Securing Your Computer

Why secure your computer?

Securing the computers of an organization is a process that needs to happen on a regular basis. It is very important because this protects that information and does not allow it to get into the wrong hands. Also, securing computers provides confidentiality with key information. Without security, vital information would be available to competitors. Information integrity happens when computers are secured as well. Basically, your organization will be able to depend on the accuracy of the information because you know that no one is able to alter the data. This is why the security of computers is so imperative to any organization. Without that security, many of the daily processes of your organization will function inefficiently.

Levels of Security

There are different types of security you can apply to your computers and/or servers to prevent unauthorized access to your computing resources. The more levels of security you apply, the more secure your computer assets.

1. **Site Level Security** refers to techniques for protecting your physical computing equipment from being lost, damaged or stolen. It also refers to techniques for protecting your organization's internal network from being accessed by those outside of your organization.
2. **System Level Security** refers to techniques that ensure only authorized people in your organization can access your computers and your internal network. It also refers to techniques that ensure malicious files and programs are not allowed to enter your computers.
3. **Application Level Security** refers to techniques that ensure only authorized users can use your application systems.
4. **Folder Level Security** refers to protecting folders (and files within the folders) from being accessed by unauthorized users.

Site Level Security

Some techniques for protecting your computer equipment from being lost, damaged or stolen include:

- Implement **key, ID card, or pin code entry** to rooms where computer equipment is stored, especially your organization's server computer. Be sure to keep a list of who has keys, ID cards with access, and pin codes in a safe place. Remember to retrieve keys and/or remove ID card and pin code access privileges when people leave their positions.
- Secure laptops or desktops to desks via **cable locks**.
- For small devices such as smartphones and flash drives, **attach devices** such as long lanyards and/or metal objects to them which make it easier for you to hear them if dropped or find them if lost.

An important technique for securing your organization's internal network from unauthorized access is the use of firewalls.

What is a Firewall?

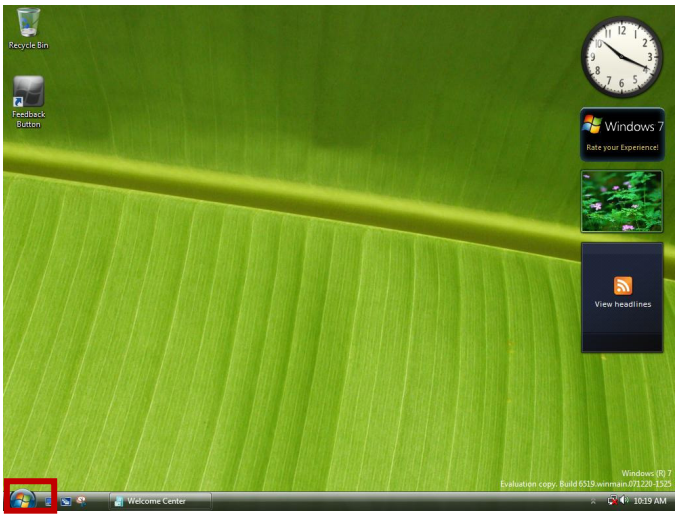
A **firewall** is used to help keep a network secure. It is similar to a filter. Its primary objective is to control all of your organization's incoming and outgoing network traffic by analyzing data and determining whether it should be allowed through or not.

A firewall can be setup either by software programs or by computer hardware. An example of firewalls that are a part of computer hardware is a gateway/router. Many gateway/routers allow you to setup filters where you can specify who to allow access to your network.

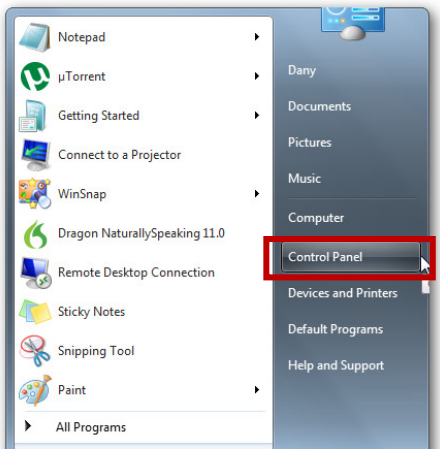
In addition to firewall protection by routers, firewalls can also be implemented in some operating systems such as Windows.

How to Use Windows Firewall

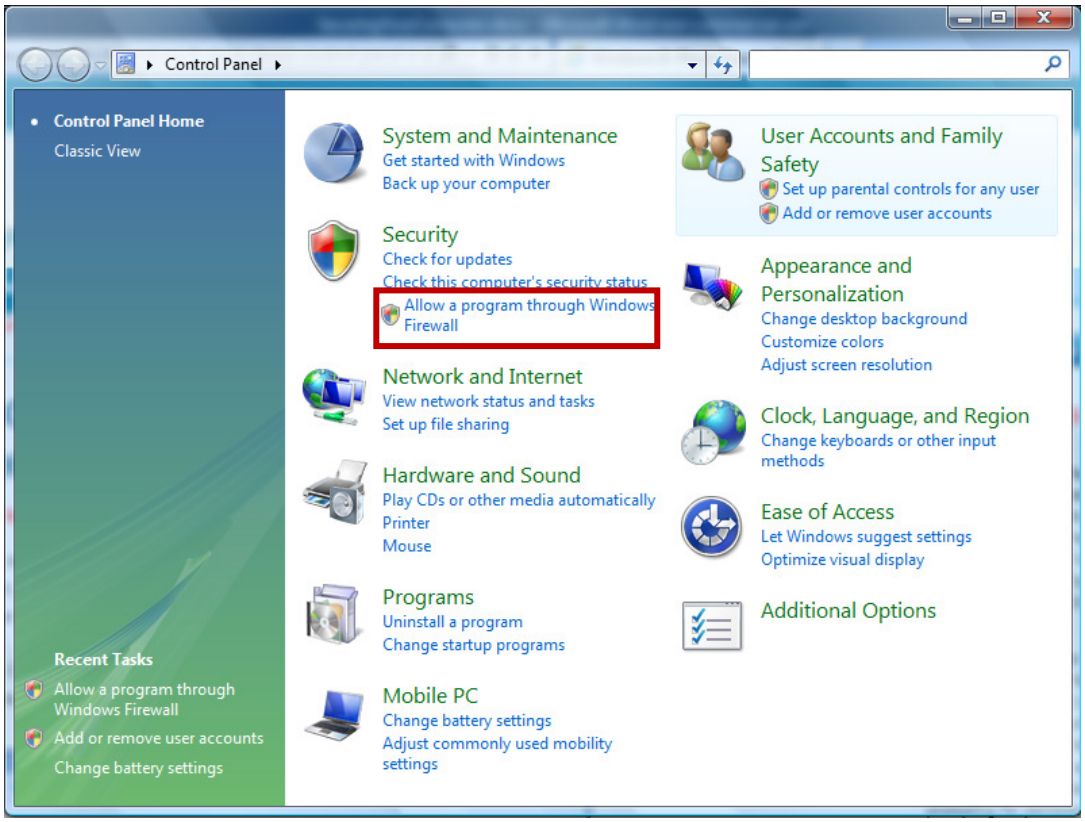
1. Click the Windows home button in the lower left corner of your screen.



