

THE SHORT GUIDE
TO
FACULTY & STAFF
COMPUTING SERVICES

Rev. May 23, 2006

support@ucdc.edu

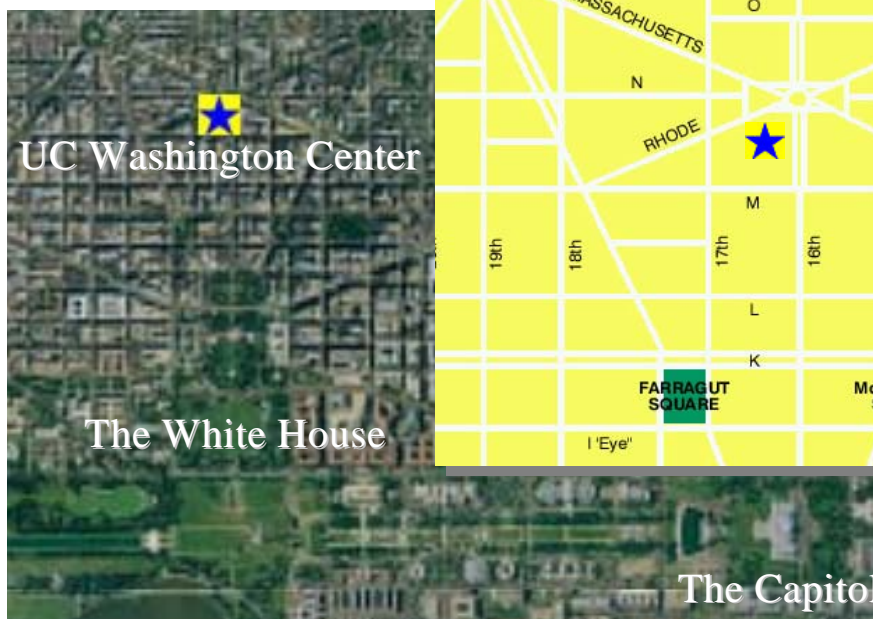


Introduction

The UC Washington Center is an eleven-story, mixed use facility in Washington DC located at 1608 Rhode Island Ave, NW. This building provides housing on its top eight floors to approximately 270 University students and faculty; offers numerous teaching venues including a 90 seat auditorium, a 300 seat multipurpose room, student computer labs, seminar rooms, and conference rooms; and houses the offices and programs of the Washington Academic Center (including programs from Berkeley, Davis, Irvine, Los Angeles, Riverside, San Diego, Santa Barbara and Santa Cruz). Additionally, the University's Office of Federal Governmental Relations (FGR) and Multi-campus Research Units (MRUs) such as the Institute on Global Conflict and Cooperation (IGCC) are located here.

The Washington Center employs a variety of leading edge technologies and techniques to fulfill its academic mission and is expected to be a point of innovation for the development of academic technology.

This document is intended to be an overview of the computing services available to faculty and staff at the University of California's Washington Center.



UC Washington Center Policy on Computing Services

Network and computing services at the University of California Washington Center are provided to faculty and staff following standards and practices laid out in University of California policy statements on computing including the *University of California Electronic Communication Policy—November 17, 2000*, related University of California Business and Finance Bulletins and other University best practices.

For personally owned software already installed on another computer, you must purchase an additional license to install that software on your office computer. Likewise, please verify software system requirements with a technical support staff member to ensure it will be compatible with your office computer.

Be aware that downloading, reproducing or distributing copyrighted media (for example, on-line books, music or videos) without the authorized permission of the copyright holder is a criminal offense.



What Are Some of the Computing Services Available to Me?

- * The Center's local network services and access to the Internet are available 24 hours a day, 7 days-a-week from all faculty and staff offices;
- * Individual network user accounts are available for all local faculty and staff at the Washington Center;
- * Every faculty or staff user is provided with a private directory on the network;
- * Program specific directories are available for all faculty and staff for passing information across the network between users within in a specific program. A center-wide global directory is also available for passing information with colleagues in other programs. Further, course specific directories are available for faculty wishing to have an area for passing class materials and other information to students.;
- * All user files are backed-up daily during the work week and network drives are mirrored for greater resilience in case of a hardware failure;
- * All University provided computers at the Center have anti-virus software installed. Anti-viral software is automatically updated on a regular basis

Principles of Technology Support

The Washington Center provides technical support for University-owned personal computers and network resources based on the following core principles. Problems are usually handled in order of severity. The severity and order of service are listed below in descending order of priority.

