INFORMATION TECHNOLOGY RIGHTS AND RESPONSIBILITIES

Presenter :

MARJORIE HODGES SHAW
Director, Computer Policy & Law Program
Cornell University
Ithaca, New York

Stetson University College of Law:

WORKSHOP: BACK TO THE FUTURE: INTERNET LAW AND POLICY, DISTANCE EDUCATION AND (AT LAST!) NOTHING ABOUT Y2K
Clearwater Beach, Florida
February 13, 2000

CORNELL
UNIVERSITY

Information Technology

RIGHTS and RESPONSIBILITIES

Cornell University has policies and codes that define responsible use of computers and networks. There are also federal, state and local laws governing many interactions that occur on the Internet. You need to be aware of what your responsibilities are and what the process is for adjudicating violations. You also need to know what rights you have and how you can get help if your rights are violated.

Table of Contents

- **CIT Publications** NEW
  Software piracy: What you should know | What to do about junk mail and harassment sent in the electronic realm | Protect Your Privacy: Network Security at Cornell | Kerberos | SideCar
- Related sites | Feedback

University-wide Policies and Codes

Campus Code of Conduct

The Campus Code of Conduct sets forth standards of behavior that **apply to all faculty, students, staff, and University-registered organizations.** The Board of Trustees and the University Assembly each have authority over different sections of the Code, and the Code is amended from time to time to foster a safe and productive learning and living environment. Regarding computer usage, the Code of Conduct specifically makes it a violation **"to recklessly or maliciously interfere with or damage, in violation of University rules, computer or network resources or computer data, files, or other information."** The Code also makes it clear that **"misappropriation of data or copyrighted materials, including computer software, may constitute theft."** Violations of University policies, including computer usage policies, also constitute violations of the Code of Conduct.

Violations of the Campus Code of Conduct are handled by the Office of the Judicial Administrator according to the procedures defined in the Code. More serious incidents (e.g., felonies) may be turned over to local and/or federal law enforcement agencies, as appropriate. Individuals who feel they have been victimized by computer abuse violations may choose to refer the matter to the JA, or may choose to pursue the matter outside the University (for example, through the civil or criminal courts).

All violations listed under the **Cornell University Policy Regarding Abuse of Computers and Network Systems** and the **Responsible Use of Electronic Communications Policy** are also violations of the Campus Code of Conduct. To direct reports to the most appropriate place, see the specific examples under the policies below. In most cases, reports regarding alleged computer or network related violations involving members of the Cornell community can be made directly to the Office of the Judicial Administrator or to OIT or the ATS helpdesk.

Code of Academic Integrity

The Code of Academic Integrity was adopted by the Faculty Council of Representatives and **applies to all students**. It prescribes adherence to a set of values, expected not only in coursework, but also in the use of University resources. The code includes computer and network related concepts and examples of violations, such as: **initiating or encouraging the promulgation of chain letters and other types of electronic broadcast messages, tapping phone lines or other network cables, subverting or obstructing a computer or network by introducing a worm or virus, supplying false or misleading information to access computer or network systems, improperly obtaining or using another's password to access computers or network systems, and unauthorized access to data, computers or networks.**

Violations of the Code of Academic Integrity are handled by the Dean of the appropriate college according to the procedures defined in the code. The computer and network related violations are also covered under the Cornell University Policy Regarding Abuse of Computers and Network Systems and the Responsible Use of Electronic Communications Policy. Refer to the examples listed below under these policies to determine where to direct reports of incidents.

Cornell University Policy Regarding Abuse of Computers and Network Systems

The University computer abuse policy was developed in 1990 and **applies to all faculty, students and staff.** It expands on the principles of behavior that were incorporated into the Code of Academic Integrity for guiding the use of computers and networks. The basic premise is that **legitimate use of a computer or network does not extend to whatever an individual is capable of doing with it.** Just because you are able to circumvent restrictions or security, doesn't mean that you are allowed to do so.

Violations of the Policy Regarding Abuse of Computers and Network Systems are handled by the Office of the Judicial Administrator according to the procedures defined in the Campus Code of Conduct. Alleged violations of this policy can be reported directly to the Office of the Judicial Administrator or to OIT or the ATS helpdesk. If the person responsible is not affiliated with the University, or cannot be identified, the incident should be reported to OIT or the ATS helpdesk. In addition, some instances may violate federal law. See Federal computer security violations for more information.

