

## What are some examples of computer abuse of University computing resources?

**Answer:** Computer abuses include, but are not limited to:

- Providing false or misleading information to obtain access to University computing facilities or resources.
- Unauthorized access to University data, computer systems/resources, or another's computer or email account. This includes using computing systems/resources to access any other computer system (on or off-campus) without authorization. If it is necessary to read another individual's mail (e.g., while they are on vacation, on leave, etc.), surrogacy or message forwarding should be utilized.
- Accessing or copying files, regardless of media (e.g., paper, diskette, etc.), of another user without prior consent from the file owner. Accessing the "private" files of others without permission, even if those files are unprotected, is prohibited. Altering another user's files or systems files without permission is vandalism and destruction of University property.
- Attempting to compromise or tamper with user passwords. This includes, but is not limited to cracking, decoding, copying password files, "sniffing" packets to search for passwords or otherwise attempting to discover passwords belonging to other individuals. This also includes taking advantage of another user's naïveté to gain access to computer systems/resources or data, or preventing someone from using their account by changing the password or by other tampering.
- Attempting to intercept any network communication for purposes including, but not limited to: reading message/file content; rerouting packets; or packet "sniffing".
- Connecting dial-up modems to workstations or microcomputers/PCs that are simultaneously connected to a network.
- Remotely logging into (or otherwise using) any microcomputer/PC not designated explicitly for public logons over the University and/or Campus networks, even if the configuration of the computer permits remote access, unless you has been given explicit permission from appropriate authorized personnel.
- Disseminating any confidential information unless such dissemination is required by the individual's job at the University.
- Deleting or copying files from another person's computer or email account.
- Posting, sending or publicly displaying or printing unsolicited mail or materials that violate existing laws or University policies/codes of conduct. Such material includes, but is not limited to those that are of a fraudulent, obscene, offensive, defamatory, harassing, abusive, or threatening nature. Additionally, the University has special concern for incidents in which

individuals are subject to harassment or threat because of membership in a particular racial, religious, gender or sexual orientation group.

- Repeated sending of unsolicited mail.
- "Rebroadcasting" information obtained from another individual that the individual reasonably expects to be confidential.
- Abusing the networks to which the University belongs.
- Using University computer systems/resources or networks for monetary gain, political purposes or illegal activities. This includes using University Internet resources to create web pages for personal business or financial gain, except as permitted by other University policies.
- Illegally using of copyrighted materials including print, audio, and video.
- Illegally soliciting or distributing copyrighted software within or outside the University through any mechanism (e.g., email, bulletin boards, disk, etc.), electronic or otherwise. Employees and students shall not copy copyrighted software unless explicitly allowed in the software license agreement, except for one backup copy to be made and maintained by the original licensee. The University and its departments license many copies of software. The University does not own this software. Employees and students are required to comply with software licenses and the U.S. Copyright Act.
- Using personally owned software on University computer systems/resources unless the software is properly licensed for such use and system administrator approval has been obtained.
- Adding, copying or removing software to/from University computer systems/resources in violation of the software license. This includes copying software from or to University computer systems/resources.
- Intentionally writing, producing, generating, copying, propagating or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software unless such action is part of authorized research or testing. Such software is often referred to as a virus, worm, Trojan Horse, or some similar name.
- Modifying the configuration of the University or Campus computing infrastructure by adding or removing network links, computers, or peripherals (e.g., external disks, printers, modems, video systems, etc.); reconfiguring any control switches or parameters; upgrading processors, expanding memory, installing extras circuit boards, etc., except as authorized by the appropriate system or network administrator.
- Unnecessarily or inappropriately using limited computer systems/resources including but not limited to such inappropriate uses as sending chain emails, spamming, mail bombing, generating unnecessary excessive print, etc. Chain letters have been illegal if sent through the United States Postal Service (USPS) for many years.

- Attempting to develop or use any mechanism to alter or avoid charges levied by the University for computing resources.
- Performing or assisting in the performance of any act that will interfere with the normal operation of computer, terminals, peripherals, networks, etc. or in any activity that interferes with the rights of others (e.g., Using public, lab or departmental equipment for personal entertainment when other authorized users need access to perform University related tasks; intentionally damaging or misusing any University computer system/resource including terminals, microcomputers/PCs, networks, printers or other associated equipment; etc.).

Reports of abuse to your account can be made by contacting your system administrator. Please also note that your campus may have additional acceptable use requirements. Contact your system administrator for more information.