are to:

- Train users what to do when things go wrong, as well as how to do it right.
- Configure email software so that the default behavior is the safest behavior.
- Use software that follows Internet email protocols and conventions religiously. Every time an online service gateways their proprietary email system to the Internet, there are howls of protest because of the flood of error messages that result from the online service's misbehaving email servers.

8.3.2 Personal Use

Since email is usually provided as an organizational tool, like a telephone, facsimile machine or photocopier, non-business use would normally be limited or forbidden (depending on the organization).

While it is tempting to simply state that all use of email must be for business purposes only, it is generally recognized that this type of policy is difficult to enforce. If a policy can not be consistently enforced, non-compliance is inevitable and the policy will have no force as a basis for punitive action. It is much more effective to define policy that places clear limits on personal use of email, in the same manner as personal use limits are defined for telephones and fax machines.

If you use your company telephone to check on your drycleaning, even if the drycleaner has CallerID™, it is unlikely to interpret the order as an official company request. But sending email from the organization's address can be likened to sending a letter on company letterhead, using the company's postage meter. If the sender use their company account to send email to an email discussion list, suddenly it appears as though the company endorses whatever opinions the sender put in their last message.

8.3.3 Marketing

In the past, when the Internet was a research network, purely commercial uses were forbidden. Also, since relatively few companies and people had Internet email, there was relatively little temptation to use it for commercial purposes. Gradually, as the Internet expanded and non-research uses were permitted, companies began maintaining email lists to communicate with their customers. In general, customers had to request to be put on the email lists. When the major online services gatewayed their email systems to the Internet, suddenly there was a convenient means to reach a large affluent audience. Unsolicited direct email marketing on the Internet was born.

People wrote software to automate the population and maintenance of email lists, and started companies to collect and sell lists of email addresses to marketers. Since the cost of sending email is nominal compared to paper mail, there is little incentive to be selective about the list of addresses sent to, the size of the message, or the frequency of the mailings. There is a bill in the U.S. Congress to put direct email marketing under rules similar to those for bulk mail, so that email marketers would be required to keep lists of addresses which do not wish to receive mailings.

8.4 *Email Threats*

The most common mail transfer protocols (SMTP, POP3, IMAP4) do not typically, include provisions for reliable authentication as part of the core protocol, allowing email messages to be easily forged. Nor do these protocols require the use of encryption which could ensure the privacy of email messages. Although extensions to these basic protocols do exist, the decision whether to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that is supported by both ends.

8.4.1 Impersonation

The sender address on Internet email cannot be trusted, since the sender can create a false return address, or the header could have been modified in transit, or the sender could have connected directly to the SMTP port on the target machine to enter the email.

8.4.2 Eavesdropping

Email headers and contents are transmitted in the clear. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message.

8.4.3 Mailbombing

Mailbombing is an email-based attack. The attacked system is flooded with email until it fails. A system will fail in different ways, depending on the type of server and how it is configured.

Some ISPs give temporary accounts to anyone who signs up for a trial subscription, and those accounts can be used to launch email attacks.

Here are typical failure modes:

- Email messages are accepted until the disk where email is stored fills up. Subsequent email is not accepted. If the email disk is also the main system disk, it may crash the system.
- The incoming queue is filled with messages to be forwarded until the queue limit is reached. Subsequent messages can't be queued.
- Some email systems set a maximum number of email messages or total size of messages that a user can receive at one time. Subsequent messages are refused or discarded.
- A particular user's server disk quota can be exceeded. This prevents subsequent mail from being received, and may keep them from getting other useful work done. Recovering may be difficult for the user, since they may need to use more disk space just to delete the email.
- The volume of mail may make it difficult for the system administrator to spot other warnings or error reports.
- Mailbombing an email list may cause subscribers to unsubscribe.

8.4.4 Junk and Harassing Mail

Since anyone in the world can send you email, it can be difficult to stop someone from sending it to you. People can get your address from company email directories, or subscriber lists, or Usenet postings. If you give your email address to any Web site, they can resell to your address to junk mailers. Some web browsers volunteer your email address when you visit a web site, so you may not realize who you've given it to. Most mail systems have some provision for filtering email, that is, searching the email header or body for particular words or patterns, and then filing or deleting the email. However, many users don't know how to use the filtering mechanism. Also, client-side filtering usually only takes place after the email has been received or downloaded, so large messages or large numbers of messages can't be discarded.

Anonymous remailers can be used as an attack and a safeguard. Someone sending junk or harassing email can hide their identity behind an anonymous remailer. Someone who wants to send email without exposing their home address to junkmailers or harassers can use addresses from anonymous remailers. If they start receiving unwanted email at an address, they can drop it and start a new one.

One common remedy used by some USENET users is to configure their news client software to put an unusable REPLY-TO address in their USENET postings, and then putting their real email

address in their signature lines or in the body of the message. That way, junk emailers who automatically compile email address lists from the REPLY-TO field of USENET postings get unusable addresses.

