II.

Today's Interesting Web Service http://www.worldwidetelescope.org

See Internet Trends at http://techcrunch.com/gallery/best-of-meeker/

The Biggest Part of the Internet: Email
The desire to communicate is the essence of networking. People have always wanted to correspond with each other in the fastest way possible, short of normal conversation – email is the most prevalent form of this. There are nearly 4 billion email users in the world: Half of all Americans send or receive email every day. About 500 billion emails are sent worldwide each day – most is spam ..

Email is the 'killer app' of the 'net - something everyone uses. Email is more popular than smoking, owning a home or earning a college degree. Email was invented in 1971 by Ray Tomlinson as he was trying to find practical uses for the forerunner to today's Internet. As principal engineer at BBN Technologies in Cambridge, MA, Ray developed a system for electronically mailing users on ARPAnet. Ray was working on a program that allowed users of the same computer to leave messages for one another – sort of a single computer version of email. At the same time, he was testing a file transfer program that would allow users to send files to remote computers linked to ARPANET. It occurred to Ray that if he melded both programs together, it would be possible to send messages to other mailboxes on the network as easily as sending files. One of the decisions Ray had to make was how to distinguish between messages heading out onto the network compared to those addressed to users in the same office. He studied the keyboard for a symbol that didn't occur naturally in peoples' names and that wasn't a digit. His designation for mailboxes on remote computers that he came up with is the now ubiquitous @ symbol. The first email message wasn't symbolic: Ray just dragged his fingers across the keyboard. By the mid-1970s, ¾ of all traffic on ARPANET was email. Initially, sending email was simple, but trying to read or respond to it was a huge annoyance – text poured another the screen in a stream – with nothing separating one incoming message from another – and there was no reply function. Lawrence Roberts, then a manager at ARPA produced the first email manager in 1972 called RD, which included a filing system and a delete function. Further improvements were made by John Vittal – then a younger programmer at USC – his program called MSG became the de facto standard on ARPANET – it included not just delete but an Answer feature. It also included BCC and CC features.

As computer use grew, various commercial email services – not connected directly to the Internet – cropped up but all of them failed. MCI Mail developed (with Compuserve) in the early 1980s was an elaborate, feature-rich service ahead of its time – A user could send emails of up to 500 characters for 45 cents, and for an additional charge have MCI print and send the messages through the postal service. The world was so unaccustomed to email that MCI included an alerting service where MCI employees called recipients to tell them to check email. US Post Service tried E-Com, introduced in '82 and abandoned in '85. Both were tough sells in the business world – the question was always – why do I need it. Not until the mid'90s when online services routinely provided email addresses to home users did it catch on. By 1996, 300 million emails were sent on an average day by 100 million people.

Email has aged so well because it's still low tech – the vast majority of messages are still sent as plain text. It's also fast, easy, cheap and relatively safe. Email succeeds because at its core, it's a selfish medium – it offers you a way to communicate whenever you wish in a setting free from all varieties of social pressures, including the need for proper clothing.

Hotmail is the granddaddy of web-based email. Created by young Stanford grad Sabeer Bahtia, it had a very simple user interface. Millions joined and Microsoft bought it for $400 million. This it was worth it?

Interestingly, in some ways, social networking has overtaken email – 1 in every 5 minutes spent online is spent globally on networking websites – up 65% in the past year.

The Elements of Email Style – How to Write Email that Gets Results!

Brevity rules – if you aim for your email to be read in its entirety, it should be no more than one screen long – about 25 lines or 230 words. Don't write emails of one long blocky paragraph full of ideas. Short paragraphs with spaces in between add energy and urgency.

Subliminalize – Use the ABC formula : Action, Background, Close.

Pick a Subject – use the subject line to give the recipient a sense of what's inside. This helps make your message clear and not considered spam by email filters. Avoid or use very sparingly: Important, Read Me Immediately, Urgent or FYI

Bullets – If recapping or listing things, use bullets or numbered items

Use Punctuation and Proper Case – Using capital letters and proper punctuation encourage people to take you seriously. Use the spellchecker too.

