CHAPTER 1

Web Hoaxes, Counterfeit Sites, and Other Spurious Information on the Internet

Paul S. Piper

LipBalm Anonymous (www.kevdo.com/lipbalm) is an intriguing site. It's a twelve-step program for lip balm addicts, an idea so absurd that it is obviously false … or is it? There are people who use lip balm quite frequently until it has become a habit. There are also people who believe that lip balm producers might have few qualms about covertly adding habit-forming ingredients, such as those that might dry the lips, to substances as innocuous as lip balm. Does it matter if it is a clinical addiction or not? This site does an excellent job of mixing credible information into a mix of probable paranoia and fantasy. When Kevin Crossman, the site's author, was contacted about the veracity of his site, his written response was that he resented the accusation that his site was categorized as misinformation. "Lip balm addiction is a REAL thing. LOTS of people take our site seriously." There you have it, straight from the creator's mouth. Is it legitimate? A hoax? A spoof? How do you know? Read on.

A Rough Taxonomy

The categories these sites fall into are counterfeit, malicious, product, fictitious, parodies/spoofs/entertainment, hacks, and disinformation. Another source of disinformation on the Web is mistakes. Anyone, from the most senior editor of the most prestigious news organization to a student putting up a class project, can make honest mistakes involving everything from typos to accidental omissions. Due to the accidental nature of these errors, they will not be dealt with here.

A true counterfeit site is one that attempts to pass itself off as an authentic site much as a counterfeit $20 bill attempts to enter the economy as currency. The sites here mimic the look and feel of the original or attempt to, in the case of the www.gatt.org site. Some organizations have as part of their agenda the hosting of Web sites that intentionally misguide information seekers and, within their free speech rights to host information on the Net, disseminate information that is often discriminatory or factually misleading. These sites are categorized as malicious. Product sites are legitimate commercial (.com) sites that slant their information toward selling a product. The information on these sites, though not false, is often misleading and needs to be taken for what it is—an advertisement. These sites include medical and business sites, areas where misinformation can have dangerous consequences. Fictitious sites are those that represent something completely fabricated, such as a city that does not exist. Parody/spoof sites are counterfeit sites that use humor to poke fun at an original site, product, or organization. Even though their intention may be political, they typically are not malicious, and their "misinformation" is fairly obvious. And hacked sites are sites that have been modified by hackers for any number of reasons.

While misinformation is typically understood to mean "wrong" information, a lot of Web content details issues of opinion rather than fact. Information that we might consider overly biased or wrong may prove useful to someone arguing against that agenda. For example, a person who is against capital punishment might benefit greatly from knowing how death penalty advocates think. Since many of the parody and spoof sites on the Web are political, they often contain antithetical information that might prove useful given the proper context. There aren't absolutes.

These categories are not airtight and often overlap. The martin lutherking.org site, while in the counterfeit category, might be considered a malicious site; the Mankato, Minnesota, site is a spoof and also a counterfeit site. Add to this mix an enormous array of opinions, polemics, prophecies, and pundits, and it all adds up to a great convoluted complex of misinformation that needs to be deciphered. What these sites all have in common is that they pass off information that is questionable or misleading, to varying degrees, and they often do it using the illusion of legitimacy.

Counterfeit Web Sites

Counterfeit sites are the most troublesome of hoax Internet sites. The Martin Luther King site just mentioned exemplifies a site pretending to be something it is not, a Trojan horse so to speak. Counterfeit sites disguise themselves as legitimate sites for the purpose of disseminating

misinformation. They are not always attempts at humor or spoof, and even when humorous, they are often misconstrued. The intentions of counterfeit sites are as varied as the sites themselves but can be roughly divided into several categories: political, for fun, or instructional.

The martinlutherking.org site is a particularly troubling example of deceptive data, while pretending to be, on the surface, an "official" Dr. Martin Luther King, Jr., site. The home page as of March 2002 depicts a photograph of King with an unflattering quote from *Newsweek* 1998, and links titled "Truth About King," "Jews and Civil Rights," "Historical Writings," "Death of the Dream," "The King Holiday," and "Suggested Books." Underlying these areas, however, are other links to sites that are of questionable relationship to Dr. King. These include instances of his supposed plagiarism, to David Duke online, and to a speech by Jesse Helms that supposedly connects King to the Communist party. One that is particularly disturbing gives a description of Martin Luther King, the night before he was shot, partying with three white women, one of whom (it claims) he beat up. The counterfeit Martin Luther King site seems specifically targeted toward student research. (Prior to March 2001, this site was less obvious in its slant, featuring a home page with a family photo, although the underlying links and pages were similar in content. The original page is still available for viewing in the Google Archives. Search the URL "martinlutherking.org" and choose the archive option.) A number of alerts appeared on library and educational LISTSERVs and warned teachers and educators of the existence of the site and the identity of the sponsor.

Two top page clues belie the true intention of this site. The e-mail link displays a link to vincent.breeding@stormfront.org. The home page for Stormfront, the site's sponsor, claims to be a resource for White nationalists, "those courageous white men and women fighting to preserve their white western culture." The link to the Web design by Candidus Productions brings up a page that states, "Welcome to the Candidus Productions Web site! We provide various Web applications for pro-White people online." But most visitors do not normally click e-mail and Web design links. Even the underlying pages, although obviously advocating White power (the recommended books include *My Awakening* by David Duke), can easily fool less sophisticated Web users because the information is presented in a "factual" manner, cites "government documents," and the design is polished and appears sympathetic to King.