- * Failure or problem with core business service (for instance, a network server crash or Internet router failure) is handled before all other requests. Core business service failures usually affect the operation of the entire network or facility infrastructure.
- * Failure or problem with a shared system (for example, a problem with a network printer).
- * Single system failure (this includes a user computer that fails to start or is otherwise unusable).
- * Failure or problem with hardware peripherals or operation of software (for instance, a dead floppy drive or a software failure resulting in a computer lockup).
- * Requests for reconfiguration of existing systems or questions about hardware or software use.

These are gross rules-of-thumb that are applied on a case-by-case basis. The underlying premise for support is the prudent use of available resources to resolve the problems that impact the greatest number of users first. Consequently, extenuating circumstances that bear upon this premise may alter the order in which a problem is handled.

The Center's regular support hours are weekdays from 8AM until 9PM. Due to limited staffing, after hours support is only available through prior advanced arrangement and is subject to the discretion of the Manager of Information Services. Support for PCs and network-based services can be requested via e-mail at **support@ucdc.edu**.

Please be aware that **support@ucdc.edu** is your quickest way to technical support. This e-mail is monitored by all of the Center's technical support staff and in many instances is a more direct way to reach the support that you need.



The Information Services Staff

Rodger Rak

Manager, Information Services – information systems manager, primary technology liaison with senior management and chief technology educator.

Room: 243 Tel: 202 974 6224 e-mail: rodger.rak@ucdc.edu

Pamela Brenza

Network Manager – supports the Center's local area and wide area network infrastructure and acts as the Center's chief technology security officer.

Room: 245 Tel: 202 974 6296 e-mail: Pamela.brenza@ucdc.edu

Michael Sesay

Computing Resources Technician – supports all UC-owned personal computers and peripheral devices. This includes installing and configuring computer hardware and software as well as troubleshooting and repair of computer hardware and software. liaison to Center users to develop solutions for academic, administrative and student needs utilizing building computing and A/V resources. This includes support of the Center's A/V resources including videoconferencing facilities, user training in the application of the Center's resources and special technology projects.

Room: 354 Tel: 202 974 6206 e-mail: michael.sesay@ucdc.edu

Regular technical support hours are weekdays 8AM—9PM.
E-mail support@ucdc.edu for the quickest response to your
technical support needs.



USING THE NETWORK

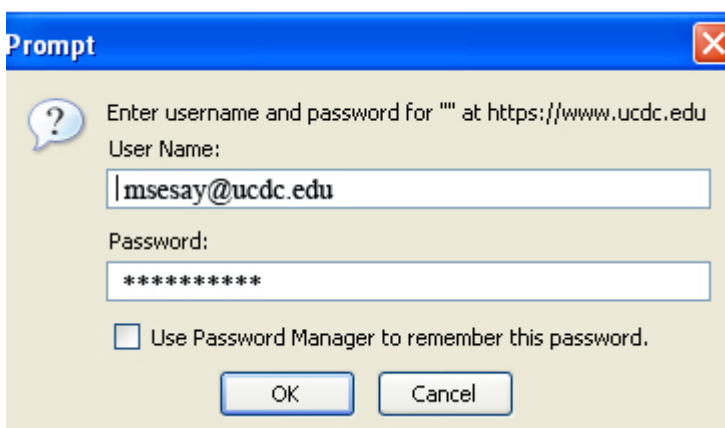
How to Logon

After turning on the computer, it will “boot” to a window prompting you to press **Ctrl-Alt-Del** to logon. Simultaneously press the **Ctrl-Alt-Del** keys. Next, the **Enter Network Password** dialog box will appear. The dialog box should look like the figure below. In the **User name:** field enter your user name. The protocol for creating your user name is to use the first initial of your first name and your last name (for example, Jannette Doe will have a user name of ‘jdoe’). In the case of more than one individual having the same user name (for example, Joseph Xavier Doe and Jefferson Davis Doe) the middle initial will be added to the user name.

Enter your password into the **Password:** field. The first time that you logon you will use the default password ‘pass01’. At that time you will be prompted to create a new password. For assistance in creating a password, please refer to the Center’s password policy below.

The last field that may appear on the **Enter Network Password** dialog box is the **Domain:** field. Our domain is UCDC. You should not need to enter this information as it is automatically retained.