Don't broadcast non-business emails such as appeals for charities
Limit the ability to send emails to all employees

Don't acknowledge every email received or just send 'thanks' emails

Use rules to route emails to folders that can be checked less frequently

Usable URLs – if you refer people to a website, include the address on a line of its own. Don't put punctuation before or after the URL – it prevents recipients from just clicking on it.

Lose Attachments – don't attach documents, pictures or spreadsheets unless you're certain the recipient wants or needs to see them. Do not forward interesting emails, jokes or chain letters. Don't forward virus warnings unless you authentic it first. Almost all warnings you get from a stranger's email are bogus. If you just have to distribute a document to a large number of people, put it on an accessible webpage instead and send them a pointer to it. If sending 3 or more attachments – do each as a separate email

Add Reply – Weave your response into the text of the original message when replying. Don't just quote the entire message. But if asking for immediate, important action, make the request at the top of the message. Don't be a dittohead and reply 'me too' and 'I agree'.

Date – Write out dates: 5/6/16 means May 6 and June 5 in different parts of the world.

SignOff – add a signature file with your name and e-mail contact information at the bottom of every email you send – resist the urge to include a cute quote. Do not include personal information such as home address or phone number.

Privacy – Don't assume the only person reading the email is the one you're sending it to. Few email systems are completely secure and noone is immune to pesky subpoenas. For security and productivity reasons, companies are increasing monitoring employees. Based on an InfoWeek survey of 2,540 businesses: 1/3 monitor instant messaging; 15% track printing and photocopying; 30% track time in office; 25% screen content of outgoing email; 1/3 monitor the opening of email attachments. 44% monitor Internet use; 1 in 5 review fax transmissions; 10% monitor home worker productivity.

Emoticons

Use emoticons to express feelings ;). At 11:44 am on September 19, 1982, Scott E. Fahlman, a computer scientist at Carnegie Mellon University posted a message on a university bulletin board suggested a colon, a minus sign and a parenthesis be used to convey a joking term when viewed sideways. His brief post was almost an aside but the idea caught on. For years, Fahlman, now a researcher at IBM, thought the original message was lost, but it was recovered. It is doubtful that Fahlman was truly the first to come up with a typographic means of denoting emotion online. More likely, it probably evolved from several different places, for example, in 1979, Kevin Mackenzie, a member of a discussion group on Arpanet made a similar suggestion. An interesting argument can be made that people once expressed emotions solely through their writing – letter-writers never required emoticons (though the Telegraphic Review and Operators Guide of 1857 documented the number 73 in Morse Code to mean 'love and kisses.' Search for the terms: SarcMark and Interrobang

Viruses

On Nov. 2, 1988, Robert T. Morris, Jr., a graduate student in computer science at Cornell wrote an experimental, self-replicating self-propagating program and injected it into the Internet. He soon discovered it was replicating much faster than he anticipated because of a software error - a bug - in it. When he realized what was happened, he attempted to anonymously to send out a solution on how to kill the worm and prevent re-infection, but the network routes were so clogged, the message did not get through until it was too late. Meanwhile computers were affected at many sites, including universities, military bases, and medical research facilities. The Morris worm disabled about 10% of all Internet-connected systems , then about 60,000 machines. Teams of programmers worked non-stop to come up with at least a temporary fix – after about 12 hours, a team from Berkeley came up with steps to help retard the spread of the virus. Another team from Purdue came up with another method. The information did not get out quickly as many sites had disconnected themselves from the network. After a few days, things slowly began to return to normal and everyone wanted to know who had done it all. Morris was identified, convicted of violating the Computer Fraud and Abuse Act and sentenced to 3 years probation, 400 hours of community service and a fine of $10,000. (He's now an MIT professor) In the wake of this virus, the Department of Defense set up the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon U. to improve communication about future incidents. See http://www.us-cert.gov – the post 9/11 home of a government monitoring effort begun in 1989 at Carnegie Mellon U. prompted by the first major virus to strike the Internet. See http://www.cert.org - it is now a federally-funded security research and development center that posts info about vulnerabilities, attacks, defenses and various security stats located in Arlington, VA, with the National Coordinating Center for Telecommunicatoions and the National Cyber Security Center.

