Email is increasingly becoming the default method of communication for many people. In 2001/02 ISS mail servers processed a staggering 23 million email messages, amounting to over 670 Gigabytes of data, an increase of over 40% on the previous year. This increase is likely to continue, and it has been forecast that over 36 billion person-to-person email will be sent daily, worldwide, by 2005.

While many people have well developed strategies for dealing with printed matter, they often struggle to deal with the large amounts of email they receive. Once you are familiar with your email program, sending an email is very easy, and it is this ease of use that can cause many of the problems. People will often send an email message to a large group of people, perhaps with a large file attached, when they would not consider sending a letter to everyone in the group. The amount of unwanted or 'junk' mail is also increasing, further filling up our inboxes.

This booklet looks at some strategies for managing your email, how ISS can help you deal with junk mail and reduce the risk of being infected by a virus, and how to make the most of email features such as attachments. page you will find a list of useful resources and email documentation.

Contents

Managing your email

More and more people are using email as their preferred method of communication, sending emails in place of letters, memos, phone calls and face-to-face meetings. It's an ideal medium for rapidly distributing information to lots of people, and we often copy extra people in to emails just to keep them informed. All this means that the volume of email arriving in your inbox can rapidly fill it, leaving your wondering how you will ever catch up. There are, however, a number of things you can do to keep on top of your email.

Develop a routine

It is estimated that every time you are interrupted, it takes at least 5-10 minutes to get back to the task in hand. If you check your email every time your computer notifies you that a new email has arrived, the time soon mounts up. Unless you regularly have to deal with emails which need an immediate response, a better idea is to set aside certain times each day to deal with your email. For example, you could set aside some time first thing in the morning and just after lunch.

Prioritise

If you have a lot of email to deal with, prioritise it first. The priorities you set will obviously vary from person to person, but most email programs can help by allowing you to sort the messages in your inbox by sender, subject or date received. Just click on the appropriate column heading to sort your messages by that column.

Be organised

All email programs allow you to create folders to organise your mail. Create a folder for every major topic you are currently receiving emails about, including sub-folders if necessary. Once you've dealt with an email, move it in to its appropriate folder if you need to keep it.

Most email programs allow you set up filtering rules, which automatically act on your email messages as you receive them. For example, all messages with a certain words in the subject could be automatically moved to another folder.

Keep your inbox clean

Don't leave messages sitting in your inbox for more than a few days. You're unlikely to leave unopened mail sat on your desk for weeks at a time, so why treat your email differently? Once you've read an email, file it or delete it. If you end up with hundreds of messages in your inbox you are less likely to want to deal with them and important messages could easily get lost.

Remember if you exceed your disk quota you won't be able to receive any new messages until you have created some space.

Delete it (and empty the trash)

You can often tell by the subject line of message whether you need to read it or not. If it's obviously junk mail or an email you're not interested in delete it. Don't feel obliged to open and read every single piece of mail. If the email is from someone you don't know, or has a suspect subject line like 'You've won!' and has an attachment, always delete it without opening it.

In many email programs deleted messages aren't completely deleted, but moved into a deleted messages folder. You may need to tell your email program to periodically empty this folder. For example, 'Empty "Deleted Items" folder' is on the Tools menu in Microsoft Outlook.

Deal with each email once

It's more efficient to read each email and deal with it immediately - i.e. respond to it, file it or delete it, rather reading it, deciding to do something about it later and having to re-read the message.

Unsubscribe

There are many email lists hosted at the University, JISCmail maintains over 4000 email lists on a wide variety of academic topics, and many other service provides and companies also maintain email lists. It is very tempting to subscribe to any list that looks interesting. However, if you find yourself regularly deleting messages from those lists without reading them, unsubscribe.

Is your reply necessary?

You don't have to reply to every email, sometimes you just need to read the email and act on it. Many emails do require an acknowledgement, but unnecessary replies just waste your time and clutter other peoples' inboxes.

Don't use email!