After all the information is entered click the **OK** button. If all of the information is entered correctly you will be logged into the network and all appropriate network resources will be available to you. If you are not successful in logging on, you have two more attempts before the system will disable your account and lock you out. This is a security measure designed to protect the network from unauthorized users. Please contact support@ucdc.edu, if you have difficulty logging on.



Passwords

As part of the Center’s network security policy all users are required to have a unique network username and password in order to access the Center’s network-based services. This username and password are only used with network-based services provided by the Washington Center and do not replace any usernames or passwords assigned by your home campus.

Consequently, users accessing home campus-based e-mail or other home campus-based systems from the Center will still need to use usernames and passwords assigned by their home campus. Following are guidelines for creating strong passwords.

How to Logoff

Always remember to log off when you are finished using the computer so another user doesn’t have access to your files and email. Click **Start**, then choose **Shutdown, Close Pro-**



Password Guidelines

- All passwords should have no fewer than seven (7) characters and no more than fourteen (14) characters. Passwords should contain at least one non-alphabetic character such as a numeral (0-9) or punctuation (!, @, #, %, *, etc.) character in the second through sixth positions (For example, "Ih8mayo").
- All passwords must be changed every 90 days. Users should not create passwords that are identical or similar to passwords that they have previously employed.
- All users should choose passwords that cannot be easily guessed, avoiding passwords containing a user's name, user logon name or based on a user's personal life or job (i.e. names of family members or pets, your office room number, an address should not be used). It is best if passwords are not proper names or common names (such as place names, words found in standard dictionaries or slang).
- Users should avoid passwords with sequences of characters based on the date or some other predictable factor (i.e. users should not employ passwords such as "Y28Aug" in August, "Z282002" in 2002, etc).
- Avoid writing down your passwords. If you must record your passwords, store the document in a secure place. Do not keep it on your desk or tape it to your monitor where prying eyes can easily find them.
- If you believe that your password has been compromised, please notify the Information Services staff immediately.
- Passwords should never be shared or revealed to others, with one exception. In some instances, members of the Information Services staff may need your username and password to assist in troubleshooting a problem. If you have a need to share data with others, please do this via the network H: and I: drives or on a diskette instead of giving others access to your personal directories.

Network resources available to you

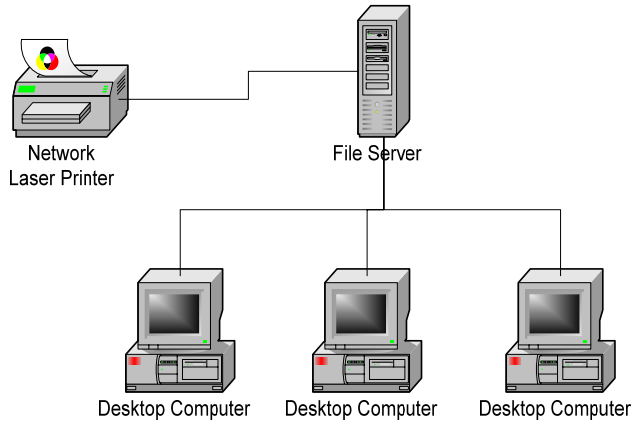
Logging on to the network provides you access to a variety of network services. These services include access to network printers, your own private home directory and other shared directories.

At logon, Windows based computers will automatically map to your network directories. Your personal network directory will appear as the **G:** drive in **My Computer** or **Windows Explorer**. Choose the **G:** drive as the primary location to save your files. This will store the files in your personal home directory so other users of the computer will not have access to them. Additionally, you will have an **H:** drive. This is your program specific directory. For example, all UCLA faculty and staff have a common directory that they share with other colleagues from UCLA. This will be your **H:** drive. The Courses directory for sharing course specific material appears as the **J:** drive.

You will have access to all networked drives and all files saved to these drives from any computer you login to on the UCDC network.



About networks in general



The 'techie' name for the relationship of your computer to the resources of the local area network (LAN) is *Client-Server*. The diagram to the left is an example of a simple network. Your computer is the *client* in that it uses the many resources of a network.

Hardware or services such as a file server, print server, e-mail server, fax server and other such resources are the *server* part of the network in that they provide you with the various services of the network. File servers are a safe place where you can store your data. They generally have large hard drives.

Some useful information about network directories

Each directory on the network has specific permissions attached to it. For example, your private home directory on the network can only be accessed with your username and password. All other users are prevented from opening your directory or even seeing what is inside. There is also a global directory called Courses that is available to all students and staff. This directory is used for storing course materials and other documents that may be of value to students at UCDC.

