

WINDOWS® VISTA™

HSLIC User Support is currently rolling out Windows Vista, Microsoft's® next generation of desktop operating system. Installing Microsoft Windows Vista at the HSC will allow the campus to take advantage of better security features.

The security features in Windows Vista including Microsoft's anti-spyware software and Windows Defender, help prevent computer slow down, privacy loss, and unwanted pop-up advertisements. Windows Vista also comes with the Windows Security Center which will notify you when your security software is not up-to-date or your security settings are potentially unsafe.

The new Internet Explorer 7 allows you to easily browse the Internet but keeps untrusted sites from modifying your files or settings which helps keep your computer safe from Web-based attacks.

For more information and updates visit:

<http://hsc.unm.edu/library/usersupport/vista.shtml>



CONTACT INFORMATION

HSLIC User Support
505-272-1694
Helpdesk@salud.unm.edu

HEAT® Self-Service
<https://hscssl.unm.edu/HEAT/hss/login.html>

Searchable Knowledge Base
<http://fastinfo.unm.edu/>

Health Sciences Library and Informatics Center
MSC09 5100
1 University of New Mexico
Albuquerque, NM 87131-0001
505-272-2311
<http://hsc.unm.edu/library/>



HSLIC User Support Staff on Field Call - Photo by Sally Bowler-Hill



"The University of New Mexico is an Affirmative Action/Equal Opportunity institution. In accordance with the Americans with Disabilities Act, this material is available in alternate formats upon request."

Cover/Back Photo by Sally Bowler-Hill



TOOLS & TIPS FOR PROTECTING YOUR DATA

SECURITY: BE A PART OF THE SOLUTION



Find out what you can do to protect data on your computer

SECURITY:

BE A PART OF THE SOLUTION

STANDARDS-BASED COMPUTING

The Health Sciences Library and Informatics Center (HSLIC) provides a variety of security related services based on standards-based computing. The HSLIC standard Microsoft Windows® Vista™ image features include:

- Elimination of unnecessary Windows services
- The inclusion of several security-related software tools
- The installation of current, patched versions of the latest Microsoft Office applications

If you are unable to use the standard Windows Vista image there are still resources available for securing your workstation.



HSLIC Help Desk - Photo by Sally Bowler-Hill

TOOLS

McAfee® ANTI-VIRUS

This software protects files and folders from malicious attacks. If you don't have the McAfee virus shield icon (or have an antivirus program from another vendor), please contact HSLIC User Support. There is no charge to install McAfee on HSC workstations.

WINDOWS UPDATE SERVER

This service will automatically keep your computer patched with all of the critical Windows updates that have been tested by HSLIC.

ANTI- SPYWARE SOFTWARE

This downloadable software helps protect Windows users from spyware, adware, and other potentially unwanted software that can slow PC performance, introduce annoying pop-up ads, change Internet settings, and lead to unauthorized access to your private information.

WINDOWS FIREWALL

This software provides a protective boundary that monitors and restricts information that travels between your computer and the network. This provides a line of defense against someone who might try to gain unauthorized access to your computer. For assistance in configuring the firewall, contact HSLIC User Support.



HSLIC Blade Server -Photo by Barney Metzner

TIPS

USE THE NETWORK STORAGE PROVIDED

- Assure data is regularly backed up and secure.
- Available to all HSC employees, including UNMH users.

PRACTICE GOOD PASSWORD MANAGEMENT

- Don't write down or share your password with anyone.
- Change your password every 180 days.
- Create a complex password.
- Consider using mnemonics when creating/changing your password.

PRACTICE GOOD E-MAIL MANAGEMENT

UNM provides spam filtering. Unfortunately, it is nearly impossible to fully eliminate spam from your inbox. Here are several steps that you can take to significantly reduce this nuisance.

- Use separate email addresses for different online activities including work, personal and e-mail lists and subscriptions.
- Never open, reply to or click on the "remove" or "unsubscribe" link in a spam message.
- Be suspicious of any email with urgent requests for personal financial information.
- Never open an e-mail attachment unless you know the sender and are expecting the attachment.