



C3 Desk Reference 2007

CYBER**ETHICS**

CYBER**SAFETY**

CYBER**SECURITY**

QUICK TIPS
&
BEST PRACTICES

PAMELA SHURKIN

Table of Contents

Introduction	1
Website Credibility	2
Netiquette	3
Acronyms & Emoticons	4
Plagiarism	5
Copyright & Fair Use	6
Acceptable Use Policies	7
Phishing & Identity Theft	8
Backing up	9
Passwords	10
Cybersafety - Recommended Links	11
On-line Bullying	12
Hoaxes	13
Cybersecurity	14
Spyware	15
Works Cited	16
Blank Sheets for Your Notes	17

Computers and the Internet have opened the door to instant communication, information sharing, and faster financial transactions. People are becoming increasingly savvy when it comes to technology and as a result more people than ever store their personal information on computers, both on- and off-line. This guide will provide tips for staying safe online, securing one's privacy, and proper etiquette in cyberspace.

Though a useful introduction, this is not a comprehensive resource and may already be dated because technological change occurs so rapidly. This simple and easy to understand reference is intended to introduce children, adults of all ages, and tech savvies to many important issues that one should be aware of when using a computer or venturing online.

This guide should be located near a computer. The blank pages in the back are included for your notes. You may want to include important phone numbers for troubleshooting computer and Internet problems.

~Pamela Shurkin

1/21/2007

1

Website Credibility

A Credible website will¹:

1. Provide [links](#) to verify the content found on their website.
2. Include photographs and a physical address proving they are a trustworthy entity.
3. Share credentials or bios of individuals to demonstrate their areas of expertise.



Image Source: Microsoft® Office 2003 Clipart

4. Include contact information (phone, email, mailing address)
5. Look professional and be easy to navigate.

6. Update the content regularly.
7. Be written in a clear, direct, and sincere tone.
8. Avoid posting ads or pop-ups.
9. ...Not have any typos.



Image Source: Microsoft® Office 2003 Clipart



Image Source: Microsoft® Office 2003 Clipart

<http://www>

Image Source: Microsoft® Office 2003 Clipart

Check the Websites you visit most frequently to see if they are credible!

Visit <http://www.cast.org/bobby> to learn how your favorite websites measure up on the quality, accessibility, and privacy test!

Netiquette

Definition: Online etiquette or how to behave properly on the Internet.

Do'sⁱⁱ:

- ~Stay on point and keep your message as short as possible and on topic.
- ~Remember that everything you post online is public and could resurface in the future, so be careful what you write.
- ~Re-read and edit postings to blogs, online communities, and emails before you click submit or send. Check for spelling and grammar errors.
- ~Provide instructions for unsubscribing from a mailing list if sending a mass e-mail.

Neverⁱⁱⁱ:

- ~Use CAPITAL letters, it appears that you are shouting and is harder to read.
- ~Provoke someone online or participate in "flaming" (an online battle of insults). Instead, contact the ISP (Internet Service Provider) or message board moderator.
- ~Use a business e-mail account for personal correspondence.

**How is your netiquette?
Take this short online quiz & find out!**

<http://www.learnthenet.com/English/flashtest/netiquette.htm>



Acronyms & Emoticons

Acronyms are abbreviations of multiple words; online slang.

Emoticons are symbols of emotion used in emails, IM's, and other written online communication to add personality to the conversation.

Just a few Acronyms

afk = away from the keyboard
asl = age, sex, location
brb = be right back
j/k = just kidding
lau = laughing at you
m.o = make out
ph33r = fear
p.o.s = parent over shoulder
ttyl = talk to you later
wayd = what are you doing

Want to learn more?

Check out the internet slang dictionary and translator at www.noslang.com

Commonly used emoticons:

: -)	Smile	: - P	Sticking out tongue
: - (Frown	O : -)	Angel
; -)	Wink	: - D	Laughing
: - O	Uh Oh!	> : - O	Yelling
: - *	Kiss	: ~ - (Crying
: - X	Sealed Lips	: - /	Hmmm

Find more fun emoticons at:

<http://computeruser.com/resources/dictionary/emoticons.html>

Plagiarism

Definition: Claiming someone else's work (written, music, film, etc...) as your own or

using another author's work without giving them proper credit.

How to Avoid Plagiarism

- ~Use quotes if using an exact phrase from a written work.
- ~Include a citation if you paraphrase another person's ideas.
- ~Credit your sources when reprinting any visual material or image.
- ~Include information about your sources as you take notes.
- ~Clearly mark direct quotes, summarized ideas, and your own thoughts to avoid accidental plagiarism.