Examples (not a comprehensive list) of policy violations include:

- **accessing, or attempting to access, another individual's data or information without proper authorization** (e.g. using another's netid and password to look at their personal information)
- **obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained** (e.g. password sharing)
- **tapping phone or network lines** (e.g. running network sniffers without authorization)
- **making more copies of licensed software than the license allows** (i.e. software piracy)
- **sending a crippling number of files across the network** (e.g. email "bombing")
- **releasing a virus, worm or other program that damages or otherwise harms a system or network**
- **preventing others from accessing services** (e.g. taking over a chat channel and kicking other users off)
- **unauthorized use of University resources** (e.g. using someone else's EZ-Remote dialin access or borrowing their netid and password to access the library systems)
- **sending forged messages under someone else's netid** (e.g. sending hoax messages, even if intended to be a joke)
- **using University resources for unauthorized purposes** (e.g. using personal computers connected to the campus network to set up web servers for illegal, commercial or profit-making purposes)
- **unauthorized access to data or files even if they are not securely protected** (e.g. breaking into a system by taking advantage of security holes)

Responsible Use of Electronic Communications

In 1995 Responsible Use of Electronic Communications became an official University policy that **applies to the entire Cornell community.** It attempts to deal with some of the newer problems resulting from widespread use of the Internet. As stated in the policy, **the University cherishes the diversity of values and perspectives endemic in an academic institution and is respectful of freedom of expression. Therefore, it does not condone censorship, nor does it endorse the inspection of files other than on an exceptional basis.** As a result, **the University cannot protect individuals against the existence or receipt of material that may be offensive to them.** The university encourages individuals to use electronic communications in a responsible manner. Finally, the policy includes information about behavior that would constitute a violation and contains a set of procedures for reporting incidents.

Policy violations fall into four categories that involve the use of electronic communications to:

- **harass, threaten, or otherwise cause harm to specific individuals**, for example, sending an individual repeated and unwanted (harassing) email or using email to threaten or stalk someone;
  Alleged violations of this type can be reported directly to the Office of the Judicial Administrator or to the Cornell police if the situation is potentially serious and requires immediate attention. If the person responsible is not affiliated with the University or if it is not possible to identify the individual, the incident can still be reported to the JA or to the police. These offices can assist by referring to appropriate sources of help outside the university. **Save electronic copies of all correspondence for evidence.**

- **impede, interfere with, impair, or otherwise cause harm to the activities of others**, for example, propagating electronic chain mail, or sending forged or falsified email;
  Alleged violations of this type can be reported to OIT or the ATS helpdesk. If the person responsible is not affiliated with the University, the incident should be reported to the site that provides the individual with Internet access (see Reporting incidents to other sites). If it is not possible to identify the origin, contact the ATS helpdesk for assistance. **Save electronic copies of anything that can be used as evidence.**

- **download or post to University computers, or transport across University networks, material that is illegal, proprietary, in violation of University contracts, or otherwise is damaging to the institution**, for example, launching a computer virus, distributing child pornography via the web, or posting a University site-licensed program to a public bulletin board;
  Alleged violations of this type can be reported directly to OIT or the ATS helpdesk. If the person responsible is not affiliated with the University, or cannot be identified, the incident should still be reported to OIT or the ATS helpdesk.

- **harass or threaten classes of individuals;**
  Alleged violations of this type can be reported directly to the Office of Human Relations. If the person responsible is not affiliated with the University, the incident should be reported to the site that provides the individual with Internet access (see Reporting incidents to other sites). If it is not possible to identify the origin, contact the ATS helpdesk for assistance. **Save electronic copies of anything that can be used as evidence.**

What are some violations of Cornell University policy?

The section on University-wide Policies and Codes describes what activities constitute responsible use as well as violations. Following is more detail about some violations that OIT frequently gets questions about.

- **Sharing netids and passwords (unauthorized use)**
  Your netid and password are provided only for your personal use. Netids provide access to a wide range of services that are restricted for use by you personally (such as grades, address information, bursar bill, salary, benefits) or are restricted for use by the Cornell community (such as email, EZ-Remote dialin, library services, news, chat). If you share your netid with spouses, family members, friends or roommates, then you are giving them access to services they are not authorized to use. They will also have access to all of your personal information. They may even embarrass you by posting to a news group in your name or by posing as you in a chat session.