The Recycle Bin does not work with network directories



Be aware, files that you delete from your network directories do not go into the **Recycle Bin** as they do on your local computer. If you accidentally delete a file on the network, contact the Network Administrator for help.

Retention of Personal Data Files

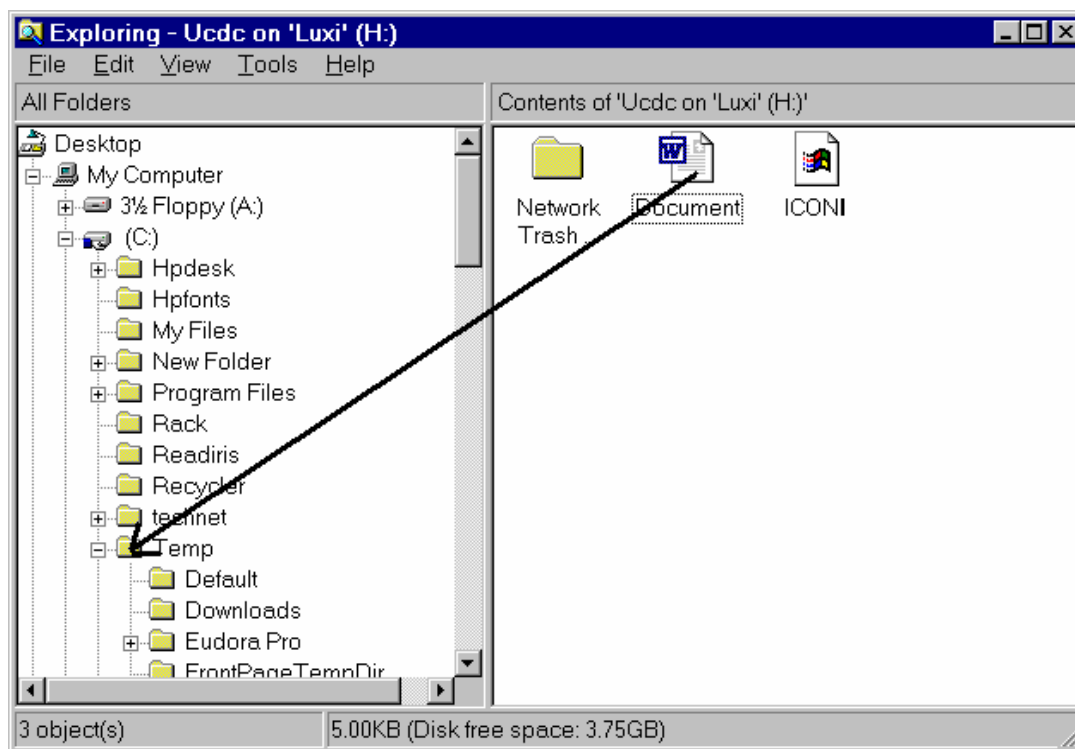
The Center ordinarily deletes network user accounts and data stored on the network one week after your departure. If you wish to take a copy of your network or local PC files with you, please make arrangements with the technical support staff, at least, one week before your departure to transfer the data to portable media such as ZIP disk or CD-R.



How to move or copy files to and from the network using 'drag and drop'

Using **My Computer** or **Windows Explorer** you can move or copy files from the network to your disk drive or vice versa using 'drag and drop'. To do so, first find the file that you wish to copy or move. Make sure that the file's new location is visible in the folder display as well. Right click on the file that you wish to copy or move. While holding the right mouse button down, drag it to its new location. When you reach the new location, let up on the right mouse button. A pop-up menu will appear. From the menu, choose **Move Here** or **Copy Here**.

If you wish to copy or move more than one file at a time, hold the **Shift** key down and left mouse click on all of the files that you wish to copy or move. Let go of the **Shift** key and repeat the steps described above. You can also move selected files in a list by holding down the **Ctrl** key and left mouse clicking on the files that you want. Once you've done this, repeat the steps above to move or copy.



E-mail at the Washington Center

Most faculty and staff users at the Washington Center prefer to retain their home campus e-mail accounts while at the Center. The Center provides unrestricted access to your campus-based e-mail and will assist in configuring your local computer to access your campus e-mail.