Email isn't always the best communication channel. If you find yourself writing long emails, consider whether a phone call or face-to-face meeting would be quicker.

Dealing with junk mail

Junk email means different things to different people, but a good working definition is that junk email is any email received by someone who considers it to be a nuisance.

Evidence indicates that being a member of national and/or international mailing lists is by far the commonest way in which an individual's email address is picked up for use by those responsible for unsolicited email. There is little evidence that the published list of Leeds email addresses on the web is regularly used as a source of email addresses by people sending out unsolicited mail.

What you can do

The best and simplest way to deal with junk email is to delete it - as with junk postal mail, we all need to develop strategies for a quick scan of the 'envelopes' (in email terms, the sender and subject details) and if necessary the content, and then to drop unwanted messages into the bin (ie, delete them).

Never reply to junk mail, especially if it asks you to reply to be removed from their mailing list. If you reply you are saying your email address is active, and you will receive a lot more junk email.

If a website asks you to register, be wary about giving any personal details including your email address. If it is a reputable site, check their privacy policy first and read the small print. Look for check boxes to tick that say you do not wish to receive any information from them or 3rd parties.

Most mail clients have filtering facilities, allowing you to collect incoming mail together into folders according to sender and/or subject.

In Outlook these are called Rules (see the Rules Wizard on the Tools menu). In the Rules Wizard is an option to act on suspected junk email, using a list of pre-determined rules. These rules include words in the subject line such as “for free!”, “100% satisfied”, “$$” and similar phrases.

In Pegasus Mail look for the ‘New Mail Filtering Rules’ button on the toolbar.

Making use of such facilities can let you handle all your incoming mail (not just the junk) more efficiently.

Should I report it?

Particular items of junk email may also be considered offensive by some of its recipients. ISS always takes seriously any complaints from users about offensive or harassing email. We follow up any incidents, identifying the sender and dealing with them an appropriate manner.

With regard to unsolicited email: again, we will investigate any reported incidents, but resources and pragmatism force us to take this less seriously than we do offensive or harassing email. Depending on the extent of the problem (for example, chain email is always taken seriously) we may take matters further.

What ISS is doing to curb junk mail

Given that the definition of 'junk' lies with the receiver, and that much of it will come from sites that are also sources of legitimate email, it is not possible to filter out junk email at the system level. There are, however, a number of approaches that can be taken to reduce the incidence of problem email.

Refusing email from invalid addresses

On the Unix mail servers all incoming mail is checked to confirm that the sender's host system has a valid DNS entry (ie, the mail is sent from a properly registered internet site). Any messages found breaking this rule are rejected. This covers all mail explicitly routed to one of the ISS Unix boxes, together with all mail addressed to name@leeds.ac.uk . This cuts out messages from people who falsify their mail headers to conceal their origin.

Email servers handling messages addressed to *@leeds.ac.uk* subscribe to RBL and RSS anti-relay services. Anti-relay service providers register offending email servers on the Internet. They advise subscribed email servers to reject messages from known open relay sources in an automatic fashion. Any messages from a site registered in RBL or RSS will be rejected.

The mail systems running on the ISS Novell servers do not have this capability. Any mail addressed explicitly to the Novell servers will not pass through the Unix servers, and will not have the originating address verified. Wherever possible, it is recommended that you publicise your email address in the *name@leeds.ac.uk* form, rather than *username@novell_server.leeds.ac.uk*

Checking incoming mail against known 'culprit' sites

There are a number of authenticated databases of known sites responsible for junk email. While it is technically feasible from Unix systems to check all incoming email against these databases it would clearly have an impact on the email throughput. The ISS has expended (and continues to

continued on page 5

Sending and receiving attachments

Email messages are not restricted to simple text messages. By using email attachments, you can easily share all sorts of documents.

They are very useful if your only alternative is putting the file on a floppy disk and carrying it across campus or posting it to a colleague. However, email attachments have three main drawbacks: their size; viruses; and not knowing whether the person you are sending the attachment to will be able to open it correctly. Let's look at these problems in turn.

