Cyber-Safety for Everyone: from Kids to Elders

M. E. Kabay, PhD, CISSP

Cyber-Safety for Everyone:
From Kids to Elders

This version is a beta-test. The next release will have an International Standard Book Number (ISBN) and will be widely available.

Published by the author at
Accura Printing / P. O. Box 529 / South Barre, VT 05670

Table of Contents

FOREWORD

By Richard Schneider, RADM USCG (Ret.)
President of Norwich University

I am happy to welcome you to *Cyber-Safety for All: From Kids to Elders* written by Norwich University Professor M. E. Kabay.

In today's world, our students – and everyone's children – are exposed to dangers that are rarely completely new but are definitely closer than they once were. This booklet will help all of us stay on guard when we are using the Internet for e-mail, instant messaging, the USENET and the World Wide Web. These wonderful tools offer the promise of tremendous power to learn and to communicate, to bring people together and even to bring nations together. With open discussion of ideas and values among adults and children, we can safeguard our young people – and even grownups – against some of the abuses occurring through the Internet.

This booklet started off as a special project to serve the spouses of Norwich University Trustees in the Spring of 2002. I am delighted to be able to distribute a copy to every incoming student at the University starting with the fall 2002 term; in addition, we are giving a copy to every faculty member, staff member and Trustee of the University.

Finally, I am proud that Dr. Kabay has chosen to put a copy of the entire text of the booklet up on a Norwich University Web site for free access by anyone. This is in keeping with the Norwich ideal of service to the nation.

Have fun reading the book!

Northfield, Vermont
August 2002

PREFACE

I wrote this booklet to help people of all ages protect themselves and their loved ones from people who use the Internet and other aspects of modern telecommunications to harm others. I have kept the writing simple and direct, usually addressing the reader as if we were talking about these issues face-to-face.

This entire document is available free for non-commercial use as a printable PDF file at

http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf

and I encourage you to let others know about it.

If you find errors – especially broken links to Web pages – I would appreciate your letting me know about them so I can fix them in the next edition.

ACKNOWLEDGEMENTS

I thank my colleagues at Norwich University and in particular, Tom Aldrich, Elizabeth Kennedy, Michael McKean, Richard Schneider and Phil Susmann, for their enthusiastic support and encouragement throughout the preparation of this booklet.

As always, I thank my beloved wife, Deborah Black, light of my life, for everything, including in particular her expert proof-reading and editing of the text.

Northfield, Vermont – August 2002
e-mail: **mkabay@norwich.edu**
Website: **http://www2.norwich.edu/mkabay**

Cyber-Safety for Everyone: from Kids to Elders

M. E. Kabay, PhD, CISSP
Assoc. Prof. Information Assurance
Department of Computer Information Systems,
Division of Business, Norwich University

1 Introduction

Adults, children, parents, grandparents, teachers, office-workers: we all face a new area of danger – the Internet. This booklet reviews the dangers that people can meet on the Internet and then examine some of the technology that is helpful in preventing harm.

Here is a list of some of the dangers children and adults routinely encounter on the Internet:

- pedophiles
- online dating and cybersex
- hate groups
- pornography
- incorrect information
- hoaxes
- threats
- viruses and other malicious self-replicating code
- junk e-mail
- chain letters and Ponzi schemes
- get-rich-quick schemes
- Nigerian 4-1-9 scam
- stolen software
- stolen music and video
- plagiarism
- criminal hackers & hacktivists
- online auctions
- online gambling
- buying on the Web
- games
- spyware and scumware
- addiction
- theft of identity.

In this booklet, each chapter ends with a list of *practical guidelines* for discussion and action and a list of *resources* for further study. *Italicized* references are to published books; "enquoted references" are for articles on the Web; Capitalized Plain Text refers to organizations or projects.

Please let me know about any broken links in the URLs provided in this booklet. Write to **mkabay@norwich.edu** and please specify which URL no longer works.

Cyber-Safety

General Resources:

- "A Parent's Guide to Internet Safety" (English and Spanish versions available). **http://www.fbi.gov/publications/pguide/pguide.htm**
- Better Business Bureau online publications list **http://www.bbb.org/library/searchBySubject.asp**
- Children's Partnership Online **http://www.childrenspartnership.org/**
- Children's Protection and Advocacy Coalition **http://www.thecpac.com/index3.html**
- "Cybersafety Guidelines" (Plainsboro NJ Police) **http://www.plainsboropolice.com/cybersafety.htm**
- *Coping With Dangers on the Internet : A Teen's Guide to Staying Safe Online* (2000) by Kevin F. Rothman. Rosen Publishing Group, ISBN 0-8239-3201-X.
- *Cybersafety : Surfing Safely Online* (in press; due July 2001) by Joan Vos MacDonald. Enslow Publishers, ISBN 0-7660-1580-7.
- GetNetWise **http://www.getnetwise.org/**
- *Internet & Computer Ethics for Kids (and Parents & Teachers Who Haven't Got a Clue)* (2001) by Winn Schwartau. Inter-Pact (Seminole, FL), ISBN 0-9628-7005-6. Available from Interpact at 1 (727) 393-6600.
- "Kids & Youth Educational Page" from the FBI **http://www.fbi.gov/kids/6th12th.htm**
- "Kids Page – Kindergarten to 5th Grade" from the FBI **http://www.fbi.gov/kids/k5th/kidsk5th.htm**
- "Sociology of Internet/Cyberspace" – For a scholarly and thorough set of readings, see course materials for a 1999 course by Prof. Carl Kuneo of McMaster University **http://socserv.mcmaster.ca/soc/courses/soc4jj3_99/sociology4jj3.htm#IPurpose**.

2 Pedophiles

Let's start with pedophiles. Pedophilia is defined as sexual arousal in response to contact with or images of prepubescent children. Some pedophiles misrepresent themselves as youngsters in chat rooms or via e-mail and trick children into forming friendships with what they believe are peers. In one notorious case, Paul Brown, Jr, a 47-year-old, 400-pound man, misrepresented himself as a 15 year-old boy in e-mail to a 12-year old girl in New Jersey. The victim's mother stumbled onto the long-range relationship when she found a package from her daughter to a man she didn't know sitting on her own doorstep; the child had put the wrong postage on it and the Post Office had sent it back. Opening the package, she found a video tape. On that video tape she found to her horror that her little girl had been cavorting naked in front of the family video camera. Frantically, the distraught mother searched her daughter's room and discovered a pair of size 44 men's underpants in one of the child's bureau drawers.

Brown was arrested in February 1997. Police found correspondence with at least ten other teenaged girls across the country through which Brown convinced his young victims, some as young as 12, to perform various sexual acts in front of cameras and to send him the pictures and videotapes. He pleaded guilty in June to enticing a minor into making pornography. In August of 1997, at his sentencing hearing, one of his many victims told the court that she had suffered ridicule and humiliation as a result of her entrapment and had left her school to escape the trauma. She accused Brown of emotional rape. Displaying an astonishing interpretation of his own behavior, Brown said at his sentencing hearing, "It was just bad judgment on my part." Using good judgment, the court sentenced him to five years incarceration.

In March 2000, Patrick Naughton, a former executive of the INFOSEEK online company, pleaded guilty to having crossed state lines to commit statutory rape of a child. In August, FBI officials said that Naughton had been providing help in law enforcement investigations of pedophilia on the 'Net. In return for his cooperation, prosecutors asked the court for five years of probation (instead of a possible 15 years in prison), counseling, a $20,000 fine (instead of the maximum $250,000) and an agreement not to have "unapproved" contact with children and to stay out of sex-chatrooms online.

The problem of Internet-mediated pedophile stalking has reached international dimensions. In January 1999, police forces around the world cooperated to track and close down a worldwide ring of pedophiles trafficking in child pornography through the 'Net.

In June 2000, child safety experts warned the U.S. congressional committee on child online protection that with the average of age of online users declining (children between the ages of two and seven are among the fastest growing user cohorts on the Internet), children increasingly are put at risk by their careless or ignorant online activities. Parry Aftab, a children's advocate, told committee members that 3,000 children were kidnapped in the U.S. in 1999 after responding to online messages posted by their abductors. A recent survey of teenage girls found that 12% admitted having agreed to meet strangers who'd contacted them online.

Pedophiles

Practical recommendations for parents and others for protecting children against online pedophiles. Teachers and other caregivers can adapt these principles for the specific circumstances of their relationship with the children for whom they are responsible:

- Explain the dangers of communicating with strangers via the 'Net in the same terms that you discuss the dangers of talking to strangers anywhere else.

- Alert children to the questionable identity of anyone they meet exclusively through the 'Net or via e-mail. Discuss the possibility that people may not actually be what they claim to be online.

- It is important that children feel confident of a supportive response from their parents when raising these issues. Establish a calm atmosphere so that children will not fear your reactions if they are troubled by what they encounter online. Worst of all would be to punish a child for reporting a disturbing incident.

- Tell children not to give their address to strangers they meet electronically.

- Children should not send pictures of themselves to strangers.

- Make a practice of discussing online relationships in a friendly and open way at home. Show interest in the new friends without expressing hostility or suspicion; ask to participate in some of the online chats and e-mail correspondence. Invite your children to sit in with you during your own online interactions.

- If a child feels that another child they have met online is becoming a good friend, parents should contact the "child's" parents by phone and, eventually, in person before allowing contacts.

- If a child wants to meet someone met over the Internet, be sure that a parent is involved at all stages. Never let a child meet anyone in the real world that they have met only on the 'Net. Any attempt to induce a child to meet the correspondent alone or secretly should be reported to local police authorities for investigation.

- Make it clear that anyone who suggests hiding an online relationship from the child's parents is already doing something wrong.

- Make it clear to your children that no one has the right to send them age-inappropriate, sexually-suggestive or frankly pornographic materials, whether written or pictorial. Suggestions that children engage in virtual sex play or sexual fantasies should be reported to parents right away. Also remember that making, transmitting and storing child pornography is a felony; report such cases to local police authorities at once.

- Children receiving a request for anything unusual (for example, a request for a piece of clothing or for nude pictures) should immediately report the incident to their parents.

Pedophiles

Resources:

- "Child pornography." **http://broadcast.webpoint.com/wphl/cybersafe/cybersafe_fbi.htm**
- "FBI warns of child exploitation." **http://www.fbi.gov/contact/fo/detroit/crimes2.htm**
- "In plain site: Pedophiles online, How to protect children." **http://www.thecpac.com/protect.html**
- "Internet safety: Warning signs." **http://www.fbi.gov/contact/fo/norfolk/intnet.htm**
- "Parents can protect their children from child predators roaming the Internet: Six simple guidelines." **http://www.yellodyno.com/html/inetpeds.html**
- "When to call the FBI." **http://broadcast.webpoint.com/wphl/cybersafe/cybersafe_fbi2.htm**
- Children's Protection and Advocacy Coalition **http://www.thecpac.com/index3.html**
- Gado, M. (2000). "Pedophiles and child molesters: The slaughter of innocence." **http://www.crimelibrary.com/serial/pedophiles/**
- Guarding Our Children's Innocence Against Pedophiles. **http://modena.intergate.ca/personal/ranubis/**
- Kincaid, J. R. (2000). "Hunting pedophiles on the Net: Is the truth about cybercrimes against children tamer than fiction?" **http://www.salon.com/mwt/feature/2000/08/24/cyber_menace/**
- Lovell, J. (2001). "Pedophiles flooding British Internet chat rooms." **http://www.siliconvalley.com/docs/news/reuters_wire/1046323l.htm**
- Monahan, M. A. (date unknown). "Protecting children from pedophiles." **http://www.afn.org/~monica/**
- Ratliff, L. (1997). "Online stalking and pedophiles: Protect yourself and your family." **http://www.carteret.com/children/**

3 Online Dating and Cybersex

There are thousands of sites on the Web specializing in helping people meet each other. Chat rooms and bulletin board systems are ways for people with similar interests to communicate about their hobbies and lifestyles; however, there are sites that specialize in helping people find others who match particular profiles. Some of these sites are free; others charge fees for participation. Dating service sites usually explicitly restrict participation to people over 18 years old, but most of them depend on possession of a credit card as their sole mechanism for authenticating age. It is very difficult to exclude teenagers or a younger children from such sites if they have access to credit card numbers.

It might be an eye-opener for parents and teachers to type in "online dating" in the search field of a search engine such as Google **http://www.google.com** and then visit a few of the sites to get a sense of what's going on. If children post information about themselves in such a cyberspace locale, even with false information claiming that they are adults, there is a real risk of attracting unsavory characters or perhaps ordinary people who can become angry at being tricked into exposing their feelings to an imposter.

In addition to match-making, users of the Internet can also get involved in *cybersex*. People chatting online can describe themselves or each other in sexual interactions that may be inappropriate for youngsters. Such online chat has also been implicated in a number of divorces, since many spouses find it wholly inappropriate that their partner is getting sexually involved with a stranger via the Internet – even if it *is* merely "virtually."

Practical Guidelines for Parents and Teachers:

- Discuss online dating with children so they understand what's involved.
- Ensure that children understand why it is inappropriate and even dangerous for them to masquerade as adults in online dating services.

Practical Guidelines for Cyber-Daters of All Ages:

- Don't rush into face-to-face contact; you need to be sure that you are meeting someone who is on the level, not an imposter who has ulterior motives.
- You may want to take advantage of anonymizing services offered by some dating sites to avoid handing out your real e-mail address to complete strangers.
- Be suspicious of anyone who tries to pressure you in any way, including demanding money or insisting on a meeting before you feel confident of their good intentions.
- As you are getting to know someone online, ask questions about lots of things you are interested in; e.g., hobbies, politics, religion, education, birth date, family background and marital history and status.

- Keep the answers you receive and beware of people who provide inconsistent or contradictory information as they are communicating with you – any lie is a danger signal.

- Be suspicious of anyone who seems to be too good to be true; if someone matches you on every single preference or interest you mention, try mentioning the very opposite of what you said earlier in the communications and see if they agree with *that* too. Trying to hard to please by lying may mark a manipulative and potentially dangerous personality.

- Be honest about yourself; state your own interests and characteristics fairly, including things you think might be less attractive than stereotypes and cultural norms dictate. A mature, good person will not necessarily be turned off if you don't look like a movie star, don't play four musical instruments perfectly, don't make a million dollars a year.

- If you get to the point of exchanging pictures, be sure that you see the person in a wide variety of situations and with other people; some online daters send false pictures to misrepresent themselves.

- Talk to the person you're getting interested in over the phone; be suspicious if the person resists such a request for a long time or always has excuses for not being available when you've agreed to talk.

- Listen carefully to how the person sounds on the phone and be suspicious if they provide information that contradicts something they wrote to you about. Any lie should alert you to potential problems.

- Before you agree to meet, get your date's full name, address and telephone number. Be suspicious if the person refuses to give you a home number: could they have a spouse or a current live-in friend they are trying to deceive? Call the home number a couple of times to see if someone else answers.

- Give the person's information and the exact details of where and when you are going to meet to friends and family. Don't ever accept a date with someone who wants to keep the location and time a secret. Be sure the meeting place is well-lit and in a public place such as a coffee shop.

- Don't allow a stranger to pick you up at your house and be sure you can get home by yourself.

- For safety's sake, think about having a background check done on the person you like using a professional service such as **http://www.whoishe.com** or **http://whoisshe.com** before considering further involvement.

Online Dating and Cybersex

Resources:

- "10 tips for online dating safely" **http://www.spankoz.com/online_dating_safety.htm**
- "Cyberdating tips from Dateable.com: 7 things everyone should know about online personals" **http://www.links2love.com/dating_sites_links.htm**
- "Cybersex and online relationships" **http://chatting.about.com/internet/chatting/cs/cybersex/**
- "Cyborgasms: Cybersex amongst multiple-selves and cyborgs in the narrow-bandwidth space of American Online chat rooms: MA dissertation" (1996) **http://www.socio.demon.co.uk/Cyborgasms.html**
- "Online dating advice from the experts: information on how to play it safe." **http://www.joylight.com/dating.html**
- "Safety tips for cyber-dating" **http://whoishe.com/safety.html**
- Teen Advice Online: Dating **http://www.teenadvice.org/dating/**

4 Hate Groups

Another source of concern for parents is the easy accessibility of hate literature on the Web. Hate mongers have taken full advantage of the largely unregulated nature of the 'Net to spread their pernicious messages. One can find Web sites devoted to hatred of every imaginable identifiable group. Race, ethnicity, religion, gender, sexual orientation, immigration status, political ideology -- anything can spark hatred in susceptible personalities. Unfortunately, some of the hate groups have been quite successful in recruiting young people through the Web; they publish propaganda such as pro-Nazi revisionist history that may fool uncritical people into believing their rants. Neo-nazi and racist skinhead groups have formed hate-rock groups that take advantage of children's enthusiasm for very loud music with aggressive lyrics.

According to the Simon Wiesenthal Center, there are over 2,300 Web sites advocating hatred, of which over 500 are extremist sites hosted on American servers but authored by Europeans; most European countries have strict anti-hate laws. Using more stringent criteria, the HateWatch group estimates more than 500 extremist hate sites on the Web; it distinguishes between hate propaganda and those pages that consisted largely of racial epithets (dismissed as mere graffiti).

The Southern Poverty Law Center monitors 500 active hate organizations in the United States. They have regularly reported on the growing number and stridency of such sites. In his comments to Keith Perine of Network World (July 24, 1000), spokesperson Mark Potok said, "A few years ago, a Klansman needed substantial effort and money to produce and distribute a shoddy pamphlet that might reach a few hundred people. Today, with a $500 computer and negligible costs, that same Klansman can put up a slickly produced Web site with a potential audience in the millions."

A fundamental issue here is that human beings find it very easy to affiliate with each other to form *in-groups*: the groups to which we feel we belong. Unfortunately, defining in-groups naturally means it's equally easy to define *out-groups*: groups to which we feel we *don't* belong. Grade-school and high-school cliques are examples of in/out-group definition. A wealth of study in social psychology confirms the validity of the universal impression that we tend to inflate our esteem for in-groups and to reduce our respect and liking for out-groups. However, research also shows that social norms against discrimination can reduce hostility towards out-groups; thus it seems likely that parental and teacher articulation of norms of tolerance can significantly reduce children's susceptibility to the blandishments of hate groups.

Practical Guidelines:

- To protect your children against the wiles of these hateful people, the most important step is to discuss the issue of hate speech and hate groups with them openly. You may even want to visit some of the sites listed below *with your children* to give them a sense of the problem and possible countermeasures.