Cyber Plagiarism Clues for Parents & Teachers^{iv}

- ~Typos, formatting irregularities, unusual punctuation.
- ~Dated material
- ~The tone and vocabulary are inconsistent with the student's usual work
- ~URL's and dates are found at the bottom of the student's work

APA Format for Online Sources^v

Online Periodical → Author, A. A., Author, B. B., & Author, C. C. (2000). Title of article. *Title of Periodical*, xx, xxxxxx. Retrieved month day, year, from source.

Online Document → Author, A. A. (2000). *Title of work*. Retrieved month day, year, from source.

Check out these sites for more tips & proper formatting techniques:

<http://www.plagiarism.org/>

<http://owl.english.purdue.edu/owl/resource/589/01/>

Copyright & Fair Use

Copyright laws protect the integrity of an author's original creation (including writing,

music, art, or any other unique work). The copyright is effective immediately after the work is created and protects the legal interests of the author.

Fair Use describes the legal use of copy written materials by educators for teaching purposes.

Consider the Four Factor Test *to decide if something qualifies as Fair Use*^{vi}.

1. What is the purpose of the work?
2. What is the nature of the work?
3. What is the amount and substantiality of the work you are using as compared to the work as a whole?
4. What is the effect of your use on the market value of the original work?



Test your knowledge with the following quick quizzes.

The Copyright Tutorial Test:

<http://www.lib.utsystem.edu/copyright/test.html>

The Research Ethics Study Quiz:

http://www.smccd.net/accounts/webready/lesson9_fairuse-check.asp

6

Acceptable Use Policies (AUP)

Definition: AUP's contain the Internet service provider's permitted actions



and behaviors. Liability disclaimers and a list of behaviors that will result in a user's account being closed are also included in the AUP.

Image Source: Microsoft®
Office 2003 Clipart

Read through your ISP's AUP.

Here are links to popular ISP Acceptable Use Policies. Can't find yours in the list? Search the ISP's homepage for common terms to describe an AUP (AUP, Acceptable Use Policy, Terms and Conditions, Terms of Service, Policies and Procedures).

Comcast: <http://www.comcast.net/terms/use.jsp>

Verizon: <http://www22.verizon.com/about/privacy/terms/>

American Online: <http://www.atdn.net/aup.shtml>

Google: http://www.google.com/terms_of_service.html

Earthlink: <http://www.earthlink.net/about/policies/use/>

AT&T: <http://www.att.net/general-info/terms-dsl-data.html>

Phishing & Identity Theft

Phishing is an attempt to con someone out of personal information such as passwords

or financial information by pretending to be a legitimate business or Website. This criminal activity is usually conducted via an e-mail or Instant Messenger and may lead to **identity theft** (stealing your personal information for another person's benefit).

How to Avoid Phishing Scams^{vii}

- ☞ Be suspicious of emails that claim to be urgent and ask for personal financial information such as social security numbers, bank or credit card account information, date of birth, or passwords. These emails may be fraudulent and attempting to steal your identity.
- ☞ Look to see if the email addresses you by your first and/or last name. Scams tend not to be personalized.
- ☞ Suspect links to Web pages that you receive via emails, chats, or instant messages. Make sure you know who sent you the link and where they are sending you online.
- ☞ Do not fill out forms sent to you in an email asking for financial information. Make sure you are at a secure Website any time you submit credit card information online.
- ☞ Always look at the address line to ensure you are visiting a legitimate Website. Look for misspellings, typos, or clear indicators that you are at a scam site.
- ☞ Regularly check your financial accounts to make sure all transactions are legitimate.
- ☞ Update your Web browser with security patches.

Report Phishing e-mails to:

reportphishing@antiphishing.org

apam@uce.gov (The Federal Trade Commission)

www.ic3.gov (The FBI's Internet Crime Complaint Center)

Always include the original email and original header in your message.

8

Backing up

Are you prepared with backup files,
just in case...

~a virus corrupts your files?

~your computer crashes?

~a fire destroys your computer?

~someone accidentally deletes your files?

Image Source: Microsoft® Office 2003 Clipart

Make sure you back up important data and computer files in case you unintentionally lose your information. Keep backups far from your computer, or in another physical location like a safety deposit box, if possible. Make multiple copies of your backup files. Protect your files with passwords^{viii}.

Backup your files using: a zip drive, a thumb/flash drive; CD or DVD; or an online backup service^{ix}.

Types of files to backup^x:











-  **Contact Information**
-  **Photographs**
-  **Music downloaded from the Internet**
-  **Calendar**
-  **Bookmarks**
-  **Bank records**
-  **Academic files**
-  **Work related files**
-  **Personal files**
-  **Software downloaded from the Internet**



Image Source: Microsoft®
Office 2003 Clipart

Definition: Keys used to protect and access computer and online accounts.

