

## Safe Computing Practices and Security Measures

This document is designed to assist you in practicing secure computing methods both in the workplace and at home. Most workplace security is managed by a central computing department. Contact your IT professionals for assistance in the workplace for those items that cannot be managed independently. This is designed as a guide – not as definitive methodology for all machines because all machines are different, and it is not possible to document absolute procedures. Always do research through web sites for your specific machine's software and hardware. These recommendations should be followed for ALL operating systems (Windows, Macintosh, Linux – machines running Windows are **not** the most or only vulnerable machines); however, specific instructions are for computers running Windows. All operating systems will follow similar methods but may not use the exact named commands as a Windows machine.

### What to do **Use strong passwords.**

---

#### How to do it

- Use a pass “phrase” rather than a password.
- Use a combination of upper- and lower-case letters, numbers and special symbols when allowed.
- Periodically change your passwords.
- Do not share your passwords.
- Do not write your passwords down and leave them in a highly visible location or store them on your computer.

#### Comments

Every account on the computer, including the limited and administrative accounts, needs to have strong passwords.

### What to do **Protect confidential information.**

---

#### How to do it

- Do NOT store your social security number, driver's license number or credit card numbers on your computer.

#### Comments

If you use confidential information in the workplace (accounting, human resources, student information, research material), check with your IT group about the best way to secure that information.

### What to do **Use email safely.**

---

#### How to do it

- Do NOT open attachments you are not expecting.
- Do NOT click on links provided in emails you are not expecting or have not requested, e.g. emails from companies advertising services or products.
- If you are cleaning out an attachments folder, do not simply open files to find out what they are; either delete them, or try to track down the original source of the attachment. Chances are if it's been sitting in your attachments folder awhile you don't need it and it can be deleted. Be especially suspicious of files with these extensions: .exe, .cmd, .bat, .scr, .pif.
- Check your email settings to see if automatic downloading of attachments can be turned off.
- Check your email setting for “filters” which can be set to automatically place “junk mail” and “spam” into the Trash. Most of these messages are identified by Cornell's mail server with a PMX in the header (you can use this as an identifier in the filter).

#### Comments

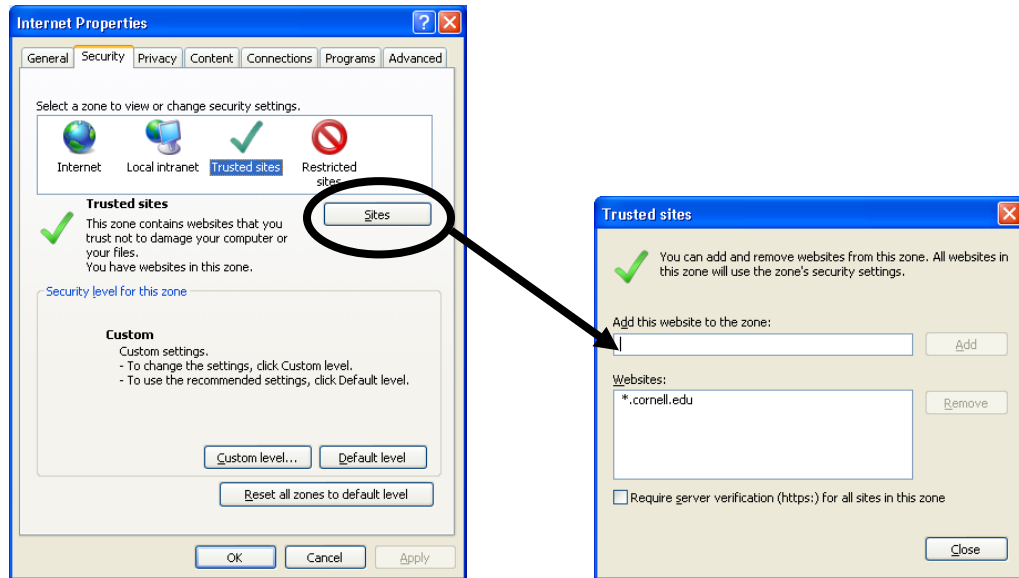
When in doubt (and you should ALWAYS be suspicious if you were not expecting the message), check with the sender or simply delete the message.

MANY emails look legitimate. A good example is a notification from a bank that your account requires some form of action. These are usually “phishing” scams and should be questioned. Always contact your institution or log into the institution's website directly before following any links provided in emails.

