**LESSON 2: Ethical Considerations and Issues**

**Netiquette**



Internet etiquette (netiquette) is the conventions for politeness to observe while using electronic communication (email, chat, bulletin boards, online sharing communities, etc.). The idea of netiquette started before the World Wide Web and was introduced in the days of Telnet, Usenet, and FTP. Since the origins of the Internet had a large educational presence, the idea of proper grammar and spelling was important. Today, the opposite is true. Most young users don’t use capitals and abbreviate nearly everything. Netiquette is in a constant state of flux and will continue to be as long as technology changes. Abbreviations came about due to the cost of text messaging and this technique continues even if costs are not as much of an issue today.

Here are a few basic netiquette guidelines:

* ALL CAPITALS LOOKS LIKE YOU ARE SHOUTING.
* Emoticons add humour and personality
:-) happy
:-( sad
:-o surprised
:-@ screaming
:-e disappointed
:-< mad
:-D laughing
;-) winking
* Keep communication to the point. Long emails are hard to read and some users pay by the hour.
* Postings are public therefore be careful if you don’t want it to come back and haunt you!
* Stick to the topic. Spamming (unsolicited bulk and/or commercial email messages) and flaming (hostile and/or insulting messages) are unpleasant.
* Clearly identify your subjects.
* Insert a closing in an email such as your name.  You don’t have to also include several lines of information about yourself either or use signature text.
* Abbreviations include:
a. btw – by the way
b. lol – laughing out loud
c. rotfl – rolling on the floor laughing
d. P911 – parent alert

Although many abbreviations are used, it is not good netiquette to consistently use them in every sentence.

Netiquette also covers other areas which are no longer easily defined. For example, if netiquette covers Internet use and the Internet is used on cell phones, does cell phone use become part of netiquette?

**Censorship and Privacy**

One of the main issues with the Internet today is about censorship and privacy. As mentioned, nobody controls the Internet and therefore a lot of material is of great quality but at the same time, many people put material that is useless and sometimes dangerous on the Net. Many organizations, governments, and Internet service providers sometimes want to control what people do on the Internet. This in turn results in the tracking of people’s activities which can lead to privacy issues.



The cookies shown above may be tasty ones but when we talk about cookies on the Web, they are entirely different. Internet cookies are files that keep track of the places you visit on the web. Whenever you visit a website, a cookie has probably been downloaded to your computer. This can help the user in that the IDs and passwords don’t need to be entered each time the same site is visited. On the other hand, cookies also keep track of the user’s activities on the web. This not only applies to government sites but businesses and other organizations that want to know what you are doing. Packet sniffers look for cookies that contain sensitive information like PINS and passwords and extract them from your computer. These types of files and programs can seriously compromise the privacy of individuals.

Since 1996, digital tracking has become much more sophisticated. Search engines exist for the purpose of typing in a word or phrase to find information. Search engines also have records of every search you have done. In 2005, the United States government demanded that Google and other search engines hand over search activities of random individuals to help boost the child protection law. The American government wanted one million random searches and email addresses in a particular week. Although this particular request did not ask for who did the searches, digital records of IP (Website or Internet Protocol) addresses, cookies, and login times would be a logical request in the future. ISPs, or Internet Service Providers may be forced to give personal information at any time. In 2003, Yahoo provided digital records to Chinese authorities which some claim resulted in an eight year prison sentence for writer Li Zhi. In 2005, Yahoo was again noted in helping release data that led to a ten year prison term for Shi Tao who was accused of releasing state secrets. In April 2006, Yahoo was again named in supplying evidence which led to the conviction of a Chinese dissident. The Paris-based group, *Reporters Without Borders* stated that Jiang Lijun was sentenced to four years in jail for a “*plot to subvert the people’s democratic dictatorship under the leadership of the Chinese Communist Party*.” In 2006, at least 48 “cyber-dissidents” were in Chinese prisons for using the Internet to promote democracy. Ann Cooper, the executive director of a group called the *Committee to Protect Journalists*, said “*Censorship in China is nothing new, technology companies in China’s repressive policies are*.” Yahoo contested that they did not know that the released material would lead to jail sentences for those individuals being tracked.

Google, the world’s largest search engine in 2006, had placed filters on their servers for blocking unwanted sites within China. Chinese officials do not want their citizens to visit “anti-state” websites such as human rights sites. Google had the world’s largest Internet filter in the world’s most populous country. In 2006, there were an estimated 30,000 Chinese Net police to keep track of these “subversive” activities perpetuated by the rapidly increasing computer literate Chinese. There is little to suggest that this trend in snooping will stop in the future. In 1996, John Barlow of the Electronic Frontier Foundation issued a “Declaration of Independence of Cyberspace.” This organization’s goal is to promote digital rights across the world.