- Discuss your children's feelings about out-groups in their own lives; for example, encourage them to speak freely (without punishment or reprimand) about whatever groups they don't like. Then pursue the discussion with explanations of such issues as cultural differences, history or whatever else you feel will help your children gain perspective on their own feelings and behavior.

Hate Groups

- Provide positive social role models for children with respect to hate groups. Speak out firmly in opposition to intolerance rather than sitting silently by when bigots display their hatred.

Resources:

- Southern Poverty Law Center **http://www.splcenter.org**
    - Intelligence Project **http://www.splcenter.org/intelligenceproject/ip-index.html**
    - Teaching Tolerance **http://www.splcenter.org/teachingtolerance/tt-index.html**
- Simon Wiesenthal Center **http://www.wiesenthal.com/**
    - Museum of Tolerance **http://www.wiesenthal.com/mot/index.cfm**
- Media Awareness Network **http://www.media-awareness.ca/eng/**
    - Challenging Online Hate **http://www.media-awareness.ca/eng/issues/internet/hintro.htm**
- Partners Against Hate **http://www.partnersagainsthate.org/**
- Tolerance.org **http://www.tolerance.org/index_flash.html**
- Center for the Study of Hate and Extremism **http://www.hatemonitor.org/**

5 Pornography

Pornography — even with the most restrictive definitions — is widespread on the Internet. Observers of 'Net culture have commented that the sure-fire way of telling if new technology is going to be a success on the Internet is to see how quickly pornographers can apply it. For example, the appearance in July 2000 of the first WAP (wireless application protocol) pornography sites signaled the adoption of WAP technology into the mainstream. Although the sites offered only tiny grainy images of naked Japanese models, sociologists said that the same sequence occurred with photography and video cameras.

Some studies of Internet traffic have claimed that more than half of the total bandwidth is used for transfer of pornography or solicitations for purchase of pornography.

Pornographers use various tricks to get people onto their Web sites. Some smut-peddlers have purchased licenses to domain names that are strikingly similar to the names of high-interest sites; examples include

- using a different domain, like "whitehouse.com" to take advantage of interest in "whitehouse.gov;"
- misspellings, such as the now-inactive "micosoft.com" which traded on the likelihood of mis-typing "Microsoft.com;"
- junk e-mail invitations with labels for URLs that don't match the actual link;
- padding porn-site metatags (normally invisible text used to describe a Web site) with inoffensive keywords that can appeal to children;
- disabling normal features of a browser to trap victims in the porn site. One villain who was shut down by the FTC even ran Java applets that disabled the "back" arrow in browsers and deleted the ability to close the browsers. People trapped in porno-hell had to reboot their computers to get out.

Porn sites are notorious for using deceit to defraud their victims. One widely-used scam is to demand a credit-card number from a visitor as "proof" (it is nothing of the sort) of their age, then to charge the card even though the site clearly states that there is a period of free use.

In 1996, viewers of pornographic pictures on the sexygirls.com site were in for a surprise when they got their next phone bills. Victims who downloaded a "special viewer" were actually installing a Trojan Horse program that silently disconnected their connection to their normal Internet Service Provider (ISP) and reconnected them (with the modem speaker turned off) to a number in Moldova in central Europe. The long-distance charges then ratcheted up until the user disconnected the session -- sometimes hours later, even when the victims switched to other, perhaps less prurient, sites. Some victims who stayed online for a long time paid more than a thousand dollars in long-distance charges. In February 1997 in New York City, a federal judge ordered the scam shut down. An interesting note is that AT&T staff spotted the scam because of unusually high volume of traffic to Moldova, not usually a destination for many U.S. phone calls. In November 1997, the FTC won $2.74M from the Moldovan telephone company to refund to the cheated customers.

Pornography

Both of the scams described above relied in part on the reluctance of porn-seeking victims to admit to their socially-disapproved interest. Few victims were willing to pursue the matter until the damages mounted into the thousands of dollars.

An entire industry has grown up to try to shield (or block) children from seeing pornography or other materials deemed offensive by their parents or by the makers of the blocking software. The popular blocking systems are universally reviled by free-speech advocates and ridiculed for their clumsy, keyword-oriented algorithms. The classic examples of ludicrous blocking include trapping access to any site that uses the word "breast" — including even possibly this very page if you are reading it on the Web. Other simple-minded traps have blocked users from accessing information pages for geographical locations ending in the old British suffix "-sex" such as Wessex, Sussex, Middlesex and so on. The village of Scunthorpe in England was blocked by software used by a major Internet Service Provider because its internal filters prevented anyone from using "vulgar" words in their mailing address.

More pernicious is that some of the blocking software products use hidden assumptions about the unsuitability of a wide range of topics, including abortion rights, civil rights, political ideology and gay liberation. Any parent is entitled to express opinions about any topic, but imposing a political agenda by stealth is an inappropriate function for software.

A different approach to interfering with the nefarious deeds of pornographers is to install monitoring software on the computers that children will use at home. These products keep a log or audit trail that allows parents to see exactly what junior has been doing for all those hours alone with the computer.

Most important, however, is the principle that machines and programs cannot by themselves teach values. Instead of relying only on passive barriers or on snoopware, parents would do well to make surfing the Internet a family activity rather than a private hobby. And when children express interest in pornography — because our popular culture is full of sexual innuendo that children read, hear and see — it makes sense to discuss the issues rather than try to pretend that they don't exist. The most powerful method for destroying the power of the forbidden fruit offered by pornographers is to explain to children in a supportive and non-punitive way why sexual exploitation and degradation are bad for people. Kids who stumble on porn sites by accident or at their friends' houses will be better prepared to cope with the sometimes disturbing images and words if their parents have prepared them for this aspect of today's world.

Pornography

Practical Guidelines:

- Place your young children's Internet-access computers in a family area of the home rather than in the children's bedrooms.

- Interact with your children while they are using the Internet; treat the Web browser like a window on the world and be present to help your children interpret that world in a way consistent with your values.

- Talk with your children about the existence and nature of pornography; as they reach puberty, assure them that there's nothing wrong with being interested in sex, but that pornography is not a healthy way of learning about wholesome, loving relations.

- Warn your children about some of the tricks used by pornographers to get traffic on their Web sites such as telling them to download special readers. Tell them about the Moldovan porn scam.

- Discuss the issue of junk e-mail that advertises porn sites. Warn children that no one should ever click on a URL from any kind of junk e-mail because it can easily be a trick to get them into dangerous territory.

- Teach your children to keep an eye on the actual URL that appears in the browser window; any discrepancy between the visible URL shown on a page and the actual URL should alert one to the possibility of fraud.

- Explain to children that pornographers sometimes charge for access to their sites without permission; be sure your children understand how dangerous it would be to give your credit card number to these people for any reason.

Resources:

- America Links Up! **http://www.getnetwise.org/americalinksup/**

- Christians Against Internet Pornography **http://members.tripod.com/~Joseph_Provencial/caip_homepage.htm**

- Feminists' Perspectives on Pornography – Academic Dialogue on Applied Ethics **http://caae.phil.cmu.edu/cavalier/forum/pornography/porn.html**

- Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories (1995) by Marty Rimm. **http://trfn.pgh.pa.us/guest/mrtext.html**

- Yahooligans Parents' Guide **http://www.yahooligans.com/parents/**

6 Incorrect Information

The Internet and in particular the World Wide Web are in some ways as great a change in information distribution as the invention of writing 6,000 years ago and the invention of movable type 600 years ago. In all these cases, the inventions involved *disintermediation*: the elimination of intermediaries in the transmission of knowledge. Writing eliminated the oral historians; one could read information from far away and long ago without having to speak to a person who had personally memorized that knowledge. Print allowed a far greater distribution of knowledge than handwritten books and scrolls, eliminating an entire class of scribes who controlled access to the precious and rare records. The 'Net and the Web have continued this trend, with a radical increase in the number of people capable of being publishers.

Where publishing once required printing presses, capital and extensive administrative infrastructure, or at least relatively expensive mimeographs (1950s), photocopiers (1960s) and printers (1970s), today publishing to a potential audience of millions can be essentially free. Many Internet Service Providers (ISPs) offer free Web-hosting services (e.g., CompuServe and AOL); free dedicated Web hosts such as GeoCities offer place for people to join electronic communities of every imaginable type. And these Web pages can lead to visibility unheard of even a decade ago. For example, one young exhibitionist named Jennifer Kaye Ringley put up a Web site to display images of her home taken through Web-enabled cameras (Webcams); this "jennycam.org" site has received up to *half a million hits per day* since it was established. Another young woman decided to put up a Web site devoted to one of her favorite literary characters. Within a few years, her site was so well respected that she was hired by a Hollywood film maker as a technical consultant on a series of movies. The exorbitant fees she was given (despite offering to help for free) significantly helped her pay for her graduate studies. It would have been impossible for her to achieve this degree of renown by, say, trying to publish her own paper fan magazine; the paper might have reached a few hundred people, but the Web site reached thousands.

Unfortunately, all of this disintermediation has negative implications as well as positive ones. Yes, freedom from publishers has liberated the independent thinker from the trammels of corporate influence, editorial limitations and standards for house style. However, this freedom has also liberated many people from responsible reporting, adequate research, and even rudimentary principles of spelling and grammar. The dictum, "Don't believe everything you read" is even more important when reading Web-based information. Individuals may publish incorrect versions of technical information (e.g., health sites that claim that massaging parts of the ear lobe can cure many known diseases), unsubstantiated theories about historical and natural events (e.g., the Tungska Impact of 1908 was caused by an antimatter meteorite), and off-the-wall revisionist history (e.g., slavery was good for black folks and Hitler never killed Jews).

Some people have taken advantage of the freedom to publish whatever they want by crossing the boundaries of libel. For example, the self-styled "reporter" Matt Drudge went too far in postings on his electronic scandal sheet in 1997 when he made unsubstantiated accusations about White House advisor Sidney Blumenthal's marriage. Professional journalists pounced on the amateur hack and tore him to bits, as it were, for shoddy journalism. Blumenthal and his wife filed a $30M libel suit against Drudge even after the scandal monger apologized for failing to verify the gossip he disseminated. Drudge then got on his high horse, claiming that public White House support for Blumenthal amounted to a threat against free speech.

In another notorious case, Walter Cronkite, whom polls revealed to be the most respected man in the United States in the 1980s, was appalled to discover a page of lies about him on the Web in 1997. A 28-

year-old programmer, Tim Hughes, invented and posted a scurrilous story about Cronkite's becoming enraged at him, shrieking imprecations, boasting about his own infidelity, and spitting in a spice cake at a Florida restaurant. In addition, the anti-Cronkite Web page included falsified photographs purporting to show Cronkite at a KKK meeting. Cronkite threatened to sue for libel; Hughes took the page down and weakly protested that it was all a joke.

You can imagine the effect of this kind of misinformation on children if they are not trained in critical thinking and skepticism about information they encounter on the 'Net.

Practical Guidelines:

Here are some practical guidelines to help children (and parents, teachers and many other adults) how to use Internet-based information wisely:

- Explain how to guess at the reliability of sites, realizing that none of the following clues is an absolute guarantee; however, meeting more of these criteria can give one more confidence in a site's value than finding very few indicators of reliability:
    - Presence of the author's name, title, institutional affiliation, academic credentials
    - Date of publication and history of revision
    - References to independent sources of validation
    - Reputation for reliability of the organizations publishing the information (e.g., Amnesty International rather than a dictatorship protesting against the latest human-rights report)
    - Lack of obvious benefit for distortion of information (e.g., Amnesty International rather than that dictatorship protecting its innocence)
    - The degree to which other trustworthy sites concur in the information on a particular site
    - Consistency – lack of obvious self-contradictions
    - By how often reliable Web sites link to the particular site under evaluation (use the Google search engine).
- Show your children some off-the-wall sites that contradict what they already know. Then go to more reputable sites and demonstrate how to cross-check information by using authoritative sources.
- Point out stylistic clues that a site may be less than trustworthy:
    - Anonymous sources;
    - Incompetent spelling and grammar;

  - Presence of obviously false information;
  - Inclusion of long-outdated information;
  - Use of lots of exclamation signs!!!!!!
  - Excessive use of CAPITALIZATION;
  - Statements expressed in absolute terms ("All ___ are ___." Or "No ___ can be ____.")
  - Intolerance of ambiguity ("There can be no doubt that _____.")
  - Overblown claims of importance ("ACME Wart Remover: the most important development in medicine in history!")
  - Claims that violate common sense ("Using rat poison is better for your teeth than using toothpaste.")
  - Intemperate and a*d hominem* remarks ("Only an idiot would believe that _____ or disagree with the statement that _____."

- Show your children examples of more reliable sources of information: scientific and professional publications, public-interest research groups, industry associations, government Web sites, reputable news sources.

Another source of information is the USENET — that collection of thousands of discussion groups on every conceivable topic. These discussion groups fall into two major classes: moderated and unmoderated. In a moderated group, messages are either passed through a *moderator* who decides whether to post them for participants or the moderator deletes offensive or otherwise inappropriate messages.

Not all moderated groups are reliable, and not all unmoderated groups are unreliable. However, many unmoderated groups distribute a farrago of unsubstantiated information from people who insult other participants and who make outrageous claims about any topic that comes up.

Children should be trained to recognize emotional and inflammatory language and should be encouraged to apply skeptical analysis to all statements, and especially to those published in rants.

Resources:

- "An Educators' Guide to Credibility and Web Evaluation" (1999) by Toni Greer, Donna Holinga, Christy Kindel and Melissa Netznik (University of Illinois/Urbana-Champaign) **http://lrs.ed.uiuc.edu/wp/credibility/**
- "Evaluating Internet Research Sources" (1997) by Robert Harris. **http://www.virtualsalt.com/evalu8it.htm**
- *WebQuester: A Guidebook to the Web* (2000) by Robert Harris. Dushkin McGraw-Hill, ISBN 0-07-235083-0.

7 Hoaxes

Pranksters have been using e-mail to fool gullible people for years using a particular sort of incorrect information: deliberate *hoaxes*. A hoax is a mischievous trick, especially one based on a made-up story. There are two major kinds of hoaxes circulating on the Internet: urban myths and false information about viruses. The archives in the Urban Myths Web site are full of hilarious hoaxes, some of which have been circulating for years. Before we get into the details, let's think about the reasons that hoaxes can last so long on the 'Net. Why don't they die out?

The problem is the distributed nature of the Internet. Information is not distributed solely from a centrally-controlled site; on the contrary, anyone can broadcast any kind of data any time. There are neither reliable creation dates nor obligatory expiry dates on files, so if someone receives a five-year-old document, they may have no obvious way of recognizing its age and they almost certainly have no instant way of knowing that its information is obsolete or flatly wrong. All they see is that the document has been sent to them recently, usually by someone they know personally.

Here are some notorious examples of the bizarre and sometimes disturbing urban myths that are thoroughly debunked on the **http://www.urbanmyths.com** Web site:

- Expensive cookies: someone claims that a Neiman Marcus department store employee charged $250 to a credit card for the recipe to some good chocolate chip cookies (this story has been traced to a false claim dating back to 1948 in which a store was accused of charging $25 for the recipe to a fudge cake).

- Don't flash your car lights: in a gang-initiation ritual, hoodlums drive down a highway with their car lights off. Flash your lights at them and die!

- Watch out for poisoned needles: insane, vengeful druggies leave needles tipped with HIV+ blood in movie theater seats / gas pump handles / telephone change-return slots.

- Lose your kidneys: visit a foreign city, go drinking with strangers, and wake up in the morning in a bathtub of ice with two neat incisions where both your kidneys have been removed.

- Poor little guy wants postcards: Craig Shergold is just one of the many real or imaginary children about whom well-meaning people circulate chain letters asking for postcards / business cards / prayers and even money. Shergold was born in 1980; when he was nine, he was diagnosed with brain cancer and friends started a project to cheer him up – they circulated messages asking people to send him postcards so he could be listed in the Guinness *Book of World Records*. By 1991, he had received 30M cards and an American philanthropist arranged for brain surgery, which worked: Shergold went into remission. The postcard deluge didn't. By 1997, the local post office had received over *250M* postcards for him and he was long since sick of the whole project.

- Wish you would stop Making a Wish: Around the mid 1990s, some prankster inserted false information about the Make-A-Wish Foundation into the outdated chain letters concerning

> Shergold. The unfortunate organization was promptly inundated with e-mail and postal mail, none of which is in any way useful or relevant to their work.

One category of hoaxes has become a perennial nuisance on the 'Net: virus myths. There is something wonderful about the willingness of gullible, well-meaning people to pass on ridiculous news about non-existent viruses with impossible effects. One of the most famous is the Good Times "virus" which appeared around 1994. It and its variants have been circulating uninterruptedly for years. Every few years, there's a new outburst as some newcomer to the Internet encounters an old copy of the warnings and sends it to everyone they know.

One of the oldest virus hoaxes is the Good Times hoax, which appeared in December 1994. The original very short warning was as follows, including the incorrect punctuation:

> Here is some important information. Beware of a file called Goodtimes.
>
> Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friends. It may help them a lot.

The Good Times virus claimed that downloading a document or reading a document could cause harm; at that time, such a claim was impossible. Ironically, within a couple of years, it did in fact become possible to cause harm via documents because of the macro language capabilities of MS-Word. Over the rest of the 1990s, foolish people modified the name of the imaginary virus and added more details, sometimes claiming impossible effects such as destruction of computer hardware. A satirical version of these hoaxes that appeared around 1996 took such claims to hilarious extremes:

> *The Latest Breaking News on the GOODTIMES Virus.*
>
> It turns out that this so-called hoax virus is very dangerous after all. Goodtimes will re-write your hard drive. Not only that, it will scramble any disks that are even close to your computer. It will recalibrate your refrigerator's coolness setting so all your ice cream goes melty. It will demagnetize the strips on all your credit cards, screw up the tracking on your television and use subspace field harmonics to scratch any CDs you try to play.
>
> It will give your ex-girlfriend your new phone number. It will mix Kool-Aid into your fish tank. It will drink all your beer and leave dirty socks on the coffee table when company comes over. It will put a dead kitten in the back pocket of your good suit pants and hide your car keys when you are late for work.
>
> Goodtimes will make you fall in love with a penguin. It will give you nightmares about circus midgets. It will pour sugar in your gas tank and shave off both your eyebrows while dating your girlfriend behind your back and billing the dinner and hotel room to your Discover card.
>
> It will seduce your grandmother. It does not matter if she is dead, such is the power of Goodtimes, it reaches out beyond the grave to sully those things we hold most dear.