Other source: http://www.justice.gov/criminal-ccips

Nice definitions: **Virus:** any piece of computer code that automatically replicates itself. Vast majority are in email attachments. **Trojan:** an email designed to trick users into opening it and launching a virus. **Worm:** a more malicious type of computer code that doesn't require the user to do anything.

One in 13 email messages carried a virus last year; up from 1 in 33. Only 1 in 40 emails is legit.

Virus / Hacker Early Timeline

1986 The Brain, the first PC virus is created. The boot virus originates in Pakistan.
Virdem, the first file virus originates in Germany

1987 The IBM Christmas worm strikes, replicating up to 500,000 times per hour on mainframes – the fastest spreading virus of the time. Lehigh virus wipes out 500 system disks at Lehigh U.

1988 Robert Morris' Internet Worm spreads to 6,000 computers, 10% of all computers on the Internet

1990 AT&T long distance switching system crashes due to hackers.

1992 Michaelangelo virus is set to trigger March 6 and predicted to cause widespread damage. A few hundred systems are hit amid panic.

1994 Hackers wreak havoc on government and corporate sites: millions stolen from Citibank

1995 First Word macro virus, Concept . DoD attacked 250,000 times; about 65% of attempts are successful.

1996 First Excel virus, Lauroux. First Access macro virus. First AOL Trojan viruses. Concept becomes the most common virus in the world, infecting Word documents on both PCs and Mac – the first cross-platform virus. Concept also adds social engineering to the mix – tempting users to open files with salacious or friendly titles.

1999 Melissa spreads rapidly worldwide. Word is infected and it emails itself to everyone in Outlook. Fastest replication ever. Thousands of email servers shut down. W32.Funlove.4099 is discovered – replicates in Outlook without having to run any attachment

2000 VBS.Loveletter spreads to Internet chat rooms using MIRC. Overwrites files and tries to download a password stealing Trojan horse program from a web site. Palm.Liberty.A, the first Trojan horse for PDAs. DoS attacks on major websites (Amazon, Yahoo and eBay) shut them down.

2001 Code Red I & II self-propagating malicious codes are released and exploit Internet Information Server systems. Code Red was designed to use the combined power of a network of infected machines against the White House website at a predetermined date. W32/Sircam appears spreading through email. W32/Nimda worm is the first virus to propagate itself through several different methods including web servers and email.

2003: Slammer virus works just like Code Red but spreads throughout the Internet in less than 20 minutes. Blaster worm infects 10 million computers in 3 weeks after Microsoft issues a patch to fix the hole the worm exploited.

2005: Zotob worm and back-door Trojan exploits patch one day after a Microsoft patch, spawns 19 sub-families of worms exploiting the same hole.

2006 Viruses spread to PDAs, cell phones, MP3 players, anything connected to the Internet.

2007: Estonia suffers a massive DDos attack that knocks out govt. and banking networks.

2008: Chinese hackers claim access to the world's most sensitive sites.

2009: GhostNet infects computers in 103 countries, stealing documents and taking control of webcams. A Chinese hack steals data on the Joint Strike Fighter.

According to the most recent Symantec report, most attacks originate in the China, Russia, the US and South Korea. The US is also the top target of Denial of Service (DoS) attacks. Internet Explorer is still the target of many web browser attacks. Home users the target of many attacks. China has the most bot-infected computers; 86% of credit cards offered for sale in the online underground economy were issued by US banks.

An unprotected PC new to the Internet will become infected by a worm or virus with an average of 6 minutes –down from 40 minutes not too long ago.

There was a time when losing a laptop was the biggest mobile computing risk – now cell phones, smart phones and PDAs are also subject to PC-to-mobile viruses, malware through downloaded sound or video files or hackers who tap into phones to make calls. Securing these devices for businesses is becoming a real challenge.