   **DO NOT SHARE YOUR PASSWORD WITH ANYONE.** If you suspect that someone may have discovered your password, change it immediately.

   **DO NOT USE ANYONE ELSE'S PASSWORD.** Using someone else's password to access services or data is also a violation of policy, regardless of how the password was obtained.

- **Chain email and virus hoaxes**
  The most important thing to remember is if you get chain email, **do not help propagate it.** Chain email usually contains phrases like "pass this on", "forward - do not delete", "don't break the chain", "this is safe, don't worry", "let's see how long this takes to get back to the start", "this has been around the world 20 times", "7 years of good luck!", "I don't wanna die", "your mom would want you to do this", etc. Often there is some story about how lucky a person has been since they forwarded the chain email, or how unlucky they were because they didn't. Sometimes chain email is disguised - it tells of some kid who is dying and wants post cards, or it warns about email viruses or internet shutdowns. Don't fall for it. It's all chain mail and it's designed to get you to forward it.

  In recent years, chain mail **hoaxes** of various sorts have become widespread on the Internet. Some are virus warnings like "Good Times", "PenPal", and "Irina". Others are like the "Naughty Robot" that claims to have all your credit card numbers. They tell you to forward the "warning" to everyone you know. Most hoaxes start out as pranks, but often live on for years, getting passed around by new people who have just joined the Internet community. Don't believe every warning you get via email. You should not pass these warnings on unless you verify the authenticity. You should contact the ATS helpdesk or check out one of the many sites on the Internet that track hoaxes:
    - CIAC
    - Computer Virus Myths
    - National Fraud Information Center

  If you get chain email from someone with a Cornell email address, you can report it to the ATS helpdesk. You will need to include a copy of the chain email in your report. In most cases, a first offense results in a warning. Subsequent offenses result in a referral to the Judicial Administrator for disciplinary action. If you get chain email from someone not affiliated with Cornell, you can reply to the sender and let them know you are not happy about getting chain email from them, or you can delete and ignore it. If you choose to complain, follow the instructions in Reporting incidents to other sites. Most places have policies regarding the propagation of chain email and will deal with it on their end.

- **Harassment**
  Electronic communication that is repeated and unwanted may constitute harassment. In general, communication targeted at a specific individual with the intent to harass or threaten is a violation of Cornell policy. If you receive unwanted email or other form of communication,

you may want to consider notifying the sender that it is unwanted. Many times a person will not realize that their communication is unwanted unless you tell them. If the sender continues to communicate after being placed on notice, or if you feel uncomfortable confronting the sender, the incident should be reported to the Office of the Judicial Administrator. You should also contact the Cornell police if the situation is potentially serious and requires immediate attention. **Save electronic copies of anything that can be used as evidence.**

- **Forgery**
  Altering electronic communications to hide your identity or impersonate another person is considered forgery. All email, news posts, chat sessions, or any other form of communication should contain your name and/or netid. Forgery includes using another person's identity or using an identity that's fake (like god@heaven or anon@nowhere). Forgeries intended as pranks or jokes are still considered violations.

- **Tapping phone or network lines**
  Running a network "sniffer" program to examine or collect data from the network is considered tapping a network.

- **Email bombing**
  Flooding someone with numerous or large email messages in an attempt to disrupt them or their site is known as "email bombing". Often this is done to retaliate because someone has done something annoying. But more often than not email bombing will either cause problems for your local system or disrupt service for thousands of other innocent bystanders. If you are having a problem with someone, pursue an acceptable method to report the situation. If it's a Cornell person, then refer to University-wide Policies and Codes and determine what violation is occurring and report it as outlined for that type of violation. If it's someone outside of Cornell, then follow the instructions in Reporting incidents to other sites.

- **Interfering with activities of others**
  This can be any activity that disrupts a system and interferes with other people's ability to use that system. In some cases, consuming more than your "fair" share of resources can constitute interference. Some examples are:
  - email bombing that causes a disk to fill up, the network to bog down, or an email application to crash;
  - taking advantage of a net split to take over a chat channel and then kicking off or blocking other users;
  - posting many messages to a single news group or mailing list making it difficult for subscribers to carry on their normal discussion;
  - flooding a chat channel with a continuous stream of messages so that it disrupts the conversation.