There are several bills in Congress to restrict junk email. One proposal would adopt stoplists like those used for junkmail. It would also require advertisements to put "advertisement" on the subject line of messages.

Another proposal would treat junk email like junk faxes. That is, any unsolicited advertisements would be illegal.

8.5 *Email Safeguards*

8.5.1 Impersonation

Impersonation can be prevented by using encryption algorithms to digitally sign the email message. One popular method uses public key encryption. A one-way digital hash of the message is encrypted using the private key of the sender. The receiver uses the public key of the sender to decrypt the hash, then checks the hash against the received message. This ensures that the message really was written by the sender, and that the message wasn't changed in transit. The U.S. Federal Government is required to use the Secure Hash Algorithm (SHA) and the Digital Signature Standard, where applicable. The most popular commercial software uses RSA's RC2, RC4, or RC5 algorithms.

8.5.2 Eavesdropping

Eavesdropping can be prevented by encrypting the contents of the message or the channel that it's transmitted over. If the channel is encrypted, system administrators at the sending or receiving end could still read or alter the messages. Various email encryption schemes have been proposed, but none has reached a critical mass. One relatively popular application is PGP (which stands for Pretty Good Privacy). In the past, PGP was somewhat controversial, because the encryption it uses is strong enough to be covered by the munitions control regulations. The commercial version of PGP includes plug-ins for several popular email clients, which makes it more convenient to sign and encrypt email within the client. Recent versions of PGP use a licensed version of the RSA public key encryption algorithm.

8.6 *Acceptable Use Of Electronic Mail*

All employees are to use electronic mail as they would any other type of official COMPANY communications tool. This implies that when email is sent, both the sender and the reader should assure that the communications complies with normal communications guidelines. No communications via email should be unethical, be perceived to be a conflict of interest, or contain confidential information.

8.7 *Protection of Electronic Mail Messages and Systems*

The protection provided for electronic mail messages, systems, and software should be consistent with the value of the information that will be transmitted over networks. In general, there should be centralized control of electronic mail services. Policies should be defined to specify the level of protection to be implemented.

8.8 Example Email Policy

Low

User

Use of electronic mail services for purposes constituting clear conflict of COMPANY interests or in violation of company information security policies is expressly prohibited, as is excessive personal use of email.

Use of COMPANY email to participate in chain letters or moonlighting is not acceptable.

The COMPANY provides electronic mail to employees for business purposes. Limited personal use is acceptable as long as it doesn't hurt the COMPANY.

The use of email in any way to facilitate the conduct of a private commercial purpose is forbidden.

Manager

All employees will have an email account.

Email address directories can be made available for public access.

If the COMPANY provides access to electronic mail to external users such as consultants, temporary employees, or partners, they must read and sign the email policy statement.

The contents of email messages will be considered confidential, except in the case of criminal investigations.

Technical

The POP server will be configured to except plaintext passwords from local machines.

Medium

User

Electronic mail is provided by the COMPANY for employees to conduct COMPANY business. The use of email for personal business is not allowed.

Confidential or company proprietary information will not be sent by email.

Only authorized email software may be used.

Anonymous remailer software cannot be installed.

Employees may not use anonymous remailers for any purpose.

Manager

Confidential or company proprietary information will not be sent by email.

Employees found to be deliberately misusing email will be disciplined appropriately.

Technical

The email system will provide a single externally accessible email address for employees. The address will not contain the name of internal systems or groups.

A local archive of approved MIME-compatible viewers will be maintained and made available for internal use.

High

User

Electronic mail is provided by the COMPANY for employees to conduct COMPANY business. No personal use is allowed.

All electronic messages created and stored on COMPANY computers or networks are property of the COMPANY and are not considered private.

The COMPANY retains the right to access employee electronic mail if it has reasonable grounds to do so. The contents of electronic mail will not be accessed or disclosed other than for security purposes or as required by law.

Users must not allow anyone else to send email using their accounts. This includes their supervisors, secretaries, assistants and any other subordinates.

The COMPANY reserves the right to review all employee email communications. Email messages may be retrieved by the COMPANY even though they have been deleted by the sender and the reader. Such messages may be used in disciplinary actions.

Manager

Directories of employee email addresses will not be made available for public access.

If confidential or proprietary information must be sent via email, it must be encrypted so that it is only readable by the intended recipient, using COMPANY-approved software and algorithms.

No visitors, contractors, or temporary employees may use COMPANY email.

(See section 5.3.1 General Encryption Policy.) Encryption shall be used for any information classified sensitive or confidential that will be transmitted over open networks such as the Internet.

Outbound messages will be spot-checked to ensure that this policy is being followed.

Technical

Incoming messages will be scanned by viruses and other malign content.

Email servers shall be configured to refuse email addressed to non-COMPANY systems.

Email server logs files will be scanned by unapproved versions of email client software, and the users will be reported.

Email clients will be configured so that every message is signed using the digital signature of the sender.