Be aware, that the Center provides only an entry point to the pathway to and from your campus e-mail server. We do not have any control either over your campus e-mail system or the pathway e-mail must travel over the Internet to reach you. Should you experience problems with your home campus e-mail, we suggest that you first try your campus e-mail technical support office. Below is a list of campus-specific web pages also known as Uniform Resource Locators (URLs) that are good sources for tracking problems your home campus may be experiencing. Should you need assistance doing this or be unable to receive satisfaction with your campus technical support, please contact us at **support@ucdc.edu**.

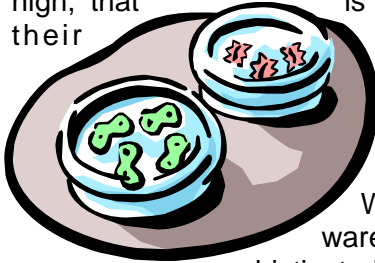
By special request, the Center will create a ucdc.edu e-mail account. We do require, however, that you use the ucdc.edu account exclusively and have all your campus e-mail forwarded to this account during the term of your stay. This is to prevent lost or crossed e-mails. At the end of your term at the Center, you will need to contact your home campus and discontinue the forwarding of e-mail. We will delete your e-mail account a week after your departure.

Home Campus	Uniform Resource Locator (URL)
Berkeley	http://socrates.berkeley.edu/Help/
Davis	https://mothra.ucdavis.edu/cgi-bin/services/index.cgi
Irvine	http://www.nacs.uci.edu/email/
Los Angeles	http://www.bol.ucla.edu/
Riverside	http://facultysupport.ucr.edu/
Santa Barbara	http://www.lsit.ucsb.edu/mail/



A number of words about computer viruses and security

In a broad sense, a virus is any software program that is placed on your computer without your permission. Technically speaking, a virus is a software program capable of replicating itself and attaching to another program in computer memory or on a disk. Viruses may damage data, cause a computer to crash, display messages, or lie dormant. Viral infection of your computer, though potentially serious, is not a cause for panic. Many viruses are benign, that is they do little more than infect a file or computer and announce their presence through silly or banal actions such as displaying a message from its creator on your monitor.



s o -

Viruses also are usually written for a specific operating system or program (for instance, Microsoft Windows 95 or Microsoft Word) and will not function with other operating systems or software. This will change as programming software becomes more sophisticated and less tied to specific operating systems.

Viruses are spread from computer to computer via a diskette traded between computers, over a network or over the Internet. The most common method now for spreading viruses is via e-mail.

Computer viruses are categorized into several broad categories viruses, worms, Trojan horses and macro viruses.

Viruses (the plain, vanilla variety) best adhere to the definition at the start of this section. They are self-replicating and attach themselves to computer memory or files. For the most part, these viruses are benign or low risk.

Worms are programs specifically created to destroy files or systems on stand-alone or networked computers. The 'Love Bug' of a couple of years ago and its ilk are examples of worms. Many worms are not technically viruses in that they are not self-replicating and need another virus to carry them as a payload from computer to computer. Worms are usually the most devastating class of virus.



A Trojan horse is a program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan Horses are not technically viruses either, since they do not self-replicate. Some Trojan horses deliver payloads that do not announce their presence but instead lurk on your system recording information such as your network user name and password or credit card information. Later, this information is uploaded without your knowledge to its creator via the Internet.

Subject: I Love You!
Does he love me or is he a worm
like all of the rest?

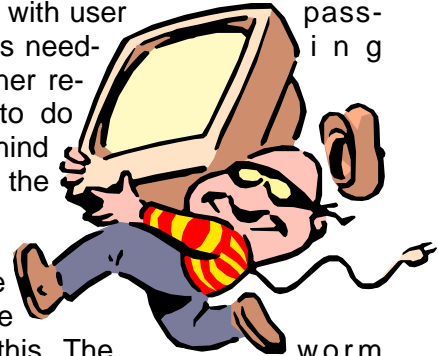
As the programs that we use have become more sophisticated and loaded with 'whistles and bells' they have also become more vulnerable to attack. Many of these programs include built-in programming functions known as macros as a part of their features. Macros



enable users to tailor and extend a program's use to better fit their needs. Microsoft Office is one such example. Macros can be very useful but they have developed a downside. They also provide creative, anti-social types with another means of attacking your files. Using a program's built-in programming language these miscreants are able to create macros that can alter or destroy your files.