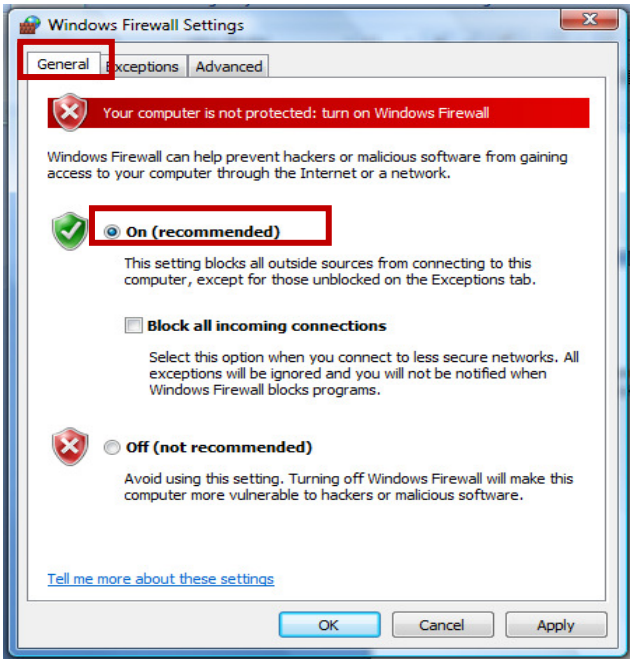
2. Click the **Control Panel** button.



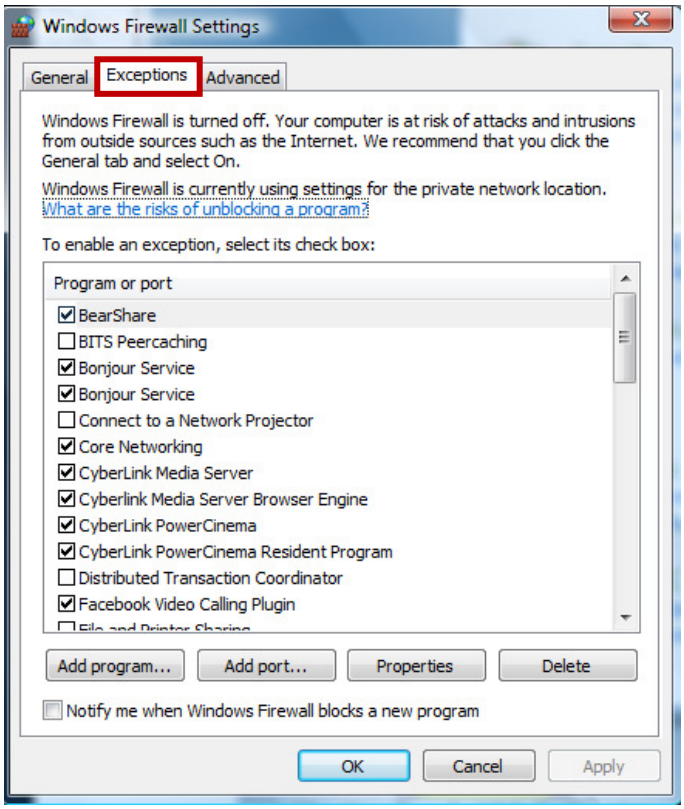
3. Click **Allow a program through Windows Firewall**.



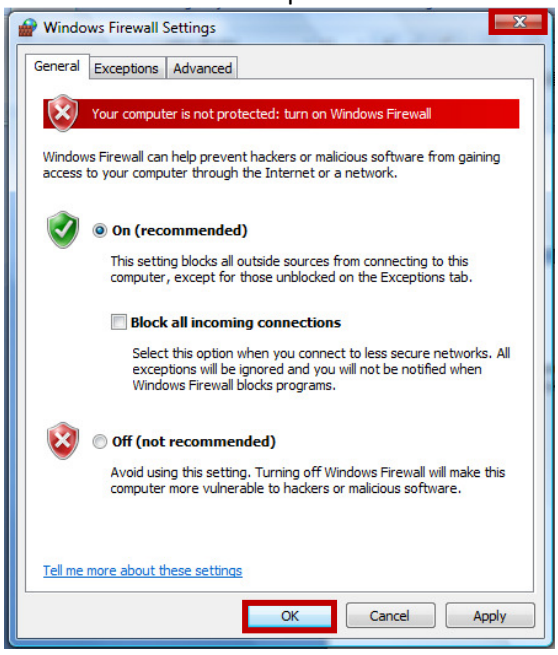
4. Click the **General** tab and make sure the green "On" radio button is selected. If not, make sure you click it to turn it on. This setting ensures anyone or any program outside your network is prevented from making a connection to your network.



5. OPTIONAL: You can set exceptions by clicking the **Exceptions** tab. This allows you to manually choose which programs you will allow to access your network from the outside. Click **OK** to finish this step.



6. Click "OK" and click the red "X" in the upper right hand corner to exit out of this screen. Your network should now be protected.



System Level Security

Some techniques for ensuring only authorized people in your organization can access your computers and your internal network are to:

- setup **user accounts and passwords** for every member of your organization authorized to access computer resources.
- ensure computer **screensavers are locked**

A technique for ensuring malicious files and programs are prevented from harming your computers is to:

- install **anti-malware programs** and regularly scan your computer for viruses and spyware using these programs.

User Accounts and Passwords

A user account or user name is a name used to gain access to a computer system. Usernames allow access to systems to authorized users only. For added security, you should create a password to accompany the user account. User accounts control which programs users can access and what types of changes they can make to the computer. Typically, you'll want to **create standard accounts** for most computer users so that they are not allowed to install new programs or make changes that affect all users of the computer. People who install programs on computers or create new computer users should be given **Administrative accounts.**

Tips for User Account names:

- Choose a name that's easy to spell, type and remember
- Keep it relatively simple

Tips for Passwords:

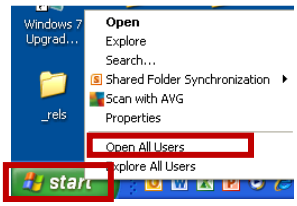
- Change your password several times a year
- Use strong passwords. Strong passwords are passwords that resist attacks. Strong passwords make it hard for humans or computers to gain access to information.
- Don't use only letters or only numbers
- Don't use names of spouses, children, friends, or pets
- Don't use phone numbers, Social Security numbers or birthdates
- Don't use the same word as your log-in, or any variation of it
- Don't use passwords with double letters or numbers

How to create a User Account in Windows

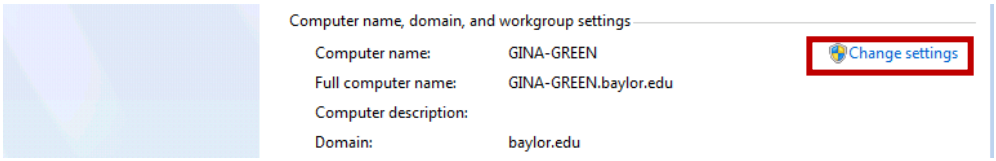
To create authorized computer users, the person creating the accounts must have Administrative rights on the computer.

To check if you have administrative rights:

For Windows XP, if you right-click the Windows Start button and see an option for "Open All Users", you have administrative rights on the computer; if you don't see this option, you do not have Administrative rights.

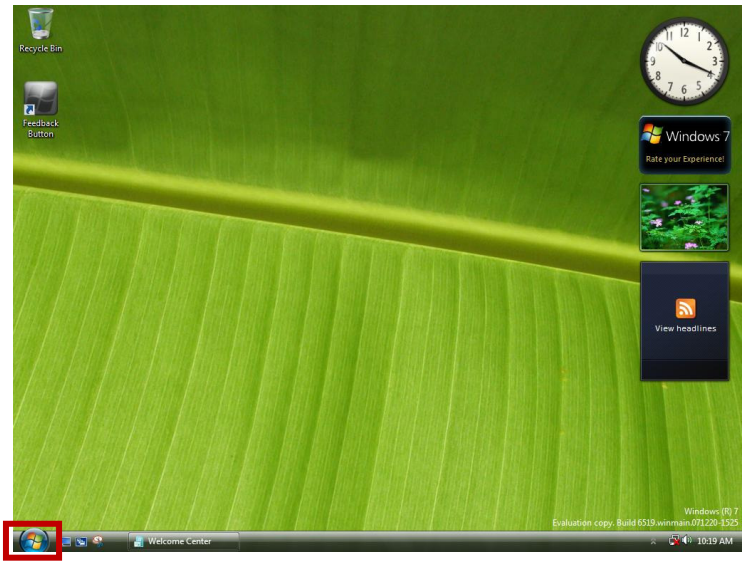


For Windows 7 Professional, right-click My Computer, and select Properties. If you see the Change Settings option, you have Administrative rights; if you don't see this option, you do not have Administrative rights.