Strong Passwords...

- ~are between 8-14 characters in length.
- ~combine letters, numbers, symbols, capital and lower case letters.
- ~use less common characters (ex. :, <, ", %)

Weak Passwords...

- ~contain sequences (123456 or ghijkl)
- ~contain your birthday, social security number, or address
- ~use words in the dictionary and word written backwards.



Image Source: Microsoft®
Office 2003 Clipart

Tips

- ~Change your passwords regularly.
- ~Keep your password secret. Don't share with friends or family and never provide your password to anyone over email since most requests are fraudulent.
- ~Avoid using passwords on public computers.

If your password is stolen...

- ~notify authorities as soon as you notice suspicious activity.
- ~close affected accounts
- ~change all of your passwords on all of your online accounts.
- ~place a fraud alert on your credit reports. Contact: Equifax (800) 525-6285; Experian (888) 397-3742; and TransUnion (800) 680-7289

Still unsure if your passwords are strong ?

Visit Microsoft's password checker:



Image Source: Microsoft®
Office 2003 Clipart

http://www.microsoft.com/athome/security/privacy/password_checker.msp

Find posters about passwords to hang up by your computer:

<http://www.itd.umich.edu/posters/>

Cybersafety - Recommended Links

This term encompasses topics covered in this guide including identity theft, cyberbullying, and scams as well as other important issues an Internet user should learn about. Follow these links to learn more about Cybersafety issues. Many of these websites have sections targeting people of different ages.

<http://www.staysafeonline.info/>

<http://www.wiredsafety.org/>

<http://www.netsmartz.org/>

<http://www.chatdanger.com/>

<http://www.kidsmart.org.uk/>

<http://www.netaddiction.com/>

http://www.educause.edu/content.asp?PAGE_ID=720&bhcp=1

<http://www.getnetworkise.org/>

<http://www.safety-council.org/info/child/webrules.html>

<http://www.mcgruffspo.com/cybersafetysat.html>

<http://www.cyber-safety.com/>

www.wiredkids.org

www.ikeepsafe.org

<http://www.fbi.gov/fbikids.htm>

<http://www.sesameworkshop.org/parents/solutions/information/listing.php?categoryId=6426§ionKey=safety>

<http://disney.go.com/webtoons/today/index.html>

<http://www.cyberspacers.com/home.html>

<http://www.safekids.com/>

Definition: Also known as "cyberbullying."

Online social aggression which may harass, threaten, intimidate or embarrass someone through emails, IM, chat rooms, or any other online environment.

Forms of Cyberbullying^{xii}

Flaming: Using angry language to provoke an online fight

Outing: Sharing secrets

Denigration: Online gossip that may damage a person's reputation

Impersonation: Pretending to be someone else

Harassment: Repeatedly sending unwanted emails or messages

Trickery: Obtain a secret by tricking someone and then sharing it online

Exclusion: Leaving someone out of a group

Cyberstalking: Repeated online harassment

Signs someone is a victim of a cyberbully^{xiii}

- 👁 S/he closes computer windows when people enter the room
- 👁 Changes in behavior
- 👁 S/he has trouble sleeping or has nightmares
- 👁 S/he avoids school
- 👁 S/he suddenly uses the computer less frequently
- 👁 S/he is performing less well in school

Tips for Parents^{xiv}

~ Talk with your children and make sure they feel comfortable coming to you with their problems.

~ Define acceptable online behavior and set consequences for misusing the Internet.

~ Find out and use safety controls offered through your internet service provider.

~ Ask your child to show you how to do a task online. You will learn how cyber savvy s/he is while boosting their self-esteem.

~ Work with your child's school.

Definition: False messages, sometimes in the form of a chain letter, sent over e-mail to harass, see how far the message will travel, con money from people, or damage someone's reputation.

Image Source: Microsoft®
Office 2003 Clipart



**TIP: If you receive a hoax,
don't become a victim,
DELETE IT!**

Recognizing a Hoax

- ~The email asks you to send the message to a wide audience.
- ~The message uses technical sounding language to appear credible.
- ~Chain letters have a hook, threat, and request.

Types of Hoaxes

Virus Warnings: These are untrue and warn users about viruses and other malicious code.

Urban Myths: These false stories sound true enough to believe but never really occurred.

Give Aways: Passing this email along will get you a free gift from a big company.

Sympathy Letters: A sick person wants you to pass this email around the world as their dying wish (or something similar).