One of the first counterfeit sites to draw attention was the www.makah.org (no longer extant) site that appeared during the controversy over the Makah Tribe's harvest of gray whales. The Makah's official tribal page is www.makah.com.

The Makahs, a Washington coastal tribe, had won federal appeals to harvest a few gray whales in an attempt to resurrect tribal tradition. They immediately came under attack by environmental and animal rights organizations. One of these protest groups created a Web site that mimicked the authentic tribal site. Behind its look-alike home page, however, the counterfeit site contained anti-whaling information and called the Makahs murderers. The Makah whaling issue attracted national press, and the counterfeit site began getting many hits from surfers, who assumed that .org was the real domain for the tribe.

Once behind the site, there was no attempt to disguise the bias of the information, and the third-person personal pronouns and verbal attacks clued the reader immediately to the site's agenda. However, on the Web, getting someone to the message is a primary achievement. The fake Makah site is now gone, the official site still exists, and the Makahs still harvest gray whales. Elaine Cubbins of the University of Arizona Library has created an insightful and thorough guide to evaluating Native American Web sites (see www.u.arizona.edu/~ecubbins/webcrit.html). She notes that potential for tribal misrepresentation arises when an individual tribal member or faction within the tribe creates a site and claims it is representative, or when a site is counterfeited. Dawn Jackson, a spokeswoman for the Native American Communications Council (NACC), which seeks to be a watchdog for disinformation on this subject, stated (*Newsbytes*, February 3, 1995), "The anonymity of online services allows for unscrupulous individuals to present disinformation on Native cultures and beliefs to serve their own personal agenda."

The spate of anti-World Trade Organization (WTO) protests in Seattle, in November 1999, launched the creation of another highly sophisticated, and extensive, counterfeit Web site that claims to be the home page of the WTO (www.gatt.org). (The official WTO site is www.wto.org.) While this site features underlying anti-WTO information and uses the names of popular radical celebrities (Andrei Codrescu, the Romanian author and commentator on National Public Radio, is listed as the fiscal manager of the Media Fund), these are largely inside jokes. It is a detailed and sophisticated site.

In a press release by the WTO (www.wto.org/english/news_e/pres99_e/pr151_e.htm), Director General Mike Moore stated that counterfeit Web sites created confusion for the public looking for legitimate information. And he is obviously right. According to the *New York Times* (January 7, 2001), a trade group in Salzburg, Austria, the Center for International Legal Studies, thought the page was the official WTO site and requested Mike Moore, via e-mail, to address their conference. The site's sponsors were only too happy to oblige, sending a Dr. Bichlbauer as their representative to the conference. His presentation, which claimed among other things that Americans

would be better off auctioning their votes in the presidential election to the highest bidder, offended many attendees. The fracas continued, with the phony Dr. Bichlbauer supposedly hit in the face with a pie and, upon returning to the states, hospitalized due to a "biological agent" that was present in the pie. Dr. Bichlbauer's death was announced via e-mail several days later, eliciting the first recognition from the legal center that the entire thing had been a hoax. It doesn't end here, however, as a representative for the site's organizers claims that an invitation to a textile conference in Finland will lead to the successor of Dr. Bichlbauer attending.

The Ed Report (www.edreport.com) is a bogus government report that was created by two creative writers, William Gillespie and Nick Montfort. The site is deliberately blasé enough to be mistaken for bureaucratic, and is broken into segments that sound legit: Letter from the National Security Council, Charter of the Ed Commission, Summary of Findings, Latest Press Release. Named after James Ed, a fictitious 28-year veteran of the National Security Agency, the authors were inspired to create this site after the mass attention given to the Starr Report that, according to CNN, triggered the heaviest Internet traffic until that date. (The Starr Report of September 1999 detailed alleged misdeeds by President Clinton.) The Ed Commission was supposedly chartered to investigate the recruitment of civilian contractors for use in short-term roles during covert operations. The text of the actual report is subtle but hilarious. It is difficult to tell this site is a hoax until one clicks on Latest Press Release, which mentions that it won an award for New Media Writing. One of the judges, Shelley Jackson, comments that the Ed Report is "a cunning piece of mimicry that manages to maintain an almost chinkless front of officialese while telling a funny, surreal, even touching story. Purporting to be a report on an ill-fated attempt by the CIA to employ civilians (including Bruce Springsteen) with a gift for ancient languages as code-talkers on a secret narcotics mission and complete with documentary trimmings, it patches into the dynamics of rumor and urban myth to run its operation in the gray area between fact and fiction—a project perfectly suited to the Web, where gray areas abound."

Checking to see who registered a site (e.g., using register.com) is one way to determine validity, but even this approach can be tricky. For example, makah.org is registered to the Makah Nation in Vancouver, Canada, while makah.com is registered to the Makah Tribal Council, Neah Bay, Washington. Only further checking reveals that the tribe headquarters *is* located in Neah Bay, Washington, and the Canadian address is a front. The martinlutherking.org site is registered to Stormfront; the gatt.org site is registered to Prince & Associates Inc., Washington, DC, with an administrative con-

tact of jonathan@KILLYOURTV.COM. An educated guess gives this one away.