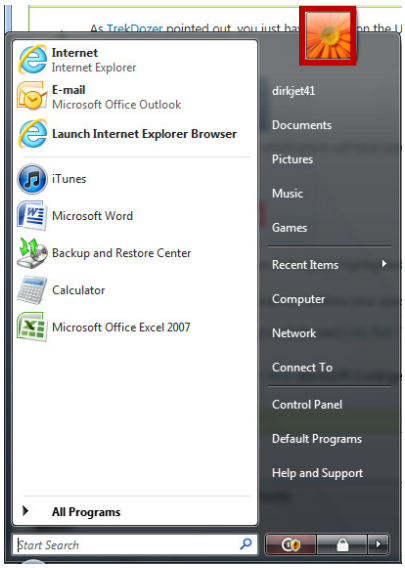


For Windows 7 Home or Windows Vista:

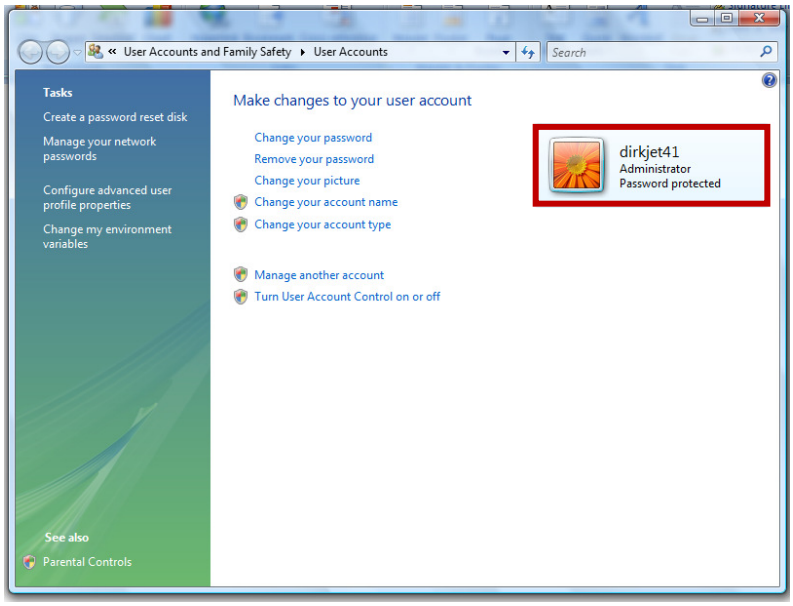
1. Click the Windows home button, which is usually located in the lower left corner of the screen.



2. Click the user icon.



3. This screen will tell you if you are an **Administrator** or not. If you are an Administrator, the word "Administrator" will appear under your user name. If you are not (i.e., you are a standard user), then either the words "Standard User" will appear under your name, or nothing will appear under your name.



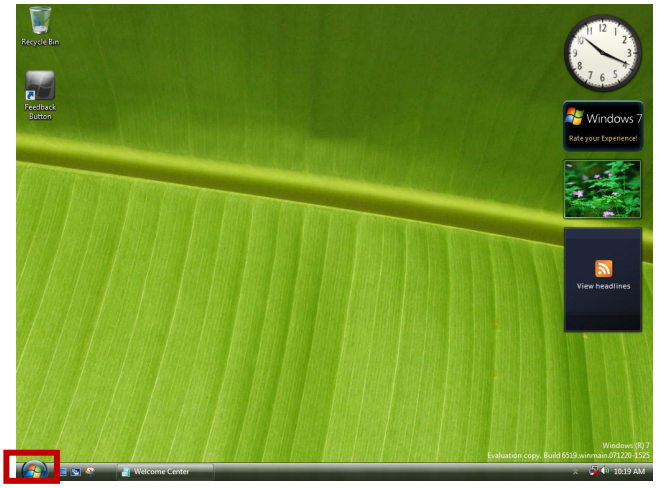
Assuming your user account is an administrator, the steps that you will follow to create a new user account will vary, depending on whether the computer is on a domain or a workgroup.

To check whether your computer is on a domain or a workgroup:

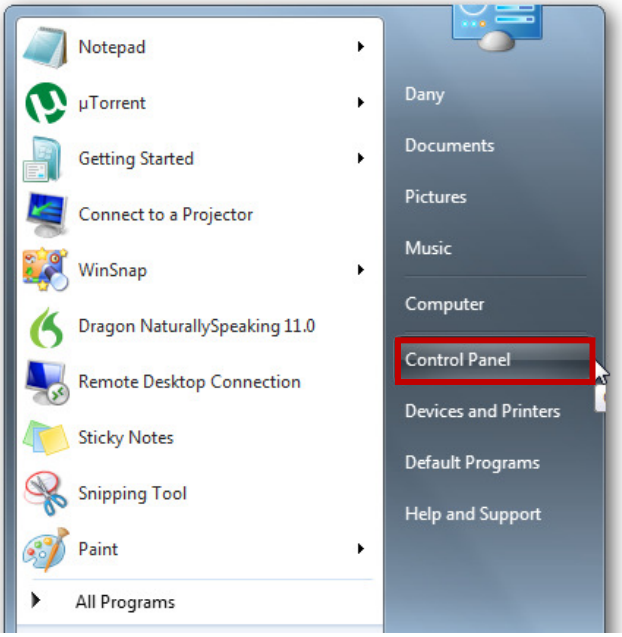
1. Right-click on My Computer and select Properties
2. For Windows XP, click on the Computer Name tab.
3. If you are in a workgroup, you should see a Workgroup name in the dialog box (e.g., MSHOME, WORKGROUP, etc…). If you are in a domain, you should see a domain name (e.g., Baylor.edu, google.com, etc…).

Create a New User Account on a Workgroup Computer (Windows 7)

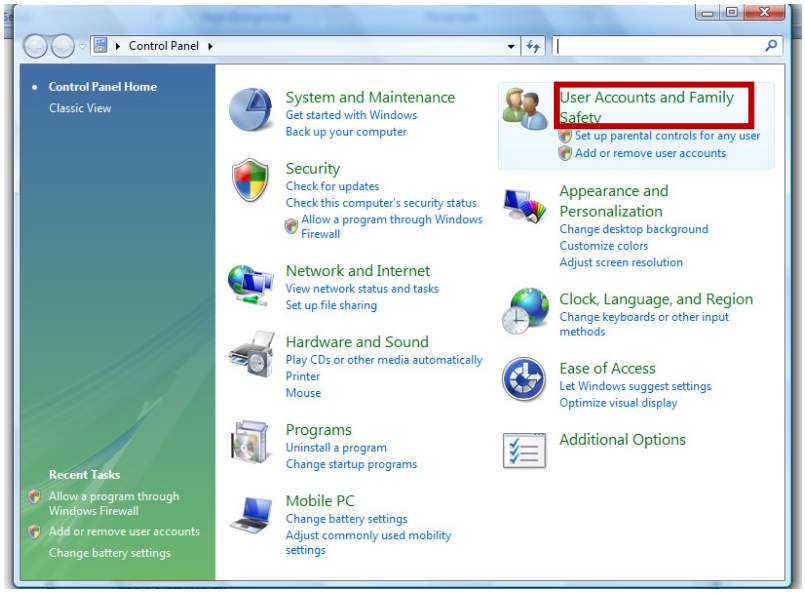
1. Click the Start button.