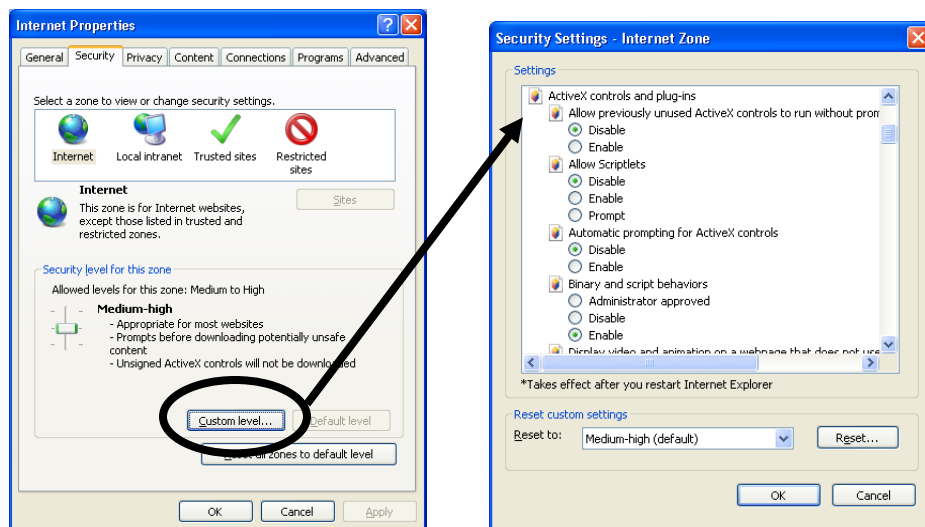
**What to do**

**Browse safely.**

- Consider using Mozilla Firefox or some other alternative browser for everyday browsing.
- The Firefox browser can be downloaded at <http://www.mozilla.com>.
- Set "Trusted" sites (This is an Internet Explorer feature only). The following instructions are for Internet Explorer but will be similar for all browsers:
- Tools | Internet Options | Security Tab
  - Click on the Trusted Sites Zone.
  - Type in sites that are trusted and click Add. Use wildcards to add all pages at a site. For example \*.cornell.edu will allow all pages from Cornell's site to load.



- Click on the Internet Zone.
- Click on the Custom Level button.
- Change those ActiveX settings which are enabled Disable or "Prompt."



**Comments**

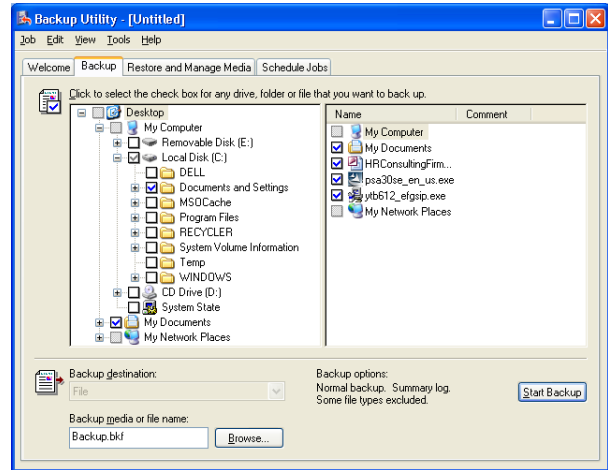
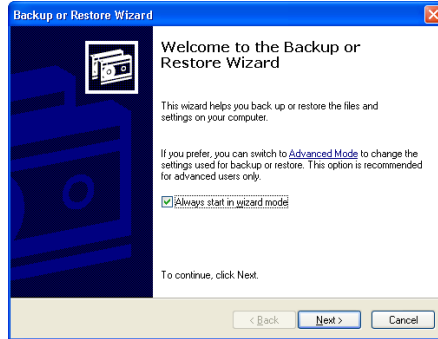
When using someone else's machine always consider where it is physically located and what you are looking at. For example, performing on-line banking transactions at an internet café would be unwise, but looking up directions would be safe.

## What to do

### Back up important files.

## How to do it

- A very simple backup strategy is to copy and paste (or use the software that came with your machine if you are using a CD) to create a back up of your important files. There are various external media devices that can be used for backup: CD, DVD, USB flash drives, or external hard drives.



- Most modern operating systems also come with backup programs installed (Macs do not currently have a built-in solution). Windows' backup program can be found at:
  - Start | Programs | Accessories | System Tools | Backup. The application will prompt you regarding what and when to back up information through a wizard or dialog box.

