E-Mail

Very common in this day and age, don’t even need to be at a computer to access it anymore (Phone’s, PDA’s, Wireless Laptop, etc).

E-mail is an ASYNCHRONOUS, can be used as POINT TO POINT, or MULTICAST.

Why is E-mail good?

**Fast** - Much faster than writing a letter, driving to a post office, waiting for it to be delivered. Simply write, and send. All of the work is done by computers as to the pickup and delivery.

**Convenient** - It is not available almost everywhere, so it you are sitting at a ‘Starbucks’ you can use your PDA or laptop to mail your friends. You can even use your phone to e-mail anyone almost anywhere.

**Low Cost** - No postage, and sometimes the address itself is free (Montclair’s Webmail). There will be a small cost for a connection to the internet and electrical charges.

**Easy** - You don’t even have to think (although you should) when you write an e-mail. You can make it as sloppy and misspelled as you want (although you shouldn’t).

Why Is E-mail bad?

**Poor Emotional Transmission** - It is really hard to ‘type’ your emotions in an e-mail (unless you are using the little smiley faces). Why is this? We send greeting cards all the time (that may contain any number of emotions), and they are viewed as fine.

The problem lies in ‘how’ it is written. E-mail is mean to be informal, impersonal, and sadly too casually written. It is hard to express sadness over the loss of a friend when you are typing in all capital letters, misspelling every other word, and not using punctuation.

**Emphasis** - It is hard to emphasize words in e-mails, although the tools are there to do so. Bold, underline, and italic fonts are available for your usage; but many are underused. Capital letters are usually reserved for yelling, but sometimes they are used for other purposes.

**Conversational Pace** - Dialog is difficult in e-mail because the
‘conversation’ is not instant; it spans different lengths of time for when the involved parties are responding. Chat rooms also have this problem, although they are almost instantaneous. What happens when someone gets up to use the restroom, or eat in a chat room? If they don’t make the announcement, people may get irritated. (Think about talking to your IM buddies who don’t use Away messages).

**Ambiguity** - Natural languages are ambiguous by nature, one word or phrase can mean several different things:

Move the mouse - Does it mean move the computer mouse, or move the pet mouse, or move the house mouse?

E-mail adds to the ambiguity in several ways. Not using the proper punctuation can cause some confusion; misspelling words can lead to different meanings.

**Flames (Anger)** - Anger is a powerful emotion, and e-mail makes anger 10 times faster, thus making it more dangerous. How is this? Because e-mail is right there for you to spout off your emotions whenever you want, you might send many angry messages to someone in a row. They may not be there to respond, making you even more angry and sending more. When they do respond they send many more back to you; this is a flame war.

**Netiquette** - etiquette we should use when on the ‘net’. These should apply to e-mail, IM, and chat rooms specifically.

**Ask/Talk about one thing at a time** - E-mail users have a nasty habit of trying to lump every single spare thought into a single e-mail, in some sort of effort to save time/money. E-mail is fast and cheap; send a lot of little messages with different topics. It is easier for the recipient to deal with one topic at a time, and it doesn’t cost you anything.

**Include Context (Subject)** - If you are talking about something vague/new to a person, make sure you prompt them for what you are talking about. For e-mail this can be the Subject, for IM maybe change the topic gradually, make sure the other person knows what is going on.

**Automated replies** - If you are going to be out of town/not answering e-mail for a while, use an automated reply to let everyone know. Most providers allow for this (Montclair, AOL, etc), and it lets a sender know not to expect anything back from you for a little while.

**Answer a pile of e-mail in reverse order** - If you were out of town for a while, the oldest items in your inbox have more than
likely ‘expired’. You should get rid of the newest items first in case they are really important.

**Get Sender’s Permission before forwarding** - Sometimes an e-mail makes sense to be viewed by others, but other times the sender may want to keep it private (even for a couple of days). Don’t go blindly sending e-mail without asking the sender first (this is more relevant to an office environment).