Size Matters

It is very easy to generate Word and other files that are several megabytes in size. If you send several large attachments to someone, their email Inbox may quickly fill up, preventing them from receiving any more email.

Each ISS server has a certain amount of space set aside for new mail, and usually there is plenty of space to cope with users' requirements. However, if someone sends a large attachment to a lot of people this space will rapidly fill up, causing problems for everyone on the server. In one incident last year, a 6MB file was sent to 480 users – requiring 2.88GB of space on the server!

Distributing large files

If you need to send a large document to a number of people, there are several things you can do rather than emailing it:

- Place the document on a shared drive
- Put the document in the Nathan Bodington Building
- Put the document on a website or an FTP server. It is possible to restrict access to documents on a website by password-protecting them.

When you've put the document somewhere, just email its location to everyone, rather than the whole file.

Mailing Lists

You should not normally send attachments to mailing lists. Not only will you be filling up people's Inboxes, but many people may not be able to read your attachment at all (see Opening Attachments below). Mailing lists set up at the University of Leeds have a default message size limit of 40K. Messages above this size will be rejected by the mailing list (unless the list owner has changed the setting).

Opening Attachments

If the person you are sending the attachment to has a different mail program than you they may well have problems opening your attachment. For example, an attachment sent in Apple Mac binhex format will be difficult to read if sent to a PC user, and a Word file may be unusable to a UNIX user without a suitable viewer. Whatever file type you intend to send, make sure the recipient will be able to handle it.

ISS recently issued some advice on sending attachments from Pegasus mail to students using the Webmail system. For more information see: *http://www.leeds.ac.uk/iss/helpdesk/email.html*

In Summary

Sending Attachments

- Do you really need to email the attachment, or can you make the file available in another way?
- Is the file in the most appropriate format? Are you sending a Word file when a plain text message would do?
- Do the recipients know you are going to send them an attachment?
- Will they be able to open the file?
- Have you checked the file for viruses?

Receiving Attachments

- Do you know who the file is from?
- Were you expecting it?
- Save the file to disk and check it for viruses before opening it.

More Information

http://www.personal.leeds.ac.uk/
The Personal Page Server provides free web space for all staff and students at the University of Leeds.

Users requiring space on the central web servers see the guidelines at: *http://campus.leeds.ac.uk/guidelines/ws1.htm*

About the Nathan Bodington building: *http://www.fldu.leeds.ac.uk/site/nbodington/*

Dealing with junk mail

continued from page 3

expend) considerable effort ensuring that email throughput is as efficient as possible, and we do not consider that the benefits arising from such a development merit the loss in service levels.

Email relaying

People responsible for junk email can use a variety of means to conceal their address, one of which is to use servers at other sites as staging posts to relay their mail. All ISS servers (Unix and Novell) now have anti-relay features built in to them, preventing their use as in this manner. The ISS can provide advice to departmental system managers on this matter.

Protect yourself – avoiding viruses

What is a computer virus?

A computer virus is a piece of software code designed to replicate and spread, generally with the victim being oblivious to its existence and often with malicious intent. Viruses can show themselves by changing the display on the screen, altering data files, erasing files or, in the case of newer 'macroviruses', by creating new email messages. Viruses have the ability to attach themselves to other programs or to the boot sector of infected disks. When an infected file is opened or when the computer is started from an infected disk, the virus can be executed and may reside in the computer's memory ready to infect another file or disk.

Viruses are never likely to go away, so all users of personal computers need to be vigilant and know how they should combat infection. There is no absolute guarantee of virus immunity of any machine.

Types of virus

Viruses fall into several categories. ***True viruses*** include boot sector, file infecting viruses (those that infect 'executables' such as COM, EXE, OVL, DLL files) and Macroviruses. ***Macroviruses*** typically infect Microsoft Word and Excel files (DOC and XLS file extensions) although they some can take advantage of the Visual Basic for Applications (VBA) support in Windows 98 and programs such as Microsoft Outlook. These viruses can be passed from one system platform to another (e.g. from a PC to an Apple Macintosh) where they share the same file format although the effects on each platform might be different.