Future Viruses

Computer scientists are predicting new types of dangerous worms are theoretically possible. These worms would specifically target vulnerable Internet hosts and equipment rather than just randomly scanning - a 'flash worm' can theoretically hit all the servers open to the Internet in less than 30 seconds. If such a worm carried a payload to destroy files or launch a denial of service attack, it could take down the Internet before a human-meditated response could be triggered. Another concern is that an off-shore terror group would infiltrate the outsourced programming industry and inject a worm into a widely used software product.

Current variants of the Bagle virus are undetectable by signature-based anti-virus programs. They employ a delivery technique that slips past gateway, desktop antivirus, firewalls and intrusion detection systems. They use email to propagate but not via attachments. Once a blank email is opened by recipients or even previewed in Outlook, the bugs exploit a flaw in IE to automatically download the virus code. And since many places don't scan incoming HTTP traffic for viruses, the file has no problem getting in. If this becomes the norm for delivery, this means antivirus software writers will have to rethink the way their products function. Just to keep things interesting, spammers are experimenting with using the same flaws to out-fox anti-spam devices.

Zombies

Viruses used to announce their presence to users, being more about bragging rights than genuine malice. Now after a computer is exploited successfully, many worms or 'bots' connect to outside servers and download new instructions or programs. Using this 'mothership' approach, the malware becomes self-updating, and removes itself after it completes its task. Many programs record keystrokes, screen shots, look for passwords, and pass the users' Web surfing through a proxy server which can record every bit of data. Malware is also becoming much more targeted. Hackers design worms to create sophisticated robot networks that infect and control thousands of computers. When this 'botnet' is up and running, the hacker 'rents' the network to criminal groups.

Thousands of computers tied are used to initiate massive DDos (distributed denial of service) attack against corporate servers – that are held for ranson. There are many very large networks of hundreds of thousands of machines that have been compromised and loaded with 'bots' – tiny applications that allow remote attackers to control the machines. Hundreds or thousands of these machines can then be used in concert to launch attacks. The easiest type of botnet to track are the spam botnets. One in particular generates nearly half of all spam. See http://websense.com for more info.

Early Trends
In the 1980s, boot disk viruses were all the rage. Files and executable viruses were huge in the 90s. Today's malware takes advantages of exploits in Internet browsers. Users surf to an infected webpage and their computers are exploited remotely.

The Russian mafia is growing in power again – hawking stolen SSN, credit card numbers, PayPal and eBay credentials and bank log-in data in bulk. Private exploits including sophisticated rootkits that are virtually undetectable are growing. There are many Trojans connected to a Web-based command and control interface that have infected thousands of machines.

How to Fight Viruses and Hackers
Just say no to all the email gimmicks and offers of free software, etc. Instead of buying a new product, you can stop virtually all potential hackers by just activating the firewall that comes built into Windows. Most of these problems are caused by problems in Microsoft's stable of products that are riddled with vulnerabilities. Why is it that fixes for the damages caused by these attacks must be provided by costly software by antivirus providers? Many integration problems are created by blue-chip antivirus software. Why do you need this $50 software + $20 subscription fee? Just say no to filesharing. Don't open attachments on emails from people you don't know or even from people you know that you do not expect. Delete chain-emails or 'forwards.'

After Windows XP came out, antivirus programs became a 'must.' XP is based on Remote Procedure Calls (RPC) designed to let help desk people take remote control of a computer over a network. Unfortunately, holes in all the various RPC schemes allows hackers to take over a machine without the operator doing anything. While Microsoft's Service Pack 2 fixed many of these holes and installed the Windows firewall for you, it caused interoperationality problems and other security issues. Windows Vista tweaked some of these issues, in both its architecture and by enhancing an annoying alert that double-checked what you wanted to do. Windows 7 has added some additional security.

Spam – Spam has more than doubled in the past year. 94% of all email in December was spam.
Categories of spam: 33% products; 24% financial; 18% adult; 16% other; 5% scams; 4% health.
Of the billions of emails sent daily, 60-80% is spam. Biggest purveyor: domain names from China, Brazil, Turkey, US, Germany, Russia
US is the world's largest spammer but its share of spam is dropping swiftly. (56% vs. 14% today)
The bulk of spam is sent between 10 am and 2 pm on Saturdays and Sundays.
Properly used, spam filters capture up to 98% of spam entering a system.