Suspicious Web Sites

Collections of photographs of lynchings, and other collections of material that some people call "hate sites," are too numerous and extensive to include here. Some of them are notorious for misinformation because they are couched in quasi-academic discourse, and are subtle or dishonest about their intentions. Others speak with seeming authority claiming that certain historically proven events did not take place at all. The Institute for Historical Review (http://ihr.org) is one example of that kind of site. A self-proclaimed nonideological, nonreligious, and nonpolitical organization, this site propagates one of the most deceitful and brutal myths around—that the mid-20th century European Holocaust didn't occur. While the site touts the number of Ph.D.s it has on its staff, claims it maintains high standards in the pursuit of exactitude in history, and is "sincere, balanced, objective, and devoid of polemics," a skeptic may question this. Certainly the statements made on this site, and others linked to it, such as "Auschwitz Myths and Facts" and the "Problem of the Gas Chambers," run counter to most of the historical literature and contain (at least) subtle anti-Semitism.

Then there's Kennewick Man. In 1996, two students discovered the remains of a 9,300-year-old skeleton on the shores of the Columbia River in Kennewick, Washington. The remains were thought by some scientists to be Caucasoid, a term referring to peoples who originally inhabited Europe, North Africa, and the Near East. The Native Americans of Washington State, however, using a law from 1990 protecting Indian graves found on federal land, claimed the skeleton as an ancestor and demanded it be handed over to them for Native American burial. A federal government agency involved agreed, and placed the remains in safe storage until the mandatory 30-day waiting period had passed. Within days, eight anthropologists, including some from the Smithsonian Institution, filed a lawsuit against the federal agency on the grounds that the tribes had not proven "cultural affiliation." It took almost five years before this case went to trial in June 2001. These are the facts about the skeleton. The Web sites, however, are not always so straightforward.

There are several sites devoted to this issue, but the one called *The Kennewick Man News* site, registered to New Nation News in Berkeley, California, (www.newnation.org/NNN-kennewick-man.html) seems to have an agenda of White power. While the controversial discussions over Kennewick Man's racial origins are legitimate, this site does not have the balance one would expect. In March 2001,

a search for "Kennewick man" on HotBot and Google retrieved this site within the first ten hits. This site is deceptive in that it includes a number of press releases that question the skeleton's origin, which makes it seem like the staff writers for the various local newspapers are agreeing with the site's premise, which denies the aboriginal roots of the Kennewick Man. However, the site goes far over that line and claims that Europeans were the true first settlers in North America and have true rights to the land, not Native American tribes. Aside from the "Confederacy News" link on the first page, there are a number of other tip-offs as to where the true heart of this site lies. For example, it posts the "results" of a survey question: "What is the best solution for racial problems?" The top six responses are as follows:

- Break the USA into White, Hispanic, Black, Asian, and Other Sections: 9 percent.
- Create a biological weapon that targets some races: 9 percent.
- Return to separate but equal solution of the 1950s South: 10 percent.
- Build an organization eventually able to ethnically cleanse the USA: 15 percent.
- Create a Caucasian Homeland in part of the U.S. and secede: 16 percent.
- Abolish all laws forcing integration and minority preferences: 18 percent.

It doesn't take a weatherman to know which way this wind blows.

News

A reputed Associated Press report stated that an anti-hunting group (the Anti Hunting Happy Association) had outfitted more than 400 deer in Ohio with orange hunter's vests in an attempt to make the hunters think that whatever was wearing the vest was a human and thus not shoot to kill. The story implicated sporting goods storeowner Guy Lockey, who offered a reward for each vested deer brought in. Even though hunting season had already ended, Guy Lockey didn't exist, and it is virtually impossible to live-trap deer and put vests on them, the story made a Fox News Network report on January 7, 2002, and was picked up by ESPN.com and the Wall Street Journal Online, and various local newspapers. In fact, it wasn't a real Associated Press report at all, something that these news organizations could have verified. This was a harmless spoof, but it shows how gullible

even news professionals can be when they aren't using critical evaluation skills.

While some may treat the news with certain degrees of skepticism, we as a nation depend on a free press to give us a dose of daily facts. We rely on their filters and verification processes to weed out the dubious (or at least label it as such) and blatantly false. That is why an Internet hoax that is picked up and disseminated as fact by reputable news sources should do more than raise an eyebrow. All media are vulnerable to unverified facts, something Internet users need to keep in mind when they evaluate news reports.

Disinformation

Disinformation, according to the Oxford English Dictionary (OED), came into use in 1954 and means "the dissemination of deliberately false information, especially when supplied by a government or its agent to a foreign power or the media, with the intention of influencing the policies or opinions of those who receive it." In this context, it is a subset of misinformation.

According to *Reuters* (January 5, 1997), the Police Chief of Dubai, Dhahi Khalfan Tamim, stated to the *Khaleej Times* that Israel had launched a disinformation campaign on the Internet. He further claimed that Israel was falsely attempting to portray itself as a peace-loving nation. Obviously, this official perceived the Web as not only having the capability to disseminate disinformation, but to do so effectively.

Just as the war in Vietnam was the first television war, and the war in the Persian Gulf in 1991 was the first live war, the NATO war with Serbia over Kosovo was the first Internet war. James Napoli, in a paper at Book Expo America (BEA) 2000 entitled *Waging War Digitally: The Case of Kosovo*, stated that the "Internet, like the so-called legacy media, was used by warring parties in traditional ways to propel a barrage of propaganda to win the global public to their perspective."