Other types of 'virus' include ***worms*** (a piece of code that gets incorporated into a legitimate program), ***trojan horses*** (a destructive program that is disguised within innocuous software). Both worms and viruses can be concealed within a trojan horse. They are not true viruses in the sense that they cannot replicate themselves. A logic bomb includes a timing device – a famous example was the *Michelangelo virus*. This is embedded within a logic bomb set to trigger on Michelangelo's birthday, 6th March.

Hoaxes are also a type of 'virus' which panic the user community and generate huge amounts of email. They are often generically 'endorsed' by Microsoft, IBM and other big names.

Dealing with virus warnings

If you receive a virus warning by email, it will probably be a hoax. Hoaxes are distributed to spread fear and to generate email traffic as most people generally forward such mail to all of their colleagues. You can cheek if an alert is real or not by looking at the following web site:

McAfee Virus Information Centre *http://vil.nai.com/villib/alpha.asp*

Please do not help to propagate the hoax by forwarding a warning to your colleagues until you have verified its authenticity, even if it originated from someone you know or trust. If in doubt, please contact the Help Desk.

Viruses spread by email attachments

Viruses are now widely distributed as email attachments. These are predominantly in the form of macroviruses incorporated into Microsoft Word and Excel documents. A new breed of virus can infect a PC just by being 'previewed' in the email client Microsoft Outlook (or Outlook Express). As viruses become more clever, however, so does the software developed to combat them. The payload of most 'email viruses' is to propagate more copies of itself via email. It is this action that can cause a mail server to become overloaded and so create a commercial 'hit'. Macroviruses can include a more disastrous 'local' payload by deleting files on an infected PC. You should take email viruses just as seriously as you would one transmitted on a disk.

How can I avoid catching a virus by email?

Delete any 'suspect' mail that you receive. This may include unsolicited mail, mail from an unrecognised sender, mail with an advertising or `too good to be true' subject title.

Do not open any attachment directly. For a Word, Excel or PowerPoint file use a document viewer. Alternatively, save the file to your PC and check it for viruses manually before opening it in Word/Excel etc.

How can ISS help me protect against viruses?

ISS scan our central fileservers for viruses. This includes the users' home directories. Our public cluster machines have antivirus software installed and will scan all disk reads for viruses. In addition, the university has a site licence for the Total Virus Defence suite of software from Network Associates.

More Information

For more information on how ISS can help you with your antivirus strategy, please contact Help Desk.

For a detailed listing of viruses, cheek out the McAfee Virus Information Centre at *http://vil.nai.com/villib/alpha.asp*

Quotas and space issues

Your Quota

For users on the IMAP system, your default quota is 50Mb (15Mb for students). This includes your inbox and mail stored in other folders, but is not affected by files in your home directory. When you exceed this you will receive a warning message, if you exceed your quota by more than 10Mb you won't be able to send or receive any new mail.

For staff on the current Novell system, there is no separate quota for email, but as your mailbox is stored in your home directory it contributes to space used from your standard username quota. The default for this is 50Mb. This includes all the files in your home directory and email stored in folders, but does not include new mail in your inbox. The maximum size of incoming message that you can receive depends which server you are on, but is usually between 8Mb and 12Mb.

Although there is no set limit for staff and research postgraduates, unread mail older than 3 months may be deleted.

If you exceed your quota, you will not be able to send or receive any new mail, so it is important you clear your mailbox regularly.

Checking your quota

When you log on with your ISS username, you will see a message box which tells you the size of your quota and how much you have used.

If you use Outlook, you can also see how much space your mailbox is taking up by choosing Mailbox Cleanup from the Tools menu. Click on the top button to check the size of your mailbox.