1978 Gary Thuerk, a salesman for Digital Equipment sends a sales pitch to several hundred names on an early APRAnet mailing list.
April 12, 1994: First reported spam occurs when a California law firm sends an ad for 'Green Card' services to more than 6,000 Usenet groups.
July 1995: Jeff Slaton offers the Web's first spamming service and also becomes the first to use forged message headers in spam.
1996: Sanford Wallace creates the first large-scale spam factory, Cyber Promotions. Maximum capacity is 25 million spam emails per day.
Oct. 1996: FBI investigates the first spam involving child pornography.

July 1997: Nevada enacts first anti-spam law – there are no penalties for non-compliance.
Dec. 1997: The first randomly generated dictionary spam attack. Previous attacks relied on email lists.
March 1999: Spam begins to target instant messaging.
April 1999: AOL users hit with email scam that lets spammers hijack their accounts – by tricking users into revealing account info.
Sept. 2000: First Nigerian email scams introduced.
Sept. 2001: Relief fund scams for Sept. 11 victims introduced.
March 2002: Spammers launch a fraudulent email masquerading as account verification from a major US bank.
Nov. 21, 2002: The Friends Greeting application uses spamming techniques to send a virus across the Web. Users are tricked into downloading a component that mass emails itself to everyone in their address book.

To fight spam – one definition is its an acronym for simultaneously posted advertising message - unsolicited commercial email – and other unwanted solicitations. Use your email spam filters; visit http://www.donotcall.gov

Lots of companies are proposing ways of fighting spam; to authenticate email like Caller ID.

How did the spammers find you? Every time you give out your email address online, even if it is in the signature of a message posted on an Internet message forum, if you list your email address on a website, or visit a chat room where the address is revealed. Spammers use free automated programs that troll millions of web pages searching for the distinctive pattern of email addresses.

Where does the name ‘spam’ come from? There are a few interesting theories. The most well-known traces the origin to a Monty Python comedy routine. In the skit, a waitress lists the items on a restaurant menu, all containing the Hormel meat product Spam. As she does this, patrons who happen to be dressed as Vikings start chanting, “spam, spam, spam, spam…”

Ever wonder why some spam contains words that make no sense like kite, defrost, tree, and the like – they try to fool spam filters which count common spam words (like Viagra)

Anti-Spam
Search for McColo and Intercage for a story about the taking down of a spam-hosting firm.

It allegedly ran systems used by various spamming and cybercrime operations. It was disconnected from the Internet by its upstream ISPs in November 2008 – about half the spam circulating on the ‘net disappeared – though it soon recovered.

To Avoid Sending Spam
If you want to send email to your customers or potential customers, follow the guidelines of the federal Can-Spam law. Offer an opt-out mechanism to cancel email from you and take less than 10 days to honor requests; label your email, and supply a postal address that indicates the email’s origin. Can-Spam has been largely a failure. It created a minimal legal definition for spam but is far behind.

Fee-based “Certified” Email. Various ISPs explored the possibilities of asking mass emailers to pay a fee to have their email delivered to their subscribers inboxes. Didn’t go anywhere.

Bacn: This acronym describes a benign but nettlesome category of email: useful but not urgent newsletters, notifications, alerts, etc.

Spim: instant messaging spam to an Instant Messaging client.

Spit: Spam over Internet Telephony- audio spam that clogs voicemail boxes.

Slogs / Sportals / Splogs: Spam-blogs to manipulate search engine rankings and fool people into clicking on their links. They rise and fall whenever Google changes its search algorithms.

Phishing
Also known as brand spoofing or carding. The spam e-mails appear to come from well-known and trusted companies. The messages tell recipients that, because of technical problems, billing information and social security numbers for their accounts must be resubmitted. Scam artists recreate pages using information from legitimate Web sites in hopes of fooling consumers into providing their personal data. Growing each month. 80 million Americans received a phishing email last year. 85% of fraudulently used brands were in financial services. The US is the country hosting the most phishing sites loaded with Trojans and other spyware. Russia is next; then China and Brazil.

