architecture. All of these works are protected online and cannot be used without written consent. There are websites that offer certain pictures, songs, and other works for free. It is important to first verify the site is legal and read the site's acceptable use policy before using the works.

Copyrighted material online can be referenced and used in certain settings. This is called "**fair use**". "Fair use" grants certain rights for educational use and out-of-print works. As a general rule, referencing works online is legal but actually downloading the work is illegal unless specifically permitted by the owner. http://www.universityofcalifornia.edu/copyright/permission.html is a good reference for determining if a work can be used under "fair use."

Software

When using software, it is important to know and understand what you can and cannot do. This information can be found in the software's End User License Agreement (EULA), which outlines the terms of use. When a user buys software, they are buying the right to use the software. If they want to use the software on two computers, they need to buy two copies of the software. This makes it illegal to share your copy of the software. When buying student software, the user is buying the right for a student to use the software. This makes it illegal for non-students to buy student software; it also typically prohibits even a student using it to create a product for resale.

Music and Movies

If you have a copy of it, you need to have paid for it. It is illegal to have any song on your mp3 player, CDs, or computer that you did not buy. When on the SPU network, it is legal to stream music through iTunes, but downloading the song onto your computer with a program like myTunes is illegal. There is currently no way to share movies legally over the network. Music stores like iTunes and MSN Music have made legal music downloading easy. Movielink and CinemaNow are similar stores for movies.

Your Copyrighted Material

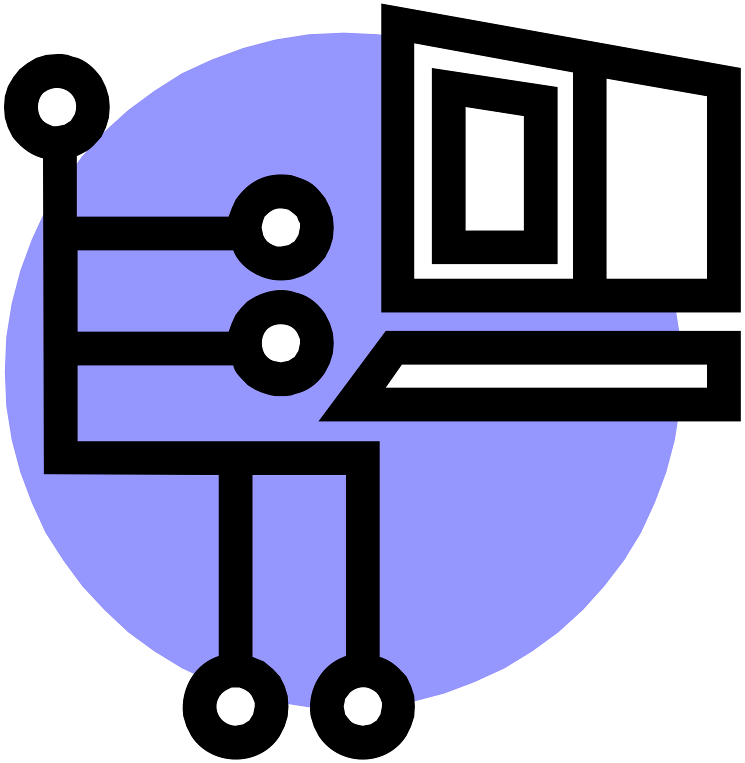
According to copyright laws, the moment a work is created it is copyrighted and the property of its creator. However, when you post something online, it becomes hard to regulate who uses it and how they use it. If a work has potential to be profitable, it might be wise to register the work with the U.S. Copyright Office.

Created for:
CSC 3899—Ethical and Social Issues in Computer Science

Text by: Tim Disney, Doug Harrison, Brad Johnson, Ryan Price, and
Eddie Strickler
Editor: Jason Stegner
Professor: Elaine Weltz

THE TRUTH ABOUT COMPUTERS:

What every computer user needs to know



INTRODUCTION

The purpose of this document is to inform and educate the SPU community of what risks and threats arise from using a computer, specifically in relation to computer networks and the Internet. These are things that effect every computer user and there are measures we can take to protect ourselves. In this new digital age there are a vast array of new threats, ethical and legal concerns, as well as technologies that effect our lives. Everyone needs to be aware of them.

SPU's Acceptable Use Policy outlines what campus resources are available, what individuals using the resources are responsible for, the terms and conditions of their use, and conditions for connecting your personal computers to the network. The SPU community needs to be aware of the Acceptable Use Policy, which can be found at: http://www.spu.edu/CISHelpDesk/computerpolicies/acceptableuse/index.asp

PERSONAL VULNERABILITIES

Viruses

A computer virus is "a dangerous computer program with the characteristic feature of being able to generate copies of itself, and thereby spreading." Being on a campus network, it is the duty of every student to make sure his/her computer is free of viruses. Here are some FAQs and answers:

Is my computer infected?