Chain Letters: These threaten you with bad luck, computer problems, or something undesirable will happen to someone else if you don't pass along the message.

View specific examples of these types of hoaxes and others at: <http://hoaxbusters.ciac.org/>.

Stay safe online! Follow the National Cyber Security Alliance's Top 8 Cyber Security Practices^{xvi}

1. Protect your personal information.

Never share your personal information with anyone unless you know how it is going to be used and protected. Read the fine print! Look over privacy policies posted on websites.



Image Source: Microsoft®
Office 2003 Clipart

2. Know who you're dealing with online. Don't open an email if you do not know who sent it to you. Always clearly label attachment files you send via email. Don't be too trusting, you never know who you are *really* communicating with online.

3. Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.

4. Be sure to set up your operating system and Web browser software properly, and update them regularly.

5. Use strong passwords or strong authentication technology to help protect your personal information. Don't share your passwords with *anyone*!

6. Back up important files. Know where your original system start up disks are and keep them safe and accessible.

7. Learn what to do if something goes wrong. Keep this guide handy and use the blank pages in the back to add any additional tips or important phone numbers.

8. Protect your children online. Keep your computer in a public room. Read through this guide book with your children and make sure they understand the importance of protecting their personal information. Set up parental controls. Assess how cyber savvy your child is but asking them how to perform an online task. Talk with your children!

Spyware is a type of program that secretly watches and tracks what a computer user does online and then sends that information over the Internet. Spyware is dangerous because it may track each website your visit, launch pop-ups, or even record what you type.

Signs of Spyware^{xvii}

- ~Pop-up advertisements
 - ~Your settings have changed
 - ~Your computer is slower than normal
 - ~Your web browser has new components you didn't download
-

Get Rid of Spyware!

Download one of these tools.

<http://www.trendmicro.com/spyware-scan/>

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

<http://www.download.com/3000-2144-10045910.html>

<http://www.spybot.info/>

- i Fogg, B.J. (May 2002). "Stanford Guidelines for Web Credibility." A Research Summary from the Stanford Persuasive Technology Lab. Stanford University. www.webcredibility.org/guidelines Fogg, B.J. (May 2002). "Stanford Guidelines for Web Credibility." A Research Summary from the Stanford Persuasive Technology Lab. Stanford University. Accessed 20 January 2007. www.webcredibility.org/guidelines
- ii "Master the basics: Netiquette." Accessed 20 January 2007. <http://www.learnthenet.com/English/html/09netiq.htm>
- iii "Master the basics: Netiquette." Accessed 20 January 2007. <http://www.learnthenet.com/English/html/09netiq.htm>
- iv Evans, J. (2000). The new plagiarism in higher education: From selection to reflection. *Interactions*, 4 (2). Retrieved 20 January 2007. <http://www.warwick.ac.uk/ETS/interactions/vol4no2/evans.htm>
- v "APA Style Essentials." Retrieved 20 January 2007. http://www.vanguard.edu/faculty/ddegelman/index.aspx?doc_id=796
- vi "Four Factor Test" Retrieved 20 January 2007. http://depts.washington.edu/uwcopy/Copyright_Law/Fair_Use/Four.php
- vii "Consumer Advice: How to Avoid Phishing Scams." Retrieved 21 January 22, 2007. http://anitphishing.org/consumer_rec.html
- viii "Tips for protecting your backup files." Retrieved 20 January 2007. <http://www.microsoft.com/athome/security/update/protectbackup.mspx>
- ix "How to choose an external storage format for backup files." Retrieved 20 January 2007. <http://www.microsoft.com/athome/security/update/wherebackup.mspx>
- x "How to decide what data to back up." Retrieved 20 January 2007. <http://www.microsoft.com/athome/security/update/backup.mspx>
- xi "Strong passwords: How to create and use them." Retrieved 20 January 2007. <http://www.microsoft.com/athome/security/privacy/password.mspx>
- xii "An Educator's Guide to Cyber bullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress." Accessed 16 January 2007. <http://www.cyberbully.org>
- xiii Source: Community Alliance for York Region Education. "Put the Breaks on Bullying." Accessed 16 January 2007. <http://www.yrdsb.edu.on.ca/page.cfm?id=IIC000023>
- xiv www.connectforkids.org Accessed 16 January 2007.
- xv <http://hoaxbusters.ciac.org/> Accessed 20 January 2007
- xvi "Top 8 Cyber Security Practices" Accessed 20 January 2007. <http://www.staysafeonline.info/practices/index.html>
- xvii "Signs of Spyware: Are you being watched?" Retrieved 21 January 2007. <http://www.microsoft.com/athome/security/spyware/spywaresigns.mspx>

