Desktop Security and Best Practices

2013.06

All computer operating systems have vulnerabilities that are targeted by are subject to security risks. In a networked environment, such as a college campus, a compromised computer can affect other computers and disrupt services throughout the campus, personal information can be compromised leading to identity theft and intellectual property can be stolen. In order to reduce the risk of a successful intrusion and to minimize the damage that can be done, this document provides you with an overview of the fundamental steps and procedures to be followed to minimize security exposures and resulting disruptions.

Basic Steps

Regardless of which operating system you are using (Windows, Mac, Linux, Unix), the basic steps for securing an operating system are the same:

- Keep operating system patches up to date
- Use encryption to securely encode sensitive information
- Install antivirus software; configure for daily updates
- Install and configure a personal firewall
- Keep application and software patches up to date (e.g., Microsoft Office, browsers, etc.)
- Follow best practices when opening email attachments
- Follow secure password policies
- Follow best practices for user account security
- Eliminate unnecessary network services, applications, and processes
- Avoid peer-to peer file sharing
- Install and configure anti-Spyware programs
- Configure system restore points to protect your current configuration
- Perform regularly scheduled backups to protect data
- Turn off computer when not in use; restrict physical access to computer

The provided links are for further reading and a more in depth understanding of the topics presented here.

Patching the Operating System

One of the most important and fundamental routine tasks to perform is to patch your computer on a regular basis. All operating systems have “holes” in them. These “holes” are vulnerabilities in the software code that can be exploited to gain access to the computer system. There are programs on the Internet that are constantly searching for unpatched computers. Prior to connecting a new computer to the Internet, please be sure that the latest critical patches are installed. Please call the OIT Service Desk for assistance in this matter.

Both Microsoft and Apple have provided programs that will automatically check for updates on a regular basis. The settings should be configured to check for updates **daily**.

To confirm or configure the proper settings follow these steps:

- Window 7
    - Open Windows Update by clicking the **Start button** . In the search box, type **Update**, and then, in the list of results, click **Windows Update.**
    - In the left pane, click **Change settings.**
    - Under Important updates, choose the option "**Install updates automatically (Recommended)**"
    - Under **Recommended updates**, select the **Give me recommended updates the same way receive important updates** check box, and then click **OK**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
- Windows XP
    - Select the **start** button
    - Select **Control Panel**
    - Double-click the **System** icon
    - Select the **Automatic Updates** tab
    - If not configured, select the **Automatic** radio button
    - Click **OK** to save the configuration and exit
    - Close the Control Panel window
- Mac OS X
    - Open **Systems Preferences**
        - While in **Finder**, click on the **APPLE SYMBOL** and select **System Preferences**
        - Or, click on the **System Preferences** icon in the **Dock**
    - In the **System** row, select **Software Update**
    - Confirm that "Check for Updates" is set for **Daily**, if not change accordingly

(Return to Basic Steps)

Encrypting Files and Folders

The best way to secure sensitive information from malware is to encrypt it. Encryption works by using a complex formula to securely scramble (or encrypt) individual files and folders, entire disks and data transmissions between devices. Once encrypted, the information can only be unlocked (or decrypted) using complex digital keys that require a password. Of course, it's critical to choose a strong password.

How to Protect Files and Folders Using Microsoft Windows

Encrypting File System (EFS) is a feature of Windows that allows you to store information on your hard disk in an encrypted format. Encryption is the strongest protection that Windows provides to help you keep your information secure.

To encrypt a Windows 7 folder or file

1. Right-click the folder or file you want to encrypt, and then click Properties.
2. Click the General tab, and then click Advanced.
3. Select the **Encrypt Contents to Secure Data** check box, and then click OK.

To encrypt a Windows XP folder or file
The EFS feature is not included in Microsoft Windows XP Home Edition.
How to Encrypt a Folder
NOTE: You can encrypt files and folders only on volumes that use the NTFS file system.

1. Click Start, point to All Programs, point to Accessories, and then click Windows Explorer.
2. Locate and right-click the folder that you want, and then click Properties.
3. On the General tab, click Advanced.
4. Under Compress or Encrypt attributes, select the Encrypt contents to secure data check box, and then click OK.
5. Click OK.
6. In the Confirm Attribute Changes dialog box that appears, use one of the following steps:
    - If you want to encrypt only the folder, click Apply changes to this folder only, and then click OK.
    - If you want to encrypt the existing folder contents along with the folder, click Apply changes to this folder, subfolders and files, and then click OK.