Chances are, you've had a virus before, and it was really obvious. Here are some signs that your computer could be infected:

- Decreased system performance
- Random reboots or system crashes (Blue Screen of Death in Windows)
- Corrupted or missing files
- Erratic behavior
- Sluggish network access

Any of these symptoms are cause to run a full system scan with a trusted virus scanner.

Do all viruses damage my computer or data?

No, not necessarily. Viruses can also be used to utilize your computer's resources without your permission. In the case of **worms**, the virus may just make countless copies of itself to send out on the network. Other viruses may turn your computer into a **zombie** and use it as a staging area for sending out spam email.

What are good practices for preventing an infection?

Keeping your computer "healthy" requires some work. It is the responsibility of the user to be savvy about keeping their computer protected. Some tips:

— **Install Antivirus software** – This is necessary for any system to have maximum protection. All Windows computers on SPU's network are required to have this software installed. Linux and Macintosh users may be less vulnerable and are not required to use antivirus software, but its use is still strongly advised.

— **Be suspicious** – If you download a program, assume it has a virus and scan it. In fact, don't download it if you don't need it. If your friend IMs you and it has a link, don't click it until you've verified their identity. Don't open attachments in emails (even documents if you weren't expecting one).

— **Back up your data** – Any data that you couldn't imagine being without (e.g. term papers, vacation pictures, music library) should be backed-up on a regular basis

out who will have access to your posted information and how you as the user could control this access.

A good rule of thumb to follow both on personal networking sites and blogs is to ***assume that everyone in the world will view what you post on the Internet***. If you remain aware of the content of your postings and assume everyone can see them, you're much more likely to avoid posting information which could be misused.

Another general rule is that ***less is best***; the smaller the number of the people that has access to your information, the less likely that some one will use it to your detriment.

Email, IM and Other Person To Person Communication

One might expect that this risk of misuse of information would disappear when one switches to email or instant messaging where messages are sent to a particular person or group of persons. However this is not the case

(See the **Hackers** section in **Personal Vulnerabilities**). There are four rules of thumb one could follow to protect oneself from the risks inherent to the using person to person communications over the Internet. They are as follows:

— ***Limit who knows your online contact information*** (e.g. email address, screen name, username, etc.) – Be picky about filling out forms on on-line that require your email address and not posting this information in public places on the Web.

— ***Never pass sensitive personal information*** (e.g. passwords, credit card numbers, social security numbers, etc.) via email or instant messaging.

— ***Be careful about what you open*** – do not open email attachments or hyperlinks that you are not expecting to receive. Also avoid opening emails from people you do not know.

— ***Never respond to spam*** – This merely confirms to the spammers you are in fact reading their advertisements. This includes ignoring opt-out links.

COPYRIGHT AND INTELLECTUAL PROPERTY

Today, most personalized work is protected under copyright laws. Their intent is to encourage creativity in society. With the rise of the Internet, reproduction and distribution of personal works is quite easy. In 2002, it was estimated that 60 million Americans had downloaded music off the Internet. However, this does not make it right.

SPU's Stance

Section 4.0.h of Seattle Pacific University's Acceptable Use Policy outlines the University's position on the issue of copyright and intellectual property. It states that it is the responsibility of the students at Seattle Pacific to follow and obey all laws regarding copyrighted material (including text, music, graphic, photographic files and computer software applications and programs). In addition, it states that in order to share files over the Seattle Pacific network, the sharer must be able to give proof that they are legally sharing the file. The responsibility is not just on the sharer. Anyone who takes a file off a share on the network is responsible to verify that it is legal. Just because a file is on the network does not mean it is legal to take and use. Any illegal file sharing could result in loss of network access and is even grounds for expulsion (Acceptable Use Policy, Section 4.0.h item 4).

The Web

What can be used from the web? Copyright laws protect literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and web sites that are completely off the wall, (i.e. no other sites agree with the information enough to link to it).

Wikipedia is an online encyclopedia that allows anyone to create and edit articles. While the complete openness would seem to cast doubt on the reliability of Wikipedia's articles, it generally works to increase the accuracy and reliability of the articles. Because many people are reading the Wikipedia articles, inaccuracies are quickly found and since anyone can edit the article the errors are corrected.

As with any source of information Wikipedia is not infallible. It should be scrutinized like all online sources. Since anyone (including you) can edit Wikipedia articles, most professors do not allow them to be used as a reference in papers. However, it is often a useful source for background research.