Students using the IMP web-based email program can find their quota in the top right hand corner of the inbox screen.

If you feel you need a larger quota, you can apply for more space by contacting the ISS Help Desk.

Making Space

There are a number of things you can do to free up space in your mailbox.

Save attachments

If you receive a file with an attachment, save the attachment to disk, then delete the email message.

Empty your deleted mail folder and Sent items folder

Periodically empty your deleted mail folder and sent items folder, particularly if you regularly send files with attachments.

Auto Archive

If you use Microsoft Outlook, you can set it up to automatically archive old items on a regular basis. For more information about these features in Outlook see TUT 104 - Archiving in Microsoft Outlook, available online at: *http://www.leeds.ac.uk/iss/documentation/tut/tut104/tut104.html*

Going on Holiday

When you go away, your email can quickly mount up. To avoid coming back to a mountain of mail:

- Unsubscribe from any mailing lists or set your options to 'no mail'
- Set up an automatic reply telling people when you will be back. For information on how to do this in Pegasus Mail see: *http://www.leeds.ac.uk/iss/news/newsletter/news236/pegasus.html*

In Outlook use the 'Out of Office Assistant' on the Tools menu. You must unsubscribe or go ‘no mail’ on mailing lists before creating an automatic reply. If you don’t your reply may be sent to everyone on the list whenever anyone posts to it.

Remote access to your email

If you are on the IMAP system (this includes all students) you can collect your email using a standard web browser. This gives easy access to your email wherever you are in the world. No configuration is necessary, just point your browser at: *http://webmail.leeds.ac.uk* logon as usual, and all your messages and folders will be available.

If you are on and Exchange Server you may have web access to your email. If you are on the Academic Services Exchange Server go to *http://asmail.leeds.ac.uk* If you are the Admin Exchange Server go to *http://centralnt.leeds.ac.uk/exchange* For information about other Exchange servers please contact your User Representative.

If you receive your email through an ISS Netware based system you will need to configure an email client which uses POP3. Instructions on how to find the information you need and how to configure Pegasus Mail, Outlook and Netscape are given in the document HOW 19 – How to Collect Your Email From Home, available from:

http://www.leeds.ac.uk/iss/documentation/email.html

Using mailing lists

What is a Mailing List?

Email's strength lies in two forms of communication. One to one, and one to many. Clearly for a one to one communication is has great advantages in terms of speed, permanency, reliability of reaching the person at the other end and control over when you reply. It also has great advantages if you want to mail more than one person, in that you only have to type the message once and send it to as many addresses as you specify.

What ordinary email can not offer is many to many discussion. Now whilst you can have a group where everyone has everyone else's email address and they all send to everyone, it is fraught with problems. If one member of the group changes, or moves their email address to another location, then everyone in the group needs to be told. This may not matter for small groups, but it becomes unmanageable in large international ones with thousands of group members. You also may want some control over what is sent to the group, and this is not possible where everyone has their own list of addresses and can send what they like to that list.

The answer is a mailing list. A mailing list is essentially an email forwarding mechanism combined with simple list management software. You send an email to a single address, and it gets copied to all the email addresses registered at that address. This means the list of email addresses can be centrally managed, there can be an element of control on what goes onto the list, and people can join or leave the list of email addresses without all the other members of the list altering their local email address books.

Mailing Lists are typically used to discuss work with colleagues at other Universities, share news, collaborate on projects and publications , announce jobs and conferences and keep in touch with current developments in your subject area.

How Do You Find Mailing Lists?

There are a number of different services you can use for finding out about what mailing lists exist, and how you can join them.

Mailing Lists at Leeds

ISS supports software for supporting mailing lists called Majordomo. Majordomo is a program which automates the management of Internet mailing lists. Commands are sent to Majordomo via electronic mail to handle all aspects of list maintenance. Once a list is set up, virtually all operations can be performed remotely, requiring little intervention by the system manager of the list site.