**Use Distribution Lists** - This helps to ‘hide’ who is (and who isn’t) getting an e-mail. The university uses these all the time for certain events.

**Screen before you hit forward** - Forwarded e-mails (like chain mails, jokes, pictures) correspond to much of the e-mail individuals send in a day. Just because you get a forward, doesn’t mean you HAVE to forward it to everyone you know. Use discretion.

**Passwords**

Everything needs a password now, your computer, your ISP, your e-mail, your subscriptions to web sites, etc.

Some passwords are important (ISP / E-mail), some passwords are not (Subscription to NY Times.com), but the common goal is to pick a password that you can remember, and also a password that no one else can easily guess.

**Keeping the Bad Stuff out:**

Let’s say you have a cable modem attached to your computer. The internet is always on, and bad stuff is always on the other end of that cable modem. You have a password that is supposed to protect your computer. You have chosen:

**cat7**

as the password for your computer. Let’s say that someone really wants to get into your computer, and writes a program to ‘break’ your password. The program will try every combination of letters and numbers to get in.

If you can try 10 combinations a second, how long will it take to get in?

Trying all 26 Capital letters, 26 lowercase letters, and 10 numbers is 62 combinations. We will then try each of the 62 for each place:

62 combinations = **6 seconds** for the first letter.
62 combinations = 6 seconds for the second letter * the original 6 seconds = **36 seconds**

62 combinations = 6 seconds for the third letter * 36 seconds = **3 ½ minutes**

62 combinations = 6 seconds for the fourth letter * 3 ½ minutes = **21 ½ minutes** (It will actually be less, because 'cat7' would be near the beginning of our attempt).

In conclusion, the smaller the password the easier it is to break. There are several ways to make a password better:

- **Add length** - Making it longer adds complexity (i.e. time) to when you are trying to break it. It doesn’t really do anything to you except force you to remember more.

- **Add non-alpha characters** - if you add punctuation to your password it increases the complexity from 62 to maybe 128 or 256 (remember **ASCII**).

- **Non-Dictionary words** - sometimes ‘crackers’ may employ programs that search for dictionary words; to defeat this just make up combinations of words, or don’t use words at all.

Although a password is your responsibility, ‘system administrators’ (people who manage computer systems) may help you out a little, because YOUR insecure password will hurt THEIR system:

- Will force you to make a password a certain length, contain certain characters, and not be a dictionary word.

- Will enforce ‘aging’; meaning that you must change the password every now and then.

- Will allow only 3 misses; then will lock you out. This prevents a ‘brute force’ tactic like the one above.

**Keeping the Good Stuff in:**

How are passwords stored? Is there just a list somewhere with users and their passwords?

It is similar to this idea, except the users and passwords are both ‘encrypted’; meaning that they are scrambled up in some way so that the computer knows what they are, but a casual reader wouldn’t.

**Ex:**
<table>
<thead>
<tr>
<th>USERS</th>
<th>PASS</th>
</tr>
</thead>
<tbody>
<tr>
<td>john</td>
<td>cat123</td>
</tr>
<tr>
<td>jim</td>
<td>jamesdean</td>
</tr>
<tr>
<td>joe</td>
<td>12eoj21</td>
</tr>
</tbody>
</table>

Encrypted:

<table>
<thead>
<tr>
<th>encrypted</th>
<th>decrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>kpio</td>
<td>dbu234</td>
</tr>
<tr>
<td>kjn</td>
<td>kbnftefbo</td>
</tr>
<tr>
<td>kpf</td>
<td>23fpk32</td>
</tr>
</tbody>
</table>

How did I get these?

Resetting passwords:

When you lose your password, and you call tech support for a new one, there are really 2 things tech support can do:

- Erase your password, forcing to enter a new one at login time.
- Give you a temporary password, and force you to think of a new one at login time.

Tech support, in their infinite wisdom, cannot see computer passwords; all they can do is change them. This is built in security to prevent the mass revealing of passwords.