While you should be careful about the information you find online, the same is true of any medium. Periodicals and books are not infallible sources of information and should also be scrutinized.

The SPU Library has an excellent resource for critical evaluation of any information source, online or off, using the acrostic CRITIC. An in depth treatment of this can be found at http://www.spu.edu/depts/library/online_services/handouts_tutorials/handouts/general_library/critic_eval.pdf.

The Internet is a powerful tool that needs to be used wisely. You can find a great deal of information very easily as long as you are careful about the sources you use.

Communication Precautions

The Internet is one of the most widely used means of communication in the world today and the variety of applications and services available for communication through the Internet is rapidly increasing. One of the problems with the popularity of the Internet as a method of personal communication is that many people are unaware that it is not as private and secure as they may wish or believe. We all too often let down our guards.

The largest of risk involved in using the Internet for personal communication is the risk that its information is used by some one in a way which it was not intended for or that harms us. If I post my email address on a forum, I run the risk of that address being picked up by any number of people who wish to send me spam. This risk is not really unique to the Internet; however of the scale of the Internet makes this risk much higher. If I posted a flyer about my lost cat around the neighborhood that had my phone number on it, I run a risk of a telemarketer using it to call me. The difference between this and the previous example is that there maybe only a few hundred people in my neighborhood, whereas it is projected that there are a billion people on the Internet.

Personal Networking Sites

Personal networking sites, which people use for dating, keeping in contact, making friends, and cementing business connections, often have much personal information posted for all to see. The danger of social networking sites is that while they often feel intimate and private, they are not. These sites are often used as information harvesting grounds of targeted and non-targeted advertisers unlike. Worse, many networking sites have become hunting grounds for physical predators.

How Can I Protect Myself?

The primary thing that you can do to protect yourself from information being misused is to be aware that the more people that can access it the more likely that it will be misused. It is important when considering whether to use a service or not to find

(say, once per quarter). In the worst case you might have to reformat your computer; if you backed up, all the important things will still be available.

Spyware

Spyware is software installed on your computer, when you download a program or view a webpage, that sends information about your surfing habits back to its source. It is sometimes installed with our your knowledge, but usually you agree to it in the EULA (see “Software” under Copyright and Intellectual Property, pg 8) Some tips for avoiding spyware:

- **Surf safely** – Did you know that just by browsing to an untrustworthy site you are at risk of being infected with spyware? Resist the urge to go to websites that you have no reason to trust.
- **Download sparingly** – While certain kinds of files (e.g. pictures, videos, audio, and some document files) are safe, many aren’t. Any file which is used to install a program is suspect. Unless it’s from a trusted source, it’s safe to assume that it includes some sort of spyware. If you need the program, look for guarantees that it is spyware free before loading it onto your computer.
- **Clean regularly** – Get in the habit of cleaning your computer on a semi-regular basis. There are several different anti-spyware programs available that are free to use. To name a few, there are Ad Aware, SpyBot, and Microsoft’s AntiSpyware. Just make sure to get the latest definition files before you run the utility for the first time.

Hackers

The term **hacker** is loosely applied to anyone who attempts to gain unauthorized access to a system (or connection). Hackers can range from electronic snoops that can read information you send and receive to the truly malicious hijackers that are able to steal active connections your computer has to web sites. Here are some FAQs and answers:

Can people other than the intended recipient read my email?

Unless you take steps to encrypt outgoing mail, anyone with some computer networking knowledge could potentially read your emails as if they were sent to them, and be completely undetectable in doing so. If you are sending an email with sensitive content, it would be very wise to learn how to encrypt your email messages.

How secure are online transactions?

There is no simple answer to this question. One should always make sure that at the very minimum any sort of financial information is sent over **https** rather than **http**. Https indicates that the connection uses **Secure Socket Layer** (SSL) which encrypts data and uses certificates to verify the source and destination computers. The more prevalent problem today is the security of the web server on which your financial information is stored. Even though sites are required to move this information off their sites immediately, this is not always done which leaves things such as credit card numbers available to any would-be hacker.

Make sure that all online transactions are made with well-known and trusted merchants. An https connection helps, but it is no guarantee of security.

How can I defend my system from hackers?

On the SPU network, hardware firewalls have already been installed by CIS. These are the best defense against outside attacks. You should also make sure the Windows Firewall (or for Mac/Linux users, the equivalent) is enabled. This serves as a second line of defense, and also provides some protection against attacks from inside the SPU network.

The use of strong passwords is also encouraged. Avoid dictionary words, or words that people who know you may be able to guess. A combination of random mixed-case letters and numbers is best, though that may be hard to remember. Also, if possible your password should be changed occasionally. Finally, don't use the same password for all your different accounts.

