Chapter 12

Computers in Polite Society: Social Implications of IT
Email Messages

Email is a great way for people to communicate. It allows messages to be sent at anytime, it is cheaper than most other forms of distance communication, and even has great multicast properties.
Problems with Email

- Conveying emotion
- Emphasis
- Conversational pace
- Ambiguity
- Flame-a-thons
Conveying Emotion

It is very difficult to convey emotions using email because it feels too informal, too impersonal, and it is often too casually written.
<table>
<thead>
<tr>
<th>Emoticons</th>
</tr>
</thead>
<tbody>
<tr>
<td>:)</td>
</tr>
<tr>
<td>;-)</td>
</tr>
<tr>
<td>=)</td>
</tr>
<tr>
<td>=D</td>
</tr>
<tr>
<td>=0</td>
</tr>
<tr>
<td>;-P</td>
</tr>
<tr>
<td>:-('</td>
</tr>
<tr>
<td>:-/</td>
</tr>
<tr>
<td>(^_^)</td>
</tr>
<tr>
<td>(^o^)</td>
</tr>
<tr>
<td>d(^_^)b</td>
</tr>
<tr>
<td>(;_;;)</td>
</tr>
<tr>
<td>(-.-)Zzz</td>
</tr>
<tr>
<td>(<em>^.^</em>)</td>
</tr>
<tr>
<td>(o.O)</td>
</tr>
<tr>
<td>v(^-^)v</td>
</tr>
</tbody>
</table>
Do you know you forgot my birthday?

DO YOU KNOW YOU FORGOT MY BIRTHDAY?

Do you know you FORGOT my brithday?

Do you know you forgot *my* birthday?

Do you know _you_ forgot my birthday?
Conversational Pace

When the conversation is asynchronous, there are a lot of cues that are no longer available.

We use audio and timing cues to indicate confusion, misunderstanding, thinking, and listening.
Ambiguity

Messages that senders to not proof read often have mistakes that make the meaning ambiguous.

Email messages tend to be casual, and as such often contain grammar that can be ambiguous.

Sarcasm used in messages is often interpreted as serious statements.
Flame comes from the term “inflammatory email.” These message threads can be started by differences in opinions, ambiguity, or other reasons.

Related terms include flame war and flame bait (trolling).
Netiquette

- Ask about one topic at a time
- Include context
- Use an automated reply
- Answer a backlog of emails in reverse order
- Get the sender's permission before forwarding
- Use targeted distribution lists
Passwords

Usernames allow computers to separate data and keep users from seeing what they are not authorized to see.

Passwords make it much more difficult for users to claim to be someone who they are not.
No Password Access

It is possible to break into a computer without prior knowledge of the password required to authenticate.

Brute force is when you try all passwords until you find one that works.

Administrators can also reset passwords, but on modern systems they cannot recover them.
Selecting a Password

Passwords should be long enough that brute force methods of guessing passwords will not be effective. They should also contain multiple types of characters so that the number of possibilities expands faster.

A pretty good method of selecting a password is converting a phrase into a password.
Many system administrators believe that passwords should be changed often to prevent people from gaining unauthorized access.

When people are forced to change passwords often, they begin to write them down, they forget more often, and they are more likely to select easy to guess passwords.
Malware

- Virus
- Worm
- Trojan
- Spyware
- Backdoor
- Botnet
Virus

A computer virus operates about the same as those found in biology.

They get into your system and find a way to be part of the systems execution. Once they execute, they try to spread themselves to other pieces of the system.

They spread by attaching themselves to files and devices that are moved or shared.
Where a virus usually relies on people to spread, a worm relies on the network infrastructure and vulnerabilities in services to spread.

Worms are usually aggressive and can hit all parts of a network in anything from a few minutes to a few days.
Trojan Program

Trojans are malicious programs that are embedded in or hidden in another useful program.
Spyware

Spyware is software that monitors your machine. It can do anything from watching keystrokes to searching your machine for information. Spyware applications often “call home” with information they have collected.
A backdoor is something that is written into an application or operating system so that once it is deployed, the system can be accessed using the backdoor credentials or methods instead of the normal system credentials.
Botnet

Many current malware applications are deployed with the intent of creating a network of systems called a botnet. Each member of the network is often referred to as a zombie. Botnets tend to be peer-to-peer style networks that allow the creators to issue commands to the zombies.

Common uses include spamming, illegal web hosting, phishing, DDoS, and super computing.
How do I get infected?

- Email attachments
- CD and USB autorun
- Copying or sharing software
- Peer-to-peer exchange
- Shareware / binary freeware
Many common virus checking software applications claim to be able to detect and remove 95-98 percent of viruses.

The best spyware/adware software packages usually can only handle about 50% of spyware/adware.
Phishing

Phishing sites pretend to be legitimate sites in hopes that you will enter your username and password, credit card information, or information about yourself so they can later use it on the real sites.
Intellectual Property

- Copyright
- Patent
- Trademarks
- Service marks
- Trade secrets
It is rare that a company will actually sell software. Traditionally, companies sell you media that contains the software along with a license to use the software as long as you abide by their End User License Agreement (EULA).

Because you do not own the software, you cannot always sell it or give it away.
The Public Domain contains:

- Works where the copyright expired
- Works produced by the US government
- Works that are not copyrightable (facts)

Anyone can use items from the Public Domain without any authorization.
Facts cannot be copyrighted.

You cannot copyright the numbers in a phone book, but you can copyright the layout and presentation of the information in the phone book.
Open Source Software

The idea for Open Source comes from the Free (as in Freedom) Software movement.

Free Software is free because it comes with a license that says you can make modifications, but all derivative works must contain the same license.

Some Open Source licenses are almost as liberal as the Public Domain.
Fair Use laws claim that there are some things that you should be allowed to do even if you do not have authorization from the copyright holders.

Is recording a family video of a child playing with a toy while the television is on or music is playing in the background an example of fair use?
Software Reliability

- Safety-Critical Applications
- Hardware Failures
- Software Failures
Programming pioneer Edsger Dijkstra first stated this fundamental fact:
Program testing reveals only the presence of bugs, never their absence.
Fail-Soft vs. Fail-Safe Software

**Fail-Soft**
When software detects a failure, it will reduce functionality to keep everything running, but will stop parts that are dangerous.

**Fail-Safe**
When software detects a failure, the application is immediate shut down to prevent damage.