8.9 Retention of Electronic Mail Messages

The National Archives and Records Administration (NARA) has issued standards for management of Federal records created or received on electronic mail. These standards require Agencies to manage such records in accordance with the provisions of the chapter pertaining to adequacy of documentation, record keeping requirements, agency record management responsibilities, and records disposition (36 CFR parts 1220, 1222, and 1228).

8.9.1 Retention Policy for Federal Agencies

When an electronic mail message is determined to be part of the official records, the storage and retention of that message must comply with the following guidelines.

Some transmission data (names of sender and addressee(s) and date the message was sent) must be preserved for each electronic mail record in order for the context of the message to be understood. Agencies shall determine if any other transmission data is needed for purposes of context.

Agencies that use an electronic mail system that identifies users by codes or nicknames or identifies addressees only by the name of a distribution list shall instruct staff on how to retain names on directories or distributions lists to ensure identification of the sender and addressee(s) of messages that are records.

Agencies that use an electronic mail system that allows users to request acknowledgments or receipts showing that a message reached the mailbox or inbox of each addressee, or that an addressee opened the message, shall issue instructions to e-mail users specifying when to request such receipts or acknowledgments for record keeping purposes and how to preserve them.

Agencies with access to external electronic mail systems shall ensure that Federal records sent or received on these systems are pre-served in the appropriate record keeping system and that reasonable steps are taken to capture available transmission and receipt data needed by the agency for record keeping purposes.

Some e-mail systems provide calendars and task lists for users. These may meet the definition of Federal record. Calendars that meet the definition of Federal records are to be managed in accordance with the provisions of General Records Schedule 23, Item 5.

Draft documents that are circulated on electronic mail systems may be records if they meet the criteria specified in 36 CFR 1222.34.

Agencies shall consider the following criteria when developing procedures for the maintenance of electronic mail records in appropriate record keeping systems, regardless of format.

Record keeping systems that include electronic mail messages must:

- Provide for the grouping of related records into classifications according to the nature of the business purposes the records serve;
- Permit easy and timely retrieval of both individual records and files or other groupings of related records;
- Retain the records in a usable format for their required retention period as specified by a NARA-approved records schedule;
- Be accessible by individuals who have a business need for information in the system;
- Preserve the transmission and receipt data specified in agency instructions; and
- Permit transfer of permanent records to the National Archives and Records Administration (see 36 CFR 1228.188 and 36 CFR 1234.32(a)).

Agencies shall not store the record keeping copy of electronic mail messages that are Federal records only on the electronic mail system, unless the system has all of the features specified above. If the electronic mail system is not designed to be a record keeping system, agencies shall instruct staff on how to copy Federal records from the electronic mail system to a record keeping system.

Agencies that maintain their electronic mail records electronically shall move or copy them to a separate electronic record keeping system unless their system has the features above. Because they do not have the features specified in paragraph above, backup tapes should not be used for record keeping purposes. Agencies may retain records from electronic mail

systems in an off-line electronic storage format (such as optical disk or magnetic tape) that meets the requirements described at 36 CFR 1234.30(a).

Agencies that retain permanent electronic mail records scheduled for transfer to the National Archives shall either store them in a format and on a medium that conforms to the requirements concerning transfer at 36 CFR 1228.188 or shall maintain the ability to convert the records to the required format and medium at the time transfer is scheduled.

Agencies that maintain paper files as their record keeping systems shall print their electronic mail records and the related transmission and receipt data specified by the agency.

Electronic mail records may not be deleted or otherwise disposed of without prior disposition authority from NARA (44 U.S.C. 3303a). This applies to the original version of the record that is sent or received on the electronic mail system and any copies that have been transferred to a record keeping system. See 36 CFR part 1228 for records disposition requirements.

When an agency has taken the necessary steps to retain the record in a record-keeping system, the identical version that remains on the user's screen or in the user's mailbox has no continuing value. Therefore, NARA has authorized deletion of the version of the record on the electronic mail system under General Records Schedule 20, Item 14, after the record has been preserved in a record keeping system along with all appropriate transmission data.

The disposition of electronic mail records that have been transferred to an appropriate record keeping system is governed by the records schedule or schedules that control the records in that system. If the records in the system are not scheduled, the agency shall follow the procedures at 36 CFR part 1228.

8.9.2 Commercial Retention Policy

Official company records communicated through email must be identified, managed, protected, and maintained as long as needed for ongoing operations, audits, legal actions, or any other known purpose. Where email is the only communications means for official company records, the same procedures should be followed as would be required if the message were transmitted via hard copy.

To prevent premature deletion of records, employees should forward a copy of any such record to the appropriate official file or archive. Both outgoing and incoming messages and attached files should be stored. Any email message containing a formal approval or constituting any commitment by the COMPANY to any outside organization must be copied to the appropriate file (in hard copy if required) to support accountability and audits.

The retention period for all messages should be defined by the legal department. If messages are retained too long, the organization may be required to make such information public in a court action.