Identity fraud and theft are also becoming easier and more refined. Social security numbers and ID numbers of living and deceased people are easily acquired off the Net and used to create new identities. U.S. identity fraud is now measured in excess of $50 billion a year according to a 2003 U.S. *Javelin* study. Records from wireless phones, phony telemarketers, impersonations, credit card schemes, ATM machines, online banking, email solicitations, website donation frauds, online auctions, online dating frauds, automatic telephone charge scams, credit reports, and birth certificates are increasingly being digitized. These are much more vulnerable for theft. Every minute of each day, somebody’s credit or debit card number is being stolen and used over the Internet. It is very important to only use a credit card on sites you can trust. It is also imperative to use different passwords and change them often to avoid the capture of it by different sources.

**Hacking, Piracy, and Viruses**



The Internet and computers have created an entire new world of side effects.  Billions of dollars are spent each year to get rid of viruses, reduce pirating or copying, and to stop hackers from breaking into secure Internet sites.

Viruses (also known as malware) are files or programs with malicious code that infect your computer and can do anything from open your disk drives to deleting all your files. Worms and trojans are similar to viruses but are more difficult to get rid of. A trojan does not replicate itself but can also release malicious code. Worms can replicate themselves from system to system without using the original infected file. A virus hoax is an email that tells you to delete a certain file because it purports to be a virus. Then the unsuspecting person does so and unfortunately deletes a file which is required to run his computer. There are few people that have not been affected by these insidious growths. It is fairly difficult to estimate the cost of malware but estimates range from 30 to 200 billion U.S. dollars per year.

With email, problems arise when the attachments carry viruses. As mentioned previously, in 2003, the “Slammer” virus, often considered the most destructive virus of all time,  infected over half a million servers around the world.

As mentioned earlier, a “phishing” email is one where a scammer sends you an email that looks like it came from your bank and it looks very real. It claims that the receiver has  overdrawn and asks you to click on a link to provide personal information like your bank account number, access code for on-line banking, etc.



Piracy has also hit new levels of sophistication in the digital world. The ability to keep up with pirated music, videos and movies is basically impossible. Sales of music CDs have dropped every year for the last decade due to downloading of digital music, such as MP3s.  Although many songs are bought legally, millions of songs are not and this is costly to the music companies and artists. More than one billion pirated music albums were sold in 2003. The International Federation of the Phonograph Industry (IFPI) reported that 35 percent of all music albums sold in 2003 were pirated copies. This is not only taking money away from the artists but also feeding into organized crime and the loss of millions of dollars in lost tax revenue. The downloading of movies from the Internet could also have catastrophic effects on the film industry. The ability to download the latest Hollywood movie awaiting release at the theatre is as simple as doing a search on the Net. It is impossible to stop file sharing sites for music and films since as soon as one is closed another one will surface.

**Authenticity**

Since anybody can put material on the Internet, it is very important to know the difference between a legitimate site and a bogus one. No one monitors the information on the Web therefore it is up to the individual to decide if the material is appropriate. For example, if you wanted to find out more information about treating a case of Poison Ivy, you would be better off to visit the Canadian Medical Association website instead of “Joe’s Underground Clinic” site. Another example is a website citing how to destroy the HIV virus by having the infected person touch a “Zapper” several times a day.  A Zapper is an electrical outdoor appliance to kill mosquitoes and wasps!

Knowing how to evaluate a site simply takes a little skill and experience.

***The URL:***



The URL gives you a good starting point. Websites developed by individual people are not necessarily bad, but they don’t have a higher authority to vouch for them. A personal page is often indicated with a ~ (tilde) in front of the author’s name. Also, any pages hosted on providers such as geocities and AOL are likely to be personal rather than professional pages. These sites are often notoriously inaccurate.

Note the suffix on the website, such as if it is .edu or .gov or .com, etc.  Each site will give its own point of view. Even though you may think a .gov site is legitimate, you must remember that it is still often one person’s point of view only.

If your source is The New York Times site or a health institute, you can be more confident that it will be factual. If you don’t know who the source is, be cautious.

***Publisher Information:***

You need other information to help validate sources that are currently unknown to you. Such information should be available in links such as About Us, Biography, etc. Sometimes if you truncate the URL you can get more info. To do this, you just delete the ending characters in the URL stopping just before each / one at a time until you reach the first single /. This is the page’s server or “publisher”.
For example, if you start with:

http://www.mtsu.edu/~baustin/holo.html

delete from the back (right) end until you get
http://www.mtsu.edu/~baustin

Often you will find information here. Keep going until you get
http://www.mtsu.edu

This is your publisher.