- **Unauthorized access**
  As stated in the Cornell University Policy Regarding Abuse of Computers and Networks, legitimate use of a computer or network does not extend to whatever an individual is capable of doing. In some cases, operating systems have security holes or other loopholes that people can use to gain access to the system or to data on that system. This is considered unauthorized access. If someone inadvertently turns on file sharing on their personal computer, you do not have the right to read or delete their files unless you have been given explicit permission from the owner. This is much like accidentally leaving your house door unlocked. You wouldn't expect a burglar to use that as an excuse for robbing you.

- **Commercial use of university resources**
  Using email to solicit sales or conduct business, setting up a web page to advertise or sell a service, or posting an advertisement to a news group all constitute commercial use. Even if you use your own personal computer, but you use the University's network (either from a dorm room, office or via dialin access from home), you are in violation of the policy.

- **Illegal activities**
  Everything listed under What is illegal under local, state and federal laws? is a violation of University policy. This is not a comprehensive list, but it contains the activities most frequently asked about.

What are NOT violations of Cornell University policy?

- **Unsolicited email or junk email**
  The amount of unwanted or unsolicited email (junk mail) has been increasing as more people join the Internet community. You get things like this in the U.S. Postal mail on a regular basis - catalogs, advertisements, solicitations, and political propaganda are some examples. This form of speech is usually protected under the first amendment, even though some people may find some of the content objectionable. Cornell does not monitor or censor email and therefore cannot prevent the flow of junk mail. When you receive ordinary junk email, you may be tempted to retaliate by flooding the sender with numerous or large email messages in an attempt to disrupt their site (also known as "mail bombing"). However, mail bombing constitutes a violation of the university Responsible Use of Electronic Communications policy and violators will be referred to the campus judicial administrator. This is because more often than not mail bombing will either cause problems for your local system or disrupt service for thousands of other innocent bystanders.

  Remember that junk mail is NOT illegal and it is NOT a violation of University policies or codes. You can either **delete and ignore junk email** (this is the recommended approach) or contact the sender and ask to be removed from any mailing list they have - just as you would do with U.S. Postal mail (for additional help see Reporting incidents to other sites). Many people ask why the University does not put a stop to junk mail. Most junk mail comes from sites around the Internet, not from within Cornell. We have no control over what these sites send and cannot distinguish unwanted junk mail from email that people want to receive. It needs to stop at the source. In fact, a growing number of people around the Internet are trying to get junk mail outlawed. If you are interested in finding out more about this movement or want to know what you can do to prevent getting junk mail, check out Outlaw Junk E-mail Now! or Stop Uninvited Commercial Email or How To Stop Spam. If junk mail becomes illegal, it will then become a violation of Cornell policy as well since any illegal activity constitutes a violation of policy.

  Note that chain mail is a form of junk mail that is a violation of policy and can be reported. See the section on the Responsible Use of Electronic Communications policy for details on reporting chain mail.

- **Breaches of network etiquette**
  Things like off-topic postings to lists and news groups, advertising by posting the same message to numerous lists (also known as "spamming"), rude or impolite behavior, heated arguments (or flame wars), and some forms of hate speech will often annoy others. Remember that the Internet spans the globe as well as numerous diverse cultures and societies. What is acceptable in one may be totally inappropriate in another. Keep in mind that it is easy to misunderstand electronic communications due to the lack of personal contact involved. You can avoid problems by "listening" for a while when you join a group. After you determine what is acceptable, then go ahead and post. If you participate in a discussion and someone posts off-topic, be polite in pointing out the mistake and do not assume it is deliberate. These Ten Principles of Civility in Cyberspace are good rules of thumb.

Cornell is not in a position to control etiquette. When these sorts of problems come up, you should try to work them out with the other people involved, just as you do in other areas of your life. For more etiquette tips check out Netiquette Guidelines.

In some cases, rude behavior can cause disruptions. Any behavior that interferes with the ability of others to access or use a system is a violation of policy. See the section on Interfering with activities of others.