Viruses, e-mail and social engineering

You may have heard the term 'social engineering'. It's a term invented to describe the activities of misguided individuals who attempt to destroy, subvert or steal user data usually via 'low tech' means. These activities can include anything from rummaging through garbage cans for carelessly discarded secrets such as pieces of paper with user passwords to phone calls purporting to be from outside technicians needing access to your network information to e-mails crafted to garner restricted information from unwitting users or persuade you to do something that is detrimental to your computer. The idea behind social engineering is to take advantage of our errors or to fool the unwary into doing a miscreant's bidding.



Social engineering techniques have been combined with the delivery of viruses to create a devastating combination. The 'Love Bug' e-mail attachment worm is a recent example of this. The worm is not activated until you open its e-mail attachment and its e-mail delivery vehicle is specifically crafted so as to fool the unwary into doing just that. When newly released, this type of virus gets by anti-viral algorithms because it does not purport to be anything other than it is. Most anti-viral algorithms look for file disparities or known viral 'fingerprints'. Consequently, by clever social engineering a 'hacker' can subvert even the best defenses.



Bill Gates personally sent me an e-mail about a new unstoppable computer virus that eats hard drives—it must be true!

Another example of social engineering is hoaxing. You've undoubtedly received e-mails purporting to be a news release that read: "AOL and IBM have just reported a terrible new virus that is unstoppable..." or other such hokum. These are invariably hoaxes that are started by individuals with too much time on their hands and due to the ubiquitous nature of e-mail are spread far and wide. They even take on a life of their own, frequently resurfacing weeks or months after their initial dispatch. Though, hoaxes cause no damage to computers, they are irritating, can cause undue distress among the uninitiated and the stir that they cause is undoubtedly equally as satisfying to their creators as a if they had released a virus. For this reason, they should be lumped together with viruses as a threat to the operation of your computer.

Should you get such a message, especially one that does not come from a reputable University of California computing services source, please verify its validity with the computing staff before passing it on to colleagues. This will ensure that the information about new viral threats is indeed legitimate and an accurate statement of the facts.



Steps that you can take to defend yourself

All of this information about viruses and social engineering can be a bit unnerving. In the sidebar below are some steps that you can take to increase your defenses against viruses and computer security.

- * **Install** anti-viral software on all of your computers and keep the viral definition files up-to-date. The viral definition files are like ‘mug sheets’ for viruses and provide the anti-viral software with a virus’s distinguishing features and ‘modus operandi’. All computers on University-owned computers at the Center have anti-viral software that is regularly and automatically updated.
- * **Scan** all diskettes and CDs that you receive for viruses. Better yet, do not accept diskettes or CDs from sources that you do not know and especially if you did not request them.
- * **Use the defenses** included with many commercial software programs. These are usually limited but still add to your security against some viral threats. Microsoft Word for instance includes limited security for macro viruses. Also, both Netscape and Microsoft web browsers include some security control. Use these.
- * **Do not** give out your network, e-mail or other computer system usernames and passwords to anyone who is not authorized to use your computer. Under University regulations you may give this information to verified UC information services personnel who are attempting to resolve a problem on your computer.
- * **Make sure** that your computer is secure. Do not leave your usernames and passwords out in plain sight or in obvious locations where prying eyes may see them. If you are leaving your computer for an extended length of time, logout or use a password protected screen saver.
- * **Do not** open e-mail attachments from someone you do not know and do not open an attachment even from a known source unless you are expecting it. Almost all e-mail viruses are still transmitted via attachments. It is true nonetheless that recently one or two viruses have appeared that can spawn themselves automatically without a user’s intervention. This happens only with certain specific versions of the latest e-mail software and under very specific conditions so it should not be a cause for undue alarm.
- * **Do not** open e-mail attachments from listservs unless you are very sure who it is from and what it contains. Several recent viral threats propagate themselves through e-mail lists. Indeed, if you can do without a particular list, unsubscribe from it.
- * **Do not** open any e-mail attachments that end in .exe, .com or .vbs extensions. These extensions indicate that the attachment is an actual program and it will run if you open it.
- * **Be diligent** when reading your e-mail. Be sure you understand who it is from and why they are sending you e-mail. Many instances of viral infection are due to people running through their e-mail without focusing their full attention on it.