The folder becomes an encrypted folder. New files that you create in this folder are automatically encrypted. Note that this does not prevent others from viewing the contents of the folder. This prevents others from opening items in the encrypted folder.

(Return to Basic Steps)

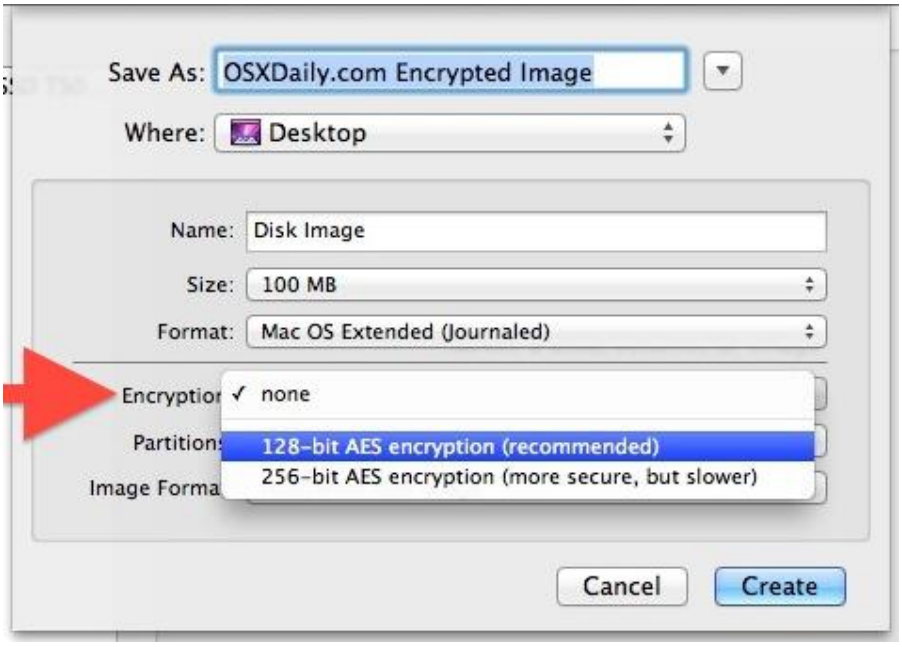
How to Password Protect Files & Folders in Mac OS X with Disk Images

Do this along with general password protection for maximum effect.

1. Launch “Disk Utility” located in /Applications/Utilities
2. Click on the “New Image” button at the top of the app

http://osxdaily.com/2012/01/11/password-protect-files-folders-in-mac-os-x/

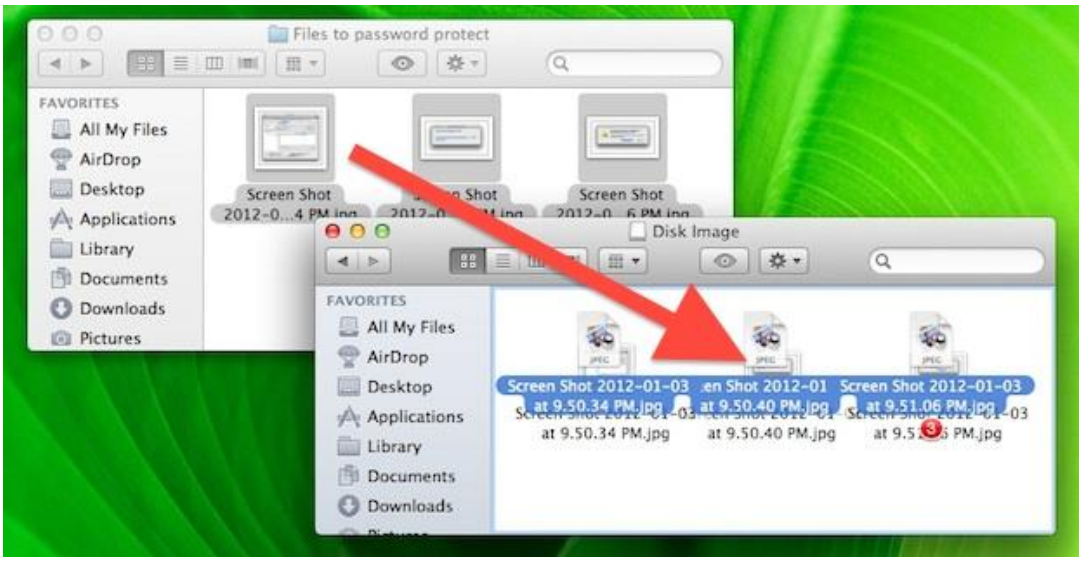
3. Name the disk image and set a file size that is appropriate for what you intend to store in there
4. Click on the contextual menu alongside “Encryption” and choose either 128 or 256-bit encryption (256 is stronger)