Online ID Theft

In the course of a normal day, you may go online and order tickets to a concert, pay your credit card bill, check the balance on your checking account, open an e-mail from Urban Outfitters and click a link that takes you to their latest sale. For most savvy online users these activities are a normal part of the daily routine. No big thing, right? Think again. An online identity thief is interested in your every click.

Online Identify theft is on the increase, and there are several methods that are used:

- The most common method of online theft is **phishing**, where e-mails are sent asking users to verify personal information via links to websites that appear valid (but aren't).
- **Pharming** is a method done by redirecting web users from legitimate web sites to fraudulent sites without any noticeable indication. The users are then prompted to provide whatever data the owners of the web site can get.
- Other methods of identify theft include installing spyware on a PC that logs the user's keystrokes and the outright hacking of banking, credit card company and credit bureau computer systems.

Security experts advise people to never provide data such as social security and credit card numbers via e-mail solicitations. They also urge banks not to use social security numbers as a means of verifying customer accounts, and allow customers to opt out of sharing their information with credit card companies and retailers.

To deter thieves from accessing your personal information:

— **Guard your socialsecurity number like it's made of gold.** Obtaining SSNs is the easiest way for an identity thief to assume your identity. Never carry your Social Security card on your person or enter it in response to an unsolicited e-mail. If your bank uses Social Security Numbers as a primary means of identifying you, ask for a PIN, chosen by you, that is required before any data is released. If they refuse, get a new bank.

— **Never click on hyperlinks sent in unsolicited emails.** Whenever a website requests personal information, ensure that it is secure (See "How secure are online transactions?" in Personal Vulnerabilities, pg 3)

— **Follow CIS Acceptable Use Policy** that requires the following of ResNet PCs:
o The system is patched with current operating system updates;
o Is virus-free; and
o Is running a current, auto-updating anti-virus program.

— **Use strong passwords** (see "How can I defend my system from hackers?" in Personal Vulnerabilities, pg 4)

— **Keep your personal information in a secure place at home**, especially if you have roommates, employ outside help, or are having work done in your residence.

One more piece of advice**.** By law, you are entitled to a free copy of your credit history once a year. Go to http://www.annualcreditreport.com/ for a free credit report.

Internet Validity

The Internet is a huge place with billions and billions of pages on every conceivable topic. Since there are no organizations to review the content of web pages, anyone can post anything online. Because of this, there is a large amount of inaccurate information to be found on the Internet. It is important to be careful with what you find online.

Here are some examples of some with false and sometimes bizarre information. Be cautious of sites like these.

- http://www.gatt.org is a spoof of the World Trade Organization web site. It has the same design as the WTO site and at first glance it is hard to tell the difference between the two.
- http://147.129.226.1/library/research/AIDSFACTS.htm is a collection of untrue "facts" about woman and AIDS. It was created as an educational tool to show the dangers of false information on the internet and has a disclaimer explaining its purpose.
- http://www.dhmo.org/ is a joke site warning about the dangers of dihydrogen monoxide (H_2O).
- http://martinlutherking.org/ is a racist web site which claims to provide the "real" history of Martin Luther King Jr., and contains completely false "facts" about Dr. King's life. WARNING: this site contains offensive material!

Here are some things to keep in mind when evaluating online resources:

— **Check to see if the site is from a reputable organization.** For instance, you can probably trust http://www.cnn.com while you may want to be careful of http://www.bobshomepage.com.

— **Check the interests.** Be careful of organizations that have a vested interest in the information. For example, a company selling a product probably won't discuss problems with their product. Watch out for bias.

— **Check the site for references.** Make sure there is a way to verify the information presented.

— **Make sure authorship and contact information are given.**

— **Make sure the information is current.**

— **Find multiple sources.** Multiples sources give support to each other. Be wary of information that can only be found on one site.

— **Check the domain name** (.com .gov .edu .net .mil). This can quickly give you a broad idea what the purpose of the site is.

— **Be careful of phishing sites.** (see "phishing" in Online ID Theft, pg 4)

If you want to cite a web page in a paper for class you should check with your professor about what is appropriate. Different professors have different standards about what online resources can be used.

Google and Wikipedia

These two web sites deserve special mention on the subject of online validity. Google's web search (as well as most other search engines today) returns results based on the number of web pages linking to each other. This means that a web site at the top of a search result will have many other sites that link to it. This allows the Internet to in essence "vote" for relevant web pages. It is important to realize that this does not mean the results necessarily contain accurate information (For example, the racist web site http://martinlutherking.org/ is usually in the top ten results for "martin luther king"). In general however, it does a fairly good job of weeding out