JISCmail

The National Academic Mailing List Service (JISCmail) is based at the Information Technology Department, Rutherford Appleton Laboratory. It hosts a wide number of different mailing lists for the academic community in the UK.

To explore the mailing lists hosted by JISCmail you connect to their home page on the web: *http://www.jiscmail.ac.uk*

Types of Mailing Lists

Open or Closed

A list is said to be Open if anyone can join it. An example would be a list about pudding recipes. No one is likely to put out anything confidential on to this list about puddings, and the more people who join it the better. Consequently anyone can subscribe to the puddings list by sending an email to the mailing list management software.

A list is said to be Closed if you cannot subscribe yourself to it, but have to ask the list manager, who can send email with passwords attached, to subscribe your email address for you. Closed lists are typically those that operate within a department where you don't want the information in the list to go outside the members of that department accidentally.

Moderated or Unmoderated

This relates to whether you can send messages directly to the list. The alternative is that the messages have to be sent to someone else (the moderator) first who then passes them on to the list with passwords attached.

List moderating is typically done for mailing lists which have a very focused remit and don't want to be cluttered by irrelevant messages, or else where the purpose of the list is to disseminate information rather than act as a discussion forum.

Be Aware...

Although your email address will not be passed on to anyone else if you join a mailing list at Leeds or through JISCmail, it will be available to list members. Lists organised by other groups may make your email address available more widely. Whenever your email address appears on a publicly available web page it can be picked up by junk mail senders.

More information

ISS Documents

http://www.leeds.ac.uk/iss/documentation/email.html

TUT 92 - Introductory Exercises using the webmail program IMP

IMP is the web-based email interface provided for all students to access their email, wherever they are.

TUT 102 Using Microsoft Outlook
TUT 104 Archiving in Microsoft Outlook

Two documents providing an introduction to Outlook. The first covers basic functions such as sending and reading email, attachments and contact. The second looks at ways of saving space.

Other documents available from this page include:

- Introduction to Pegasus Mail
- Pegasus Mail FAQ
- Advice on setting up and using Mailling Lists

Viruses

http://www.leeds.ac.uk/iss/helpdesk/viruses.html

Information from ISS about dealing with viruses

Symantec

http://www.symantec.com/avcenter/index.html

Symantec provide information about the latest virus threats, and an online virus encyclopedia.

Email Programs

Outlook

http://www.microsoft.com/office/outlook/

Microsoft's Outlook home page, including a link to their support pages.

Pegasus Mail

http://www.pmail.com/

Information and downloads for Pegasus Mail, including an FAQ.

Mailling Lists

JISCmail

http://www.jiscmail.ac.uk

The JISCmail site provides a web interface to its mailing lists.

CataList

http://www.lsoft.com/lists/listref.html

A catalog of public mailing lists which use the ListServ software.

NeoSoft

http://paml.alastra.com/

A large list providing information about many mailing lists around the world.

Managing Email and Netiquette

Email 911

http://www.email911.com/

An American site with articles and other resources to help you manage your email.

The Net: User Guidelines and Netiquette by Arlene H. Rinaldi

http://www.fau.edu/netiquette/net/netiquette.html

Lots of good advice on using the net. The guidelines opposite are based on this document.

Netiquette

Do:

Include a relevant subject line.

Identify yourself – add a signature to the end of your messages.

Make sure you send your email to the correct address. Don't 'Reply to All' if your response is to just one person. This is particularly important when replying to messages from email lists.

Use humour and sarcasm with care – they are much more likely to be misunderstood in email than in person.

Delete any unwanted messages and move read messages out of your inbox.

Ask permission before reproducing anyone else's email. Never copy an email (or any part of it) without acknowledging the source.

Check your mail regularly and reply promptly, even if it just an acknowledgement.

Remember that laws relating to written communication, e.g. defamation, copyright, obscenity, etc also apply to email.

Keep it short!

Don't:

Send large attachments, unless the other person is expecting them.

Send junk email – you don't want to receive it and neither does anyone else.

Reply to chain letters.