The *Washington Post* (January 25, 2000) detailed the propaganda war Russia had been fighting in Chechnya and how the Web was one of the primary media for dissemination. From false field reports to exaggerated data, information that supported a particular point of view was hosted on an array of Web sites belonging to the various players. Chechen fighters, often isolated from traditional news media, used a Web site as their platform to communicate with the outside world. When they claimed that documents posted on that site were secret Russian documents, the Russians retorted that the documents had been altered from the originals or forged. NATO put its spin on events,

Serbia responded with theirs, and private sites sympathetic to the Serbs, NATO, or the Albanian Kosovars appeared all over the world.

The efforts to sabotage the use of Internet communication accelerated into the creation of a group of Serbian hackers called "Black Hand" who sought to destroy Albanian and Croatian Web sites. Croatian hackers retaliated and brought down the server that hosted the pages of the Serbian National University Library (*Press Now,* October 5, 1999). Online attacks from presumed Serbian saboteurs also corrupted the NATO site, and pro-Serb Russian hackers were suspected in the temporary shut down of the White House site, attacks on NATO's servers, and the U.S. Navy's servers. NATO's Webmaster, Baul Magis, claimed there would be no in-kind retaliation (*MSNBC*, April 1, 1999, April 6, 1999).

According to the Israeli government, a number of Israeli Web sites voicing their government's perspective on the conflict with the Palestinians in the fall of 2000 were jammed with fake traffic by Islamic groups abroad, causing them to crash. The sites targeted were the Prime Minister's Office, the Foreign Ministry, and several army sites, with some of these down for as long as two days. In a separate attack, the Web site of the Knesset, Israel's Parliament, was hacked and files were tampered with and modified. This war continues. On the day that Ariel Sharon took office as Prime Minister in Israel, "hackers, in a growing cyberwar, sent visitors seeking the Hamas Web site to a pornography site" (*Wall Street Journal*, March 7, 2001). It is not clear who is responsible for any of these malicious hacks.

September 11, 2001

The aftermath of the September 11th attacks on the World Trade Center and the Pentagon has spawned enough real dangers without Internet hoaxes adding to the chaos, but unfortunately the hoaxes and misleading sites were up and running quickly. The predominant form these took were e-mail hoaxes, which are easy to create, bulk-mailed, and in times of crisis and extreme sorrow or shock, can dupe even the critically minded. Among the first of these were charity scams. (For more on this subject, read Chapter 5: Brother Have You Got A Dime? Charity Scams on the Web.)

Charity scams follow any disaster and prey on innocent, grieving people. They are as insidious in intention as the attacks themselves. They began within 24 hours, according to the Coalition Against Unsolicited Commercial Email (www.cauce.org/pressreleases) and SpamCon Foundation (http://law.spamcon.org). The fraudulent e-mail messages claimed to be part of a relief or survivor fund, and asked for donations to help those in need.

To avoid these scams, the recommendations for potential donors are as follows:

- Go directly to the Web site of the organization you want to donate to.
- If you don't know the organization or the person who solicited you, stay away from it.
- Keep in mind that, generally, no legitimate relief organization solicits for donations through bulk e-mail.
- If you do click on any link to make a donation, examine the URL shown in the browser to make sure you are still where you think you are.

Perhaps second to the scams in maliciousness are e-mail messages that capitalized on the post-traumatic panic and sought to stir up more of it. The most notable of these was the "Halloween Attack" e-mail, which basically stated that a friend of a friend had been dating a man from Afghanistan who left her shortly before the attacks. Being a loving terrorist, however, he sent her a letter warning her not to take commercial airliners on September 11th, and to stay out of malls on Halloween. The FBI investigated the e-mail and concluded that the information was "not credible."

Other e-mail hoaxes involved allegedly phony disaster predictions, most notably via astrology, numerology, and a fake Nostradamus prediction. This particular one was easily debunked within a day of its posting as it was dated over 100 years after he had lived. There will always be susceptible people who will believe these hoaxes, but the rest of us should suspect the commonly nebulous language of predictions and post-event verification, i.e., "See, I said something big would happen this fall."

A number of fake photographs hit the Internet immediately after the disaster as well. One popular one shows "the devil's face" in the smoke of the towers' collapse. Another, supposedly shot from the observation deck at the top of the World Trade Center, shows a plane flying into the second tower. Clearly bogus, since the observation deck didn't open each day until after the time of the attacks. Can everybody say Photoshop?

There are three excellent resources for tracking hoaxes and misinformation following the 9/11 attacks: The Committee for the Scientific Investigation of the Paranormal CSICOP (www.csicop.org/hoaxwatch), The Central Iowa Skeptics (www.dangerousideas.net/infowatch.asp), and SNOPES (www.snopes2.com). Their information is credible, well researched, and timely.

Subject-Specific Misinformation

While many degrees of misinformation exist on the Web, from deliberate to accidental, serious to comic, and obvious to subtle, the consequences are perhaps nowhere as severe as in the areas of health and business. Erroneous health information can quite simply lead to serious injury and even death. Bad business information can result in financial ruin. Those subjects are addressed at length in full chapters in this book.