- **Hate speech**
  Uncivil, antagonistic or derogatory speech that is disrespectful of classes of people is commonly referred to as hate speech. Although hate speech may be extremely offensive (particularly to members of the targeted group), posting hate speech does not generally constitute a violation of University policies or codes. This is because, especially as an educational institution, Cornell is committed to the protection of freedom of expression. In exceptional cases, however, the University may decide that hate speech directed to classes of individuals presents such a hostile environment that certain restrictive actions are warranted. Refer to the Responsible Use of Electronic Communications policy for more information.

- **Adult pornography**
  Possession of adult material is not a violation of policy or code unless the material is illegal. See sections below on Obscenity, Child Pornography, and Distribution of Pornography to Minors. Cornell does not monitor or censor newsgroups, electronic mail or any other electronic communications. However, if you would like to set up your personal computer to block pornography, you can obtain one of the many tools available for this purpose. These include Cyber Patrol, Net Nanny, and SurfWatch.

 Because the University does not censor adult materials, these materials are easily accessible on the network. If you are concerned about exposing your children to such materials, this is another reason why YOU SHOULD NOT SHARE YOUR PASSWORD with them. In any case, please remember that it is a violation of University policy to share your password with anyone, including members of your family.

What is illegal under local, state and federal laws?

Any activity that is illegal is a violation of Cornell policy. Alleged violations will be referred to the campus Judicial Administrator. In addition, offenders may be investigated and/or prosecuted by the appropriate local, state or federal authorities. For more information on the law, check out Cornell Law School's Legal Information Institute.

- **Child pornography**
  Child pornography, material that depicts minors in a sexually explicit way, is illegal. Under the federal child pornography statute (18 USC section 2252), anyone under the age of 18 is a minor. States also have child pornography statues and the age of minority varies by state. **Knowingly uploading or downloading child pornography is a federal offense.** It is also illegal to advertise or seek the sale, exchange, reproduction or distribution of child pornography. Lewd exhibition of genitals can constitute sexual conduct and therefore, any graphic files containing images of naked children could violate the federal child pornography statute.

- **Distribution of pornography to minors**
  Possession of non-obscene adult pornography is legal, but it is illegal to distribute to minors.

- **Obscenity**

Obscenity is illegal. Virtually every state and municipality has a statute prohibiting the sale and distribution of obscenity, and the federal government prohibits its interstate transportation. The Supreme Court in Miller v. California, 413 U.S. 15, (1973), narrowed the permissible scope of obscenity statutes and applied this three part test to determine constitutionality: (a) whether the average person applying contemporary community standard would find the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes in a patently offensive way sexual conduct specifically defined in applicable state law; and (c) whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

The contemporary community standard is historically the standard of the community in which the material exists. Many on-line activist argue that the contemporary community standard in cases that arise on-line ought to be determined by the on-line community. However, a federal prosecution of a California couple that offered a members-only bulletin board service, concentrating on pornography, resulted in a conviction of the California couple under the federal obscenity statute and Tennessee community standards. In that case a postal worker in Memphis downloaded some material from this California bulletin board service. See United States v. Thomas, 1996 U.S. App. LEXIS 1069 (6th Cir. Jan. 29, 1996).

- **Scams and pyramid schemes**
  Beware of money-making "opportunities" on the Internet. A common scam is the pyramid scheme. You get an email message with a subject like "MAKE MONEY FAST" and it instructs you to send money to the people on the list and then add your name to the bottom of the list and send it on to some number of people. At Cornell, this is considered chain mail, but it is also illegal under 18 U.S.C section 1302. The US Postal Service and the Federal Trade Commission provide information to help individuals identify scams and report them. Pyramid schemes that use US Postal mail to send money are considered mail fraud and can be reported to the USPS.

- **Copyright infringement**
  Almost all forms of original expression that are fixed in a tangible medium are subject to copyright protection, even if no formal copyright notice is attached. Written text (including email messages and news posts), recorded sound, digital images, and computer software are some examples of works that can be copyrighted. Unless otherwise specified by contract, the employer generally holds the copyright for work done by an employee in the course of employment.

  Copyright holders have many rights, including the right to reproduce, adapt, distribute, display, and perform their work. Reproducing, displaying or distributing copyrighted material without permission infringes on the copyright holder's rights. However, "fair use" applies in some cases. If a small amount of the work is used in a non-commercial situation and does not economically impact the copyright holder it may be considered fair use. For example, quoting some passages from a book in a report for a class assignment would be considered fair use. Linking to another web page from your web page is not usually considered infringement. However, copying some of the contents of another web page into yours or use of video clips without permission would likely be infringement. See Guidelines for Publishing Web Pages at Cornell University for details. For lots more information, check out Cornell Law School's Legal Information Institute or Stanford's Copyright & Fair Use.