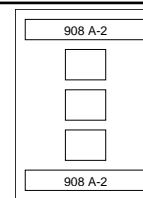
Personal Laptops:

To connect to the internet from a laptop in an apartment, your laptop must have a **PCMCIA 10/100 Base-T ethernet card** installed and an ethernet patch cable to connect the laptop to the network data jack on the wall. If you do not have a patch cable, one can be checked out from Information Services.



Plug one end of the ethernet patch cable into the ethernet card on the laptop and the other end into the data port on the apartment wall outlet.

Data Port = dark blue, bottom port ➤



Open a web browser and try to connect to a couple of websites.

If you are not connecting to the Internet, follow the instructions below to change your settings and try again. Send an e-mail to support@ucdc.edu if you have trouble getting connected to the Internet after following these procedures.

Win 95/98/NT/ME Laptop Settings for Accessing the Internet

1. From the Windows desktop, choose **Start, Settings, Control Panel, Network**
2. In the list *protocols*, choose **TCP/IP Protocol** or **TCP/IP -> your Ethernet card** where "your Ethernet card" is the installed PCMCIA network card.
3. Click **Properties** and record all settings for future reference, then check **Obtain IP Address automatically from DHCP**
4. Choose the **DNS** tab and record all settings for future reference, then remove all settings.
5. Click **OK**
6. Choose the **WINS** tab and record all settings for future reference, then remove all settings.
7. Click **OK** and answer **Yes** to restart the computer
8. After rebooting the computer, open a web browser and try connecting to a couple of different web sites.

Win 2000 Laptop Settings for Accessing the Internet

1. From the Windows desktop, choose **Start, Settings, Control Panel, Network**
2. RIGHT-CLICK on **Local Area connection**
3. In the list of adapters and protocols, choose **Internet Protocol TCP/IP**.
4. Click **Properties**
5. Check **Obtain IP Address automatically** and **Obtain DNS Automatically**.
6. Click **OK**
7. Click **OK** again and **Restart** the computer.
8. After rebooting the computer, open a web browser and try to connect to several different web sites.

For personal computers running Windows-based operating systems, we offer internal FTP (within the Center only) for accessing your network files. FTP, or File Transfer Protocol, is a means by which you can easily transfer files from one computer to another computer that have access to the internet.

To request FTP access, please email Support@ucdc.edu with "FTP Request" in the subject field. You will receive a reply email with instructions on how to use FTP once your account is activated.

See following page for Mac procedures...



Macintosh Laptop Settings for Accessing the Internet in a Washington Center Apartment

Please see Michael Sesay or Dianne Lessman if you have trouble getting connected to the Internet after first following these procedures.

Connecting your MAC to the Internet:

Connect a network patch cable from your MAC ethernet card to the data port on the wall (dark blue, bottom port).

1. Choose **Apple Menu, Control Panel, AppleTalk**
2. Choose Connect Via: **Ethernet**

1. Choose **Apple Menu, Control Panel, TCP/IP**
2. Verify it is set to Connect via: **Ethernet** and Configure: **Using DHCP Server**
3. Leave all other fields blank

Open a web browser and attempt to connect to several websites.

To logon to the UCDC network on a MAC:

1. Choose **Apple Menu, Chooser**
2. Select **AppleShare**, then click **Server IP Address**
3. Enter **LUX4** then click **Connect**
4. Verify that the **Registered User** radio button is selected
5. Enter your username and password and click **OK**
6. Place a checkmark in the box next to your username and click **OK**
7. Close **Chooser**

An icon with your username will appear on the desktop. This is your personal network folder in which to save files. This personal folder can also be accessed from Windows based computers as the **G:** drive. Please, save files to your personal folder so you can retrieve those files from any computer you login to using your username and password.



Security for Home Computer Users

The increasing availability of high-speed Internet access into the home (DSL & cable modems) has increased the risk of home computer systems being compromised by unscrupulous individuals lurking on the Internet. Below are some steps recommended by the Center to increase the on-line security of your home computer.

- For Windows and Macintosh computers we recommend that you upgrade to a recent version of the operating system. For Windows users, Windows 2000 or better; for Macintosh, OS X. Especially for Windows users, the Windows 2000 and XP operating system can provide a much more secure operating environment.

- Install anti-viral software such as Norton or McAfee and keep it up-to-date. Antivirus programs automatically scan files received via email and files or programs being downloaded from the internet. Do not run a program or open an email attachment without first running a virus scan. The small annual fee you pay for this service becomes insignificant when measured against the loss of your PC and its information.



- Turn off File Sharing.