There should be a *Last Updated* date on the page. You need to know if it is current or not.

***Credentials:***

Does the author have any credentials? Are they listed? If not, an email address is only good enough for you to use to politely ask for credentials and possibly permission to use the info presented. Scholarly research should have just as many credentials (references cited or bibliography) posted electronically as they would on the printed page. If a contact email address is something like *joeblo@hotmail.com*, be wary of its legitimacy. (My apologies to joeblo!) Here is also a tip, use a proper email address if you are inserting it in a résumé. It sounds more professional to have *AlDante@mtn.net* instead of *EatMyShorts\_for\_supper@hotmail.com*.

If your article is legitimate, there should be a copyright statement and/or permission to reprint. If not, chances are this article is not original and therefore possibly not correct. Having said that, remember that people can simply copy and paste any text or image onto a website to make it look legitimate. For example, this course could have on the Homepage: “*One of the Top Ten Most Visited Sites in the World!*”  This is, of course, not true, however, who knows in the future!

When you will create your own Web pages and websites in this course, what type of credentials will you have? What would you list on your website to legitimize your information? What would you include or not include? What would you change if you could or had the money to do it?

**Plagiarism and Citing Sources**

***Plagiarism***

Plagiarism refers to the copying of material and giving the impression that it is your own material.  Authenticity refers to the accuracy and legitimacy of the material or website.  Both of these issues have come to the forefront on the Internet.

The ability to copy and paste is very easy today due to the digital format of text and images.  Before computers, people had to write down the material which took a lot longer. Plagiarism can result in getting zero for an assignment, losing privileges on the computer, expulsion from a course, or even being sued.  It is a serious matter and is treated as one in almost all cases.  If you are to quote or reference material from a website, you must acknowledge that site by citing the source.

***Citing Sources***

If somebody is using material from a website, it must be documented.  The referencing includes the following guidelines:

* The website address and page or anchor if necessary
* The author
* The date
* Other material relevant to the citation or quoted material
* Separate items of citations with periods
* Use hanging indents following the first line (usually .5 inches indented)
* List entries alphabetically by author, if there is no author, list the title first

There are three different styles to cite Web sources.  Choose one of the following:

1. **MLA:**

Author. “Title of Page”

Title of Website (underlined). Editor. Publication or update date (date you visited the site). Sponsor (organization that brought the site into being). Date you visited the site (site URL)

2. **APA:**

Author. (Date of Publication). *Title of Webpage*. Month day, and year you visited the site,  URL.

3. **CHICAGO:**

Author. “Title of Page.” Title of Website. URL (date you visited the site).

An example is shown below:

Towel, Scott.. *A Study in Two-Ply Paper.* Retrieved January 13, 2009, from http://www.towelsaregreat.com .

**LESSON 3: Internet Safety and Health**

**Health Related Issues**

There are several health related issues when it comes to Internet use, some are physical and some are emotional.  Typical ailments include:

* Carpal Tunnel Syndrome (CTS)
* Chronic Vision Syndrome (CVS)
* Internet Addictions

Some causes for health concerns include:

* Electromagnetic fields (EMF)

Here is a little more detail about these subjects:

***Carpal Tunnel Syndrome*** (***CTS)***

**

More measurable aches and pains due to computers include neck strains, back problems, and Carpal Tunnel Syndrome.  CTS is caused by the repetitive motion of a particular part of the body, such as when you keep banging your head against the computer when you have lost all the data you entered in the last four days. CTS is extremely common and will usually afflict everybody at some point if a computer is used to any extent. Other variations include iPod finger, BlackBerry thumb, cell phone numb thumb, and Nintendonitis.  Numbness in the hands and wrists is very common and the best way to stop the ailment is to stop using the computer for a few days. In reality, ergonomics help, such as a good table and desk, proper height, good posture and supports for your wrists and arms.

***Chronic Vision Syndrome (CVS)***



Chronic Vision Syndrome is characterized by eye strain associated with prolonged use of computers. Symptoms can include eye irritation, fatigue, difficulty focusing, headaches, backaches and muscle spasms. The pixels on the screen force the user to focus and refocus continuously and this causes stress on the eye muscles. This constant glare of artificial light also throws off the levels of the hormone melatonin in the body. People living in societies where florescent lighting and computer monitors are prominent also suffer from the highest rates of insomnia. Melatonin regulates the body’s sleep patterns and light-dark cycles.