- **Software piracy**
  Unauthorized duplication, distribution or use of someone else's intellectual property, including computer software, constitutes copyright infringement and is illegal and subject to both civil and criminal penalties. The ease of this behavior on-line causes many computer users to forget the seriousness of the offense. As a result of the substantial amounts of money the software industry loses each year from software piracy, the software companies enforce their rights through courts and by lobbying for and getting stiffer criminal penalties. It is a felony to reproduce or distribute ten illegal copies of copyrighted software with a total value of $2,500 within a 180 day period. Penalties for a first time felony conviction of software piracy include a

jail term of up to ten years and fines up to $250,000. Software Piracy: What You Should Know

- **Sound recording piracy**
  Another form of copyright infringement is the unauthorized duplication and distribution of sound recordings. Online piracy is increasing as many people use the Internet to illegally distribute digital audio files (e.g. MP3 format). The Recording Industry Association of America (RIAA) monitors the Internet daily and scans for sites that contain music. They have been successful in getting the sound recordings removed from those sites. You can report violations to the RIAA directly (see section on Outside agencies).

  Federal copyright law grants the copyright owner in a sound recording (typically, a record company) the exclusive right to reproduce, adapt, distribute and, in some cases, digitally transmit their sound recordings. Therefore, the following activities, if unauthorized by the copyright owner, may violate their rights under federal law:
  - Making a copy of all or a portion of a sound recording onto a computer hard drive, server or other hardware used in connection with a web site or other online forum. This includes converting a sound recording into a file format (such as a .wav or mp3 file) and saving it to a hard drive or server;
  - Transmitting a copy or otherwise permitting users to download sound recordings from a site or other forum; and/or
  - Digitally transmitting to users, at their request, a particular sound recording chosen by or on behalf of the recipient.

  If you reproduce or offer full-length sound recordings for download without the authorization of the copyright owner, you are in violation of federal copyright law and could face civil as well as criminal penalties. **Placing statements on your web site, such as "for demo purposes only" or that the sound files must be "deleted with 24 hours," does not prevent or extinguish this liability.** See Copyright infringement for more information on what is considered "fair use".

  There are several entities you may need to contact before you can use recorded music online. First, you should understand that the copyright in a sound recording is distinct from the copyright in the recording's underlying musical composition. Thus, even if you have secured the necessary licenses for publicly performing musical compositions (from, for example, ASCAP, BMI and/or SESAC) or for making reproductions of musical compositions (from, for examples, the Harry Fox Agency), these licenses only apply to the musical composition, not the sound recording. Licenses to utilize particular sound recordings must be secured from the sound recording copyright owners -- generally the record company that released the recording.

- **Federal computer security violations**
  The primary federal statute regarding computer fraud 18 U.S.C section 1030 was amended in October, 1996 to protect computer and data integrity, confidentiality and availability. Examples of violations are:

  - theft of information from computers belonging to financial institutions or federal agencies, or computers used in interstate commerce;
  - unauthorized access to government computers;
  - damage to systems or data (intentionally or recklessly);
  - trafficking in stolen passwords;
  - extortionate threats to damage computers.

- **Bomb threats and hoaxes**
  It is illegal to send a message via e-mail that threatens other persons or property. While this might seem obvious, every year a number of individuals send what they believe are "hoax messages". Such messages may be investigated by federal authorities with the result that the

senders end up with their names in the files of the FBI and/or CIA. This is not an exaggeration!

It also violates Cornell's policies and the Campus Code of Conduct to send certain kinds of hoax messages (for example, April Fool's jokes that appear to be from a professor or some other University official). Such hoaxes constitute forgery and will be referred for appropriate disciplinary action.

Reporting incidents to other sites

Identifying the source
The return address on an email message may not be the real source of the email. It's possible that a third party is trying to enlist your unknowing help in mail bombing the supposed sender. The third party first sends you and thousands of other people an annoying message that appears to come from the intended victim, then just sits back and waits for the victim to receive the angry responses. Email can be forged, and detecting a forgery can be difficult.