Hoaxes

> It moves your car randomly around parking lots so you can't find it. It will kick your dog. It will leave libidinous messages on your boss's voice mail in your voice! It is insidious and subtle. It is dangerous and terrifying to behold. It is also a rather interesting shade of mauve.
>
> Goodtimes will give you Dutch Elm disease. It will leave the toilet seat up. It will make a batch of Methamphetamine in your bathtub and then leave bacon cooking on the stove while it goes out to chase grade-schoolers with your new snow blower.
>
> — circulated through the 'Net via e-mail in Jan 97

Unaware people circulate virus hoaxes because they receive the hoax from someone they know. Unfortunately, the friendliness of a sender has nothing to do with the accuracy of a message. Transmitting technical information about viruses without verifying that information's legitimacy and accuracy is a disservice to your friends. It makes it harder for experts to reach the public with warnings of real dangers and clutters up recipients' e-mail in-baskets with alarming information of no use whatever.

Practical Guidelines:

- Key indicators that a message is a hoax:
    - use of exclamation marks (no official warning uses them);
    - use of lots of UPPERCASE text (typical of youngsters);
    - misspellings and bad grammar;
    - no date of origination or expiration;
    - inclusion of words like "yesterday" when there is no date on the message;
    - references to official-sounding sources (e.g., Microsoft, CIAC, CERT) but no specific document URLs for details (URLs for the general site don't count);
    - no valid digital signature from a known security organization;
    - requests to circulate widely (no such request is made in official documents);
    - claims that someone is counting the number of e-mail messages containing copies of the hoax;
    - threats about dire consequences if someone "breaks the chain" by refusing to forward the message;
    - claims of monetary rewards that, upon reflection, make no sense (e.g., the Disney organization will send you $5,000 – for forwarding an e-mail message);

  - use of complicated technical language such as "n-th dimensional complexity infinite control loops" that doesn't make sense;

  - claims of damage to computer hardware from viruses or other computer software.

- Before alerting anyone to apprehended threats, check the anti-hoax pages on the Web, as suggested in the *Resources* listing below.

Resources:

- Virus hoaxes:

  - Computer Virus Myths **http://www.vmyths.com/**

  - Datafellows Hoax Warnings **http://www.datafellows.com/news/hoax.htm**

  - Good Times Virus FAQ (1995) by Les Jones
    http://www.urbanlegends.com/misc/good_times_virus_faq.html

  - ICSA Labs Hoax List **http://www.icsalabs.com/html/communities/antivirus/hoaxes.shtml**

  - Trend Micro Hoax Encyclopedia **http://www.antivirus.com/vinfo/hoaxes/hoax.asp**

Hoaxes

- Other hoaxes:
    - Alt.folklore.urban and Urban Legends Archive **http://www.urbanlegends.com**
    - CIAC Hoaxbusters **http://hoaxbusters.ciac.org/HoaxBustersHome.html**
    - Hoax FAQ **http://chekware.com/hoax/**
    - Urban Legends and Folklore **http://urbanlegends.about.com/science/urbanlegends/**
    - Urban Myths **http://www.urbanmyths.com/**
    - Gullibility on the 'Net **http://www.cwrl.utexas.edu/~roberts/gullibility.html**
- For a scholarly (and fascinating) analysis of why hoaxes spread, see the paper by Sarah Gordon entitled "Hoaxes & Hypes" at
    - **http://www.av.ibm.com/InsideTheLab/Bookshelf/ScientificPapers/Gordon/HH.html**
- and also her excellent overview entitled "Received. . . and Deceived" at
    - **http://www.infosecuritymag.com/sept/cover.htm**

8 Threats

One particular class of hoaxes deserves a brief mention: threats. If you or your children receive threats through e-mail, you have a right to inform your local law enforcement officials. In today's climate of fear and violence, any threat to your children warrants attention. In addition to the distress such messages can understandably generate in the family, they may be warning signs of serious trouble. In particular, threats about violence at school or against any definable group may be the early warning that allows authorities to step in to defuse an explosive situation.

The other side of the coin is that your children must be made to understand that sending threatening e-mail is not an acceptable joke or a minor prank, especially if the threat involves violence. Some children, believing that they can mask their real identity, have foolishly sent death threats to the White House; because the Secret Service is obligated by law to investigate *all* threats to the President and his or her family, agents show up within a few hours to interrogate the miscreants — much to the horror of the children and their parents. For example, youngsters in grade 10 at Profile High School in Bethlehem, NH sent death threats to the White House Web site from their school computers. The messages were traced within minutes by the Secret Service and the children were suspended from school and lost their Internet privileges for the next two years.

On a related topic, it would be wise to explain to children that it is also a poor idea to insult people using e-mail. Sending *flames* that belittle, ridicule and demean other people is likely to generate more of the same in response, and it's an ugly practice that distorts the children's standards for public and private discourse. Even if you decide to respond to rudeness, you don't have to be rude yourself. Tell your children about maintaining the moral high ground by refraining from obscenity, profanity, and vulgarity in written discourse. Not only is this a good habit in general, but it avoids the possibility of enraging total strangers who may be physically or electronically dangerous. Criminal hackers have been known to damage credit ratings, participate in identity theft to rack up large bills in the victims' names, and to tamper with phone company accounts.

Anonymizers are services that strip identifying information from e-mail and then forward the text to the indicated targets. However, even anonymizers respond to subpoenas demanding the identity of people involved in libel or threats. The service called *annoy.com* is designed to allow people to send annoying messages to people without reaping the consequences; even that service has a particularly clear message on its refusal to tolerate abuse:

> **WARNING**
> It has come to our attention that certain people have been using annoy.com to deliver what some might consider to be threats of physical violence or harm to others.
> Do not mistake our commitment to freedom of speech for a license to abuse our service in this manner.
> We plan to cooperate fully with law enforcement agencies in whatever efforts they make to find you and punish you - even if it's some renegade authoritarian dictatorship that might crucify your stupid ass if they catch you.
> Free speech and annoy.com are not about harassment and definitely not about harm or violence. If you think for a second we will allow cowardly idiots to spoil our free speech party you are making a mistake. A huge mistake.

Threats

You might also want to point out that on the USENET, in particular, a message is forever: there are archives of USENET messages stretching back for a decade, and — although it may be hard to get this across to younger children — being an abusive foulmouth online may not permanently damage a person's reputation, but it is not likely to *improve* a child's prospects for being accepted in a good college or getting a good job. Some of the abuse is so inane that it actually becomes funny; here's a tame sample from a real and very long posting dated 2001-03-09 from someone called "Hate Jerry Too" to the newsgroup rec.pets.dogs.behavior:

> Troll? YOU are the TROLL, Smegma-boy! BWWWWAAAHAHAHAHAHAHAHAHAAAA!!!
>
> If you would just IGNORE stuff you don't like, Smegie, and not FLAME and TRASH people all over the place, maybe people would LIGHTEN UP a bit on you. HOWE's it feel getting your BALLS BUSTED CONSTANTLY throughout the day??
> BWWWWAAAHAHAHAHAHAHAHAHAAAA!!!
> BWWWWAAAHAHAHAHAHAHAHAHAAAA!!!
> BWWWWAAAHAHAHAHAHAHAHAHAAAA!!!
> BWWWWAAAHAHAHAHAHAHAHAHAAAA!!!
>
> *[remainder deleted]*

Practical Guidelines:

- Parents and teachers: teach your children never to utter threats of violence or other harm, and in particular not e-mail messages or chat rooms.
- Encourage your children to report all threats directed at them or at others to parents, teachers or librarians immediately.
- Search the USENET archive at **http://groups.google.com/** using a variety of mildly offensive terms (e.g., "jerk") to illustrate the foolishness of people who spew abuse at each other.

Resources:

- Annoy.com policy on threats **http://www.annoy.com/scripts/censure/index.asp**
- "Sample handbook language re: threats of violence" from the School Administrators of Iowa **http://www.sai-iowa.org/threats.html**
- "Special report: When e-mail threats become real" (2001) by Jay Lyman **http://www.newsfactor.com/perl/story/8252.html**
- "Maryland man arrested after Santana High e-mail threat" (2001) **http://www.cnn.com/2001/US/03/10/school.shooting.01/**

9 Viruses And Other Malicious Self-Replicating Code

As this text is being updated in early July 2002, there are over 61,000 distinct forms of malicious self-replicating program code circulating in cyberspace. Most of these harmful programs are limited to anti-virus laboratories and to the computers of virus hobbyists — people who derive a perverted pleasure from playing with dangerous toys.

Viruses are self-reproducing programs that insert parts of themselves into various forms of executable code — i.e., instructions that can tell a computer what to do. There are several forms of executable code that have been used for viruses:

- Boot-sectors: the first piece of information on a disk (sector 0, cylinder 0); *boot-sector viruses* reproduce by being loaded into memory when a computer boots (restarts) with an infected disk in the boot-device

- Program files: files on PCs that end in ".exe" or (more rarely) ".com" and some other less-used extensions. *Program-file infectors* are viruses that insert instructions into a program file so that viral code can be loaded into memory where it can modify the functioning of the computer to, among other things, allow replication of the viral code. Another form of harmful code using programs is called the *Trojan Horse* and refers to programs that have been modified without authorization and without documentation so that they contain unexpected functions. Examples include the Moldovan porn Trojan mentioned in a previous section and programs that supposedly allowed people to cheat AOL out of connection fees (but actually stole passwords and sent them to the criminals who had written the programs).

- Document macros: Microsoft Office includes an automatic execution feature for stored operations; *macro viruses* are macros that are written in the Visual Basic programming language and can be executed automatically by several programs in the MS-Office suite. *Macro viruses* are the most frequently-encountered viruses in the world today. They reproduce through the exchange of infected documents such as MS-Word ".doc" files and MS-Excel spreadsheet ".xls" files.

- E-mail attachments: In addition, the newest generation of macro-based malicious software, known as *e-mail-enabled worms* use Visual Basic to exploit a feature of MS-Outlook, MS-Outlook Express and other MAPI-compliant e-mail packages to send copies of themselves to many or all of the recipients listed in standard e-mail address books. These worms spread through the 'Net thanks to the automatic execution of file attachments that occurs when an e-mail recipient opens the attachment.

- Active content: Java and ActiveX are programming languages used by designers of Web pages to accomplish functions such as displaying a list of options, checking a response to a question to see if the value is acceptable, and transferring data from a user to a database or other programs on a Web server. Both Java and ActiveX can be used to cause harm to users; examples have shown that such code can generate an endless number of new windows (eventually freezing a Windows computer), reading information from a user's hard disk and transmitting it to an address on the Internet, and causing every imaginable form of harm that the operating system allows.

Today, there are virus-creation kits that allow untrained children to create virus variants that can cause havoc to individuals and organizations. Writing (or modifying) viruses seems to appeal to children because it is so easy to cause trouble for many people at once – it's one of the few ways a child can feel really powerful in the world of adults. It is important to discuss these problems with children from the earliest ages so that they can get used to the idea that writing viruses is just as bad an idea as, say, arson.

Practical Guidelines:.

- Keep your virus strings up to date (e.g., at least twice-monthly updates); if you have a persistent (permanent) Internet connection, you may be able to configure your antivirus software to check for updates automatically as often as the maker recommends (e.g., daily).

- Don't download or use software that purports to help you break the law or cheat people and businesses.

- Don't download or use stolen software (i.e., software copies without permission or in violation of license restrictions).

- Don't execute software that anyone sends you through e-mail even if you know and like the person who sent it to you. Just because they're nice people doesn't mean they are qualified to inspect programs for safety.

- Before sending someone an attachment (e.g., a picture or any other kind of file) by e-mail, let your recipient know what to expect via a preliminary message; if you don't know the person personally, send an e-mail requesting permission to send the attachment.

- Never open attachments you have received without warning, regardless of who sent them or what the subject line or text say. Be especially suspicious of generic subjects such as "FYI" without details or "You'll like this." If you are really curious about the attachment, phone or e-mail the supposed sender to find out whether it is legitimate. However, remember NOT to run programs you receive as attachments *regardless* of what the sender thinks about them.

- Don't forward programs, even reliable programs, to anyone; instead, tell your friends where to download useful programs from a trustworthy source (e.g., a legitimate Web site).

- Before sending anyone an MS-Word document as an attachment, save the document as an RTF file instead of as the usual DOC file. RTF files don't include document macros and therefore cannot carry macro-viruses.

- Disable automatic execution of macros in MS-Word using the TOOLS | MACROS | SECURITY menu and select the HIGH option (which restricts macro execution to digitally-signed macros from trusted sources — none, by default).

- Use the patches offered by Microsoft to shut off automatic execution of attachments in Outlook and Outlook Express.

- Don't circulate virus warnings unless you have personally checked their validity on any of a number of virus-information and hoax sites on the Web.

Resources:

- 18 USC 1030: Computer Fraud and Abuse Act of 1987 **http://www4.law.cornell.edu/uscode/18/1030.html**
- Computer Virus FAQ for New Users (1999) **http://www.cs.ruu.nl/wais/html/na-dir/computer-virus/new-users.html**
- F-Secure Virus Database search **http://www.f-secure.com/v-descs/**
- IBM Antivirus Research **http://www.research.ibm.com/antivirus/SciPapers.htm**
- ICSA Labs Virus Alerts **http://www.icsalabs.com/html/communities/antivirus/alerts.shtml**
- Online VGrep Search **http://www.virusbtn.com/VGrep/search.html**
- Top Ten Viruses (Trend Micro) **http://www.antivirus.com/vinfo/default.asp**
- Virus Bulletin **http://www.virusbtn.com/**
- Virus Primer (Trend Micro) **http://www.antivirus.com/vinfo/vprimer.htm**
- "What makes Johnny (and Janey) write viruses?" (2001) by Kim Zetter **http://www.itworld.com/Net/3271/PCW01051534405/pfindex.html**
- WildList Organization **http://www.wildlist.org/**
- Word Macro Virus FAQ from Michigan State University **http://www.ahdl.msu.edu/ahdl/macrofaq.htm**

10 Junk E-mail

Unsolicited commercial e-mail (UCE) is derisively known as "junk" e-mail but also, much to the distress of the Hormel Corporation, as "spam." Junk e-mail is spawned by foolish or unscrupulous people who send out thousands or even millions of identical messages to unwilling recipients. Junk e-mail clogs victims' in-baskets and wastes their time as they open these unwanted messages and take a few seconds to realize they are junk. Junk e-mail advertising pornography may be highly offensive to the recipients or to their parents. Junk may even push people's e-mail systems over their server limits if they are not picking up their messages regularly; in such cases, additional wanted e-mail may bounce because the mail-box is full.

Most junk e-mail uses forged headers; that is, the senders know they are doing something wrong and they deliberately put misleading information in the FROM and REPLY fields to avoid receiving angry responses from the victims of their rudeness. Forging e-mail headers is illegal in the states of MA, VA and WA and, if the perpetrators can be identified, can lead to court cases and financial penalties for each message involved in the fraud.

In one famous case, a clueless college student called Craig Nowak sent out a few thousand junk e-mail messages and followed the instructions in his spam kit by putting a made-up REPLY address using "@flowers.com" without checking to see if there really was such a domain. Indeed there was, and the owner of this reputable floral delivery service, Tracy LaQuey Parker, was none too pleased when her system was flooded with over 5,000 bounce messages and angry letters from customers saying that they would never do business with her again. She sued Nowak for damages and was awarded over $18,000 by a judge who said he wished he could have been even more punitive.

Practical Guidelines:

- Don't buy products or services from anyone who has sent you junk e-mail. If they are unprofessional or stupid enough to use such methods of advertising, they don't deserve either your business or your trust.

- Don't assume that the FROM or REPLY-TO addresses are correct, because often they are either non-existent or, worse, fraudulently point to an innocent legitimate business. And *never* bombard the FROM or REPLY-TO address with multiple copies (or even one copy) of abusive e-mail (a practice known as *mail-bombing*), since you will likely be reaching the wrong target.

- Never respond to the address listed for removal from a junk e-mail list unless you know the organization who sent you the message. Since bounces (returned e-mail due to bad addresses) never reach them and there is no incremental cost for sending out addresses to unwilling people, these operators really don't care how you feel about the junk they send. Therefore, the people who send junk e-mail often use the REMOVE function primarily to harvest correct e-mail addresses so they can sell them to some other spammer.

- Don't visit the URLs listed in junk e-mail messages. Some of them are deliberately mislabeled and may bring you to offensive Web sites.

- If there is a toll-free number listed in the junk message, you *may* use it at the sender's cost to let them know how you feel about being on a junk e-mail list. However, never be rude to the people answering the phone; in general, they are poorly-paid employees who have no responsibility or even knowledge of the sleazy methods being used to reach the public. Just ask to speak to a manager so that the perpetrators' cost of doing business can be increased.

- If you *really* feel angry about a particular e-mail and you have the time and technical know-how, it is possible to locate the Internet Service Provider or Web-hosting service that carries an offending Web site by analyzing the forged headers or doing a Domain Name System (DNS) lookup on a domain listed by the spammer for contact. Sometimes, a well-written report can result in cancellation of the perpetrators' Internet access and perhaps even domain registration.

- Last, in case the message has not already come through the vigorous invective above, do not send junk e-mail yourself, nor allow your children to send junk e-mail.

- On a similar note, if you are involved in an e-mail discussion group (especially an unmoderated group) about a specific topic, do not post e-mail to members of the list on a subject that is outside the topic area. A typical class of inappropriate posting is an appeal for support to a worthy cause that has no or only a tenuous relation to the subject area; e.g., appealing for support to save whales in a discussion group about gardening. The reasoning is, "Likes plants; probably environmentally sensitive; likely to be interested in conservation; therefore will be glad to hear about whales." The problem is that such reasoning could be extended to practically any topic at all, disrupting the focus of the group and often causing angry retorts which are mistakenly sent to the entire list instead of to the sender of the inappropriate stuff. Then the mistakenly distributed retorts cause further angry retorts, and pretty soon the gardening list has turned into – you should pardon the expression – a *hotbed* of dissension and wasted effort and generates a *flowering* of bad feeling and *plants* the *seeds* of distrust. It *leaves* a bad taste in everyone's mouth and provides *grounds* for departure and is *mulch* to be regretted.