Managing Passwords:

Odds are you have many to manage, it is not always a good idea to use the same password for everything you use (think identity theft).

Things that go ‘crash’ in the night:

Just like there are a lot nasty people out there who want to do bad things to your computer, the nasty people write nasty software to do things to your computer.

Types:

**Virus** - A program that ‘infects’ another program by embedding a (possibly an ‘evolved’ [mutated]) copy of itself so that when the infected program runs, the virus will create more copies of itself and infect other programs.

**Worm** - Similar to a virus, but this program will travel from computer to computer over a network connection infected others as it travels. Each infected computer will then spawn new worms that will infect others.

**Trojan Horse** - This is more of a mechanism really, it can be either a virus or a worm. A Trojan horse works much like it’s
namesake. A user will usually willingly take a piece of software and install / or use it. This software will then contain a virus or a worm that will do some damage.

Spyware - Many people don’t count this as a virus, but I do. This is software dedicated to spying on you. It will periodically send information to a location over the internet. What kind of info, well I would like to say it is simple things like what programs you regularly run, or what web sites you visit…but it CAN (does) often send much more.

How Was I infected?

Internet Connection - This applies mainly to cable modem/DSL/network users. Worms will usually enter through a running piece of software (MS Windows is famous for letting these in), store themselves out of view, and then replicate to other computers on a network. The best way to stop this is to use firewalls, and keep software up to date.

Downloading software - When you download internet games, screensavers, etc. often you get a lot more than you want. Napster was famous for allowing other pieces of software (GATOR) to install along with Napster. Usually it is Spyware you are getting; sometimes you get a virus/worm in the form of a Trojan horse (Remember ‘Elf Bowling’?). Use discretion when you download.

E-mail - Attachments are common in e-mail, but before you go clicking away on the ‘picture’ or ‘movie’ that someone sent to you think about a couple of things:

  Do you know the person?
  Are you expecting an attachment?
  Do you know what the attachment does?

Remember that a file extension ‘.jpg, .mov’ really means nothing. If there is bad stuff in the file, and you run it, it will do bad things to your computer.

Passing the infection

If something bad happens to your computer, sometimes you may not know about it. If you are connected to the internet, or are a big fan of e-mailing lots of people you are now infecting others at a rapid rate.

Wearing Protection
Get Anti-virus software and keep it up to date. This is usually your last line of defense against the bad stuff.

Get a firewall if you are on a constant connection (Cable / DSL). This keeps bad stuff out (first line of defense).

Screen your e-mail, you can get a program like ‘Spamassassin’ which identifies strange e-mail, or mails from people not in your address book.

Don’t open attachments unless you know who it’s from AND you ask them if they sent it.

Don’t download software from the internet. This is a hard one to follow, so at least be careful when you do.

Links:

- [http://www.lavasoftusa.com](http://www.lavasoftusa.com) - Makers of Ad-Aware, and anti-spyware and anti-adware program. This is a must download for anyone who downloads a lot in the internet. This is free.

- [http://housecall.antivirus.com](http://housecall.antivirus.com) - This is a free online virus scanner. It can’t really do much to fix your viruses, but at least it will let you know what you have.

- [http://www.zonelabs.com](http://www.zonelabs.com) - This is a free firewall, again it is a must have for all constant connection internet users.

- [http://spamassassin.org/where.html](http://spamassassin.org/where.html) - Spamassassin is a free add-on filter for your e-mail that will eliminate spam as well as some known viruses.

Hoaxes

These circulate through e-mail mostly, and are meant to strike fear into the hearts of all computer users.

Recent hoaxes I can remember include ‘Elf bowling’, which was a hoax about a popular game being a dangerous virus, ‘jdbmgr.exe’, which is really a harmless program that is found on most computers; the hoax said to delete it.