It's all part of the growing trend of identity theft, the FTC said. Reports of stealing a person's financial information surged 88 percent last year. Research suggests a relative handful of people are responsible for the majority of attacks using a rotating series of zombie networks to launch them. Nearly 1/3 of these zombies are in the U.S. However, most phishers appear to be associated with organized crime groups in Russia and Eastern Europe.

Phim: IM phishing Also **Smishing:** SMS phishing. Sending a phone text message encouraging a user to go to a spoofed website where malicious code is inadvertently downloaded or username and passwords are collected.

Vishing: Voice phishing. Breaking into VOIP structures to make large volume of phone calls for free – either dialing consumers directly or substituting hijacked phone numbers for URLS in traditional email come-ons.

Spear Phishing or **Whaling.** Highly targeted phishing attack against a key exec, rich person or celeb where criminals include personal information to lend credibility to their emails trying to get passwords and other info. Has 80% success rate…

Security Breaches
The media is full of stories about tapped customer databases and millions of stolen credit card numbers. What are the real risks?

The Real Risks
In this era of uncertainty, let's look at different classes of security risks from a recent Computer Crime and Security Survey. Percentage of business respondents reporting these types of incidents in the previous year:

Most of the more common 'exploits' are of vulnerabilities that were announced and patched five or more years ago. This threat could be mitigated by simply patching on a regular basis, but this is tedious and time-consuming and many do not do it.

Virus infection: 50%
Laptop theft: 42%
Unauthorized access: 29%
Targeted malware attack: 27%
Denial-of-service attack: 21%
Bots: 20%
Theft/loss of customer data: 17%
Abuse of wireless network: 14%
System penetration: 13%
Financial fraud: 12%
Theft/loss of proprietary information: 9%
Password sniffing: 9%
Sabotage: 2%

System sabotage – such as viruses, spam and denial-of-service attacks. Likelihood: very high. Harm potential: often overstated based on the dubious theory that business interrupted is permanently lost. 15% of all online computers are part of botnets – infected with code that effectively puts them under control of a remote botmaster. Cyberwar is a real possibility: witness Russia vs. Latvia; Georgia. Safeguards: firewalls, intrusion-protection systems, virtual private networks, antivirus and antispam software.

Physical security – hacking a power grid or chemical plant. Likelihood: moderate. Harm potential: very high. Safeguards: Keep process-control systems isolated. Monitor systems for unusual patterns of data access.

Transactional fraud – such as bogus banking transactions. Likelihood: moderate. Harm potential: depending on industry. Safeguards: protect core transactional databases. Exploit database management security tools without inconveniencing customers. Intellectual property theft – product designs, customer lists. Likelihood: greatly exaggerated. Harm potential: exaggerated. Courts provide redress. Safeguards: basic security. Do not alienate employees.

Internet misuse – porn, instant messaging friends, offensive email. Likelihood: very high. Harm potential: low except for wasting time. Safeguards: Internet filters.

Customer data exposure – stolen credit card numbers – likelihood: moderate. Harm potential: High and somewhat unappreciated. Safeguards: keep core data offline. We humans with our legacy analog-only sensoriums represent a terrible security list (the receptionist confirming accounts aloud on the phone in front of other clients; reading someone's laptop screen on the train or plane.

Some of the latest scares are exaggerated. Examples: 'Puddle phishing' where identity thieves target customers of small banks, or mobile malware, which are programs that disrupt wireless services; hotspot eavesdropping where hackers try to invade connected devices; VOIP breaches where digital phone systems are targeted.

Identity Theft: How to Protect Yourself
Expect to see the 2 billionth personal record compromised by year end, according to U Wash researchers. 60% of compromised records are attributable to organizational mismanagement: missing or stolen hardware, administrative errors, insider abuse or theft, accidental posting. 30% is related to hacking.

Safeguard passwords. Remove Personally Identifiable Information from your computer. Encrypt your hard drive. Monitor your credit report. What else do you do?