Science and Health Information

Health information is perhaps among the most problematic of all information on the Web. Teenagers and the elderly are most susceptible to misinformation in this area, and more seniors are getting online, capitalizing on what they see as a plethora of health information, particularly with regard to drugs, disease symptoms, cures, alternatives, and so forth. The Web site *Senior Focus Radio* runs an article (as of February 2002) claiming that a "recent" survey of seniors indicated "their biggest concern about cancer information on the Internet was misinformation" (www.seniorfocusradio.com/cancerinformation.html). An example of such misinformation is a site that claims at the top of its page: "There is no cure for the common cold. There is a very simple CURE for cancer" (www.ioa.com/~dragonfly/news/kelley.html). A number of sites like this can be retrieved by anyone searching "cancer and cure" or "cure for cancer" on an Internet search engine. And although some highly respectable and authoritative medical Web sites have emerged, medical misinformation is more accessible today than it has ever been.

The AIDS Myth Site (www.virusmyth.com/aids/index.htm), registered to the Institute for Investigative Medicine, Netherlands, is an example of information that represents an extreme minority view but is not necessarily malicious. Citing a number of prominent scientists, including Kary Mullis, Nobel Prize winner for Chemistry, the site claims that there is no proof that the HIV virus causes AIDS, that AIDS is not sexually transmitted, and that people die because they are poisoned to death by anti-viral drugs. In addition, the site claims that its views are victimized by censorship.

The Group for the Scientific Reappraisal of the HIV-AIDS Hypothesis, the organization apparently behind much of the site, came into existence as a group of signatories to an open letter to the scientific community (dated June 6, 1991) submitted to *Nature*, *Science*, *The Lancet*, and *The New England Journal of Medicine.* All refused to publish it. In 1996, the group finally got a letter published in *Science*.

The site is over 500 pages long and represents a mammoth effort to argue their claims. Because of its "authority," a site like this could represent a source of dubious and potentially destructive information, or it could represent a rare doorway into another legitimate but unpopular perspective. This type of source could be dangerous to inexperienced researchers who do not compare this information to the mainstream medical literature or who do not understand that the information presented represents a minority view of the subject. This is an excellent example of how there is no easy "right" answer, and it is important to research all sides of an issue before one makes a decision.

The Global Warming Information Page (www.globalwarming.org) is an anti-global warming site that is not upfront about its position. One of the more deceptive practices is the statement near the top of the page: "Need Information for a research project? Check out our *Student Research Page* [hyperlinked] to help you quickly find the information you need." Many students will read no further and go directly to this area of the site. Here they will encounter information, including a handy "Synopsis of the Issue" that denies global warming is occurring. Global warming is obviously a complex issue, and the jury is still out, but this site is definitely a case of research entrapment.

Some unusual health-related hypotheses have been spread on the Internet. Antiperspirants cause breast cancer. Cooking in aluminum pans causes Alzheimer's disease. Costa Rican bananas carry flesh-eating bacteria. These and similar unusual scientific hypotheses can be checked at reliable public health sites, such as The Centers for Disease Control and Prevention (CDC) (www.cdc.gov), Quackwatch (www.quackwatch.com), or the sites listed at the end of this chapter. While you may think these are quackery, remember that Galileo was imprisoned for life for refusing to renounce the theory that the Earth and planets orbit the sun.

Business

The volatility of markets can undermine anyone's faith in the rationality of our economy, and nowhere is volatility more obvious than on the Internet.

In April of 1999, a counterfeit Web site of Bloomberg.com, a news service, touted a U.S. $1.35 billion acquisition of PairGain Technologies of California by ECI Telecom of Israel. The ruse sent PairGain shares soaring 31 percent on April 7, but the stock fell back to Earth after the story proved false. The frenzy started when a financial discussion page on Yahoo! included a link to the fraudulent Web site. For further information see *WiredNews* (www.wired.com/news/business/0,1367,19094,00.html). More on that in Chapter 3.

It used to be that a dissatisfied customer would yell at the clerk through an "Exchanges" window, but the Web has amped up that scenario considerably. In 1997, millions of Internet users received what was apparently unsolicited e-mail from Samsung Electronics, and thousands of recipients responded with angry e-mails of their own, protesting what they thought was corporate spamming. Those who protested received a follow-up e-mail, apparently from Samsung's legal department accusing them of illegal acts and suspected Internet terrorism. In response to this threatening e-mail, Samsung received up to 10,000 angry e-mails a day. The company estimated that damage control for the incident extended into millions of dollars. As you might have guessed, neither of the offending messages had originated with Samsung Electronics. They were apparently the output of one upset customer (*Management Review*, Jul/Aug 1998).

The majority of attacks on corporate Web sites is by disgruntled employees or customers or the politically motivated. Tommy Hilfiger, McDonald's, and other corporations have been victims of politically oriented Web attacks aimed at costing them business. And in the case of the infamous K-Mart Sucks page (www.concentric.net/~rodf/mart.htm) put up by Rod Fournier, K-Mart's original Web designer, K-Mart recognized that the content was either true or opinion, but threatened him legally for his use of the K-Mart logo. He changed the logo and his page to the Mart Sucks. You can read his side of the story at the site.

To counteract the rash of business and investment misinformation on the Internet the Securities and Exchange Commission (SEC) has set up what it calls a "Cyberforce" to surf the Internet for suspicious sites and postings, particularly those pointed out by investor complaints. By mid-2001, the SEC had received and responded to over 100,000 complaints and questions. The SEC page (www.sec.gov/investor/pubs/cyberfraud.htm) has sound information on avoiding a number of Internet scams. More on that in Chapter 6.