5. Click “Create”
6. At the next screen you will set a password to access the folder – do not lose this password, you will not be able to open the disk image if you do
7. Optional: Uncheck the box next to “Remember password in keychain” – only do this if you’re the only user on the Mac, otherwise anyone can open the image without the password

8. Click “OK” to create the disk image

The encrypted disk image is now created. Now you need to locate the image, mount it which will require the password set in the creation process, and drag files and folders into the mounted image that you want password protected. The default location for new disk images is the Desktop, but if you saved it elsewhere, look there instead.



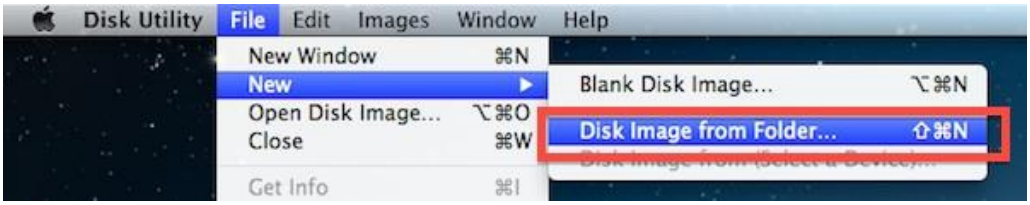
Once you are finished copying files and folders to the mounted disk image, eject it like any other disk and the contents will be safely protected within, requiring the password to access

again. Because the files and folders have been copied, you'll want to delete the originals so they aren't visible to anyone else. Again, do not lose the password set or you will not be able to get access to the contents of the encrypted disk image.

This should not be considered a replacement for setting a general password for a Mac, and it's always a good idea to lock down the screen when you're away from the computer. Filevault also provides encryption and security features, but older version have some potential speed drawbacks that are particularly noticeable on non-SSD drives, this is mostly a non-issue for OS X Lion, however.

This specific "Image from Folder" trick requires OS X 10.8 or later to use:

1. Open Disk Utility, found in /Applications/Utilities/
2. Pull down the "File" menu and select "New" and then "Disk Image from Folder"



3. Navigate to the folder you wish to turn into an encrypted drive and click "Image"
4. Set the Image Format to "read/write" and the Encryption to "128-bit AES"

5. Choose a strong password (or **generate one** by pressing the black key icon) and – this is important – uncheck the box saying "Remember password in my keychain", then click OK

If you do not intend on using the encrypted image as a working folder that you can add and remove documents from, you can choose an Image Format other than "read/write".
An encrypted disk image will be created based on the folder you specified, it may take a while if the folder is large or your Mac is slow.

(Return to Basic Steps)

Accessing the Encrypted Folder & Contents

After the encryption procedures is finished, you'll now be able to access and use the encrypted folder. To summarize steps of accessing the encrypted folder and how to properly use it to maintain security:

1. Open the encrypted folder image with a double-click, treating it as a normal disk image
2. Enter the password used during the initial encryption setup – do NOT check "Remember password"

3. Access the encrypted folder and the contents as a mounted virtual disk, you can modify, copy, edit, delete, and add to it
4. When finished, close the files and eject the virtual image to re-secure the folder and files and require a password for future access

You will want to locate the encrypted dmg file and store it somewhere accessible enough, since you will be using a double-click to try to mount the folder image in the Finder when it needs usage, and of course you will need the password to access the files. Just as when creating the disk image password, always uncheck the box saying "Remember password in my keychain" or else you will store the password and lose the security benefit of the encrypted image since anyone with access to your user account could open it. This also applies to transferring the encrypted folder image to another Mac.

With a readable and writable encrypted disk image, you can treat it as a normal folder and copy, delete, or move files from the image. Anything brought into the image while mounted will become encrypted automatically under the same protective layer with the same password. When you are finished working with the folder and want it password protected again, simply unmount the disk image. Regaining access again will require the password before it can be mounted and available.

(Return to Basic Steps)

Anti-Virus Software Installation and Configuration

Every computer issued by the CCNY Office of Information Technology has McAffee's anti-virus software installed and configured. It requires no intervention on the user's part. The settings are properly pre-configured.

Do not **uninstall** this software without first conferring with CCNY helpdesk technicians.