As a rule of thumb, don’t automatically go and do what an e-mail tells you to about some virus, spend some time and look it up. There is probably information on it, good or bad.
Intellectual Property

Everyone has some sort of property; such as clothing, books, a computer, a car music, etc.

Even though you physically own the property in question, you may not always have full and complete control over it.

Some property will always belong to an original owner, and some things (even though it can’t be seen such as digital music or ideas) are still considered property.

Think of music, because it is a very easy example. If a singer decides to perform a song that someone else wrote (a cover), and include this performance on their album there are several layers of property that are involved.

The original author of the cover owns the music and words.

The artist owns the performance.

You own (rent) the CD.

Think of a company, which is a little harder. All work that you produce for this company is the possession of the company. The reason for this is that they provide you with materials, and a conducive atmosphere to think, therefore whatever you do is theirs. Is this fair?

Licensing of Software

When you buy a new game or application for your computer there is usually a giant disclaimer you have to click in the installation process. Ever read one?

If you ever did read it, you would learn a very important fact:

You did not buy this software, you are renting it.

This is not the same everywhere, but it is a general rule. Because you are renting the software you can’t do a lot of things with it. You can’t copy it, you can’t share it, you can’t change it, you can’t re-sell it, etc.

Copying - This is self explanatory, you really shouldn’t duplicate it for any reason. Because you are the one who rented it, you should be the only one using it. Why would you need a copy?

Sharing - Look at copying, you are the one who bought it and will use it, why would you share it? If the software is
‘Shareware’ then feel free to break this rule.

**Changes** - It would be very hard to make changes, but even if you wanted to, you can’t, so don’t try. ‘Open Source’ software allows you to make changes worry free.

**Re-Sale** - You are renting this, if you don’t want it anymore you should send it back. Would you sell a U-haul truck when you were done with it?

Feel constrained, you should. Is any of this fair, to a certain extent yes, it is. They are selling a non-standard product to you, and therefore they must protect it in a non-standard way. Software is easy to copy, share, distribute, and change. There has to be something done to prevent it. Does this work?

**Copyrights**

Simply concept; not easily understood or followed. If you create something, weather it be a document, a piece of software, or some music; as the owner you have the copyright. This copyright is understood for the US (and most other nations).

If you worked alone you own the sole copyright, if you worked for hire you own it jointly with whoever else is involved (or in the case of a big company you may not own it at all).

Even if you don’t put a © on something, you still own the copyright. The symbol rule was phased out some time ago.

What is a copyright?

A copyright protects the owner’s rights to:

Make copies of the work.

Use as the basis for new work.

Distribute or publish the work (including electronically).

Publicly perform the work (read, sing, perform, or play a VCR or CD-ROM)

Publicly display the work (images on a screen, paintings)

The owner(s) have the right to license any or all of these items to the general populous. They also have the right NOT to license them. Usually there are guidelines set up.

E-mailing the address of a web page is legal, and reading information is (still) legal.

If information is in the public domain (web sites, books,
newspapers, etc) it is legal to use the information, provided that the owner’s copyrights are not violated. If not specified, a citation is generally all that is needed. If a citation is missing, you are breaking the law. When in doubt, it never hurts to ask permission.

If you are using the information for a scholarly purpose (not for profit); you can usually claim ‘fair use’ if someone gives you a hassle about it. This basically means that information, that is properly cited, can be used to instruct or educate without expressed permission.

Fair use has some guidelines to protect the owners:

The planned use must be acceptable.

The nature of the work in which the material will appear must be acceptable.

The quantity of the material being used must be acceptable.

The effects on the original material, due to the new work, must be acceptable.

These questions may not even affect you, but if you think they may ask the original owner.

Violations

Violations usually occur when you profit (or stand to profit, or cause loss of profit) from the material in question.

Penalties are stiff (up to $100,000 in some cases per violation).

Best course of action, don’t use other people’s material in a way it was not meant to be used. Don’t steal other people’s ideas. Don’t listen to music unless you have a license to do so. Don’t copy software period.