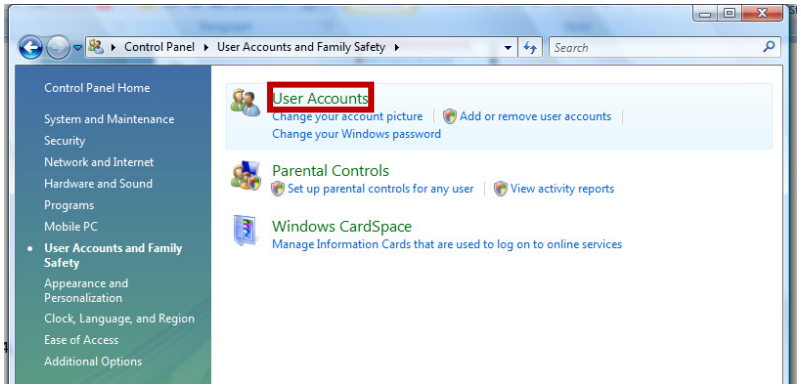
2. Click Control Panel.



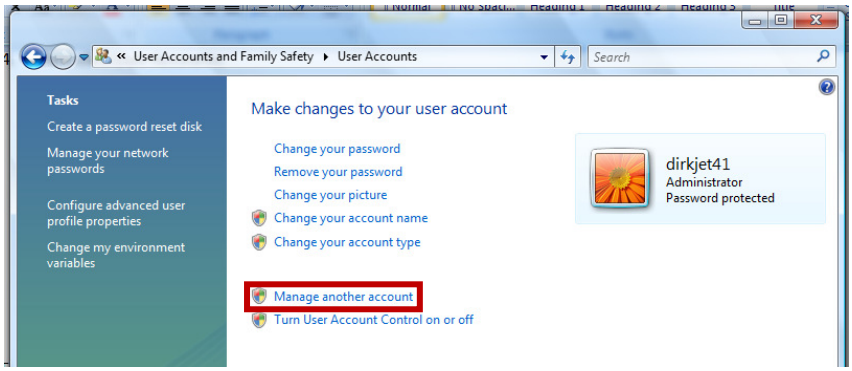
3. Click User Accounts and Family Safety (if there).



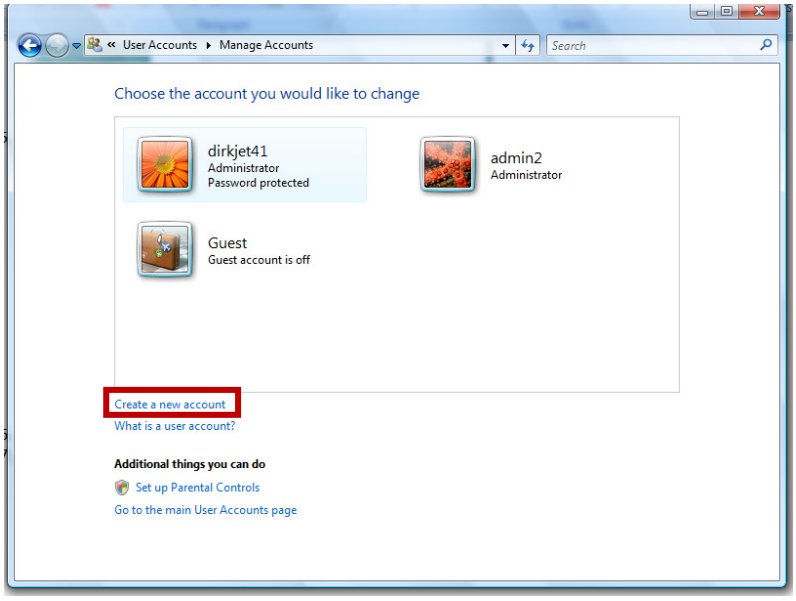
4. Click User Accounts.



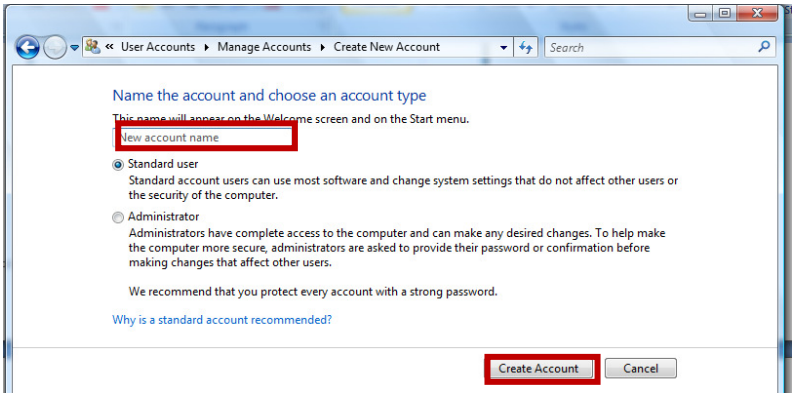
5. Click Manage another account. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.



6. Click Create a new account.



7. Type the name you want to give the user account, click an account type (typically Standard user), and then click Create Account. The new user account will be created.

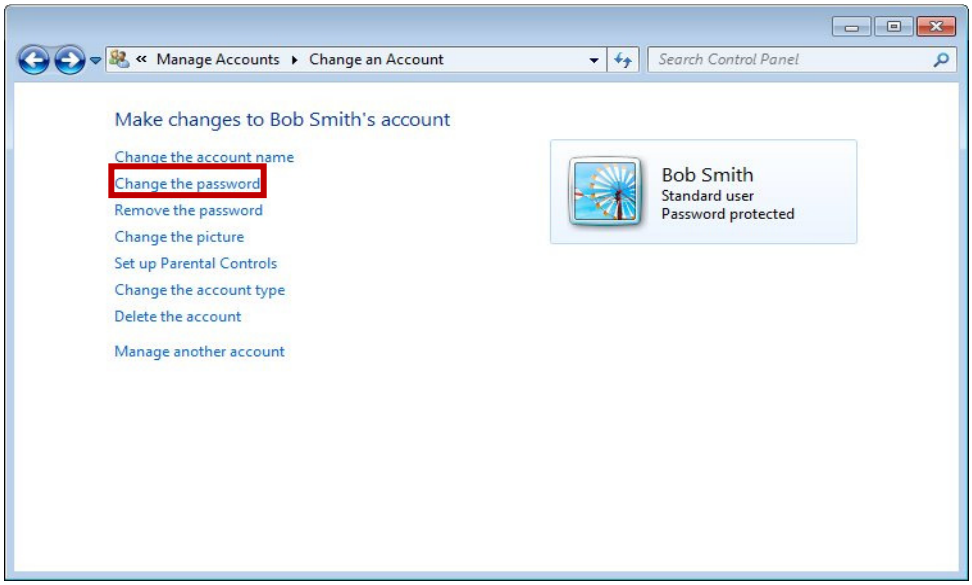


Create or Change another user's Password on a Workgroup Computer (Windows 7)