(Return to Basic Steps)

Personal Firewall Installation and Configuration

Many of today's operating systems include a personal or software firewall. Both Windows XP, Windows 7 and Macintosh OS X provide this feature.

To enable **Windows XP Internet Connection Firewall** (ICF), follow these steps.

- Select the **start** button
- Select **Control Panel**
- Double-click the **Network Connections** icon
- Select the connection to be protected (e.g., Local Area Connection, Wireless Network Connection, etc) and double click
- Select the **Advanced** tab (for Wireless Network Connection, click the **Advanced button**, then the **Advanced tab**)
- To enable ICF, check the check box for **Protect my computer and network by limiting or preventing access to this computer from the Internet**

For a detailed information about ICF, click on the link displayed.

(Return to Basic Steps)

To enable **Windows 7 Internet Connection Firewall** (ICF), follow these steps:

- Open Windows Firewall by clicking the S**tart button**, clicking **Control Panel**, clicking **System** and **Security,** and then clicking **Windows Firewall.**
- Click **Turn Windows Firewall on or off**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click **Turn On Windows Firewall** (recommended), and then click **OK**.

Turning on and Configuring the Mac OS X Firewall

- From the Apple menu, select **System Preferences**.
- From the personal tab select **Security & Privacy**.
- Click the **Firewall** tab.
- Click the lock icon and authenticate with your administrator username and password
- Click **Start**. The firewall turns on - you'll know it's enabled when you see the green light and the **Firewall: On** message.

Patching applications and software

Just as operating systems require patches to correct security flaws, so do applications. Please make sure that your application have been patched and are up to date. In particular, pay close attention to the browser(s) you use (e.g., Internet Explorer, Mozilla Firefox, Apple's Safari, Netscape, etc.). These programs are often the object of attack.

Similarly, other applications are vulnerable if not patched appropriately. Patching is also required in order for the applications to operate properly with the operating system as it changes over time due to patching.

In order to update Microsoft Office for Windows or Macintosh open one of the programs (Word, Excel, Access, Power Point), click the **Help** button, and select **Check for Updates**.

(Return to Basic Steps)

Email Attachment Best Practices

Email attachments are a primary source of malicious code (viruses, worms, etc.). The Office of Information Technology deploys an enterprise solution from McAffee to protect the campus from such transmissions. Nevertheless, it is still prudent to follow best practices when opening attachments.

One should always verify that the sender intended to send the attachment in the first place. Although this would seem to be self-evident, there are many variations of viruses that automatically propagate themselves by first infecting a given computer and then sending emails to all addresses housed on the infected machine. The sender message appears to be legitimate even though the actual individual never sent the message. Also, it is common to find a message in which the sender's address has been "forged" by the virus. The virus gathers a legitimate address and enters it into the sender's information even though the messages has been sent from a different account entirely.

(Return to Basic Steps)

Password Policies

User names and passwords are the primary means of authentication used to access a desktop system. While the Office of Information Technology assigns the user name, the individual user selects the password. The point in creating a password is to make the password as hard as possible to guess, or "crack". There are numerous programs and applications that can be used to crack a password, but if the password is complex enough and properly constructed, these

attempts can be thwarted to a large extent. It is also important to realize that the perpetrator of such an attack does not need to be sitting in front of your machine; this can be an attack initiated from anywhere provided there is network connectivity.

Passwords should be changed at least once every **90 days**. Even a well-constructed password can be cracked with enough time. By changing passwords often and not re-using old passwords frequently**,** this type of access is limited.

The following guidelines for password creation are adapted from the SANS Institute web site:

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words “CCNY”, "nyc", "new york" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

(Return to Basic Steps)

User Account Policies

Modern operating systems provide user accounts for individuals using a desktop. Through the deployment of user accounts, multiple people can use the same machine without interfering with one another's work. Each operating system has different designations for different levels of access to the computer system. Complete access is granted to the administrator account (Windows, Macintosh) or the root or super user account (Linux, UNIX). Accounts that restrict access to the system but enable users to conduct normal computing tasks are generally referred to as "user" accounts.

For day-to-day usage always use your limited or user account. If you need to perform a simple administrative task, such as installing software, follow these guidelines to use the Run As function.

- Locate the application to be installed.
- While holding down the **SHIFT** key, right click the application
- Select **Run as …** from the context menu
- Select the **The following user** radio button
- Enter the requested information for the administrator account user name and password
- Click **OK**

The program will now install. This method allows one to elevate one's account privilege to that of an administrator for the duration of the task.