- As suggested in the preceding point, if you do see inappropriate messages on a e-mail list you care about, do not reply to the entire list: reply only to the sender, with possibly a copy to the moderator if there is one. And be polite.

Resources:

- ChooseYourMail **http://www.chooseyourmail.com/**
- Coalition Against Unsolicited Commercial Email **http://www.cauce.org/**
- "Fight Spam on the Internet" **http://spam.abuse.net/**
- JunkEmail.org **http://www.junkemail.org/**
- JunkBusters **http://www.bbb.org/library/email.asp**
- "Tips For Consumers: What You Should Do About Unsolicited Commercial E-mail" (1998) from the Better Business Bureau **http://www.junkbusters.com/**

11 Chain Letters and Ponzi Schemes

A particularly annoying form of junk e-mail is the chain letter. Some chain letters include obviously ridiculous stories about terrible diseases and accidents that have befallen people who refused to forward the nonsense, but others are focused on getting victims to send money to a list of names and then add their names to the list before sending it on to everyone they know.

This type of pyramid is known as a Ponzi scheme, which is an investment swindle in which high profits are promised from fictitious sources and early investors are paid off with funds raised from later ones. The scam is named after Charles Ponzi (1882?-1949), an Italian-born speculator who organized such a scheme in 1919 & 1920). The "Ponzi scheme" tricked thousands of people in Boston when Ponzi guaranteed a 50% profit on contributions in 45 days and a doubling of value in 90 days. The con man claimed he was redeeming 1-cent Spanish postal certificates for 6-cent U.S. stamps – a claim ridiculed by financial analysts at the time. Nonetheless, Ponzi took in around $15 M (in 1920 dollars, mind) and stole around $8M, paying out the rest to the victims who eventually received 12¢ on the dollar. Six banks collapsed because they invested their depositors' funds in the scheme. Ponzi eventually served over three years in jail but escaped in 1925.

The modern-day e-mail Ponzi scheme typically includes passionate assurances from vaguely identified people about how skeptical they were about the scheme but how they succumbed to curiosity, participated in the scheme and earned vast amounts of money (e.g., $50,000) within a couple of weeks. The letters often include assurances that everything is legal and point to nonexistent postal information phone lines or claim "As Seen on TV" at various points in the letter.

These letters claim that all you have to do is send in $1 (or $2 or $5) to each of a short list (e.g., 4) people to receive their "reports" and then add your name and address to the list while removing the first one before sending a copy of the new letter to as many people as possible. Some letters go through computations involving such assumptions as "Imagine you send out a hundred / thousand / ten thousand) messages and get a mere (1% / 2% / 10%) response" and then calculate enormous returns.

In fact, the "reports" are nothing but one-page, meaningless blurbs about chain letters. The scammers are trying to get around regulations such as the U.S. Post Office's bar against fraudulent uses of the mail.

Here is the text of a letter sent to me on 1 December 2000 by V. J. Bellinger of the Operations Support Group of the United States Postal Inspection Service in Newark, NJ. It has some interesting information that I hope will be helpful to readers attempting to convince employees (or family and friends) that such chain e-mail involving postal addresses is illegal.

> "A chain letter or a multi-level marketing program is actionable under the Postal Lottery, False Representation, and/or Mail Fraud Statutes if it contains three elements: prize, consideration and chance. *Prize* is usually in the form of money, commissions, or something else of value that the solicitation claims you will receive. *Consideration* is the required payment to the sponsor in order to obtain the prize. *Chance* is determined by the activities of participants over whom the mailer has no control. These types of schemes constitute lotteries and are barred from the mails because they violate the following statutes: Title 18, United States Code, Sections 1302 and 1341 and Title 39, United States Code, Section 3005.

Chain Letters and Ponzi Schemes

> "In attempts to appear legal, many chain letter or multi-level marketing mailings offer, for a fee, a product or `report.' However, since the success of the program is dependent on the number of people willing to participate, all three elements that constitute a violation continue to be present.
>
> "The promoter of this scheme has been advised of the potential violations involved and has been requested to discontinue this type of mailing activity. . . ."

A superficially similar phenomenon is known as multilevel marketing (MLM). In this *non-fraudulent*, legitimate system of selling products and services, people are encouraged to recruit distributors from among their friends and acquaintances, but the emphasis is on the value of the products. In a legitimate MLM system, no one claims that anyone is going to become wealthy without work, and there is no demand for investments. The products have an established market, and the company makes money through sales, not through recruitment.

Practical Guidelines:

- Do not participate in any scheme that relies on forwarding large numbers of letters or e-mail messages to everyone you know or to strangers.
- Differentiate between pyramid frauds and legitimate multilevel marketing systems: the former emphasize collecting participants whereas the latter emphasize the value of products and services.
- Do not participate in alleged multilevel marketing systems if they require substantial investments.
- If you are interested in a multilevel marketing operation,
    - Check out the owners and officers;
    - Talk to people who have bought the products to see if they are happy with their purchases.
    - Contact your local Better Business Bureau to see if there have been any complaints.
- Do not send money to addresses listed in pyramid frauds.
- Make a project of working with your children to demonstrate how a pyramid fraud takes money from a growing number of later victims and shifts it to people who participate earlier in the fraud. Show what happens when the number of new victims drops.

Chain Letters and Ponzi Schemes

Resources:

- "Gifting Clubs: A New Twist to the Age-Old Pyramid Scheme" from the Better Business Bureau **http://www.bbb.org/library/giftingclub032000.asp**

- "Multi-Level Marketing (How to Tell a Legitimate Opportunity from a Pyramid Scheme)" from the Better Business Bureau **http://www.bbb.org/library/tippyra.asp**

- "Internet Fraud: Ponzi Schemes - Mail & Wire Fraud - Chain Letter Scams" by John R. Osgood **http://pw1.netcom.com/~jrosgood/fraud.htm**

- "Pit Stop, Dinner Party, and Other Schemes Target Washington and Idaho Regions" from the Better Business Bureau **http://www.bbb.org/alerts/pyramid0802.asp**

- "Ponzi Schemes" on the LA FBI Site **http://losangeles.fbi.gov/contact/fo/la/ponzi/ponzi.htm**

12 Get-Rich-Quick Schemes

Get-rich schemes on the 'Net play on the victims' wishful thinking, lack of skepticism and lack of plain common sense. There have been claims that you can earn a quarter of a million dollars a year – grooming poodles in your home?? Become a millionaire – working four hours a week – sending out promotional literature for products you don't even have to sell. Some such schemes are promulgated by dangerous people; for example, some extremist militia groups have been charging people hundreds of dollars to learn how to defraud the government by claiming liens on government property and then claiming the nonsensical liens as collateral for loans. Other criminals circulate programs for generating fraudulent credit-card numbers and using them to steal goods for fun and profit (they never mention jail).

To illustrate the kind of trouble children can get into using these techniques, consider the case of Drew Henry Madden. In 1996, this 16-year-old Australian boy from Brisbane started defrauding businesses using stolen and forged credit-card numbers just after leaving school. He stole A$18,000 of goods and in February 1997, pleaded guilty to 104 counts of fraud and was sentenced to a year in jail However, further frauds were discovered and it turned out that he had stolen an additional A$100,000 in goods and services. In October 1997, he pleaded guilty to an additional 294 counts of fraud. He was given an additional suspended sentence. His defense attorney blamed poor security for the losses: "Madden started with very minor credit card fraud, but it escalated alarmingly, because the safeguards were so inadequate." Despite the youngster's unusual revenue stream, his mother appeared to have accepted his globe-trotting ways and massive purchases of lottery tickets without comment. At one point, she told reporters, ""If we were a wealthy family he'd be at a private school, where his talents could be directed properly."

Some people have bad luck or bad judgement and develop bad credit histories or end up in bankruptcy. They can be susceptible to criminals who charge money to teach victims how to falsify their rotten credit records so they can obtain yet more fraudulent credit, all they while claiming that their illegal methods are 100% legal. On the contrary, such "File Segregation" by creating new identities is definitely illegal and may result in fines or even jail sentences.

A relatively new kind of fraud on the Internet is the diploma mill. These organizations pretend to be educational institutions; actually, they are fraudulent people (often one individual) who sells bogus documents purporting to represent degrees or certificates and which fool no one but the purchaser.

Practical Guidelines:

- Get your children started quickly on the road to common sense: earning lots of money with little or no effort usually marks something impossible or illegal.

- Teach them the mantra of the skeptic: "If it sounds too good to be true, it usually is."

- Discuss Internet-mediated theft in the same terms as you discuss shoplifting. Explain how commerce works; point out that everyone suffers from all kinds of theft, including electronic shoplifting. Talk about the victims of such fraud: everyone who pays higher interest rates on unpaid credit-card bills – and sometimes also innocent shop-keepers who lose merchandise to e-commerce crooks.

- Explain how dangerous it is to get involved with criminal schemes like using stolen or falsified credit cards.

Resources:

- "A New Credit Identity: A New Credit Repair Scam" from the 'Lectric Law Library **http://www.lectlaw.com/files/cos21.htm**
- "Credit Repair" from the Better Business Bureau **http://www.bosbbb.org/lit/0105.htm**
- "Credit Repair: Self-Help May Be Best" U.S. Federal Trade Commission **http://www.ftc.gov/bcp/conline/pubs/credit/repair.htm**
- "Credit Repair Scam Could Lead You to Commit Fraud" **http://www.quicken.com/cms/viewers/article/banking/39349**
- "File Segregation: New ID is a Bad Idea" from the U.S. Federal Trade Commission **http://www.ftc.gov/bcp/conline/pubs/credit/creditid.htm**
- "How to Spot Credit Repair Scams And Correct Your Credit History Yourself" from the U.S. Federal Trade Commission **http://www.cslib.org/attygenl/credhelp.htm**
- "Is the Internet Becoming a Haven for Diploma Mills?" from the Better Business Bureau **http://www.bbb.org/library/diplomamills.asp**
- Tips for Consumers: Internet-Related Business Opportunities – Don't Let Them Fool You! **http://www.bbb.org/library/internetbus.asp**

13 Nigerian 4-1-9 Scams

In 2002, the number of Nigerian 4-1-9 fraud letters circulating on the Internet has been growing to the point where many people receive at least one pathetic letter per day telling them about how some dishonest person in a developing country (Nigeria, Ghana, Mozambique, to name a few) has found or inherited a huge cache of illicit money skimmed off from the starving masses. Sometimes it is described as money from bribes; in other cases the vast amounts of filthy lucre come from accounting mistakes in public accounts. In return for the victim's revealing full details of name, contact information and bank account details (yeah, right!), these self-avowed criminals will transfer amounts such as $50 million into a total stranger's very own personal bank account and then move it out in a money-laundering scheme. The addressee will supposedly benefit by keeping some large percentage (10%, 20%) of this stolen money. The scam is generally referred to as a 4-1-9 because of the applicable Nigerian laws governing fraud.

Here's a typical letter drawn at random from my personal collection (spelling and grammar mistakes in the original):

* * *

From: Some nonexistent e-mail address (forged headers)
To: [unknown], mkabay
Date: 2002-07-11 23:46
RE: URGENT BUSINESS PROPOSAL
FROM: EDWARD YEBOAH
Email: edwardyeboah@[someISP].com

Sir,

My name is Edward Yeboah 42 yrs, a secretary a Ghanaian national married with a wife and four children. I work as an Administrative secretary to STANDARD SECURITY & SERVICES LTD in Accra – Ghana. I earn a salary of ¢1.4M – 200 USD equivalent monthly. i joined the services of this company in 1991 as an office assistant.

I got the information concerning you and your company from the Ghana chamber of Commerce and after due consultation with my spiritual adviser, I decided to contact you believing that by the grace of God that you will accept to be my partner in this business.

I have been working with this company for nine years. Within this period, I have watched with meticulous precision how African Heads of States and government functionaries have been using STANDARD SECURITIES to move huge sums of money USD, Pound sterling, French France – (Cash) to their foreign partners. They bring in these consignments of money cash and secretly declare the contents as jewelleries,gold, diamond, precious stones, family treasure, documents etc. Gen. Sani Abacha of Nigeria (dead), Mobutu Sese Seko of Zaire (dead) Foday Sankoy of Siera – Leone. Babangida of Nigeria etc. All these people have hundreds of consignments deposited with STANDARD SECURITIES.

Their foreign partners, friends and relatives, are claiming most of these consignments.

A lot of them are lying here unclaimed for as much as 15 yrs. No body may ever come for them because in most cases, the documents of deposit are never available to any body except the depositors most of them dead. Since the inception of the 2000 millennium, STANDARD SECURITIES MANAGEMENT changed the procedure of claims of consignments.

As soon as you are able to produce all the secret information as contained in the secret file of any consignment, it will be released to you upon demand. From our record, more than 120 consignments belonging to Gen Abacha /Mobutu Sese Seko, has been claimed in the past six months. This is why I am soliciting for your co-operation and assistance.

Gen. Abacha has 85 consignments deposited with several names and codes.35 have been claimed in the past six months. Since he's dead, his first son is dead in a plane crash, the second son is facing trial for murder and embezzlement, the family members are under restricted arrest without communication.

I have finished every arrangement for you to come and claim consignment No 1201 containing USD 9M and consignment No 1200 contain USD 15M. My duty is to supply you with all the information and documents by fax. You will deal directly with the management. The procedure is simple: - Apply officially to the Director of Operations of STANDARD SECURITIES for the release of consignment No 1200 and No 1201. They will demand some documents and secret codes. Call me, I'll supply you with every detailed information. Fax it to them.

As soon as they confirm it to be correct. They will invite you for the collection. If you do not want to come to Accra, you can arrange with them to transfer the consignment to anywhere on agreement. No body will ever know I am involved in the deal except the Lawyer who will write an agreement for us. I'll suggest upon conclusion we share 50 – 50.

At the successful conclusion of the deal, you'll arrange for me and my family to come over to your country.

I assure you that the business have been hatched for 5 years now, it is very secure and risk free.

God bless you .

Thanks.

* * *

Back in 1996, Deputy Assistant Attorney General Mark Richard warned a House International Relations Committee hearing, "Nigerian nationals are involved in perpetrating a variety of financial and other crimes upon U.S. citizens and businesses from the safety of Nigeria." They and other criminals using the same tactics are robbing Americans of hundreds of millions of dollars a year. In 1995, said Deputy Assistant Secretary of State Jonathan Winer, the U.S. embassy in Lagos received many requests for help from Americans defrauded by Nigerians: "[T]he embassy rescued several American citizens lured to Lagos in scams, taken hostage and held for ransom."

Sally Miller, director of the Commerce Department's Office of Africa in 1996, said, "We are aware of at least two incidents, one in 1991 and a second in 1995, in which Americans who had unknowingly become involved in a fraudulent business deal traveled to Nigeria and were killed after refusing to put more money into the deal."

David Kennedy, Research Director for ICSA Labs, told me, "The Secret Service rescued one victim in his hotel room, already doused with gasoline, about to be set on fire (conscious). If they get social security numbers they set up credit cards and max out the accounts. The victims put a fraud alert on their credit reports, but that alert lasts only one year unless the victim renews it. The Nigerian gangs know this, so they wait a year and use the same personal information to get another batch of credit cards hitting the same

victim's credit twice. Do not answer solicitations to help import U.S. dollars from Africa. The Secret Service has set up a database to track these people; turn solicitations over to them."

Since the mid-nineties, the problem has grown worse. Using cheap junk e-mail lists, the criminals have bombarded millions of people with this nonsense hoping to find victims – and they do.

So let's think clearly about an offer to give a complete stranger millions of dollars for essentially nothing. First off all, only an astonishing gullible person would give anyone, let alone a *self-avowed embezzler*, details of their bank account. Second, only a larcenous twit would actually send anyone money for the fees and bribes demanded by the fraud artists – yet thousands of people have actually fallen for this scam, which has been around for over 20 years. A few American victims have spent up to tens of thousands of dollars on the illusory ill-gotten gains; a very few have traveled to Nigeria (in particular) and promptly been kidnapped and held for ransom.

Practical Guidelines

- What more can one say? If you don't want anything to do with the problem, simply delete every message of this type without ever answering it.
- If you feel like collaborating in the fight against this nonsense, send a copy of the message to the abuse department of the Internet service provider to shut down the *receiving* e-mail address.
- Send copies of the e-mail scam letters to **mailto:419.fcd@usss.treas.gov** and put "No Monetary Loss" in the subject line.
- Whatever you do, *don't respond to the messages* and don't send information and money to these criminals.

Resources

- For more information about this nonsense, see the "419 Coalition Website" at **http://home.rica.net/alphae/419coal/** where you can find a concise description of the fraud and an extensive list of links for further details.
- The FBI also has a number of informative pages on the scam; e.g., **http://www.fbi.gov/contact/fo/nyfo/fraudalert.htm#nigerian**
- Other Web sites dealing with the 4-1-9 fraud:
  - **http://www.cbintel.com/nigeriafraud.htm**
  - **http://www.nigerianfraudwatch.org/**
  - **http://www.scambusters.org/NigerianFee.html - How the fraud works**

14 Stolen Software, Music and Videos

People have been stealing software since personal computers became common. Families where the parents would be shocked at their child's stealing a $1 candy bar from the local supermarket seem blithely unconcerned about those same children's theft of software costing hundreds of dollars. Unfortunately, some of those parents are guilty of stealing software themselves: many of the "customers" at software "lending libraries" are adults who know that what they are doing is illegal but just don't care.

Software theft is a serious problem with serious consequences. For example, in May 2000, the FBI arrested 17 people, five of them former or current employees of Intel, on charges of involvement with Internet sites devoted to pirated software. The five were described as having held low-level engineering jobs, and an Intel spokesman said four of the five were no longer with the company. All 17 suspects were members of a loosely organized group called *Pirates with Attitudes*, which operated one of the Internet's oldest "warez" sites -- a term describing a hacker variation of software sold in stores by merchants. Most warez sites are run as hobbies and their users are often teenage boys who view downloading a pirated software program to be a rite of passage. The indictments did not allege that the perpetrators were attempting to make money through their activities, but the potential penalties include a $250,000 fine and five years in prison. "This is the most significant investigation of copyright infringement involving the use of the Internet conducted to date by the FBI," said a spokeswoman for the Bureau's Chicago office. "It demonstrates the FBI's ability to successfully investigate very sophisticated online criminal activity." (Wall Street Journal 5 May 2000 as reported by NewsScan, edited by John Gehl and Susanne Douglas)

Even some teachers have fallen into the trap of believing that they are entitled to copy proprietary software without permission. They are quite wrong. For example, in 1998, the Business Software Alliance audited the Los Angeles Unified School District and found 1400 illegal copies of proprietary software in a single school in the District. Total costs of replacing illegal software throughout the District reached ~$5M. Imagine trying to explain fines and costs at such a level to the voters when the next budget came up.