Finding header information
The "envelope" contains important header information. Most email applications hide headers (known as SMTP or trace headers) that help identify the source of the message, but they can be displayed by issuing the appropriate commands. With Eudora, open the message and click on "blah blah blah" (upper left corner of window). For other email applications check with your system administrator for details on how to display headers. News reader applications usually have an option to display header information (e.g., Newswatcher has a "show details" option).

Deciphering headers
Deciphering the headers is not easy, even for experts. Here is a typical email header. Not all headers contain the same information, so you may need to check with your local computer support staff for additional help. The bolded parts are the most useful to examine.

1. **Return-Path: dork@geeks.com**
2. Received: from server1.geeks.com (SERVER1.GEEKS.COM [111.222.333.444]) by postoffice2.mail.cornell.edu (8.7.5/8.7.3) with ESMTP id JAA28319 for ; Fri, 19 Jul 1996 09:50:30 -0400 (EDT)
3. Received: (from daemon@localhost) by server1.geeks.com (8.7.5/8.7.3) id JAA01199; Fri, 19 Jul 1996 09:50:29 -0400 (EDT)
4. **Received: from [111.222.333.999] ([111.222.333.999]) by server1.geeks.com** (8.7.5/8.7.3) with SMTP id JAA01159 for ; Fri, 19 Jul 1996 09:50:24 -0400 (EDT)
5. **X-Sender: dork@server1.geeks.com**
6. Message-Id:
7. Mime-Version: 1.0
8. Content-Type: text/plain; charset="us-ascii"
9. Date: Fri, 19 Jul 1996 09:50:11 -0400
10. To: my-netid@cornell.edu
11. **From: dork@geeks.com**
12. Subject: chain mail - pass this on for luck

To identify the sender, look at lines 1, 4, 5, and 11 in the example above. If they exist, they should contain similar information about the email address of the sender. If the information is very different, then it's a possible forgery. The most reliable field to use to identify the actual sender is in line 5 (X-Sender).

To identify the client computer used to initiate the email, look at line 4 in the header above. It was sent from a computer with the IP address of 111.222.333.999. In some cases, this can be traced to a

specific location or person.

To identify the server used to receive and deliver the email, look at line 4. In this example, the server that received the email and later delivered it to postoffice2.mail.cornell.edu is shown as server1.geeks.com. If you want to complain, use the domain name from line 4 (geeks.com in this example) and follow the instructions below.

In some cases, the message may be sent via an anonymous remailer. Mail from a remailer is usually identified as such and will often contain a disclaimer about the contents. Sometimes the message will identify an address to complain to. However, these sites rarely take any action and will never disclose the true identity of the sender without a court order. Often they do not know the identity of the sender.

Who can you report the problem to once the source has been identified?

- **Postmaster**
  Every site is supposed to have a postmaster, though some sites ignore email sent to postmaster. To copy the postmaster, take the sender's email address and replace the sender's user name with "postmaster". For example, if you wanted to complain about email you received from dork@geeks.com, and you have verified that this is the origin by examining the headers (as described above), you would send email to postmaster@geeks.com. If there is no postmaster account set up, the email will bounce back to you. Then try sending to root or admin, for example, root@geeks.com or admin@geeks.com. Keep in mind that the postmaster or system administrator might be the same person you are complaining about and you may only make the situation worse.

- **Administrative Contact**
  All Internet sites are supposed to list an official contact person for their domain. Contact this person only for serious incidents. The easiest way to find this person is to go to the InterNIC Registration Services Center. Use their search facility to search for the domain name of the sender's site. For example, if the sender was dork@geeks.com, then the domain to search for is geeks.com. Again, keep in mind that the administrative contact might be the same person you are complaining about and you may not get any resolution.

- **Outside agencies** If a situation is serious, you may get results by reporting the incident to the appropriate outside agency.

  - **Law enforcement agencies**
    These agencies accept reports of illegal activities in their jurisdiction.
    Cornell University Police 255-1111
    Ithaca Police 272-3245
    NY State Police 273-4671

  - **Federal Bureau of Investigation**
    The FBI pursues cases of wire fraud (applicable to the Internet since communications travel over phone lines). However, note that the FBI is mainly interested in "big" cases involving large sums of money (for example, over $10,000) or large numbers of victims (perhaps more than 20).

