



Prevention is the best protection against computer vulnerabilities.

As a member of the UNM computing community, it is your responsibility to help keep computing resources safe and available for use. Follow these best practices.



Workstation & Data Security

- Require password to log in to your computer.
- Use a screensaver or screenlock that requires a password to access the computer's desktop.
- Use the UNM Portal for file sharing, AVOID Windows file sharing.
- Encrypt sensitive files. www.unm.edu/cirt/pgp/windowsdata.html
- Assure the privacy of personal information. DO NOT store sensitive personal information on your UNM computer.



OS and Software Updates

Be sure to get all available critical updates and security patches for your operating system. Remember that an Internet connection is required, whether the automatic check feature is enabled or you check for updates manually.

Windows 2000, NT and XP operating systems include an update feature (*Start> Windows Update*) that connects to <http://windowsupdate.microsoft.com> (Internet Explorer is required).

Macintosh OS X updates are available via *Apple Menu> System Preferences*, click *Software Update* (if you've disabled automatic checking). If you have automatic checking enabled, set it to *daily* or *weekly*. Apple is no longer providing updates for Macintosh OS 9, but be sure to have the last updates installed (*Apple menu> Control Panels> Software Update*).

Most software companies provide incremental updates via their Web sites, e.g., a security vulnerability may be discovered in an instant messenger program and the company will release an update to correct the problem. Check weekly for available updates.



Viruses & Worms

In general terms a computer virus or worm is malicious code that corrupts data by writing over reserved areas of the operating system or attaches itself to other programs. Viruses originally spread through removable media; more recent viruses and worms exploit vulnerabilities in operating systems and e-mail programs.

Buy and install antivirus software and keep the definition files up-to-date (check your specific software for version update and definition update procedures). Scan your computer daily for viruses.

Never open unsolicited or unexpected e-mail attachments. A virus/worm can be attached to an e-mail with any subject, from anyone, even those people you correspond with regularly.

Find additional information at www.unm.edu/cirt/virus.html. Find information about virus/worm attacks affecting the UNM campus, go to <http://cirtalerts.unm.edu>.



Scumware

Scumware is often used as an umbrella term when talking about *spyware*, *adware*, and *malware*. Generally, all four terms describe applications that can be installed on your computer without your knowledge. These programs do a variety of damaging activities including tracking what web sites you visit and sending the information back to advertising companies.

The worst of these programs — spyware and malware — do something more malicious, your personal details (e-mail address, credit card number(s), social security number) are collected when you fill in forms on the web, and that information is sent back to criminals who can resell or use the information for identity theft.

Products available free for UNM-owned and for home computers include: Spybot Search & Destroy (www.safer-networking.org/en/download/) and WinPatrol (www.winpatrol.com/). Products that must be purchased for UNM-owned and free for home computers include: Spyware Blaster (www.javacoolsoftware.com/spywareblaster.html) and Ad-Aware (www.lavasoftusa.com).

Like antivirus software, definition files for scumware detection software must be kept up-to-date. See your specific scumware software for updating procedures.

Removal can be difficult. Contact the CIRT Support Center for help (277-4848) <http://support.unm.edu>.



Firewall

ZoneAlarm is desktop computer software that helps protect Windows from malicious network activity. If you are technically savvy, ZoneAlarm can provide additional network protection. ZoneAlarm is available from CIRT's Software Distribution for \$21 per license/\$6 yearly renewal (departmental or open PR). Find information about ZoneAlarm at www.unm.edu/cirt/zonealarm. Students and others requiring a free individual license should visit the ZoneAlarm Web site: www.zonelabs.com/store/content/home.jsp (follow the *Download & Buy* or *Free ZoneAlarm and Trials* links).

Windows XP SP2 installs a firewall that is automatically enabled. CIRT recommends using this firewall if you are not using other firewall software.



Backup

Back up your important data. In the worst case scenario, your computer could be compromised and you could lose all your data. A backup ensures that you will have your most important files available. 20MB of space is available with the Briefcase feature at the UNM Portal (my.unm.edu). Removable media like CDs or zip disks will meet most needs for larger data backup requirements. Newer computers ship with CD-RW drives and CDs will hold 750MB of data. The newest zip drives and disks will also store about 750MB of data. If multiple CDs or zips are required and become cumbersome or you need to backup a larger amount of data you may want to consider an external hard drive. Find basic instructions for burning multi-session data CDs at:

www.unm.edu/cirt/howtos/ht617.html for Windows (Roxio 5) and

www.unm.edu/cirt/howtos/ht717.html for Macintosh.



Copyright

The Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) are aggressively pursuing copyright violations effectuated through Peer to Peer (P2P) software like Kazaa, et al. In 2004, the RIAA filed a round of lawsuits that included claims against individuals using computer networks at universities around the country. Statutory infringement penalties for these cases (as provided for in the Copyright Act), can range from \$750 to \$30,000 per infringed work, though the amount may be raised to \$150,000 per infringed work in cases of willful infringement.

In general, while P2P is a legitimate manner in which to share, for example, lecture notes (with the lecturer's permission) and other materials covered by the "fair use" doctrine; UNM students, faculty, and staff should always use caution in sharing materials, or verify that the material represents an exception to copyright law. The safest approach, of course, is not to use P2P software, and to keep computers up to date with the latest security patches so that no one can remotely share via P2P technologies without your knowledge.

While there are legitimate uses of file sharing technology, it generally is not acceptable to share MP3 files over the Internet via P2P software. Neither the fact that the technology makes it easy, nor the fact that it is done for free, is a viable defense to a copyright infringement suit.

UNM Legal Counsel has assembled information on the DMCA, the TEACH Act, and "fair use" issues so that students, faculty, and staff can be aware of how best to protect themselves from legal action. For P2P specific information, see: www.unm.edu/~ripls/copyinfo/cyberspace.htm. For copyright information see: www.unm.edu/~ripls/copyinfo.htm.

More copyright information at these Web sites:

<http://fairuse.stanford.edu>

<http://copyright.iupui.edu/>

www.utsystem.edu/ogc/IntellectualProperty/



CIRT Information Resources

<http://cirtalerts.unm.edu>

CIRT Alerts lists current major issues affecting multiple clients/buildings. Also find information about current security threats and other computer-related problems affecting the UNM Campus.

<http://fastinfo.unm.edu>

Query the fastinfo knowledge-base for a solution to your computing problem.

<http://support.unm.edu>

Support information for popular software.

www.unm.edu/cirt/support

CIRT Support Center hours and contact information.

www.unm.edu/cirt/download

Some licensed software and other freeware for use at UNM (UNM NetID required).

www.unm.edu/cirt/swdist

Find available software for faculty and staff only (UNM computers) for purchase (PR required).

www.unm.edu/cirt/zonealarm

Notes and initial settings for using ZoneAlarm at UNM

www.unm.edu/cirt/security

Additional information and resources for secure computing at UNM.

<http://list.unm.edu/archives/index.html>

Scroll down the page and click the *SYSINFO-L* link to view the current week's postings (find weekly archives here).