Instant Messaging
This was a sort of a 'subset' of email claimed to be invented by an AOL vice chairman who wondered who else he knew was online when he was. Many computer users used IM in the early part of this century – it was faster than and in real time. Free desktop messaging products from Google, AOL, MSN and Yahoo informed you when colleagues, friends and family were online and let you chat one-on-one or in a group to 'conference' – it was largely superceded by text messaging using mobile devices.

Some of the more common acronyms.
BBL: be back later BBS: be back soon BF: boyfriend BFF: best friend forever
BRB: be right back CYA, SYL: see ya GF: girlfriend GHW: got homework GLZ: girls GTG, G2G: got to go GYZ: guys HW: homework
JC: just chillin' JK: just kidding K: OK LOL: laugh out loud
LYL: love you lots NM: nothing much OMG: Oh my God Peeps: people
POS: parent over shoulderSN: screen name TMI: too much info YR: your

Chat
Chat-rooms were synchronous portals where communicators could engage in an abrupt text-based conversation. Less formally, it's a place like a coffee house or bar where patrons come to mix and mingle. In 1988, Internet Relay Chat was invented by a Finnish programmer and presented for downloading – it allowed multi-user real-time communication. Zillions of variations on IRC now exist. MUDs (multi-user dungeons) were invented in the late 1970s and ported to the Web in the late 1980s. MOOs (multi-user, object-oriented interfaces) are a formal version of the fantasy role-playing MUD.

An Old Part of the Internet: Newsgroups / Usenet
See https://groups.google.com/forum/#!overview Newsgroups date back to the 'Dark Ages' of the Internet. It's a communications medium that is similar to a bulletin board. It was an informal network of 40,000 individual server computers storing the dialogues of many, many specialized subject groups (100,000 +) where people shared knowledge, insight and concerns, find help and ask questions with those who share a common interest. Usenet groups were organized according to their specific areas of concentration called hierarchies: comp (topics related to computers), misc (topics not easily classified into any of the other headings), sci (topics related to the established sciences); soc (topics related to social issues or socializing) talk (debate oriented), news (group and software maintenance); rec (related to hobbies and recreational activities). Also available were alternative hierarchies: alt – anything and everything, biz (related to business). A caveat: one can get buried in information and there were lots of 'dark' topics.

Usenet was a major component of the Internet long before the advent of the World Wide Web. It is a set of machines that exchange articles tagged as belonging to newsgroups. It was invented in 1979 by two Duke University grad students and another at UNC who connected three machines at both campuses for discussions about the programming language UNIX. It remains the noisy commons overlooked by the vast majority of Internet users. While many high-traffic newsgroups degenerated into a sinkhole of spam and white noise, the local and highly specialized groups were a priceless resource.

Google's Usenet offerings contains the complete archive to present - 850 million messages. These posts contain such things as the first Usenet mention of Y2K and Tim Berners-Lee announcement of the World Wide Web.

Internet Communications Etiquette (or 'Netiquette)

There is a special protocol for interacting with each other online via email, instant messaging or in newsgroups. See http://www.albion.com/netiquette/

What do you do?

Lurk first in groups. Read for a while before posting. Read the FAQ. Carefully choose words. Keep it short. Try to reply on same day. Don't forward messages you think are interesting or funny to everyone you know. Express emotions with ;) Choose informative heading. Post to appropriate group. DO NOT SHOUT. Avoid sending on junk mail. Do not flame. Avoid embarrassing info in email. Do not do business unless that is the purpose of the group. Make sure your audience understands your acronyms. Use a signature line with your credentials and email address when communicating to unknown people – but do not include personal information like home address or phone number.

Online Personas

When communicating online, the amount of info people have about you is very limited. Your identity when you use email is based, in large extent, on what you write. What sort of person should you be online? If you want people to think positively of you and respect what you say, you should try to construct an *expert* persona for yourself. Here are some guidelines:

Stick to facts: don't spread rumors.

Stick to what you know: if you don't know much about the topic in question, don't say anything.

Don't just ask questions, answer them: offer thoughtful, well-crafted responses; an advantage to email is the change to take your time and polish your messages.

Be a resource for others. Stretch ideas that others have posed.