Fictitious Sites

While all the above sites employ some degree of fiction, the sites categorized as fictitious are not primarily humorous in intent and are not true parodies.

The Ruritania (a fictitious country) home page (www.homepages.udayton.edu/~ahern/rurindx.htm) is an ambitious project hosted by the Political Science department of the University of Dayton and used in various classes. The site is a composite of various simulations and games developed by social scientists over the past 20+ years. Ruritania is a medium-sized country of approximately 4 million people located in Scandinavia between Sweden and Norway, and the site details its history, demographics, political system, and culture. The

URL and references to simulation will give this site away immediately to sophisticated researchers, but junior high school students might not be so fortunate as to know how to evaluate them. Actually, Ruritania was a mythical kingdom with a Central American feel created by Anthony Hope in his *Prisoner of Zenda* and *Rupert of Hentzau* novels. During the process of publishing this book, this page was taken down. You can still see it by visiting www.archive.org and submitting the URL above. This service works for many URLs that are no longer extant.

The New Hartford, Minnesota, home page (www.lme.mnsu.edu/newhartford/newhtfd.html), unlike its twin sister Mankato, Minnesota (what is it about Minnesota?), is not obviously a fake site. The biggest clue is in the URL that points to an academic server. Since one usually has faith in the veracity of an academic site (.edu), it becomes a subtle clue for some users that the domain is not governmental (.gov). Missing this clue, however, one would need to consult an atlas to ascertain it is a fictitious town.

Parodies and Spoofs

While sites that seriously counterfeit a legitimate organization's home page are relatively rare, there are a huge number of sites that parody or spoof persons, companies, and organizations. The difference between parody (a satirical imitation) and spoof (a light parody) is slight and a matter of degree, so I lump these two categories together. Because the satire is fairly obvious, there should be little occasion to mistake its content for truth. Many times you can figure this out by the name. Parody sites are often political and typically employ humor to get their message across. They can often be extremely useful to researchers looking for antithetical or alternative information. Unfortunately, people often seem more gullible with Web information and check their common sense at the door.

These sites can cause particular problems when underlying pages that are retrieved by a search engine appear as discrete bits of information divorced from the site as a whole. Many stories exist about "news" from The Onion (www.theonion.com) being used and cited in academic research. The probable cause, aside from sloppy work, is the appearance of an Onion story in a list of hits without reference to its home site.

A good directory of these sites has been compiled by the Open Directory Project (http://dmoz.org/Recreation/Humor/Computer/Internet/Parodies).

The White House, as one might suspect, is a convenient target. Several sites have counterfeited it: www.whitehouse.com (a porn site), www.whitehouse.org (a scandalous site), and www.whitehouse.net (a

comic look at White House antics). These sites also capitalize on domain name appropriation. The whitehouse.net site features viewer's feedback, much of it serious. One woman thought it disrespectful to paint the White House pink. The real White House home page is, of course, www.whitehouse.gov.

A number of fake George W. Bush sites have arisen and gotten some publicity. One extant site, the George W. Bush Campaign Headquarters (www.bushcampaignhq.com), was a spoof that admitted in its top-of-the-page introduction "For those of you who are new, a word of caution: this is not the real, official George W. Bush Election Committee's site." Another counterfeit site (www.gwbush.com) was attacked by Bush as malicious. His campaign filed a complaint with the Federal Election Commission (FEC), which delivered a cease-and-desist order demanding the parody material be killed. "It is filled with libelous and untrue statements whose aim is to damage Governor Bush in his effort 'for President' in the upcoming election," a copy of the FEC complaint reads. The parody site received 6,451,466 hits during the first 25 days of May 1999, thanks in part to the story's front-page treatment by the *New York Times* online edition. Meanwhile, the real George W. Bush Web site received only about 30,000 hits that May, according to Bush spokeswoman Mindy Tucker (*ABCNEWS* online). The authentic George Bush site is www.georgewbush.com.

Nor were Al Gore (www.algore-2000.org was taken down after the election) or Steve Forbes (www.cais.net/aschnedr/forbes.htm) immune. And, while a bit off the subject, check out the design of the Bill Gates for President page (www.billgates2000.net/intro.html). Domain grabbing and squatting have accounted for enormous traffic to a number of counterfeit sites.

Another popular parody site is the Mankato, Minnesota, page (lme.mankato.msus.edu/mankato/mankato.html), a site that depicts Mankato, Minnesota, as a tropical paradise and is described in detail by LaJean Humphries (*Searcher*, May 2000). Don Descy, who teaches instructional media and technology courses, including Web evaluation, at Mankato State University, created the Mankato site. One would be hard-pressed to see how this site could fool anyone, yet the reaction, printed on the site, by Maureen Gustafson, President/CEO of the Mankato Area Chamber & Convention Bureau is damning. She writes, "For some time, your project on the Internet has troubled us. Though you claim it was done in the name of education many are laughing at our community rather than with it. Our office has received numerous inquiries on the fictitious information and it is very embarrassing to have to explain it as nothing more than a prank." She has apparently told Don that people do show up in

Mankato expecting palm trees. The real Mankato page is www.ci.mankato. mn.us.

Products succumb to parodies quite regularly. Adbusters (www.adbusters.org/spoofads), an advertising literacy organization, has created a number of one-page spoofs on products including Absolut Vodka, Obsession Cologne, and Prozac.