The plague of intellectual-property theft has recently been extended to music CDs and DVD movies. Napster, Gnutella, Wrapster – do you know if your children are using these *peer-to-peer* packages and others like them? Such software allows people to share digital music and video files through the Internet; most of the material being exchanged among enthusiasts is restricted by copyright. Napster lost its court cases and was forced to begin cooperating with the recording industry to screen out stolen property from its exchange networks. Individual thieves received legal notice from angry bands such as Metallica warning them to destroy their pirated copies of stolen music tracks by the heavy-metal group.

In summary, stealing other people's intellectual property and depriving them of royalties is illegal, unethical, and rude.

Now go tell your children about this.

Practical Guidelines:

Discuss the following arguments over theft of intellectual property with your children. The following sections are written aggressively, as if directly to people violating intellectual property laws.

14.1 Everyone's doing it.

That's simply not true: not everyone breaches copyright. Furthermore, the fact that some people are violating laws and norms of civility is irrelevant to whether they ought to be doing so. What did *your* parents tell you the last time you tried that excuse ("Aw Mom / Dad! Everyone's staying out late / using drugs / driving without a license / shoplifting / plagiarizing.") to violate the law or to ignore a family standard of integrity? The number of people who use other people's work without recompense does not make this action right or even legal. Ethical behavior is not conditional on popularity.

14.2 We won't get caught.

So what? That's irrelevant to whether they ought to be doing it. Being caught has no bearing on whether an act is moral or legal: what do you think hit-and-run accidents are all about? Knocking someone over with your car is OK as long as you don't get caught? Doing bad things gets to be a habit regardless of whether anyone finds out about it. And companies that tolerate any kind of illegality by their employees while on company time or on company systems are opening themselves up to blackmail, denunciation, and lawsuits.

14.3 It's the music / software industry's fault: if they don't want theft, they should charge less.

First of all, even shareware authors get cheated by people who use their software without paying for it — and these are packages for which the authors ask for a few dollars.

Second, the owner of the software or of the music copyright has no obligation to meet someone else's view of appropriate pricing.

Third, no one has a right or entitlement to use intellectual property without an agreement with its owner; if you don't like the price, find a more cost-effective alternative within the law.

Fourth, it is just plain rude to disregard the express wishes of software designers or musicians by using their creative output without their permission. Would you do this if you were face-to-face with these people? If not, examine your motivations and justifications.

14.4 It's the producers' fault: if they don't want theft, they should make it technically impossible.

And if someone hits you over the head with a baseball bat, it's your fault for allowing them to do so? Why should the victim of a deliberate criminal action bear the weight of condemnation? How would you feel if someone entered your home by breaking down the door and then used your TV, leaving a note saying that their unpaid and unauthorized use of your property was entirely your fault for not having a steel door? Criminal hackers, for example, go out of their way to violate security measures on the systems they compromise; every attempt to defend against intrusion is met with vigorous activity to find ways around the defenses. How can anyone seriously accept the notion that the victims are to blame in such cases?

14.5 It doesn't hurt anyone.

Yes it does. Software vendors, for example, including individual entrepreneurs and employees, suffer from having half to seven-eights of their potential sales eliminated through theft. How would you like it if you were trying to earn a living providing a service or a tool — and half the potential clients simply stole your product without paying you anything at all? And furthermore, every theft of intellectual property makes the next theft even more likely (hence the "everyone's-doing-it" argument above).

14.6 It only hurts a company — I wouldn't steal it from an individual.

Oh, Robin Hood, eh? The company isn't a machine, it's *a group of people* who agree to work together according to terms they agree on. Steal from the company and you steal from employees, owners and other stakeholders. You may even hurt honest users by contributing to higher prices. I once met a criminal hacker who earnestly assured me that he would steal a radio from a business office if it had a corporate asset sticker on it but not if it were the property of an employee there. Where's the line you're drawing? Would you steal from a corner store owned by Mom and Pop? How about it they had one employee? three? fifteen? And if this is such a big political and ideological issue, why not use the standards of civil disobedience and present yourself for arrest and legal action as a public rejection of the law instead of violating copyright in secret and for private benefit?

14.7 The music industry is violating the rights of the musicians, so breaching copyright is a Good Thing.

Many people feel that musicians are being violated by the big music distributors' stranglehold on copyrights and distribution; see for example "The Battle for the Heavenly Jukebox" by Charles Mann in the Atlantic Monthly **http://www.theatlantic.com/issues/2000/09/mann.htm** . However, taking the musician's work without recompensing anyone at all hardly seems like a principled stand against greed — rather the reverse. It reminds me of people who listen to Public Radio in the USA but never contribute anything to support the stations and the programs: who, exactly, is supposed to do so? And using the categorical imperative, if no one pays for music, or if everyone steals intellectual property, the results would be bad for everyone.

14.8 Our theft is helping the software / music industry increase their sales.

And when they ask you to help them with their marketing strategy, you can propose this model and discuss it. It is truly bizarre to think that forcing a marketing strategy on unwilling participants is an acceptable action. How would you feel if you were running a store and someone else decided to take your products and give them away without your permission because "the give-away is a great loss-leader and you'll recoup your losses with increased visibility and sales"?

14.9 No software / music / art should ever be copyrighted — it should always be free.

Do you earn a salary or do you ever plan to do so? Why don't you donate your time instead? Did you pay for your computer? But why? Why not decide that computer hardware shouldn't be patented — it should be always be free? Since when did people who buy their computers, drive purchased automobiles and own

VCRs decide they're in favor of communal property and voluntary labor? And who gave these people the right to determine that other people's labor should be free? If you want to give away your music, do so. If you want to copy music by bands that have released it for free distribution, do so. But don't claim to be following a principle that you won't apply to your own labor.

14.10 But I need it and I don't want to pay for it.

Even if you could define *need* so flexibly as to include your wish to use someone else's tools or art without paying for them, how does that justify theft? Are you going to rob a bank tomorrow so you want — oh, excuse me, *need* — a car? Or why not just mug someone so you can have their jacket? Why should the use of the Internet and special software negate our normal attitudes towards fair dealing with other people? *Cyberspace is not a place,* it's just a word for a method of communications; normal obligations and constraints that govern civil society are hardly to be ignored simply because we're using modems and T1s. Being dishonest by using a computer is not fundamentally different from being dishonest in any other way.

14.11 In addition to the specific arguments above, it would be a *Good Thing* to discuss ethical decision-making with your children.

We should challenge those who use sloppy thinking in condoning their own or others' abuse of other human beings' work. Here is a hierarchy of questions that we can all use in making ethical decisions:

- Are there explicit laws making the proposed action illegal?
- Are there formal guidelines such as codes of ethics or policies that bear on the issue?
- Who gains and who suffers from the action?
- Would you be proud to have your name broadcast on national TV with a description of your act?
- Would you like to tell your boss about what you're doing?
- Would you be happy to describe your behavior to your parents or to others in your life whose opinions you respect?
- Would you object to having the proposed action be done to you?
- Does your proposed action violate standards of trust? integrity? truthfulness? gratitude? justice? kindness?
- Are you treating other people with respect by engaging in the proposed action?
- Do you approve of the consequences if everyone acted as you are proposing?

Resources:

Stolen Software, Music and Videos

- Business Software Association (BSA) **http://www.bsa.org**
- Copyright and Fair Use Site at Stanford University **http://fairuse.stanford.edu/**
- Recording Industry Association of America (RIAA) **http://www.riaa.org**
- Software Information Industry Association (SIIA) **http://www.spa.org/**
- "The Napster Cantata" and "Making Ethical Decisions" by M. E. Kabay in HTML and PDF at **http://www2.norwich.edu/mkabay/ethics/index.htm**
- Zeropaid: The File Sharing Portal **http://www.zeropaid.com/**

15 Plagiarism

A different kind of fraud involving intellectual property is misrepresenting someone else's work as if it were your own. Older children know that this is supposed to be bad, but for young children, this issue is completely. The problem today is that plagiarism is easier than ever and harder for teachers to detect.

Academic guidelines try make it clear to students that copying other people's work without attribution is *plagiarism* and is severely frowned upon. Plagiarism includes not only direct quotation without acknowledgement of origin but also paraphrasing that merely shuffles the ideas around a little or substitutes synonyms for the original words. In many institutions, plagiarism is grounds for suspension or expulsion. In all cases, plagiarism defeats the purpose of writing assignments by eliminating the critical thinking and creative expression. Few plagiarists remember what they have copied once they hand their material in.

Assuredly, students have traded term papers and other assignments for centuries. However, the availability of electronic documents and of the World Wide Web has enormously increased the fund of material that can be plagiarized and the ease of copying. Worse still, some people are profiting from easy accessibility by selling papers specifically for plagiarism and even writing papers to order. In one study by Peggy Bates and Margaret Fain of the Kimbel Library at Coastal Carolina University, the authors easily located over 100 sites on the Web selling or donating papers to students.

Happily, science has come to the aid of beleaguered instructors by providing automated similarity analysis of any paper submitted electronically. The system uses a bank of more than 100,000 term papers and essays as well as documents located on the WWW; analysis uses pattern recognition to measure similarities among different documents and to estimate the probability of plagiarism. According to the **turnitin.org** documentation, "Our system is now being used in the majority of universities in the United States and the U.K., as well as a large number of schools around the world. Many of these institutions, among them UC Berkeley and the fifty-eight member schools of the Consortium of Liberal Arts Colleges, an association of the most respected liberal arts schools in the U.S., have chosen to ensure the academic integrity of all their students by selecting institution-wide subscriptions to our service. Other universities, such as Harvard and Cornell, have elected to make use of our system on a departmental or single-instructor basis."

Practical Guidelines:

- Discuss plagiarism clearly at home and at school.
- Use examples to illustrate the difference between plagiarism and legitimate, honest and open use of other people's work.
- Encourage children to practice summarizing information in their own words.
- Practice writing references to quoted material.
- Have a student submit a sample term paper to the **turnitin.org** analysis program for an automatic *Originality Report.*

Plagiarism

- Discuss how anti-plagiarism sites analyze documents to measure similarities and help teachers identify plagiarism.

Resources:

- "Cheating 101: Paper Mills and You" (revised 2001) by Margaret Fain and Peggy Bates **http://www.coastal.edu/library/papermil.htm**
- "Plagiarism and the Web" by Bruce Leland of Western Illinois University **http://www.wiu.edu/users/mfbhl/wiu/plagiarism.htm**
- Plagiarism.org **http://www.plagiarism.org**
- "Plagiarism: What It is and How to Recognize and Avoid It" from the Indiana University student manual **http://www.indiana.edu/~wts/wts/plagiarism.html#plagiarized**
- **turnitin.org** overview: **http://www.turnitin.org/new.html**

16 Criminal Hackers & Hacktivists

At some time, someone is going to tell your children how much fun it is to hack into computer systems and networks. It's a bad idea. I'd like you and your children to understand what happens on the other side of that modem – on the other side of that Internet connection – when someone uses a computer system without permission. In the following text, I am going to address your children directly.

16.1 Story of an Operations Manager

Let me tell you a little about myself first.

I began programming computers when I was 15. It was 1965: that's probably around the time some of your parents were born. Then, computers were bigger than a sports-utility vehicle (SUV). The equipment needed enormous power cables many inches thick to supply all the electricity. The computer rooms depended on gigantic air-conditioning units the size of four refrigerators to carry all the heat away. And all of this expensive equipment could serve exactly *one user at a time.*

Some big computers had about the same ability to do arithmetic as a hand-held programmable calculator of today. We used to tell the computers what to do by writing instructions – *programs* – using punch cards (rectangular cards with holes in rows and columns).

Gaining unauthorized access to computers back then was hard because they were locked up. The only way you got to program the computer was to hand in your cards through a window. If the technicians knew you or if you could show them your identification, they would feed your cards into the computer.

Whenever you finished running your program, it would disappear from the computer – that is, from the random-access memory or *RAM* – and someone else's program would be loaded into memory so it could be run or *executed.*

Giving your name to the technician was a form of *identification.* Identification means telling who you are. The next step was *authentication. Authentication* means proving that you are who you say you are.

Showing your ID card from your school or from your employer is a form of *authentication* because it represents something that only you are supposed to own. When you or your parents enter a bank-card into the automatic teller machine, that card is the *identification.* When you or your parents punch in the personal identification number (PIN), you are *authenticating* yourselves to the bank's computers.

Identification and authentication (known to security people as "I&A") are very important in today's computer systems. There are four ways to authenticate oneself:

- what you have,
- what you know,
- what you are, and
- what you do.

For example,

- Some computer systems read a special card (a *smart card*) that has a *microprocessor* in it. The microprocessor is the part of a computer that does computations and comparisons. This smart card belongs only to you: this is *what you have*. This method of authentication is similar to how we carry physical keys with us to let us into homes or cars. The microprocessor in a smart card makes it harder to make a fake smart card because it contains secret and unique information. That is, it is hard to *counterfeit* smart cards.

- Today, instead of speaking to a technician, now we usually type in a *user-ID* and give a *password* that no one else is supposed to know. This is *what you know*.

- Sometimes modern computers use other forms of I&A; for instance, some computers look at your fingerprints, the shape of your hand, your eyes (retinas or irises), or your face. They identify and authenticate you by *what you are*.

- Some computer systems recognize your voice or your handwriting to identify and authenticate you: they use *what you do*.

Well anyway, back in the 1960s and 1970s, computers and communications continued to evolve. Computers began to allow several people – even hundreds or thousands of people – to use them all at the same time. It also became possible to use computers from much farther away than in the old days. The development of *modems* meant that you could reach a computer from many miles away by using the phone system. Computer *networks* became more important in the world of computing during the 1980s.

However, remote access made it easier to use computer systems without permission. For example, people could find out your user-ID and password and pretend to be you – after all, there was no technician to check to see if it really was you.

16.2 Early Hackers

Many computers back then had tight limits on how many hours of use you had on the computer every month. Someone who used your user-ID was really stealing computer time from you. These people who used the computer in your name were among the earliest *criminal hackers*.

Criminal Hackers & Hacktivists

For a long time, people in the computer field used the word "hacker" to mean someone who enjoyed learning about technical matters such as amateur radios and computers. Unfortunately, the news media started using the word to refer to people who used computers and networks without permission and now they often see the word as bad. I prefer to refer to *criminal hackers* to make it clear that being interested in computers does not have to mean breaking the law.

So let's go back to criminal hacking.

Some people used passwords that were easy to guess. They used their own name, or their dog's name, or their favorite sports team. Finding that kind of password is easy because there are only a few words to try. Trying out all the words in a list of likely possibilities is known as a *dictionary attack*.

But even if your password is not in a dictionary, it is still possible to try all possible passwords. Trying all possible passwords is called the *brute-force* method. Because today's computers are so fast, using the brute-force method to find out your password is easy, especially if your password is short or has only letters. To make brute-force attacks harder, use passwords that are at least eight characters long and have at least one number or special character (e.g., !$%?&*_-+=<>) in them.

- Other criminal hackers *trick* people into revealing their user IDs and passwords using deception or threats. The criminals call this *social engineering* and it remains an important method of getting into closed systems even today.

None of you should reveal your password to anyone. On some big networks (like AOL and CompuServe), some people (even children) have been posting fake messages that appear on your computer screen when you are online. The messages claim that you have to send in your user name (user ID) and password; some of them ask for your credit card too. The messages threaten that if you don't send in this information you will lose your access to the service. This is not true.

No real official of any Internet Service needs to ask you for your password anytime. These demands on your screen are social engineering by criminals or sometimes by children who are trying to trick you into letting them into your accounts.

Don't ever give anyone your password.

So what do we mean by *criminal hacking*? It means using a computer without the permission of the owners. Criminal hackers claim that what they do is harmless as long as they don't change any information on the systems they break into.

You may very well already know some criminal hackers, because some of them are still children. Many children who become criminal hackers think that what they're doing is just good harmless fun – like a neat video game. They are wrong, and I'm going to explain why they're wrong.

16.3 The Parkerian Hexad

To understand why using a computer system without permission causes problems, you have to understand the goals of information security. Information security involves six different aspects that need protection:

- confidentiality,
- control,
- integrity,
- authenticity,
- availability, and finally
- usability.

These principles are called the "Parkerian Hexad" in honor of the famous information security expert Donn Parker, who first identified these six elements as the fundamental goals of information security back in the 1980s.

Let's look at these one by one.

16.3.1 Confidentiality

Security experts talk about *confidentiality*. Confidentiality refers to limits on who can get what kind of information. For example, you might want to keep it secret that you have a crush on that cute kid who sits in front of you. If someone were to find that out and tell other people, that would be a breach of confidentiality.

Your parents' bank account number and their secret number (the PIN, or Personal Identification Number) can allow a thief to take money out of their account at the banking machine. If somebody were to find out those numbers, that would be a breach of confidentiality.

16.3.2 Possession or Control

Possession or control is another kind of protection for information. Imagine what would happen if you wrote down your parents' bank account number and PIN in an envelope and then gave it to a stranger. Even if the stranger promised not to open the envelope, your parents would be frantic. They would be worried because they would no longer have *control* over their own secret number and over their own bank accounts.

Something very similar – a *loss of control* – would occur if strangers broke into your house when everyone was away. Even if they didn't do anything, you would still feel uncomfortable. You would feel that you couldn't trust the food because you wouldn't know if maybe the strangers did something bad to your food. Your parents might even want to throw the food away just in case. You might feel uncomfortable because maybe

the strangers looked in your diary. These would all be indications of a breach of control. In the world of computing, we say that such a loss of control destroys the *trusted computing base*. There's more about the trusted computing base in section 16.5.

16.3.3 Integrity

Security people next consider the issue of *integrity*. Integrity refers to being correct. For example, suppose somebody took one of your exam papers and made your answers wrong. This would be a breach of integrity.

If someone were to take a check that your parents wrote and changed the amount payable, *that* would be a breach of integrity. Changing information without permission is a breach of integrity.