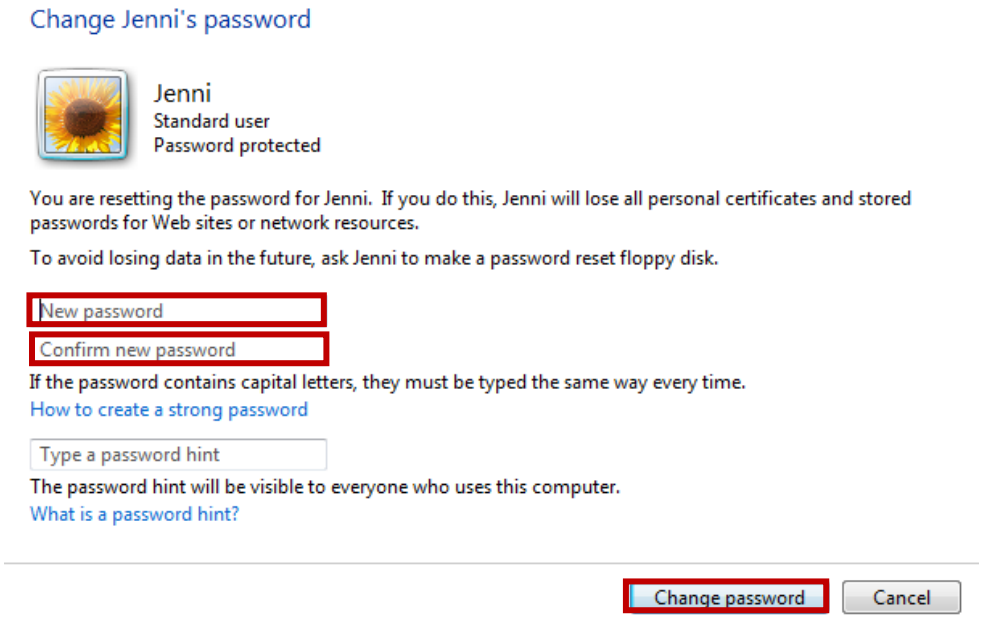
Repeat steps 1 through 5 from the previous section, then proceed with the following steps.

1. On the **Manage Accounts** screen, click the user account that you want to Create or Change the password for.

2. Click **Change the Password**.

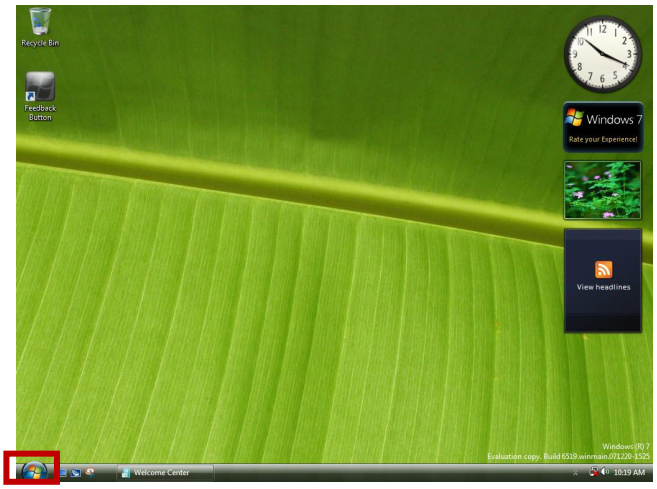


3. On the **Change** Password screen, enter the new password into the **New password** field as well as the **Confirm new password** field and click **Change password** to finish the process.

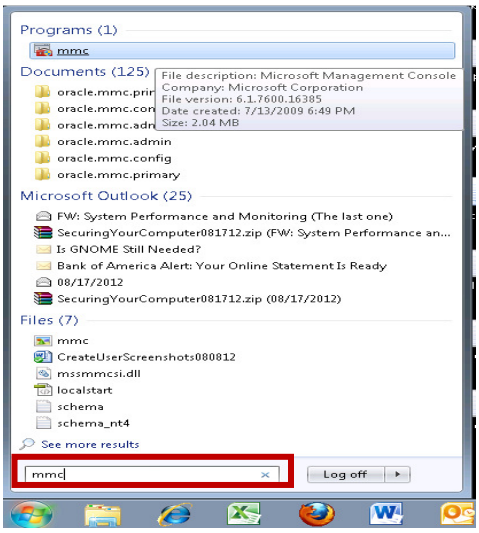


Create a New User Account and Password on a Domain Computer (Windows 7)

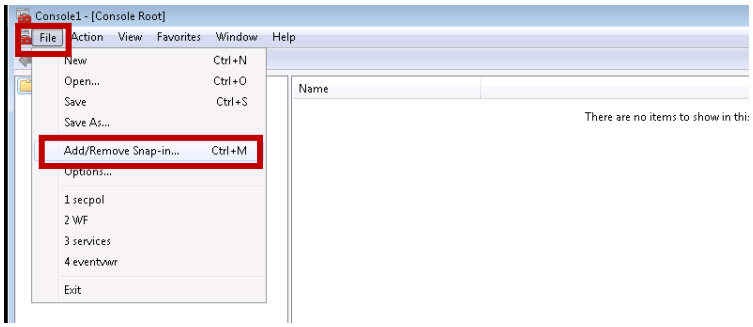
1. Click the Start button.



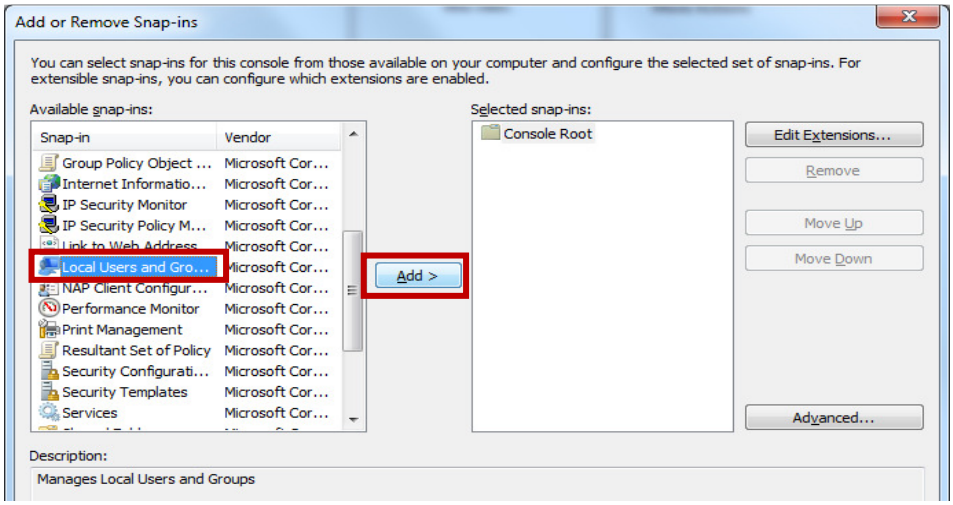
2. In the search box, type mmc then press the Enter key. If you are prompted for an administrator password or confirmation, type the password or provide the confirmation.



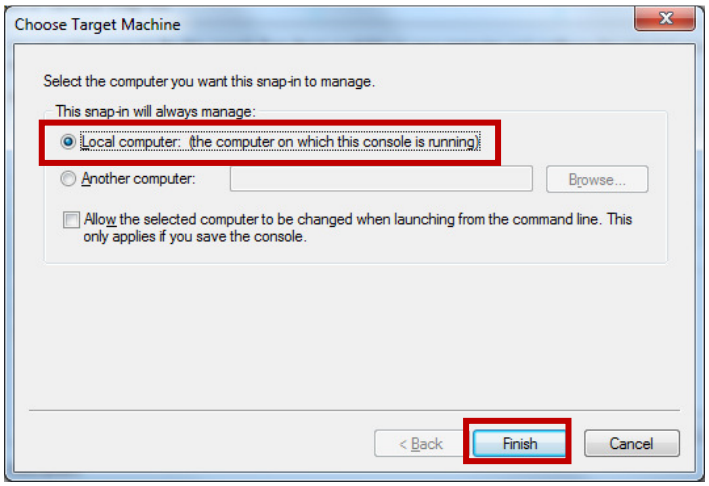
3. In the left pane of the Microsoft Management Console, click Local Users and Groups. If you don't see the Local Users and Groups option, it's probably because that "snap-in" hasn't been added. Follow these steps to add it:
    a. In the Microsoft Management Console, click File, then click Add/Remove Snap-in.