***Internet Addictions***

****

The Internet can be a vehicle for getting hooked on an addiction, as the Internet can be an addiction in itself. Online gambling, for example,  has become a multibillion dollar industry. According to Merrill Lynch, online betting revenues will reach $50 billion by 2010 and balloon to $177 billion by 2017. In addition, there were over 53,000 online gambling sites in 2004. Nancy Petry, a professor at the University of Connecticut’s Center for Gambling Research and Treatment, found that online gamblers were more likely to have serious gambling problems than other gamblers. She states:

*“The availability of Internet gambling may draw individuals who seek out isolated and anonymous contexts for their gambling behaviours. With Internet gambling, it’s going to become a major problem to treat people. Already, only about ten percent of those who have an addiction problem seek help. With Internet gamblers, it’s likely the percentage will be even less.”*

*AngelCiti Entertainment* acquires interests in companies that provide software to the online gaming industry. They estimate that the total amount of money wagered annually worldwide is in excess of one trillion dollars. They say that the growth of the Internet has exceeded the growth of any other communication medium in the history of mankind. The Internet took four years to reach the penetration level that  it took television 13 years and radio 30 years to reach. Online gambling had grown from $17 million in 1996 to $21 *billion* in 2005.

***Electromagnetic fields (EMF)***

**

Artificial light, Internet WiFi areas (hotspots), and computer monitors also emit various levels of electromagnetic field exposure (EMF). This area of study is a contentious one with no conclusive evidence indicating that EMF exposure is dangerous. Symptoms of electrical sensitivity include aches and pains, insomnia, fatigue, and headaches. In 2005, the World Health Organization (WHO) issued a report about this malaise and named it “*electromagnetic hypersensitivity*.” The WHO believes the symptoms are real and can be disabling for those affected by it. The change in power quality caused by the digital variants and pattern of power usage causes more variable electromagnetic fields. This variability does not give a chance for the body to adapt to the EMFs.  Dr. Madga Havas, an associate professor at the Environmental Studies Department of Trent University in Canada has been studying this phenomenon. In 2003, she installed filters at a Toronto private school to “clean up” the EMF. After a six week period, the staff and students felt they could concentrate better and were less fatigued. The staff which was not told of the filters also reported that 60 percent of their classes showed an improvement in student behaviour when the filters were in place.

In early 2006, Lakehead University in Thunder Bay, Ontario banned the implementation of WiFi networks on campus due to the risks associated with wireless connections. The president of the university was concerned about exposing young people to electromagnetic fields. He stated,

*“These are particularly relevant in younger people (who have) fast-growing tissues, and most of our student body are late teenagers and still growing, so it's just a matter of taking precautions and providing an environment that doesn't have a potential associated risk.”*

**The Internet is a wonderful tool with many spectacular applications. However, like everything else, it is important to use it wisely and not over do it!**

**Ewaste: Physical waste generated by technological products**

****

Ewaste is the by-product of computer and Internet technology gone to waste. For example, already by the year 2000, laid end to end, the sheets of paper produced by personal computers each year would circle the earth over 800 times. Much of this paper is from emails that were printed out.  The Internet has certainly created a lot of interest in computers and large servers. Unfortunately, hazardous materials make up a good part of a computer.  Below are some materials found in computers.

* Lead in cathode ray tubes and solder
* Arsenic in older cathode ray tubes
* Antimony trioxide as flame retardants
* Polybrominated flame retardants in plastic casings, cables and circuit boards
* Selenium in circuit boards as power supply rectifiers
* Cadmium in circuit boards and semiconductors
* Chromium in steel as corrosion protection
* Cobalt in steel for structure and magnetivity
* Mercury in switches and housing
* Bisphenol A used to coat CDs and DVDs

The above toxins and chemicals have been linked to a multitude of cancers, abnormal tumour growths, hormone imbalances, diabetes, organ abnormalities, neurological damage, attention disorders, skewed mammary gland development, and infertility.

A report released by the National Safety Council’s Environmental Health Center estimated that the number of obsolete computers in 2004 was estimated at 315 million in the U.S. alone. Also, for every computer that is sold, one becomes obsolete. Most of these computers simply end up in landfills. Most of these hazardous materials listed will also leach into the ground.  Some of the old computers are recycled but they are often sent to China and India to be taken apart. It is usually much cheaper to ship the junk to third world countries than it is to recycle it in North America. The workers in these Asian countries have little knowledge of the hazards of taking computers apart. They usually do not take proper precautions and eventually many become ill from the exposure.

It is important for all computer and Internet users to try to limit the creation of ewaste. Use of the Internet certainly has the potential to reduce paper use because of its digital form. This format allows for storage without having to print it in large quantities.