Hatchoo (www.hatchoo.com/parody/index.html), a parody of Yahoo, has a brief directory of other spoof and parody sites, including "Smart Cars," "Benneton," "Mercedes Renz," and Sinatra prints (and other life) on Mars.

We've all read about cloned sheep and frogs. We now assume science has progressed so far and fast that much of what's happening behind the closed doors of labs we haven't even read about yet. So how about male pregnancy? www.malepregnancy.com is an extremely creative and intriguing site that features Mr. Lee, the first pregnant male. This is now possible we read. In-vitro fertilization (IVF) techniques were used to induce an ectopic pregnancy by implanting an embryo and placenta into the abdominal cavity just under the peritoneum. Through a rigorous infusion of hormones, the male body is stabilized to nourish the fetus. Birth is through caesarian section. The site is the creation of two artists involved in social critique, Virgil Wong and Lee Mingwei.

With entirely different intentions, the University of Santa Anita (fictitious) AIDS FACTS page (http://147.129.1.10/library/research/AIDSFACTS.htm) was created by John Henderson of the Ithaca College Library for the purpose of Web evaluation. It lists a number of bogus AIDS "facts" attributed to, and even citing, organizations like the CDC and Johns Hopkins. Although these facts seem false to most of us ("New evidence from John Hopkins: Married women can reduce their risk from AIDS by 73.8 percent if they do not share their toothbrushes with their husbands"). There is a disclaimer at the bottom of the page ("The 'facts' on this page are intended to be outrageous and obviously bogus, because I don't want someone stumbling onto the site to mistake them for true facts."), but more naive users, or users who know nothing about AIDS/HIV and who don't bother reading thoroughly, may take these jokes as fact. It is the parody of seriousness that qualifies this as deceptive.

Clones-R-Us (www.d-b.net/dti), hosted by Dream Technologies International, claims to be the first and largest reproductive cloning provider. "We maintain fully owned labs in Costa Rica, Liberia, and Vanuatu, as well as an extensive roster of qualified surrogate birthing candidates." While elaborate, the site states in the "About Us" section, "As you've *hopefully* realized, this site is a spoof site, which simulates one possible ramification from advances in cloning science. It is hoped that this site will stimulate thought on the pros and

cons of reproductive cloning—and hopefully also foster some discussion." For some great laughs, check out the price list.

The infamous article "Feline Reactions to Bearded Men," (the product of a site, www.improb.com, which also publishes the partially online journal *The Annals of Improbable Research*) is a great parody of an academic research article. A similar example is the equally infamous "report" on California's Velcro Crop (http://home.inreach.com/kumbach/velcro.html). Obviously, a traditionally formatted Web article that was not so over-the-top could easily be perceived as credible. Then again, some people may actually think that velcro is an agricultural product and not synthetic and may try to use the data with less than fulfilling results.

The employees of FunnyCrap.com (www.funnycrap.com/fake) actually create fake Web sites for a living, or they do it while they're supposed to be working. Their current list includes: God's Home page, Da Mafia's Home page, Boris Yeltsin's Super Fansite, and the Chris Cam (a spoof of Webcams).

Entertainment

Even the entertainment industry has been experiencing a rash of Internet misinformation, largely involving counterfeit stories, scripts, plot exposés, and show endings. It's hard to see most of these as anything but practical jokes, but they are troubling to the producers who often produce red herrings and alternate endings for shows they feel will generate hoaxes. The fan infatuation with a show like *The X-Files* fuels counterfeits. A search on Google for *X-Files* plots delivered 4,820 hits. Hoaxes are not the only problem, and the *X-Files* producers have witnessed entire authentic scripts of future episodes turn up on the Internet while the segment was still under production.

Rick Berman, producer of the eighth and ninth *Star Trek* films put an interesting spin on Internet plot and script hoaxes when he claimed them beneficial since there will be eight bogus scripts for every real one and fans can't tell which is authentic (*Los Angeles Times*, Mar 16, 1998).

News Groups—LISTSERV and UseNet

As a matter of course, one should seek a second opinion to any information found on UseNet groups, chat groups, or LISTSERVs. This is perhaps less true for moderated lists, but still the danger of misinformation is prevalent. Several common techniques that have been used in the past to trick readers are impersonation of a person or status (how hard is it after all to add Ph.D. or MD after your name on

a UseNet posting?) and the planned leak, usually regarding business or health information.

A truly dangerous deception on the Web, particularly for children, is that of the sexual predator who pretends to be a child himself. This predator typically strikes up an online friendship with the victim, then arranges a meeting. For the first six months of their AOL chat-room romance, Katie Tarbox thought her cyber-soulmate was just a sweet and understanding 23-year-old Californian named "Mark." He turned out to be 41-year-old Frank Kufrovich. "He cared about me," she writes in her memoir about the experience, *Katie.com*, "he listened to my feelings and he always supported me with encouragement and advice."

Hacks

There is one final category of misinformation that we should probably mention, although instances are usually ephemeral and obvious—hacks. When a Web site is hacked, the content of the site is altered. Many hacked sites are simply tagged with a slogan or statement "This site hacked by …" Hackers often want to brag and leave identity clues for other hackers. Hacked sites are usually corrected immediately, although some hacks will require the site being taken down and rebuilt, which can take a few days. There are groups that specialize in political hacks, including some that target only White power sites. An incredibly extensive archive (1996–present) of hacked sites exists at 2600.com's site (www.2600.com/hacked_pages).