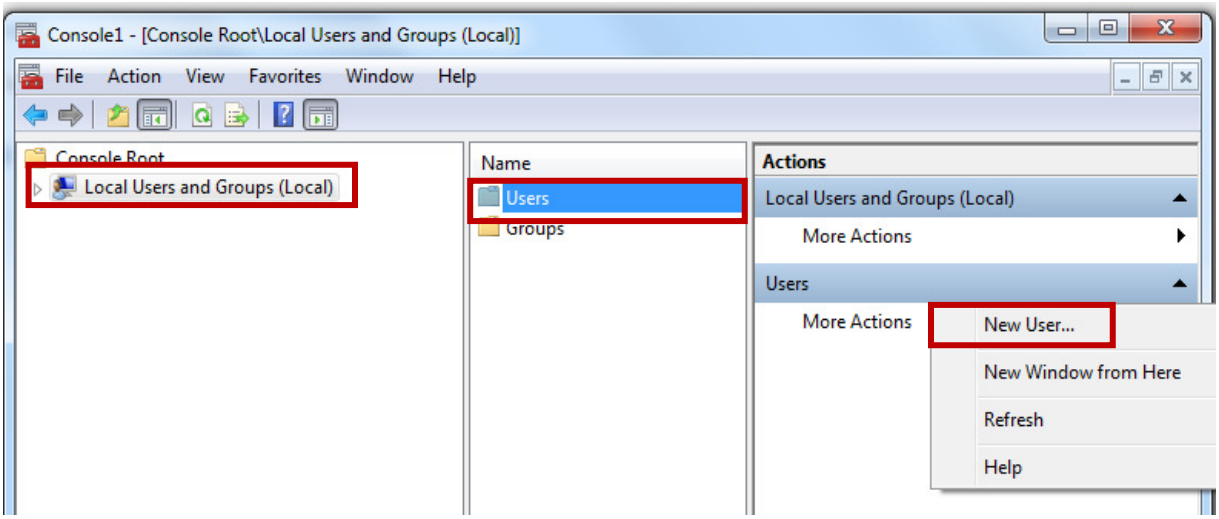
    b. Click Local Users and Groups, then click Add.



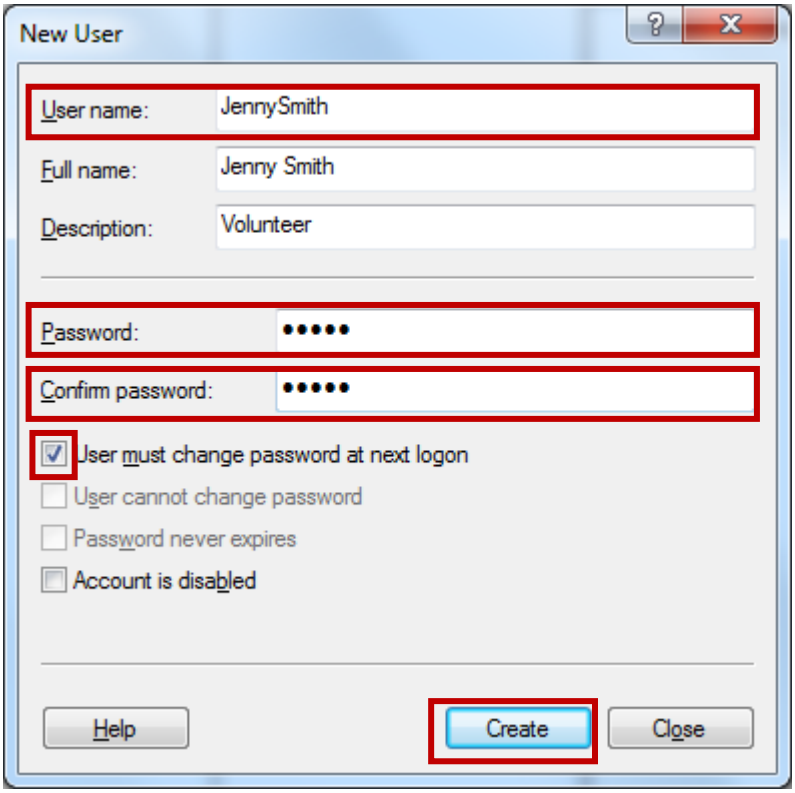
    c. Click Local computer, click Finish, then click OK.



4. After clicking Local Users and Groups, click the Users folder, then under Actions click New User...

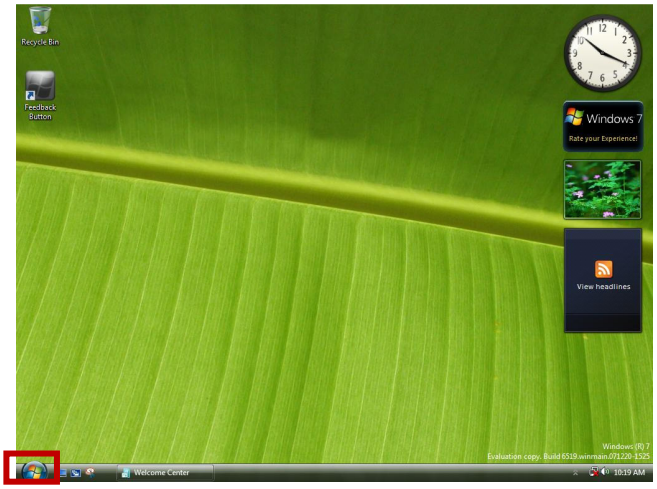


5. Type the **user name** you want to give the new user account, the **Password** you want to assign to the user, and retype the password to **confirm** it. Ensure the "User must change password at next logon" **box is checked** if you want to force the new user to change their password for privacy reasons the first time they log on. Finally, click **Create**. Your new user account is now created.

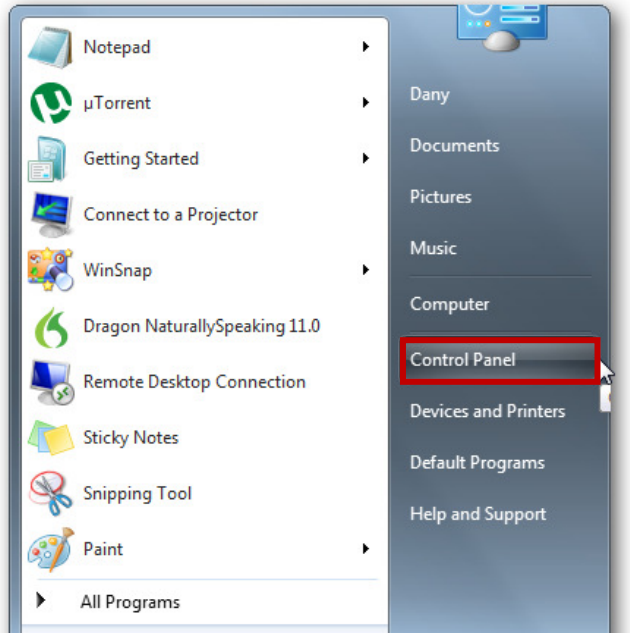


Change another user's Password on a Domain Computer (Windows 7)

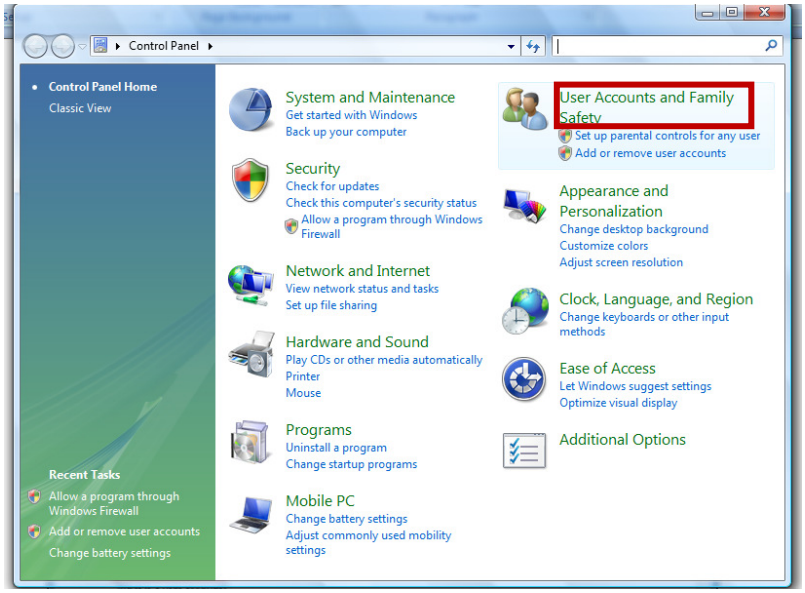
1. Click the Start button.