Criminals have altered medical data. Changing medical records can lead to very dangerous situations for the patients. For example, sick people might be given the wrong medication.

Some criminal hackers have played around in school records. They changed grades that were recorded by teachers. Now of course, this may sound funny, but it stops being funny when you think about what would happen if somebody changed *your* grades and made them worse or made someone else's grades a lot better. Unauthorized modification of data is a *breach of integrity*.

16.3.4 Authenticity

Another principle of security is *authenticity*. Authenticity means that we should label or describe information correctly. For example sometimes a criminal hacker sends electronic mail in somebody else's name. In one case, a professor in a Texas university found that someone had broken into his e-mail account. The hacker sent out two thousand e-mail messages in the professor's name. These e-mail messages were full of hateful, racist language and therefore people who got the messages became very angry with the professor. This was not fair, because the professor didn't write the messages. However, he and his family received death threats and had to be put under police protection when people threatened to burn the family house down. This is an extreme example of the harmful results of a *breach of authenticity*.

Think about how embarrassing it would be if someone sent e-mail messages in *your* name that said things you didn't agree with. Suppose someone were to insult your teachers by sending them messages signed with your name. You might get into a lot of trouble even though you had not done anything wrong.

Protecting authenticity is one of the reasons that you must never reveal your password to anyone. You have to protect the authenticity of your communications.

16.3.5 Availability

The fifth principle of information security is preservation of *availability*. Availability means having timely access to information. *Timely access* refers to getting hold of the information you need when you need it. For example, suppose you have to write an essay on the novel, *The Wind in the Willows*. You want to read the novel before you write the essay. If someone hides all the copies of the novel at the library and at the bookstores, you can't read the novel in time for your essay. That would be a *breach of availability* of that novel.

We call one of the most serious and widespread problems in today's computers *denial of service*. Denial of service can occur when someone overloads a computer system or network with bogus requests.

One bad case of denial of service occurred when someone who called himself "Johnny [x]Chaotic" subscribed dozens of people to hundreds of e-mail lists. These poor people began receiving e-mail on basket weaving, engineering, plumbing – you name it. One writer received 20,000 e-mail messages in a single day. Imagine trying to find your own e-mail messages if someone sent you 20,000 messages you did not want. It would take hours just to read through the subject lines to find the e-mail you wanted. That would be a *denial of service*. Denial of service is a *breach of availability*.

Perhaps you have heard about the massive denial-of-service attacks that took place in February 2000 against many large e-commerce sites such as Amazon, e-Bay and so on. The FBI (in the U.S.) and the RCMP (in Canada) cooperated to track down the perpetrator, a 15-year-old Montreal boy who went by the *handle* "Mafiaboy" on the 'Net. A *handle* is an online nickname (or *pseudonym*). It seems that this child boasted about shutting down businesses in the denial-of-service attacks and gave detailed information about the exact timings of the attacks – clues which led the federal police forces to find him.

16.3.6 Utility

Finally, the sixth principle of information security is *utility*. Utility means usefulness. For example, suppose you went to the local store and all of the prices were listed only in Dalgadian Blowati Units (I made that up) but nobody knew how many Dalgadian Blowati Units there were in the Dollar. That pricing would not be very useful to you even though it might technically be correct.

If a criminal hacker were to change your grades in the school computer so that they were *encrypted* (converted using a special rule) but no one knew how to convert them back to normal numbers, that would be a *breach of utility*. This kind of problem has actually occurred in some businesses, where programmers encrypted the programs needed for work. Without the special *decryption keys* the information was no longer useful, even though there were no other breaches of security. After all, the information locked up in the encrypted form was still confidential, under the control of the owners, still had complete integrity, was authentic, and was available. It just wasn't *useful*.

Here's an example of a normal message and its encrypted form just to show you what encrypted information looks like (I used a program called PGP, which stands for "Pretty Good Privacy"):

Original message: Hi, this is *plaintext* that I will convert to *ciphertext*.

Encrypted message:

```
-----BEGIN PGP MESSAGE-----
Version: PGP Personal Privacy 6.5.8
Comment: Digital signatures increase security for everyone.

hQBsAzPd6/an40lzAQMAozojZYxZNZNwSAS/1mxCekAv/GvGTKxN67DMSwigL1/3
mMiDJKSEY+6ajbtsZU7uMvvsqdYu4+8q7FK4HO3a4tN1FPJ5j5Cr9z4zcqbkCfir
Li6p3glXSZFPzQwKAKMMpMdZO3zgzSAGtakTek2GkVp8PWR+uGV1Z7h9SWyj9azl
rFvztKIOylSndcTATDEyTHiera9EZShSGnZz18OOCqYavg1KjRmOUO+d20zni2wG
tkPoOL2/vm9gsrmKNsWvGTd1rOcwfcEFXFSx1VnJo/NssB3PAoH+SjV5lqAqyuSA
28np6rn4vFxkasMBpOZqtzI1RUH5HYEeYKdnN+kCsORgMvs29knWbO2t9MSopQKk
Hsi5Gxceh8z/s7WDqnwl6VKMzsO22/N3
=5/S/
-----END PGP MESSAGE-----
```

16.4 The Effects of Computer Penetrations

Now that you have some idea of what information-security people worry about, it's easier to understand why breaking into somebody's computer system is really bad.

Of course the obvious problems concern confidentiality, integrity, availability and authenticity.

Going into a computer system and reading other people's documents, other people's e-mail, or information relating to national security in military computers are obvious breaches of confidentiality. Such breaches can cause real problems. For example, one thirteen-year-old child in Florida got into the medical records of people at the clinic where her Mom worked one Saturday a few years ago. The girl called a dozen people who had gotten blood tests the day before and she lied to them: she told them they had AIDS. The victims of her sick joke were terrified. One teenager's parents stopped her just as she was about to shoot herself with her dad's pistol. So taking and using confidential information can lead to terrible consequences.

Changing accounting records, stealing money by making false bank transfers, altering prescriptions so that people can become sick, sending out false e-mail using other people's names – these breaches of integrity and authenticity are all obviously bad.

One of the most popular forms of criminal hacking today is Web vandalism: damaging Web sites by substituting often obscene pictures and offensive text for the original materials. The CIA was renamed the Central Stupidity Agency; the Florida Supreme Court's Web page was turned into an illustrated sex-manual – you get the idea.

The people doing the damage are often children or young teenagers. These *cybervandals* are just like the youngsters who throw rocks through people's windows or who spray-paint curses and foul words on buildings. Maybe they are expressing their rage and rebellion – or maybe they're just trying to be liked by the crowd they hang around with. From the point of view of the Webmasters, though, they're childish nuisances who cause extra work for nothing.

Another group of criminal hackers claim to be noble political idealists; they call themselves or are called *hacktivists* and they deface Web sites that they think belong to political enemies. In the recent Kosovo war, both sides in the conflict damaged each others' Web sites. Hackers in the People's Republic of China and in Taiwan have been attacking Web sites in each other's countries for years.

The recent denial-of-service attacks that may have been launched by children have caused billions (yes, billions) of dollars of lost sales and costs of recovery. These attacks used hundreds and perhaps thousands of computers to swamp the victims with requests for information. Criminal hackers installed special *slave* or *zombie* programs on poorly-secured computer systems. These slave programs were then ordered to attack the main victims using coded communications from the criminal hacker controlling them. The slave programs made the computers they were on send out thousands of messages to the victims' computers, swamping their communications. No one else could get much of a response from the computers under attack

Part of the cost of cleaning up after the denial-of-service attacks came from having to pay employees to search out the slave programs and remove them.

Some criminal hackers claim that if they don't alter information, they haven't done anything wrong – or at least, they haven't done anything *really* wrong, as they say. This point of view is simply, flatly incorrect and I want to explain how it's incorrect.

16.5 The Trusted Computing Base

The fundamental problem caused by unauthorized access to information systems is loss of control. Let me explain what really happens when somebody breaks into a computer system – that is, accesses the system without authorization.

First you have to understand that many people depend on computer systems to get their work done. The computer systems they depend on are known as *production systems*. For example the local banks need to have computers to process people's paychecks. The computers must take the right amounts from the employer bank accounts and must deposit the right amounts in the employee bank accounts. What do you think happens in the bank if someone breaks into their computer system? I'll tell you: it's a real mess.

The poor bank employees don't know whether the intruders have damaged some of their bank records or programs. Even if the criminal hackers leave a note (you know, "W3 D1DN'7 D0 4NY7H1NG WR0NG C4U53 W3R3 313373" using that silly code (technically a *monoalphabetic substitution algorithm*) of theirs – see if you can figure it out), how do the employees really know if everything's still OK or whether the hackers have damaged something?

The only thing to do is to check. Security experts say that such a system is no longer *trusted*. We say that these systems have been *compromised*. The employees have to reestablish trust in the data and also in the programs.

Criminal hackers have been known to insert their own changes to certain computer programs. Criminal hackers often leave what are called *back doors* into the systems they've already broken into. Back doors allow the hackers to re-enter the compromised computer systems anytime they want. This kind of change to

system software is a real threat to the people that have been victimized. It can take days to check all of the information on a computer system that has been broken into. Sometimes the checking costs hundreds of thousands of dollars in wasted salary or consulting fees.

I remember that when I was in charge of a big computer center in the 1980s, my staff and I would spend from midnight to six in the morning every day for five days testing the new version of the computer operating system (something like the Windows or MacOS or LINUX programs that you may use on a personal computer) for the large computers or *mainframes* that we used. We would work hard to see if the new software was working properly.

Now remember, that software was sent to us by the computer maker. If we were willing to spend five nights testing the *manufacturer's* software, doesn't that tell you how important trust was for us? Now think about why on earth we would trust a production system that might have been damaged by a criminal hacker. It wouldn't make sense. *We have to check the system after every intrusion.* So that's why it's not true that breaking into computer systems is harmless fun.

So you see, breaking into somebody's computer system isn't a video game. *Hacking computers hurts real people.* The victims of hacking spend sleepless nights away from their families working hard to see if their computer systems have been damaged by intruders. They worry about it. If there has been damage, it can cost lot of money to fix the data and the programs. This money lowers profits for companies or increases costs for nonprofit organizations. Sometimes the damage makes companies raise their prices.

16.6 Stealing Services

If the criminal hackers laugh at the costs and tell you that "it's only a company – it's not real people" then you will know that they are either stupid or they are deliberately lying to you. Organizations are made of real people. Real people lose because of criminal hacking.

Criminal hackers also sometimes take services from the telephone companies without paying for them. For example, they use special phone numbers called *teleconference bridges* to talk to each other. The company that rents the bridge ends up paying a lot of money per minute for those stolen phone calls. Stealing telephone services is known as *phreaking*.

Some criminals claim that phreaking doesn't hurt anyone. I have spoken with phreakers who argue, "Well, the phone company's stuff is already paid for and it's just sitting there, so how can it hurt to use their networks as long as they are not all being used? It doesn't cost them anything."

This argument is wrong because in fact even ordinary telephone calls do cost something to the company that is being cheated. Any phone call that goes between the areas controlled by different local phone companies must be paid for by transfers of money from the originating phone company to the destination phone company. It gets even worse for international calls. International agreements govern long-distance phone calls; these laws force automatic payments from the originating telephone company to an *interexchange carrier* and then to every other company that carries the signal. So stealing phone calls is truly stealing, with money flowing from the company that is cheated to all the other companies involved in the call.

If your friends tell you they are playing with *blue boxes* or *red boxes*, it means they are stealing phone services. These boxes (which may be computer programs nowadays rather than physical boxes) generate the sounds that control the long-distance telephone switching computers and trick the companies into granting free calls. Don't get involved with these thieves.

16.7 Persistent Internet Connections

Recently many homes have been wired with coaxial cable or satellite dishes for Internet access. Many of these systems allow the subscriber to be permanently connected to the Internet. The difficulty is that all the users on the same segment of cable in the neighborhood or, in some cases, on a *subnet* of the satellite system, may have access to each other's computers. Because the default security on ordinary systems is to *share* devices such as printers and disks, it is trivially easy to read other people's files, modify or delete them, and to print nasty pictures on old Mrs Olsen's color printer next door. It is therefore crucial to install *firewalls* on computers that are left connected to the Internet to prevent unauthorized access.

16.8 Scanning for Vulnerabilities

Some children are having fun using hacking software to scan other people's computers for vulnerabilities. One of the most valuable functions of firewalls on personal computers is that they can demonstrate the magnitude of the problem: every time someone tries to look at your computer, your firewall can pop up a window to let you know and ask if you want to allow the inbound connection (*No,* you *don't*). The log files can then be used to measure the level of attacks.

16.9 Denial-of-Service Attacks

Finally, parents should be aware that their children may be involved in the kind of amusement that brought down Amazon.com and eBay.com in February 2000: denial-of-service (DoS) attacks. There are two broad types of DoS attacks: individual and distributed. Individual attacks use software that launches a stream of requests at a target system; usually these are forged packets that contain incorrect information about their origin, causing the target system to waste resources and generally slow down. In severe cases, a DoS attack can shut down a Web page or a Web site. Worse still are the distributed DoS (DDoS) attacks, in which automated attack tools locate vulnerable systems and install *zombie* programs on them. The zombies listen via the Internet for coded signals from a *master* program that tells them when to launch their DoS attacks against a particular target. Because hundreds or even thousands of infected computers can be involved in this launch, the cumulative effect can be overwhelming. Some victims of DDoS are pushed completely off the Web or the Internet during the attacks. For e-commerce sites, such unavailability may be catastrophic.

Practical Guidelines:

- If you are interested in computers and want to know more about criminal hackers, you don't have to go to meetings of the *2600* group in your city (these are people who read *2600: The Hacker Quarterly* and talk about computers and – sometimes – how to break into them or steal services). You can learn a lot by joining the computer club at school, participating in discussion groups online, and reading.

- To learn more about real computer security, make arrangements (get your parents and teachers to help) with computer system administrators at your school, local hospitals, offices and factories. Ask them what happens if someone breaks into their systems.

- Get system and network administrators to speak to your school computer club.

- Contact your local FBI office and find out if they can send a speaker to your school for a discussion of computer crime.

- If you do visit Web sites that support criminal hacking, be sure to use a personal firewall, as discussed in the section on persistent Internet connections.

Resources – these are written for adults but are accessible to children who are willing to work hard at finding the words they don't know in a dictionary.

- Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition.* Wiley (New York). ISBN 0-471-41258-9. 1200 pp. Index.

- Campen, A. D., D. H. Dearth, & R. T. Goodden, eds. (1996). *Cyberwar: Security, Strategy, and Conflict in the Information Age.* AFCEA International Press (Fairfax, VA). ISBN 0-916159-26-4. vii + 296.

- Fialka, J. J. (1997). *War by Other Means: Economic Espionage in America.* W. W. Norton (New York). ISBN 0-393-04014-3. xiv + 242. Index.

- Forester, T. & P. Morrison (1990). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing.* MIT Press (Cambridge, MA). ISBN 0-262-06131-7. vi + 193. Index.

- Freedman, D. H. & C. C. Mann (1997). *@Large: The strange case of the world's biggest Internet invasion.* Simon & Schuster (New York). ISBN 0-684-82464-7. 315 pp. Index.

- Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century.* O'Reilly (Sebastopol, CA). ISBN 1-56592-653-6. vii + 312. Index.

- Goodell, J. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick--and the Man Who Hunted Him Down.* Dell (New York). ISBN 0-440-22205-2. xix + 328.

- Gordon, S. (1993). Inside the mind of Dark Avenger (abridged). Originally published in *Virus News International* (January 1993). **http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html**

- Gordon, S. (1994). Technologically enabled crime: Shifting paradigms for the year 2000. Originally published in *Computers and Security*. **http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html**

- Gordon, S. (2000). Virus writers: The end of innocence? Presented at the 10th International Virus Bulletin Conference. **http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm** and **http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.pdf**

- Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368. Index.

- Kabay, M. E. (2002). "Information Security Resources for Professional Development" available in HTML and PDF from **http://www2.norwich.edu/mkabay/overviews/index.htm**

- Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick--The Inside Story of the Great Cyberchase.* Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.

- Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace.* Que. ISBN: 0-78972-443-X. 450 pp.

- Schwartau, W. (1991). *Terminal Compromise* (novel). Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5. 562 pp.

- Schwartau, W. (2001). *Internet & Computer Ethics for Kids: (And Parents & Teachers Who Haven't Got a Clue).* Inter-Pact Press (Seminole, FL). ISBN 0-962-87005-6. 200.

- Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--by the Man Who Did It.* Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.

- Slatalla, M. & J. Quittner (1995). *Masters of Deception: The Gang that Ruled Cyberspace.* HarperCollins (New York). ISBN 0-06-017030-1. 225 pp.

- Smith, G. (1994). *The Virus Creation Labs: A Journey into the Underground.* American Eagle Publications (Tucson, AZ). ISBN 0-929408-09-8. 172 pp.

- Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* Bantam Doubleday Dell (New York). ISBN 0-553-08058-X. xiv + 328. Index.

- Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Pocket Books (Simon & Schuster, New York). ISBN 0-671-72688-9. viii + 356.

- Winkler, I. (1997). *Corporate Espionage: What it is, why it is happening in your company, what you must do about it.* Prima Publishing (Rocklin, CA). ISBN 0-7615-0840-6.

17 Online Auctions

The theory behind an auction is that the competition for an object or service helps participants determine a fair price. This process can be corrupted in a real-world, physical auction if the seller conspires with confederates to bid up the price artificially. Unfortunately, such shenanigans are even easier online, where anyone can have as many identities as they want. The ease with which browsers and e-mail systems allow forged headers and forged identifiers means that someone could inflate the price of their own offering.

The Federal Trade Commission of the United States reports that online auctions cause the largest number of complaints they receive annually about fraud.

This theoretical discussion does not even begin to address such questions as whether the auctioned items really exist, are as described, or will ever be delivered. A recent case of such fraud occurred on eBay, where Robert Guest of Los Angeles admitted in court in July 1999 that he defrauded victims of around $37,000 by offering goods for auction via eBay but failing to deliver anything. The customers of Mr Guest certainly found out the hard way that they were being cheated — but how, exactly, were they to know in advance that he was untrustworthy?

EBay has responded to these concerns by (a) suggesting the use of escrow services and (b) telling its users that it does not guarantee the legitimacy of the transactions it facilitates.