If the task is of a more complex nature and cannot be conducted with the Run as … feature, log off as a user and log on as an administrator. It is advisable to disconnect form the network during the duration, if possible.

A user should periodically examine his or her computer's user accounts. Remove any accounts that are not required or that have not been created by you or the Office of Information Technology.

(Return to Basic Steps)

Peer-to-Peer File Sharing

Peer-to-peer file sharing programs designed to allow the unlimited sharing of music and videos, such as Grokster, Kazaa, etc., present known and well-documented risks. By opening up a hard drive to anyone on the Internet who uses a given p2p program (e.g., Kaza, BearShare, etc.), the security risks are obvious. Malware, spyware, viruses, Trojan horses, worms, and key logging programs have all been downloaded during the process of p2p file sharing. Once installed on a

computer, the integrity of a system can no longer be maintained. Sharing copyrighted material in this manner without permission is, of course, illegal, and copyright holders have brought suit against users on college campuses who have engaged in such practices.

Peer-to-peer file sharing for research and other academic purposes should be used with great caution. Feel free to contact OIT for assistance.

(Return to Basic Steps)

Spyware

Spyware is seemingly ubiquitous: an Internet site guide to known spyware programs listed over 1500 programs. These programs range from the relatively benign to the criminal. Identity theft is on the rise. Anytime a program is downloaded form the Internet, one runs the risk of installing a spyware program as well. P2P programs are notorious for this problem. The problem for the individual user is simply that these programs are installed without his or her knowledge, and they remain hidden. To remove such programs, an anti-spyware program is recommended. There are several free programs available, which work well.

Click on the link provided to see recommended list.

http://en.wikipedia.org/wiki/Spyware

http://www.pcworld.com/downloads/collection/0,collid,1347,pg,1,00.asp

To further protect your computer, a firewall is recommended. Windows XP computers with Service Pack 2 installed, Windows 7 with Service Pack 1 and Mac OS X provide software firewalls. A firewall limits the type of access to a given resource. By properly configuring a firewall, you can add a layer of security to your desktop that is otherwise unavailable.

Windows XP
Use the Internet Connection Firewall:

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_enable_firewall.mspx?mfr=true

Understanding Windows Firewall:

http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspxhttp://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
Mac OS X

Using a Firewall to help protect your computer:

http://support.apple.com/kb/ht1810

There are also a number of firewalls available for download or purchase.

(Return to Basic Steps)

Configuring System Restore

Windows XP and Windows 7 has a facility whereby the operating system takes an image of itself and the installed applications at different points in time. This feature enables a user to return his or her computer to a previous (functioning) state should a change in the system (through application or patch installation) result in a partially or fully inoperable system. One can set restore points at regular intervals and/or one can set a restore point before installing a new and untested application. This procedure does not affect the data on the computer. It does, however, offer a measure of security and should be utilized.

For details on how to configure System Restore please click on the following link:

http://technet.microsoft.com/en-us/library/bb457025.aspx

http://windows.microsoft.com/en-us/windows7/products/features/system-restore

A general note of caution is also warranted at this point. The Registry is the heart and soul of any Windows operating system. System Restore takes a "snapshot" of the Registry for restoration purposes. The Registry can also be changed manually.

WARNING: Manual manipulation of the registry is discouraged.

One can easily disable a computer and render it useless. The reinstallation of the operating system all applications is then required, which can result in a total loss of data.

(Return to Basic Steps)

Data Integrity and Recovery

All computers malfunction at some point. Hard drives will fail at some point. In order to protect the data on a computer, backing up the data is of fundamental importance. One should regularly back up one's files to a media disk (cd or zip) or to an external hard drive.

(Return to Basic Steps)

Computer Access

All too often one forgets that the simplest way to gain access to digital information is to walk into a room and sit down at the computer, or walk away with an unattended laptop. Just by locking the door to your office, you can decrease the risk of information theft considerably.

Similarly, the act of turning off your computer when not in use is the electronic equivalent of locking the office door. Hackers cannot scan your computer if it is not on.

(Return to Basic Steps)

Remember, your information is your responsibility. Protect it!

Additional Resources and Links

The Center for Internet Security (CIS) is a nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration. Its Security Benchmarks Division provides standards, metrics and step-by-step guides to dramatically increase the security of your IT assets.
http://www.cisecurity.org/

Before You Connect a New Computer to the Internet:
http://www.cert.org/tech_tips/before_you_plug_in.html

Home Network Security:
http://www.cert.org/tech_tips/home_networks.html

Home Computer Security:
http://www.cert.org/homeusers/HomeComputerSecurity/