1. In **Windows**, open **Windows Explorer**
2. Right-click on the Local **C:** drive and choose **Sharing**
3. Click the option for **Do Not Share this Folder**
4. Click **OK**
5. Repeat for any other **harddrive** partitions only (i.e., D:\)



1. On a **Mac**, click the **Apple Menu**
2. Choose **Control Panel, File Sharing**
3. In the File Sharing section, verify that "**File Sharing Off**" and you see a **Start** button. If **File Sharing** is **On**, click the **Stop** button.

- Windows systems, rename TFTP.exe to TFTP.old. TFTP is a file transfer protocol that comes standard with the operating system which hackers can use to access your files.

1. Right-click on the Local **C:** drive and choose **Search...**
2. In the **Search for Files** field, type **TFTP.*** and click **Search Now**
3. If the results display a file named **TFTP.EXE**, then right-click on this file and choose **Rename**.
4. The filename will become a highlighted, text box in which you can then change the **EXE** to **OLD** and press **Enter** to accept the changes.
5. Close the Search window and Windows Explorer



Security for Home Computer Users (Continued...)

- Install the **Microsoft Baseline Security Analyzer (MBSA)**. The Analyzer checks computers for common security misconfigurations and gives warnings, suggestions and solutions when appropriate. MBSA is available for download at: <http://download.microsoft.com/download/win2000platform/Install/1.0/NT5XP/EN-US/mbsasetup.msi>

System Requirements for MBSA:

- Windows 2000 or Windows XP
- Internet Explorer 5.01 and later



- It is highly recommended that a hardware router or firewall be installed on your computer. Personal firewalls monitor computers for suspicious activity while connected to the internet. Inbound intruders are stopped before they can get into your computer and a record of the repelled attacker, including IP address, is stored in a log file. Firewalls can also protect against hostile cookies, applets and ActiveX controls while you surf the Web. (Personal firewall software can also be installed, but this method is less user-friendly and requires tedious configuration of settings.)

For a small home network, consider a low cost router with [network address translation \(NAT\)](#). For more security, consider a firewall router with [stateful packet inspection \(SPI\)](#).

Hardware Router Brand Selection Guide:

Firewall Routers (SPI):

2Wire
D-Link
Hawking
Netgear
Snapgear
SofaWare
SonicWall
WatchGuard
Zyxel

NAT Routers:

Asante
D-Link
Linksys
Macsense
MultiTech
NetGear
Nexland
SMC

- Use strong passwords to logon to your home computer that differ from those that you use on your work computer. See the password recommendations posted earlier in this handout.



Welcome to Washington, DC!

Many of you will be bringing personal computers with you to DC so here is a reference handout you can follow to help you get service for your computer related needs.

PhotoCopy/Color Printing Services

<u>Kinko's</u>	1612 K Street, NW	Washington, DC (202) 466-3777
<u>Press Express</u>	1611 K Street, NW	Washington, DC (202) 429-5550
<u>Sir Speedy</u>	1429 H Street, NW	Washington, DC (202) 408-8485

Parts and Accessories

<u>Computer Accessory Store</u>	1522 K Street, NW	Washington, DC (202) 628-4940
<u>Radio Shack</u>	1835 K Street, NW	Washington, DC (202) 467-5052

Renting and Leasing

<u>Capital Computer Rental</u>	2931-F Eskridge Road	Fairfax, VA	703-698-5500
---------------------------------------	----------------------	-------------	--------------

- offers free delivery and pickup
- will load any applications of choice (WordPerfect, MS-Office, Web browsers)
- 15% discount coupons available ; ask Dianne Lessman for details

Service and Repair

<u>Richards Computer</u>	2803 Merrilee Drive	Fairfax, VA	703-876-5355
---------------------------------	---------------------	-------------	--------------

- offers in warranty and out of warranty service on Toshiba laptops.
- does not provide pickup and delivery.

<u>Dupont Computers</u>	1761 S Street, NW	Washington, DC	202-232-6363
--------------------------------	-------------------	----------------	--------------

- honors warranty service for IBM and ACER laptops and out of warranty service on Toshiba and Dell.
- offers pickup of your system for a nominal fee.
- offers parts and supplies.

<u>Notebook Computers, Inc.</u>	50 S. Pickett Street	Alexandria, VA	703-823-6555
--	----------------------	----------------	--------------

- honors in warranty and out of warranty work on most major brands of laptops.
- does not provide pickup service.