Web hijacks are URL redirects to unwanted sites. A user will click on a familiar URL only to be taken to an unwanted site. Since exposure on the Web is paramount, redirecting from a well-known site can result in millions of hits before the redirect is fixed, exposing millions of people to unwanted information or ads.

One Person Gathers What Another Person Spills

Many researchers think that information on the Web is suspect and not nearly as credible as that appearing in print sources. Hoax sites don't do much to alleviate this mindset, but one person's misinformation can be another person's gold mine. Hoax sites offer a number of possibilities, some of which have already been mentioned. Many such sites offer alternative perspectives to topics that have an almost hegemonic truth. Even so-called hate sites can provide useful information in bringing to light material that is typically censored from

most public discourse. Only a truly free society can allow free exchange of ideas regardless of how reprehensible they might seem.

Hoax sites offer "teaching moments," and a number of them have been created for this very reason. For example, the University of Santa Anita Aids Facts; Mankato, Minnesota; malepregnancy.com; and Clones-R-Us. The best of them make us question why we believe some things and not others, providing a self-examination of how we view the world if we are going to analyze information. I found that the Lip Balm and AIDS myth sites had this effect on me.

By learning how to deconstruct hoax sites we become empowered, and we can share this knowledge. One example of this is broadcasting who is behind a counterfeit site. Finally, some of them are absolutely hilarious. But beware, you might find yourself addicted to them for your daily giggle.

While Web literacy demands intelligent Internet use, Web literacy is not really qualitatively different than information literacy. All information has bias and has to succumb to rigorous evaluation. This was driven home to me when I worked for disaster relief and we began exploring refugee statistics. The number of refugees crossing a border was not the product of some simple count, any more than the U.S. Census statistics are. It is the product of a complex set of variables. The statistics, which look hard and fast in black and white, are really estimates but are accepted by many as truth. Even when reading an article in the *New England Journal of Medicine*, it doesn't hurt to look again later on—there may be an article in *JAMA: The Journal of the American Medical Association* the next month that refutes it.

Remember, while it is important to know what you're getting, hoaxes, parodies, and other misinformation are often of value to the right person in the right context.

Where to Go for Help

The following sites are dedicated to tracking Internet hoaxes:

About's UrbanLegends and Folklore (http://urbanlegends.about.com/library/blhoax.htm) features an extensive directory that uses these codes:

- Hoax = False, deliberately deceptive information, including pranks & jokes
- UL = Urban Legend: a popularly believed narrative, most likely false
- Rumor = Unsubstantiated information forwarded with gusto
- Junk = Flotsam and jetsam of the Net

Don't Spread That Hoax, one of the oldest and most reliable of the hoax busters, features a directory as well as links to useful authoritative resources (such as www.Thomas.gov for legislative information) for checking information. However, it is not as comprehensive as one might wish (www.nonprofit.net/hoax/default.htm).

Scambusters, a comprehensive site that has been endorsed both by Yahoo! and Forbes, among others, features an e-zine, mail group, story of the month, directory of scams, tips to avoid scams, testimonials, ways to stop spams, phony and real viruses, and much more. The site is a bit difficult to navigate but well worth the look (www.scambusters.org).

SNOPES, otherwise known as The San Fernando Valley Folklore Society's Urban Legend Pages is one of the largest collections of urban legends and hoaxes on the Internet. The hoaxes and legends are all coded with colored dots indicating true, false, undetermined, and of indeterminate origin (www.snopes2.com).

The Computer Incident Advisory Capability (CIAC) of the U.S. Department of Energy produces an updated list of hoaxes. Though not an extensive list, it specializes in hoax Internet viruses and a detailed and interesting history of hoaxes on the Internet (http://hoaxbusters.ciac.org).

While the National Fraud Center, a consumer's center for fraud, including Internet fraud, doesn't have a list of fraud sites, it does give overviews of techniques, industries, and demographics and includes an online form for reporting suspected fraud. It has invaluable information covering the most common Internet frauds: auctions (which they currently list as the worst), business opportunities and franchises, credit card safety, online credit repair, employment services, online

magazine solicitations, online travel offers, pyramid schemes and illegitimate multilevel marketing, scholarship scams, sweepstakes and prize offers, and work at home offers (www.fraud.org/welmes.htm).

Countermeasures

The spectrum of misinformation on the Net will continue to proliferate unless the Internet is strictly regulated, which seems unlikely if not impossible, not to mention undesirable. Adopting a critical stance toward everything you read on the Web is the best protection you can have against misinformation.

1. Look for clues in the URL. Almost all sites have some bias to the information posted, and though it may be slight and one you agree with, it's usually there. If you encounter a URL with a slight deviation in the name, or there is a dot-org when you expected a dot-com, stay on the alert. A [~] "name" reflects a personal site and, as such, will represent personal views only.
2. On the site itself, look for comic or incendiary language, lack of citation or authority, lack of currency, a particular bias toward audience, or slant of information.
3. Search smart. Use the advanced capabilities that a number of search engines now provide, such as domain searching. And use specialized search engines and directory services or meta-sites with holdings selected by librarians or other authorities in a field.
4. Check suspicious domain names with an agency like register.com.
5. Use print sources for verification when needed.
6. Check underlying pages, top-level pages (if at an underlying page), and suspicious links to verify what you get is the real item.
7. Regularly visit Web sites that post hoaxes.
8. Realize that misinformation is often contextual and can possibly prove useful in some circumstances.