Avoid language that diminishes your power – avoid being hesitant and self-critical, using slang or vulgarities unless it's appropriate for your audience and cultural context.

Small group research has identified several individual roles you want to avoid in communicating online.

Aggressor: attacks others to feel stronger

Blocker: generally disagreeable for no apparent reason

Recognition Seeker: spends all their time boasting

Self-Confessor: uses group for therapy.

Playboy/girl: disrupts group with inappropriate messages

Dominator: attempts to take over all decisions for their own gain.

How to Protect Your Privacy Online or Foil a Snooping Boss

Safety pays in many ways, especially when you concerned about protecting your privacy online. Let's look again at this issue: Here are a few resources and tips to make your online experiences fun and safe:

Privacy Learning Initiative: http://www.understandingprivacy.org
Electronic Frontier Foundations http://www.eff.org
Electronic Privacy Information Center http://www.epic.org

If asked to register at a website, remember don't have to disclose any personal info. Remember YOU decide what info about yourself to reveal, when, why and to whom.

Never ever ever give out a password.

Cloak your surfing with http://www.the-cloak.com which masks the addresses you visit

Read the posted privacy statements of individual websites. It's up to you to find out what personal information is collected and how and with whom it is shared. If you have a problem with how a site handles consumer information, don't enter it. Look for certified privacy seals and make sure they are real.

You'd be surprised at how much information your computer (not the lab computer) carries – try http://network-tools.com

Chat smart. It may sound like common sense, but never reveal personal information in a chat group. Remember that when you offer your name or contact info in a newsgroup or chat room – strangers will be able to contact you whether you like it or not. When choosing a chat name, make sure it's different from your email address.

Check your cookies. Don't accept cookies from sites you don't know. According to Cookie Central http://www.cookiecentral.com/ A cookie is a text file saved in your browser's directory or folder and stored in RAM while your browser is running that identifies your computer to a website. The name *cookie* derives from UNIX objects called *magic cookies.* These are tokens that are attached to a user or program and change depending on the areas entered by the user or program.

Most of the info in a cookie is pretty mundane stuff, most websites use cookies to store personal preferences. There are two kinds of cookies: good cookies called 1st party – sent by a website so it can recognize your computer in the future – and bad cookies: 3rd party - sent by advertisers through the banner ads that pop up when you're looking at a website and allow your web surfing to be tracked. If you have a PC, look in the Temp Internet Folder for IE – remember to delete offline content.

Realize that you may be monitored at work, avoid sending highly personal email to mailing lists, and keep personal files on your home computer. See http://tor.eff.org Tor is a good free product that uses a technique called onion routing which uses multiple routers to pass communications. Each point on the Tor network only knows where the data is going and where it came from. It is easy to turn on and off. Even so, it's pretty hard to remain anonymous online. It only takes a subpoena or inadvertent data display by your ISP to reveal your Internet surfing record.

Internet censorship is becoming more pervasive in at least 25 countries that vet political, social, cultural content and apps such as Google Maps and Skype. China, Iran (two biggest in number and type of sites blocked), Burma Syria, Tunisia and Vietnam led the pack. See http://www.opennet.net

Beware of websites offering some sort of prize or reward for contact information.
Don't ever reply to spammers, for any reason.
If you have DSL or other 24 hour Internet access, turn off your computer when it is not in use.

Safety Begins at Home with Children and the Internet

a. Role-based Usage: Define how you'd like your children to use the computer. Create user privileges and restrict children administrator roles to ensure they cannot change policies or download software.
b. In plain view: locate a computer with Internet access in a common room – not a bedroom.
c. Accentuate the positive: Set a list of acceptable Internet sites in browsers, teach them about the benefits of online information and research.
d. Make kids be themselves. Don't allow them to take on aliases in their IM account or group chats.
e. Limit information sharing: Tell them not to fill out forms on web sites requiring personal information and to stop any online conversation with someone asking for personal details.
f. Monitor, Monitor, Monitor: Incidents can take place even with safeguards. Monitor your system for ad-ware and spyware – Look at the browser history file and cache and email or IM chats.