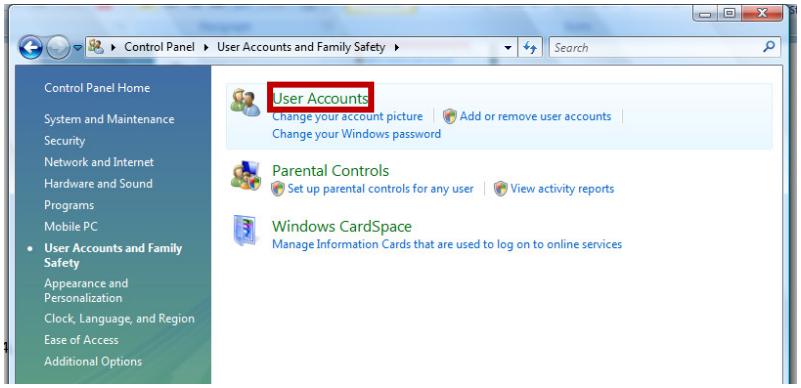
2. Click Control Panel.



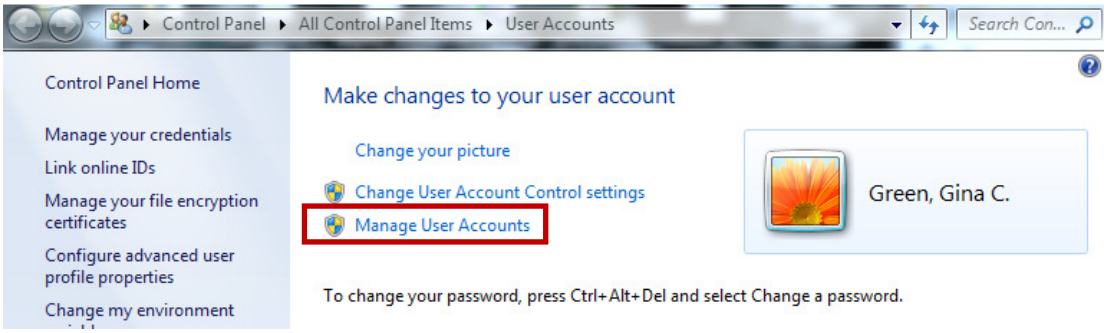
3. Click User Accounts and Family Safety (if there).



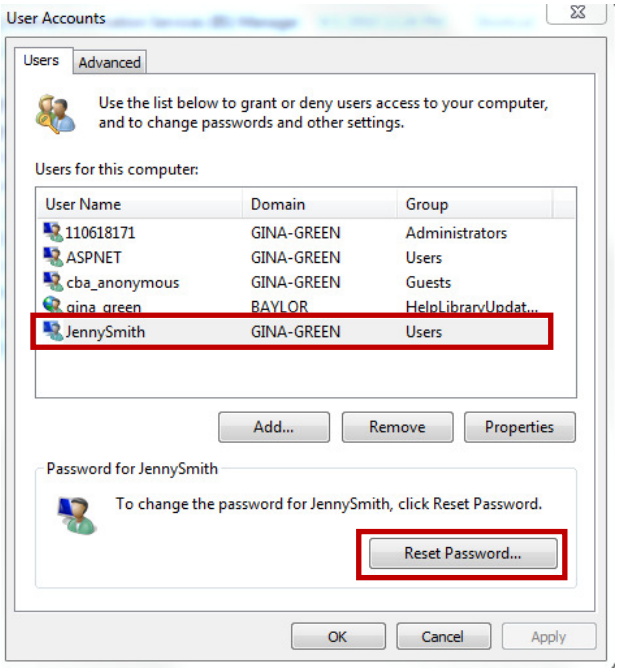
4. Click User Accounts.



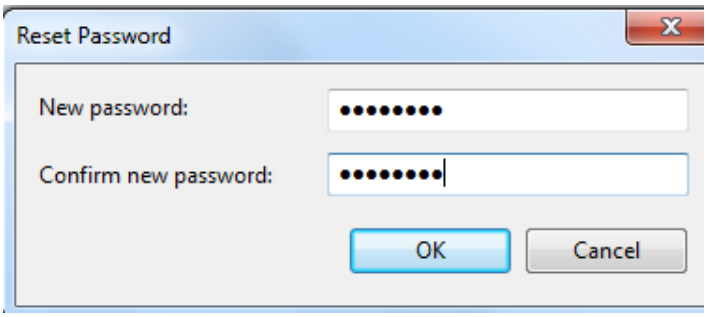
5. Click Manage User Accounts.



6. Highlight the user account that you want to Change the password for, then click Reset Password.

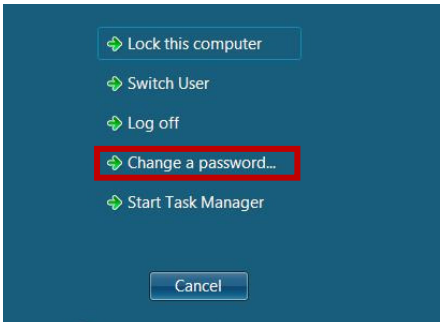


7. Enter the new password into the **New password** field as well as the **Confirm new password** field and click **OK** to finish the process. The user's password is now changed.



Changing Your Own Password

1. Press **CTRL-ALT-DELETE** on the keyboard all at the same time.
2. Click **Change Password.**



3. Fill in all of the information to complete the process.

Locking Screensavers

Most of us have screensavers that appears on our computer screen when there has not been any computer activity for a specified period of time. Screensavers have several uses, including protecting our privacy when we are away from our computers so that others cannot see our work, and securing our computer in instances where, for example, we leave the office without properly logging off the computer.

For these reasons and more, it is a good idea to "lock" your screensaver so that a password must be entered in order to remove the screensaver and resume computer activity. To do this in Windows 7:

1. Right-click anywhere on the desktop and select "Personalize" (Windows 7) or "Properties" (Windows XP).
2. Click on Screen Saver
3. Ensure the "On resume, display logon screen" box is checked. You may also want to ensure that the "Wait:" time is not very high so that the screensaver appears soon after there is no activity on the computer.
4. click OK.

Anti-Malware Security Software (Anti-Virus / Anti-Spyware)

Security software prevents, detects and removes malware. Malware are simply programs designed to harm systems. Computer viruses, computer hackers, and spyware are examples of malware. It is vital for an organization to have some sort of security software if they value their information.

Anti-malware software can often be configured to run scans of your computer on a regular basis automatically. In addition, you can (and should) manually scan your computer periodically to ensure it is free of harmful programs.