There are also concerns about the legality of some of the items put up for auction. Someone offered items made from endangered species for sale on eBay, in violation of the Convention on International Traffic in Endangered Species. The revolting products included dried feet of elephants and gorillas caught in snares and allowed to die excruciating deaths before being hacked into pieces. In the U.S., buying, selling and possessing such contraband can lead to arrest, prosecution and fines or imprisonment.

More ludicrously, someone put up a human kidney for sale through eBay in September 1999 and received bids of up to $5.8M. The auction service canceled the sale because selling human organs is a Federal felony with up to $250,000 in fines and at least 5 years in jail. A week later, eBay had to shut down an auction for an unborn human baby. Prices for the supposed baby had risen into the $100K range before eBay pulled the plug. Finally, a fool or a prankster — it's unclear which — tried to sell 500 pounds of fresh marijuana online via eBay. The auction was shut down after 21 hours, during which prices offered had reached $10M.

So do you think that all the bids were legitimate? Did everyone who bid for kidneys, babies and pot really intend to pay for what they were claiming? Or was it more like a video game, where no one was taking any of it for real? And what does it mean for ordinary users to realize that nobody knows for sure which explanation was correct?

Even if the items being offered for sale online are ordinary things such as software or physical products, how does one know if they are legitimately obtained? Online auctions are a perfect channel for fencing stolen goods.

Online Auctions

Practical Guidelines:

- Before becoming involved with online auctions, do some research about the value of the goods you are interested in buying. Check bricks-and-mortar stores as well as online retail outlets that provide you with specific prices.

- Examine the policies and costs on shipping, warrantees, and refunds.

- Set your upper limit before you get involved in an auction. Don't let yourself be influenced by other people's apparent view of the value of a particular product or service.

- Don't treat online auctions as a competition you have to win by placing the highest bid.

- Look for auction services that provide a guarantee of support if you are cheated in a transaction. For example, check for language in the terms of service that covers losses up to a suitable limit. Check for insurance policies, costs, terms, and limits. Use search engines to evaluate the trustworthiness of the service you are thinking of using.

- If possible, use a service that provides an escrow function so that you pay money to the service and then you can release it only when the product is received in good condition.

- Use the browser functions to print documents and save Web pages to disk at every stage of your transaction.

Resources:

- "Buying at online auctions" **http://gcorner0.tripod.com/other/onlineauction.html**

- "eBay.com Rules & Safety Overview" **http://www.zdnet.com/zdnn/stories/news/0,4586,2569405,00.html**

- "Fraud grows among online auctions" by Jim Carlton and Pui-Wing Tam
  http://pages.ebay.com/help/community/index.html

- "How to survive online auctions: Avoiding the swindlers of cyberspace (1999) by David Noack
  http://www.apbnews.com/safetycenter/specialreport/onlineauctions.html

- "Online Auctions: Deal or Steal" (2001) by Audri & Jim Lanford Internet ScamBusters #43
  http://www.scambusters.org/

- "The scoop on online auctions" by Robin Boyd **http://www.bbb.org/library/auctions.asp**

- "Tips for Consumers: Online auctions" (1998) from the Better Business Bureau
  http://www3.lifeserv.com/essentials/fun/article.asp?ArticleID=2438

18 Online Gambling

In 1998, the Arizona Lottery discovered that no winning number in its Pick 3 game had ever included a single numeral 9 [see the RISKS Forum Digest volume 19 number 83, usually referred to as "RISKS 19.83"; an archive copy is at **http://the-other.wiretapped.net/security/info/textfiles/risks-digest/19/risks-19.83**]. It turned out that the pseudo-random number generator algorithm had an elementary programming error; Alan Hamilton wrote, "Why do I have a sneaking suspicion that their code probably looked like INT(RND * 9)?". You can imagine the howls of outrage by everyone who had used a 9 in their lottery numbers — especially when they were told they could have a refund, but only if they had kept their old losing tickets.

The Arizona lottery was using a simulation of a random process to provide the illusion to gamblers that they were betting on a physical process such as balls mixing together in a barrel and falling out of a tube.

One of the problems with the Arizona simulation is similar to a genuine vulnerability in proprietary (i.e., secret) cryptographic algorithms. As Prof. Dorothy Denning of Georgetown University and many other cryptographers have stressed over the last two decades, the security of an encryption scheme should not depend on the secrecy of its algorithm. Had the lottery algorithm been exposed to public scrutiny, its flaws would have been detected sooner. For example, in the 1980s there was much excitement over a new encryption scheme called the knapsack algorithm; it proved to be flawed after extensive examination by cryptographers. Mind you, it is conceivable that someone detecting the flaw in the Arizona lottery might have made bets with a higher probability of winning than those of uninformed people, but that would have been made less likely by exposing the algorithm and its implementation to scrutiny before it went into production.

I hope that by now, any of my readers who gamble online (or for that matter, use an electronic gambling machine of any kind) are thinking nervously about how much trust they ought to place in such gambles.

On another level, at least physical devices (electronic or mechanical) are located in real-world establishments under the nominal control of regulatory and law enforcement officials. Gambling schemes based on real-world events such as races and contests have a form of validation in external news reports. But on what basis should a gambler trust the results of computer-generated pseudo-random numbers displayed on a display screen or on a browser page?

It's not as if one can use the laws of the market to count on identifying screwy results from online gambling. Most individual gamblers will never know if the long-range analysis of the pseudo-random numbers supports their hope in the fairness of the odds. No one is keeping track of these data except the people making money from the participants, and they're not distributing the results of their goodness-of-fit and runs tests.

The disclaimer at one Internet gambling portal, "FINDinternetCASINO" is not very encouraging:

> Although every attempt has been made to ensure fairness and security toward the player at each of the links that can be found in the directories, FindInternetCASINO® cannot be held responsible if discrepancies occur between an Online Gambling operation and you, the player, after following a link from this WWW site. Consult your local authorities prior to registering with any online wagering

service. U.S. Citizens: The information at this site is for entertainment and news purposes only. Use of this information in violation of any federal, state or local laws is prohibited.

In some jurisdictions, betting online is illegal. In the United States, for example, it is illegal to use interstate telecommunications to place bets; in addition, there are several initiatives to ban Internet betting even if the host is outside the United States. On February 28, 2000 in Manhattan federal court, Jay Cohen was convicted of operating a sports betting business that illegally accepted bets and wagers on sporting events from Americans over the Internet and telephones. Cohen was convicted of conspiracy to violate the Wire Wager Act and seven substantive violations of the Wire Wager Act in connection with his operation of World Sports Exchange ("WSE").

If you insist on gambling, you may want to check the ratings for a specific operation on the Fair Bet site.

In summary, Garrison Keillor of the "Prairie Home Companion" radio show from Minnesota Public Radio says, "Buying lottery tickets is a tax on people who aren't very good at arithmetic." I'm sorry to say that at this point in their development and regulation, *online gambling* may be a tax on people who are just too trusting.

Practical Guidelines:

- Don't gamble with money you can't afford to lose.
- If you do gamble, don't gamble with money using online gambling.
- If you do gamble online, don't gamble with money at sites hosted outside your own country.
- Don't give your credit card number to online gambling centers that are outside your own country.
- If you gamble online at a site hosted in your country, do some research to find out if there have been complaints about its service: contact your Better Business Bureau or equivalent and see if you can find friends or acquaintances who have played on the site you are considering.

Resources:

- "Borderless betting: The emergence of online gambling" (1999) by Elliot Almond **http://seattletimes.nwsource.com/news/sports/html98/gamb_012499.html**
- [Interview with founder of Fair Bet describing fraudulent casino] **http://fairbet.org/cgi-bin/display.pl?page=pop_up**
- Fair Bet **http://fairbet.org/cgi-bin/display.pl**
- "Hill stymied by online gambling" (2001) by Patrick Ross **http://news.cnet.com/news/0-1005-200-5192243.html**

Online Gambling

- "Jay Cohen convicted of operating an off-shore sports betting business that accepted bets from Americans over the Internet" (2000) U.S. Department of Justice press release
  http://www.usdoj.gov/criminal/cybercrime/cohen.htm

- "Log on, double down" (1997) second of two articles by Michael Bradley
  http://www.shorecast.com/html/Features/ScFeatures/FeatOnlineGam2.html

- "Online gambling: sleazy or safe?" by Herman Manson
  http://www.mediatoolbox.co.za/new/aspen_viewartaspen.dll?Aid=1071&temp=12

- "Wanna bet? Look offshore" (1997) first of two articles by Michael Bradley
  http://www.shorecast.com/html/Features/ScFeatures/FeatOnlineGam.html

19 Buying on the Web

What about buying stuff from normal merchants through the Web? Surely e-commerce can't be all bad?

Of course not. If you know about the organization selling goods and services, there is no more reason to be worried about buying from them through a Web connection than buying from them over the phone or in person in a store. Web sites belonging to recognized merchants or other organizations (e.g., non-profit charities) are trustworthy, especially if they show any of several symbols representing compliance with various standards of security for customer data. Some of the safety seals you can look for include:

- TrustWatch from GeoTrust: "Potential buyers won't spend time on a site unless they know from whom they're getting information or who's really selling the goods and services. All businesses want a Web presence, but they need to be sure it will be effective in helping customers 'know' the business. Big stores and long-recognized brands are recognized in the physical world, but what about online? In the anonymous world of the Web, consumers want to be certain about the site they're visiting, to know the business behind the site is real. Identity is the foundation for trust. When identity is known, trust can develop and business can follow. Without identity, legitimacy will always be suspect. TrustWatch is an identity solution for business Web sites. Site association with a business is checked, and site owners are provided with an active digital icon for their Web site. Consumers, seeking to know and trust the Web domains they visit, will know from the icon if the Web site owner is a TrustWatch member. And, if the site belongs to a TrustWatch member, consumers will have access to business information about that enterprise. It's a way to show legitimate sites and make eCommerce safer." – from the TrustWatch page at GeoTrust.

- TRUSTe: "TRUSTe is an independent, non-profit privacy initiative dedicated to building users' trust and confidence on the Internet and accelerating growth of the Internet industry. We've developed a third-party oversight 'seal' program that alleviates users' concerns about online privacy, while meeting the specific business needs of each of our licensed Web sites." – from the TRUSTe Web site.

- WebTrust: "WebTrust is a service jointly developed by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) and adopted globally by the accounting profession. WebTrust enables consumers and businesses to purchase goods and services over the Internet with confidence that vendors' Web sites meet high standards of privacy protection, business ethics and security." – from the WebTrust Web site.

One alarming technique that some firms have been studying is *dynamic pricing*. Dynamic pricing presents a different price to different customers. By building a profile of a specific customer's buying habits, an unscrupulous crew of vendors can inflate prices for people who appear to be more willing to buy higher-priced goods and lower prices for those who are cost-conscious. Many bricks-and-mortar stores do the same, in that stores in some parts of town may cater to richer people than in other areas; similarly, some chains of stores have been documented as charging higher prices to poor people in ghettos than in suburbs in part because there is less competition in poor neighborhoods. A different kind of dynamic pricing occurs in the airline industry, where seats on planes vary in price according to when they are booked and where they are placed in a plane.

However, unlike these examples, in dynamic pricing on the Web, the fundamental difference is that the prices are varied secretly so that only the victim of the predatory pricing sees the offered price. Without mechanisms for sharing information among purchasers, this model of pricing puts the buyers at an immense disadvantage with respect to the seller.

Another key area of concern when buying products on the Web is privacy. Many consumers prefer their buying habits to remain their own business; receiving unwanted paper mail or junk e-mail seems intrusive and irritating to them. Other consumers like the convenience of receiving news about new products and special sale prices. Whichever you prefer, it's important to pay attention to the privacy policies offered by online vendors. Signup options often include choices on whether to opt into or opt out of distribution lists; if you do accept to be contacted by the vendor, there are often questions about whether you want to allow other firms to be given your personal details so *they* can contact you with special offers.

Some sites such as bookstores and music services may keep a detailed record of what you browse and what you buy from them. With time, these Web sites tailor the face they present to you so that you see advertisements that are more and more appropriate to your interests. Amazon.com, for example, tries to be helpful to visitors by suggesting books that may interest the returning visitor based on previous behavior. However, one of the unexpected consequences of such customer profiling is that the appearance of such a Web site may inadvertently reveal more about the user than they expect; if you watch one of your children enter such a Web site and discover that the predominant theme is, say, weapons and techniques of terrorism, you might want to have some serious discussions with your young person to learn more about this interest. Conversely, if you have been searching the Web for really good sex manuals and videos, you might want to be prepared for questions yourself when you log on to your favorite online bookstore with your eight year old watching.

Another issue often raised in discussions of privacy is cookies. Cookies are small text files that a site stores on a visitor's hard disk to store information that can be used the next time the user visits the site. Properly-defined cookies can be used only by the site that deposited them. The information stored can include the sequence of Web pages the visitor saw or personal identifiers that allow the Web software to recognize the visitor so that the Web site can build up a preference profile for each visitor or client and to enable those cheery greetings like, "Welcome back, Bob! We have a special deal for you on the newest title in *The Real Man's Guide to Heavy Artillery* series!"

In general, cookies are harmless. If you don't like the idea of having identifiers stored on your system, you can either block cookies globally or on a site-by-site basis using settings in your browser or in your personal firewall. You can also use cookie-sweeper programs that get rid of all cookies whenever you want.

Practical Guidelines:

- Before spending whatever you consider to be a lot of money on a new online merchant's site, do some basic research into the site's reliability. Check the company's reputation; see if it belongs to the Better Business Bureau and contact the appropriate chapter of the BBB to see if there have been complaints about the vendor.

- Do a Web search using a good search engine such as Google to see if there are any up-to-date reports about customer experience on the site you are interested in.

- Pretend that you already have a problem and look for the customer service pages. Are there clear instructions on how to communicate problems? Would you have the choice of e-mail, letters and phone communications? If you have the time, you may even want to try calling customer service and find out just how they handle calls. If you hit a company that hangs up on you when their lines are busy ("We are sorry, but all our agents are busy; please call back later."), you might want to give serious thought to whether it is safe doing business with such people.

- Read the company's return policy; how do they handle breakage in transit or defective goods? Do they offer guarantees on delivery time? What happens if they are out of stock on a specific item — do they ship partial shipments or wait for everything to be ready? If they split your shipment, do they charge extra for delivery for the later parts?

- Read the site's privacy policy. If the text is practically invisible 6-point yellow on white, be suspicious. Look for weasel-words in the clauses that say that, for instance, the policies can be changed at any time without notice (what are you expected to do, check the site regularly to see if the policy has changed?). Look in particular for firm, clear assurances that the firm will not sell, trade or give your personal information to other unrelated businesses without your permission (usually there are explanations that the Web site owner may have to divulge your contact or delivery information to partnering organizations that handle such normal functions as billing and fulfillment of your orders).

- Keep a detailed record of your transactions. Use the browser functions to save copies of or to print the relevant Web pages (descriptions of the product, prices, summary of your order, order number, promised delivery date and method).

Resources:

- "Be An Educated Consumer: Know the Danger Signals of Scams" from the Better Business Bureau **http://www.bbb.org/library/educatedcons.asp**

- "Buying computers by mail" from the Better Business Bureau **http://www.bbb.org/library/compmail.asp**

- "Check out a company" at the Better Business Bureau **http://www.bbb.org/reports/bizreports.asp**

- "Cybershopping – What you need to know" from the Better Business Bureau **http://www.bbb.org/library/cybershop.asp**

- GeoTrust **http://www.geotrust.com/** and **http://www.geotrust.com/building_trust/safe_market/trustwatch.asp**

- "Learn to Identify Deceptive Ads" from the Better Business Bureau **http://www.bbb.org/library/deceptads.asp**

- TRUSTe home page **http://www.truste.org/**

- "WebTrust Certification: Your essential e-commerce Web site enhancement **http://webtrust.net/**

20 Games

Parents may want to read reviews of video games before allowing their young children to play them. Some games have astonishing levels of graphic violence ("Brilliant Bleeding! Detailed Decapitations!!") and unusual values ("Win points by burning as many residents to death as possible!"). This latter example is based on a notorious case in which a video-game vendor was apparently surprised by the public wave of revulsion over a game that glorified arson. Some military and police shoot-'em-up games explicitly take points off for hitting innocent bystanders; others do not. Some games use graphic nudity; others are more modest. The main point is that relying on the judgement of eight-year-olds is not necessarily the best approach to choosing entertainment for children.

Practical Guidelines:

- Learn to play some of the games your children are enthusiastic about. Take the time to immerse yourself in the imaginary worlds they play in and study the underlying values that are being communicated by the game creators.

- Use published reviews from online or paper sources that reflect your own family's values before allowing games into your home.

- Accompany your children to the stores when buying video games. Check for parental warning labels. Talk to the salespeople if you think they are reliable.

- Know the characteristics of your hardware and software before buying recently-released games. Don't buy a souped-up game only to discover that it doesn't run on your ancient Windows 3.11 system with 16 Mb of RAM and a 90 MHz processor — you could find that a disappointed child can apply astounding pressure to spend money on a new system. Some games are computationally intensive and require advanced (read, expensive) hardware such as 32 Mb video cards with fast vector graphics and large amounts of system disk space (up to a Gb for a single game) and extra system RAM. In addition, some games are not satisfactory without modern sound systems (e.g., woofers and subwoofers on a 60 watt RMS per channel amplifier).

- Try making game playing an opportunity for family fun or parent-child bonding instead of the isolating experience games can sometimes be. See if you can all have fun with puzzle- and exploration-oriented games such as *Myst* and *Riven* (neither game involves violence and both are visually beautiful).

Resources:

- "Content rating and filtering" **http://www.efa.org.au/Issues/Censor/cens2.html**

- "Guide to parental controls/Internet safety products" **http://www.microweb.com/pepsite/Software/filters.html**

- Platform for Internet Content Selection (PICS) **http://www.w3.org/PICS/**

21 Spyware

In December 1999, computer scientist, cybercrime investigator and writer Richard Smith became curious about a program called *zBubbles* that he had installed on his system to improve online shopping. Created by Alexa, a subsidiary of e-tailer Amazon.com, the program provided competitive information about alternative and possibly cheaper sources for particular products. However, Smith discovered that there was more going on than met the eye.

Smith monitored his own Internet traffic while he was using zBubbles by using a packet sniffer (a tool that displays details of every piece of information being transmitted through a network connection). He found that zBubbles was sending a steady stream of information about him and his surfing habits to Alexa, including his home address, the titles of DVDs he had browsed on Buy.com, and the details of an airline ticket he had verified online. In addition, the program even continued to send information regularly to Alexa's servers even when Smith was not using his browser.