  - **Federal Trade Commission**
    The FTC deals with consumer protection. Investigates deceptive marketing practices and scams that cross state lines.

  - **US Postal Service**
    The USPS investigates cases of mail fraud, including pyramid schemes and other money-making scams that use the Postal Service to send money via the mail. If you have

done business over the Internet and received an item via US Postal Service that wasn't what you paid for or you shipped an item via US Postal Service and never received payment, this is where you should file a complaint.

- **Better Business Bureau**
  This is a private organization dedicated to helping consumers. They accept complaints about businesses and try to assist in settling disputes.

- **Software Publishers Association**
  This is an international organization of software companies and developers that pursues software piracy. They accept reports of ftp and bulletin board sites containing pirated software. You can also report if software you developed has been pirated.

- **Recording Industry Association of America**
  This is a private, not-for-profit corporation whose member companies produce, manufacture, and distribute approximately 90% of all legitimately recorded music in the US. You can get more information on their web site or you can report sound recording piracy by calling 1-800-BAD-BEAT or sending email to BADBEAT@RIAA.COM.

Preparing the complaint or report

- Include a brief, concise description of the problem, and be sure to identify yourself.
- Include copies of any communication that is relevant, including all header information.
- Send only one message. Remember that mail bombing is a violation of Cornell policy.
- Be polite and do not threaten.
- Do not blame the site administrator because one of their users misbehaves.
- Do not assume that the incident was intentional or malicious. Email is easily misdirected due to typos.
- Do not expect an immediate response, some sites, like AOL, get lots of email.

Departmental Policies

These policies have been provided by the various departments and colleges that have additional policies further restricting the use of their own computing and network facilities. It may not be a complete list. Check with your department or college if you have questions about local policy.

CIT (Cornell Information Technologies)

- **Terms and Conditions Governing Use of Network IDs**

  The CIT Terms and Conditions Governing Use of Network IDs applies to all netid owners. Netids provide Cornell community members access to a wide range of network services. However, **netids cannot be used for profit-making or illegal purposes and cannot be shared with others.**

- **CIT Computer Abuse Policy**

  The CIT Computer Abuse Policy covers use of all computers and networks maintained by CIT. In addition, use of your netid automatically constitutes acceptance of all policies, terms and conditions.

- Questions? Contact the ATS Helpdesk

Useful Contact Information

- **Office of the Judicial Administrator (JA)**, 223 Day Hall, 255-4680
  Open to anyone, this office handles complaints of alleged violations of the Campus Code of Conduct as described in The Campus Judicial System.
- **Office of Information Technologies (OIT)**, 308 Day Hall, 255-3324
  Open to anyone, this office accepts complaints of alleged violations of computer and network policies and works with appropriate authorities to investigate and prosecute.
- **Cornell University Police**, G-2 Barton Hall, 255-1111
  This office accepts reports of possible criminal or illegal activities and is open 24 hours. All serious or potentially dangerous incidents should be reported to the police immediately.
- **ATS Helpdesk**, 124 CCC, 255-8990, E-mail: helpdesk@cornell.edu
  Open to anyone, this office accepts reports of alleged violations of computer and network policies and forwards them to the appropriate office to investigate.
- **Office of the University Ombudsman**, 118 Stimson Hall, 255-4321
  Open to all members of Cornell, this office assists in resolution of problems and conflicts within the Cornell community.
- **Office of Equal Opportunity (OEO)**, 234 Day Hall, 255-3976, E-mail: equalopportunity@cornell.edu
  Open to Cornell faculty, staff and students, this office handles allegations of discrimination and sexual harassment.
- **Office of Human Relations**, 431 Day Hall, 255-5358
- **Judicial Codes Counselor (JCC)**, call for appointment: 255-6492
  This office provides free assistance to Cornell community members charged with violations of the Campus Code of Conduct and to students charged with violations of the Code of Academic Integrity.

Related sites

- Computer Policy and Law Program
- FindLaw Internet Legal Resources
- The Virtual Magistrate
- The Electronic Frontier Foundation
- The Online Ombuds Office
- Legal Information Institute

This page is developed and maintained by the Office of Information Technologies. Please write to us with your feedback.


E-mail: it-policies@cornell.edu

Last updated 1999 March 15