Suggestions for Anti-Malware Software:

Below are some popular options for free Windows anti-malware programs:

Program Name	Website
AVG	http://free.avg.com/us-en/homepage
Malwarebytes	http://www.malwarebytes.org
Avira	http://www.avira.com/en/avira-free-antivirus
Avast	http://www.avast.com/free-antivirus-download

Below are some popular options for Windows anti-malware programs that can be purchased:

Program Name	Website
Norton Antivirus	http://us.norton.com
Webroot Antivirus	http://www.webroot.com/En_US/index.html
BitDefender	http://www.bitdefender.com/solutions/antivirus.html

In addition, you may visit this site to view a more comprehensive list of malware software that is able to be downloaded: http://www.cnet.com/topic-software/malware.html.

Security Options in Browser Settings

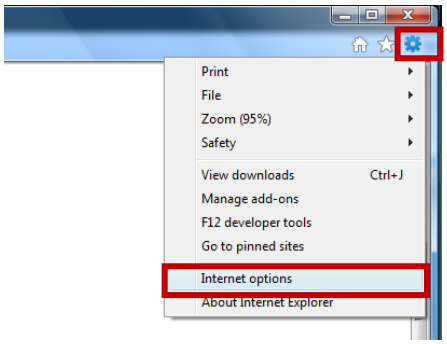
Some forms of malware infect your computer by hiding in your browser's memory or through files deposited on your computer as a result of visiting websites through your browser. Within your browser settings, you can do a variety of things to reduce the risk of contracting malware in these ways. Some of the security-related tasks that can be accomplished within browsers settings are:

- Set Homepage
- Clear Browsing History

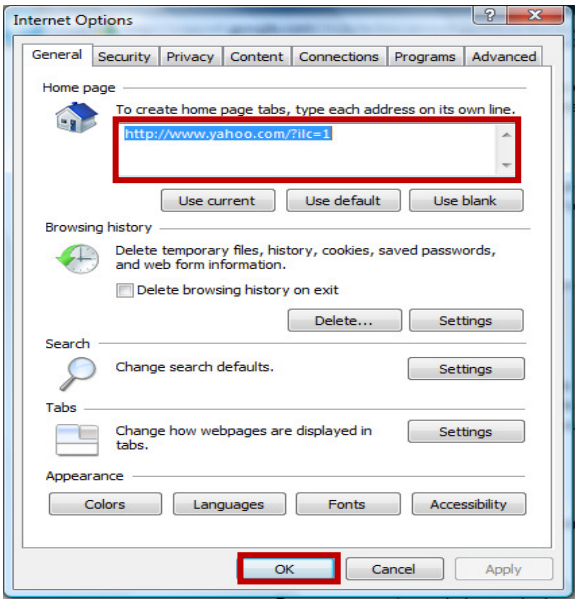
The instructions that follow are for Microsoft's Internet Explorer. However, similar tasks can be accomplished in Mozilla's Firefox by clicking on File, Options, and then the Privacy tab.

Set Homepage

1. Open Internet Explorer then click **Tools,** then select **Internet Options.**

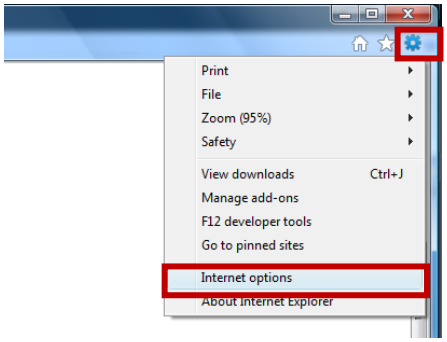


2. In the home page section, type the desired website that you would like to connect to each time you open the browser; click **OK** to finish.

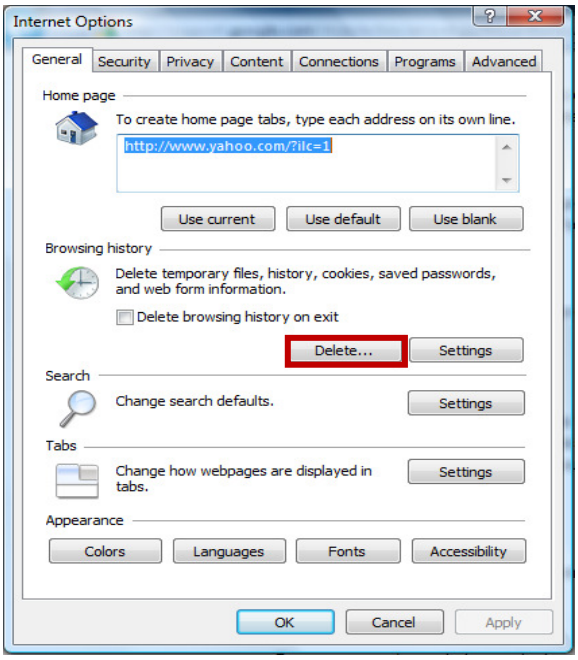


Clear Browsing History

1. Open Internet Explorer then click **Tools,** then select **Internet Options.**

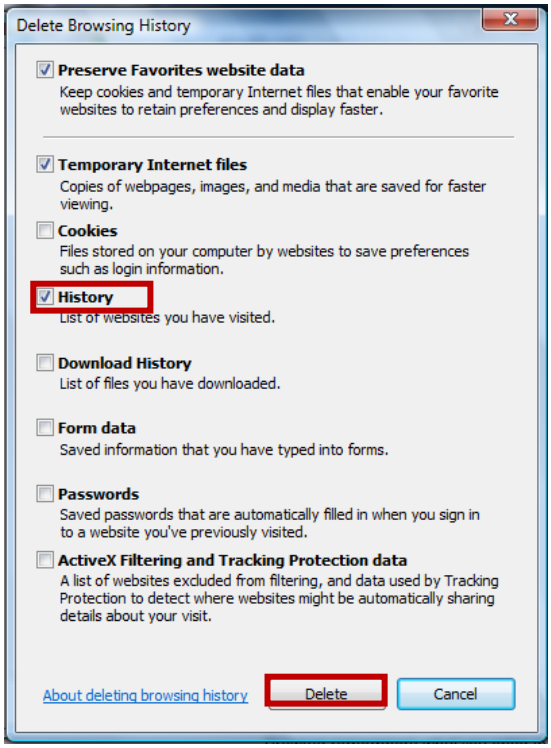


2. In the browsing history section click **Delete…**.



3. On the Delete Browsing History screen, a good practice is to have at least Temporary Internet Files and History checked. Checking "Temporary Internet Files" will ensure that any files that were placed on your computer by websites you visited will be deleted. Checking "History" will remove the list of previous websites you have visited which can prevent malicious software from knowing your browsing patterns. You may also consider checking the Cookies box. Cookies are small files placed on your computer by websites you have visited, usually to store information to personalize your website visits such as your preferences, login information, etc. Although most cookies are harmless, some cookies may be used for malicious intent. Checking the "Cookies" box will remove cookies stored on your computer.

   Click **Delete** to remove the files and finish the process. Depending on how many files you have, this process may take some time.



Application Level Security

In addition to the security mechanisms described in previous sections of this document, many programs used by nonprofits also implement their own security mechanisms. For example, your donor management program may require you to log in with a username and password prior to you being able to access the program. Additional application-level security is another way to ensure that even if an unauthorized user is able to access your network and log on to a computer, unless that person knows the separate login information for your applications they will still be unable to access your sensitive application programs and data.

Folder Level Security

Securing specific folders on a computer is another way to prevent unauthorized access by individuals, even if those individuals are authorized to access other computer resources.

To restrict access to a folder:

1. Right-click the folder you want to restrict access to, and select Properties.

2. Click on the Security tab to show a list of user accounts that currently have access to the folder.

3. To remove or reduce access by a specific user, highlight that user's account name and click Edit…

4. in the permissions box, check or uncheck permissions as desired. From this same location you can also Add users who can access the folder by clicking the Add… button. Click OK to complete the process.