Many programs are available which, once installed, report on which Web sites you visit, which banner advertisements you click, what products you search for and any other information the programmers have defined as interesting. Even widely-used file-download software such as NetZip have been shown to report to their providers on the names of every file downloaded by their users.

Sometimes these programs are informally known as "E.T." applications, in a reference to Steven Spielberg's movie of that name, in which an extraterrestrial person strives to "phone home" – exactly what the spyware programs are doing.

The term *spyware* is applied to any technology that transmits information without the knowledge of its user. Several *freeware* programs distributed through the Internet secretly collect information about the user, monitor user behavior and then send those data to advertisers. The more general class of monitoring software that collect information for use by advertisers is known as *advertising-supported software* or *adware*. These programs allow freeware to make money for its creators by generating revenue based on how many users transmit information to the advertisers about their habits.

Although defenders of the advertising-supported programs claim that they are harmless, privacy advocates argue that the issue is control: do users know what these programs are doing, or are they collecting and transmitting information covertly? Some adware comes with complicated contracts which use complex legal language to bury the fact that they will monitor and report user behavior. Worse, many such contracts explicitly authorize the software supplier to alter the privacy conditions without notification and, preposterously, instruct the user to check the contracts on the Web frequently. No one has the time to monitor countless suppliers to see if privacy conditions have been altered, especially if there is no attempt to highlight changes.

Another issue is that some spyware modules have used *stealth* technology characteristic of viruses, Trojan horses and other malicious software. For example, some adware (e.g., TSADBOT) installs itself as a system process and is not listed in the Windows task list – and therefore cannot easily be aborted by a user. TSADBOT also resists removal; even if the carrier product is uninstalled, TSADBOT persists. If a user's firewall blocks outbound transmission by the TSADBOT process, the spyware initiates attempts to reach its target at a rate of ten per second, potentially leading to CPU and network resource overload.

Spyware

Spyware, like any software, can contain errors that cause system problems. In particular, components of the Aureate/Radiate spyware have been shown to cause system instability and crashes.

One of the most egregious cases of spyware erupted in 1999, when it was discovered that CometCursor, a supplier of cute cartoon-character cursors aimed at children, was sending information back to its servers about what the children were browsing on the 'Net. According to some attorneys, this kind of covert data gathering about children is potentially a violation of the U.S. federal Child Online Privacy Protection Act.

Several free software programs have been written to help users identify and remove spyware. In addition, personal firewalls can identify, and block unauthorized outbound communications. There is also a specialized program available that runs in the background to monitor and thwart attempts to install spyware.

Practical Guidelines:

- Before installing freeware or adware, read the terms and conditions carefully to see if they include language permitting automatic transfer of information to the supplier or to third parties. Be aware that these contracts often include language authorizing the supplier to change the terms and conditions at any time and without notifying you.

- Install and use a spyware scanner and removal program such as the free *Ad-aware* program from Lavasoft or the more extensive PestPatrol, which spots about 30,000 different types of unwanted software

- If you are particularly irritated by spyware, install a real-time spyware monitor and blocker such as the $15 program *Ad-aware Plus* which is also available from Lavasoft.

- Support legislative attempts to force software manufacturers to disclose their use of spyware.

Resources:

- Information on TSADBOT **http://cexx.org/tsadbot.htm**

- Lavasoft **http://www.lavasoft.de/aaw/aaware.html**

- PestPatrol **http://www.pestpatrol.com**

- Radiate/Aureate spyware information **http://grc.com/oo/aureatemail.htm**

- Spyware Control Act **http://grc.com/spywarelegislation.htm**

22 Scumware

In recent years, a new way of abusing computer users has spread like a disease through the Web: *scumware*. Scumware is any software that significantly changes the appearance and functions of Web pages without permission of Webmasters or copyright holders. For example, a number of products overlay banner advertisements with other ads, sometimes for competing products. Scumware may add unauthorized hyperlinks to a user's view of a Web page – sometimes using links to possibly objectionable sites. Such programs can interfere with existing hyperlinks by adding other destinations to the intended target. In addition, some products install themselves without warning users of these functions; others bury the details of their Web-page modifications in the extensive legalise of end-user license agreements. Some scumware is difficult or impossible to control; for example, the programs are difficult to uninstall, introduce instability into the operating system, and conflict with other applications.

Scumware is sometimes known as *thiefware*.

One of the best-known instances of scumware was better documented than most: the Microsoft XP Smart Tags "feature" was announced as an improvement for MS-Office products. Using Smart Tags, specific words in lists could have pop-up menus; these menus could offer options for useful functions such as choosing the style of pasting wanted for text (e.g., formatted, unformatted and so on). Smart Tags were also planned for the MS Internet Explorer (IE) v6 Web browser; however, many critics argued that the way Smart Tags were to be implemented, there would be an opportunity to hijack Web content by showing extra hyperlinks. These extra links would direct users to MS-related sites or to sites which had bought space in the Smart Tag space. There were waves of outrage all over the industry and MS withdrew its proposal for Smart Tags in IE.

The essential problem can be summarized as follows: a Webmaster creates a Web page and includes links and advertisements. Some other company or person provides software to a user that alters the functions and appearance of the Web page before the user can see the intended Web page. Many vendors and users say that it's the user's own business what they do to the Web page once it reaches the user's own computer; however, many Webmasters and other content providers argue that their work is being modified without their permission.

But how is what scumware does any different from, say, having a user put a Post-It (TM) note on her monitor that obscures part of a Web page? Surely users can do what they want with Web pages that have been copied to their own cache?

Well, no, not really.

From my point of view as a lay observer, the arguments presented by the opponents of scumware boil down to the following:

- Scumware makes unauthorized changes in the appearance and content of Web pages that affect more than a single user.

- The changes imposed by scumware interfere with contractual relationships between Web content providers and advertisers.

- The introduced advertisements and links may convey a false impression implying relationships and possibly endorsements that do not exist.

- The modifications may be creating an unauthorized derivative work.

From an international perspective, European laws are more restrictive than U.S. laws in defining what are called the *moral rights* of not only a copyright holder but also the rights of the creators of intellectual property. Scumware, under this doctrine, may violate the content-creator's rights of integrity, disclosure, retraction, and replies to criticism. Unauthorized modification of what users see on a Web page may violate all of these rights.

Those opposing scumware will have to articulate why they don't also go after firewalls and ad-blockers that speed up Web access by reducing the amount of graphical data transmitted to a browser. Perhaps one factor reducing the outrage over *blocking* ads is that no one is going to be offended by *not* seeing an ad; although the advertisers may not like the idea, at least there is no chance of casting the Web site in a false light (an important element of the concept of defamation in US jurisprudence).

From a purely ethical (as opposed to narrowly legal) standpoint, it seems to me that scumware is a bad idea on several grounds:

- The people who benefit from the introduced materials (links and ads) are not the people who invested time and money in creating the underlying content; this situation seems unfair.

- If everyone engaged in such behavior, Web pages could become cluttered with extraneous matter and obscure the underlying content entirely – just imagine running several different scumware programs at once to see what might result.

- Obscuring other people's messages and adding unauthorized linkages seems disrespectful of the human beings who created the original Web page; such behavior seems to me to be disregarding the Web designers' feelings and intentions.

Scumware

Practical Guidelines:

- First, you must decide if you approve of having advertisements and hyperlinks inserted into the views of Web pages that appear on your screen. If you do, there's no problem and you can stop reading this column.

- For those who don't like the idea of extraneous links and ads, the most obvious measure for preventing infestation is not to install scumware at all. Unfortunately, this is not as easy as one would like. As we have seen in previous articles, scumware can infest other software and be installed with little or no notice to the user. Nonetheless, before installing freeware, shareware, or adware (products that offer services in return for sending the user targeted ads), everyone would do well to read about the product using an Internet search engine such as Google.

- Check the lists of known scumware at Scumware*Links **http://www.freegraphics.com/zz-scumware/** to see if the product you are thinking of installing is a known offender. Without gritting your teeth too hard, read the end-user license agreement (EULA). Look for language, no matter how convoluted or how tiny the point size, that indicates that the product is likely to add to or modify the appearance of Web pages you download. In addition, look for language that threatens to delete or inhibit any of your *other* programs.

- After you have installed *any* software, from no matter what source, always keep your firewall active if at all possible. Be sure to configure your firewall to alert you to any attempt to contact an external address from inside your system; although such attempts may be necessary (e.g., for updates to critical components), in many cases they can be blocked safely. You can always study the issue more closely if necessary by examining the TCP address of the target and doing a reverse IP-block lookup to find out where the critter is trying to connect. Once you know the name of the registrant and the Domain Name System entry for the target, block the transmission without hesitation if you don't know why a module on your system is trying to communicate with a site you know nothing about. You can always reverse your decision later if you determine that the connection is in your interest.

- To identify undocumented or forgotten adware, spyware and scumware, several real-time scanners can spot trouble for you. For example, Lavasoft makes Ad-aware, a simple, free and reliable product that scans your system for unwanted intruders and removes these programs from your computer. See **http://www.lsfileserv.com/** for details of Ad-Aware.

Resources

- Definitions:

  http://wuas.org/

  http://www.thiefware.com/

  http://stacks.msnbc.com/news/618966.asp

- Smart Tags:

  http://office.microsoft.com/assistance/2002/articles/oQuickSmartTags.aspx

  http://news.cnet.com/news/0-1003-200-6210768.html?tag=mn_hd

  http://www.alistapart.com/stories/smarttags/

- Analyses of the scumware problem:

  http://scumware.com/press.html

  http://stacks.msnbc.com/news/618966.asp

  http://www.suniltanna.com/ezula.html

  http://stacks.msnbc.com/news/618966.asp

  http://catless.ncl.ac.uk/Risks/21.47.html#subj8

  http://twcny.rr.com/technofile/texts/bit100301.html

  http://twcny.rr.com/technofile/texts/bit101001.html

  http://twcny.rr.com/technofile/texts/bit101701.html

23 Internet Addiction

Any activity can become the basis of compulsive exaggeration. A small proportion (perhaps around 5%) of the Internet-using population may qualify as addicted to any of the following computer-mediated activities:

- Uncontrollable desire to find and organize more information about an enormous range of topics;
- Excessive involvement in games, gambling, and buying things on the Internet;
- Excessive concentration on relationships mediated through e-mail and chat rooms to the detriment of real-life relationships;
- Involvement in long sessions of viewing pornography or sexual simulation via e-mail, chat rooms or sexual-fantasy games.

The issue here is what constitutes *excessive* involvement in these activities. Professional psychologists such as Dr Kimberly Young have identified some of the diagnostic criteria for these disorders, including the following based on her *Internet Addiction Test:*

- Regularly staying online longer than intended
- Often neglecting obligations to spend more time online
- Consistently preferring to spend time online instead of with one's partner
- Frequent complaints by friends and family about excessive Internet use
- Suffering consequences at school or at work because of time spent online
- Giving e-mail a higher priority than other important issues
- Concealing the extent of Internet usage
- Turning to the Internet as a substitute for dealing with disturbing issues
- Feeling that life without the Internet would be devoid of meaning and pleasure
- Getting angry when disturbed during Internet usage
- Losing sleep due to late-night Internet activity
- Yearning to be back online.

Internet Addiction

Anyone who feels uncomfortable about their level of involvement with the Internet would do well to take the little test offered by Dr Young and seek counseling to prevent possible tragic consequences of untreated addiction.

Practical Guidelines:

- Know the warning signs of Internet addiction and self-monitor.
- Discuss Internet addiction and its warning signs with your children.
- Encourage open discussion of feelings about the 'Net so that children feel free to turn to you for help if they become uncomfortable or unhappy about their own experiences on the 'Net.

Resources:

- *Caught in the Net: How to Recognize the Signs of Internet Addiction – and a Winning Strategy for Recovery* (1998) by Kimberly S. Young. Wiley, ISBN 0-4711-9159-0.
- Center for On-Line Addiction **http://www.netaddiction.com/**
- Computer Addiction Services **http://www.computeraddiction.com/**
- *Virtual Addiction : Help for Netheads, Cyberfreaks, and Those Who Love Them* (1999) by David N. Greenfield. New Harbinger, ISBN 1-5722-4172-1.

24 Theft of Identity

In the last few years, theft of identity has become a problem affecting a growing number of victims.

Published stories in the news media tell dreadful tales of people whose identity has been appropriated by criminals. The perpetrators use detailed information about the victims to obtain new credit cards, new lines of credit, new bank accounts, new cars, and new criminal records. The victims often find out about the theft of their good name when a loan is turned down, a credit-card application is refused, a new employer becomes alarmed by a criminal record, or the police arrest the victim after a routine traffic check.

Worst of all is the reversal of the burden of proof. Where normally the immense apparatus of the state has to establish a reasonable basis for arrest and a strong basis for conviction, in identity theft the victims have to prove their innocence by proving their identity. Being handcuffed and dragged to the local police station is never fun but it's even more humiliating and enraging when you are innocent but the police assume you're guilty.

Practical Guidelines:

How can one defend oneself against such theft?

- Basically, until it gets harder for imposters to appropriate someone else's identity, the only method is vigilance.

- If you have an existing relationship with your local bank, try asking your customer service officer to check your record for you and let you know what (s)he finds.

- You can write directly to the credit bureaus to obtain your credit records, but it's a hassle. PrivacyGuard, a $59.95/year service, reports on what the three major credit bureaus are carrying about a subscriber and summarize their findings in a single consolidated report. The welcome package has printed labels for easy access to the subscriber's file at PrivacyGuard. Most important, they also monitor corrections the subscriber sends in to the credit bureaus to ensure that the corrections get into the files and they alert the subscriber to all enquiries and changes in the records. PrivacyGuard includes a toll-free hotline for help in an emergency. They also supply envelopes and forms for requesting reports directly from the MIB (Medical Information Bureau) and for the national driver's license database. You can get information about PrivacyGuard from **http://www.privacyguard.com/ctg/cgi-bin/PrivacyGuard**.

- Make sure that all your financial institutions are instructed not to change your contact information without checking with you personally.

Theft of Identity

Resources:

- The U.S. government's Federal Trade Commission (FTC) has a comprehensive ID Theft central site at **http://www.consumer.gov/idtheft/**. It has downloadable booklets, forms, and even videos dealing with the problem.

- The FTC also has a page full of links to helpful credit-related documents (in text or in Acrobat PDF) at **http://www.ftc.gov/bcp/menu-credit.htm**, including several dealing with identity theft – especially "Identity Crisis… What to Do If Your Identity is Stolen" and "Identity Theft: Identity Thieves Can Ruin Your Good Name."

- For a helpful booklet from the FTC, download **http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf**

- Another excellent resource packed with material is Mari J. Frank. Esq.'s site at **http://www.identitytheft.org/** where you can find an "ID-Theft Survival Kit" and "Identity Theft Resources" for prevention and response.

- In the broader sense, stay aware of breaking news on the issues of privacy legislation and case law. For information on legislative issues in the USA centering on privacy in the electronic realm, see the Web site of the Electronic Privacy Information Center at **http://www.epic.org/**

- For a global perspective on electronic privacy issues see Privacy International at **http://www.privacyinternational.org/**

About the Author

M. Kabay began teaching himself assembler at age 15 and was programming in FORTRAN IV G at McGill University by 1966. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. Until 1979, he was a university professor in applied statistics. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S., being responsible for developing the statistical syntax, writing the parser, error traps and code generation for statistical functions in the command language. Kabay joined Hewlett-Packard in 1980 and became a performance specialist, winning the Systems Engineer of the Year Award in 1982. After a few years working in a large service bureau as operations manager, he founded and ran JINBU Corporation from 1986 to 1998. Kabay has specialized in consulting and training for systems performance, systems operations, and systems security.

Kabay was Director of Education for the National Computer Security Association (later ICSA, Inc. and TruSecure Corp.) from 1991 to the end of 1999. He attained the status of Certified Systems Security Professional (CISSP) in 1997. He was Security Leader for the INFOSEC Group of AtomicTangerine, Inc. from January 2000 to June 2001 and joined the faculty at Norwich University in July 2001 as Associate Professor of Information Assurance in the Department of Computer Information Systems. In January 2002 he became the director of the graduate program in information assurance at Norwich (see **http://www3.norwich.edu/msia**).

Dr Kabay has published over 450 technical papers in operations management and security, including columns for *Computer World, Network World, Computing Canada, Secure Computing Magazine, NCSA News, Information Security Magazine* and *Network World Fusion* (see **http://www.nwfusion.com/newsletters/sec/**).

He won the Best Paper Award at the 16th National Computer Security Conference in 1993 for his submission, "Social Psychology and INFOSEC: Psycho-social Factors in the Implementation of Information Security Policy." He wrote a college textbook, *The NCSA Guide to Enterprise Security: Protecting Information Assets* (ISBN 0-07-033147-2), published by McGraw-Hill in April 1996. He was the technical editor of *The Computer Security Handbook, 4th Edition* published (ISBN 0-471-41258-9) by Wiley in April 2002.

Kabay was the leader of the International Delegation of Computer Security Experts to China in April 1994 organized by the Citizen Ambassador Program. He was the Program Chair for the First and Second International Conferences on Information Warfare in Montreal in 1993 and 1995 and was the organizer of the "Interdisciplinary Perspectives on Information Security" series of symposia at the National Information Systems Security Conferences. Kabay was invited to lecture on computer security to the chiefs of the counter-intelligence services of NATO in Germany in 1995. He was asked to present his comments to the President's Commission on Critical Infrastructure Protection in Washington in 1997 and was invited to address INFOSEC specialists at NATO HQ in Brussels in March 2000. Kabay has been a frequent keynote speaker at security conferences in the U.S. and in Germany. He has been program chair for over 50 technical conferences since 1986 and serves as Program Chair for the annual eProtect-IT Conference on Infrastructure Protection at Norwich University (see **http://www.e-protectIT.org**).

M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Program Director, Master of Science in Information Assurance (MSIA)
Program Director, Bachelor of Science in Computer Security and Information Assurance (BSIA)
Dept of Computer Information Systems, Dewey Hall
Norwich University
158 Harmon Drive
Northfield, VT 05663-1035 USA

V: +1.802.479.7937
E: **mkabay@norwich.edu**
W: **http://www2.norwich.edu/mkabay/index.htm**