## Comments

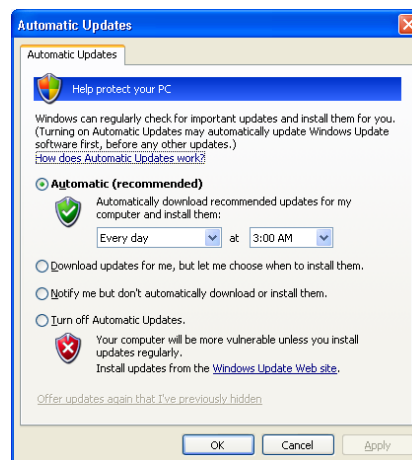
Program files should not need to be backed up, as presumably they could be reinstalled using the disk(s) that came with your machine.

## What to do

### UPDATE operating systems and programs.

## How to do it


- For Microsoft products (including the operating system as well as Office applications – Word, Excel, Access, PowerPoint, etc.):
  - Go to <http://www.microsoft.com>.
  - Follow the links for security and updates.
  - Make sure to select the links for updating ALL Microsoft products.
  - The site will analyze and update all software automatically.
- Go to Control Panel | Security Center to automatically set security update downloads.
- Not only should Microsoft Office and Windows be updated, but most modern software has security updates. Go to the web site of all software you are using to check out the updates available.

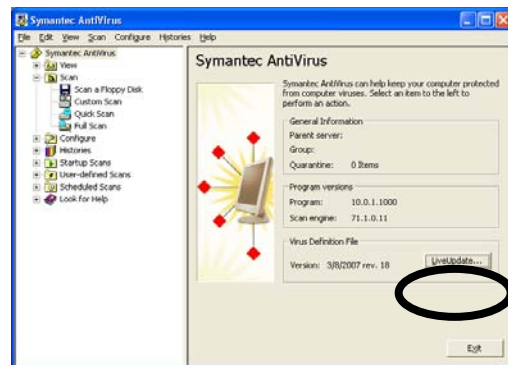
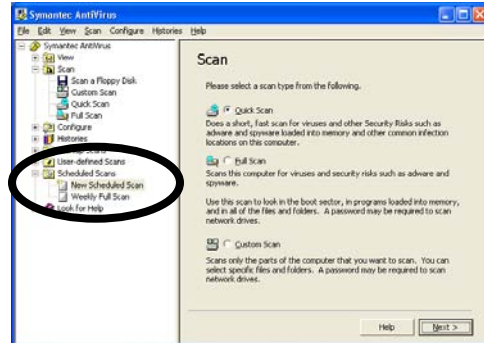
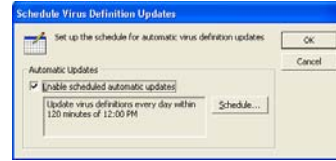


## What to do

### Use and UPDATE virus protection and SCAN your computer for viruses.

## How to do it

- All members of the Cornell community can use Symantec AntiVirus for free. The software can be downloaded at <http://uportal.cornell.edu> from the Bear Access tab. CDs can also be obtained from CIT's HelpDesk located at 119 CCC. If you are using a dial-up connection, installing from CDs will be much quicker.
- As an administrator, once Symantec is installed, set automatic updates and scans by:
  - Double clicking on the  Symantec icon located in the lower right corner of your screen.
  - File | Schedule Updates | Daily
  - Click on the + icon next to Scheduled Scans on the left of the window.
  - Click New Scheduled Scan.
  - Step through the wizard and set a weekly quick scan for you computer.
- If you have heard about a serious threat or a "zero day" virus coming out, open Symantec as an administrator, and click the Live Update button.



## Comments

It is highly recommended that you use Symantec AntiVirus (SAV), even if your machine came with a different package. Running more than one antivirus application is not recommended. Any other antivirus application must be uninstalled before SAV is installed to avoid conflicts. Disable the current antivirus application; then use the Add/Remove Programs Control Panel to remove it. Make sure to immediately install SAV after uninstalling the old antivirus application.

Your machine must be on to run any scheduled scans; if it is not, the scan will be run as soon as the computer is turned on.

## What to do

### Use a firewall.

## How to do it

- Modern operating systems come with firewalls. Check your machine's security center to verify the use of a firewall. For Windows: Start | Control Panel | Security Center. If there does not seem to be a firewall running, go to your operating system's site and research how to download and use the OS's firewall.



## Comments

Running more than one software firewall is not recommended. If you are using the latest version of Symantec's firewall (Symantec Client Security), the installer offers to turn off the Windows firewall for you.

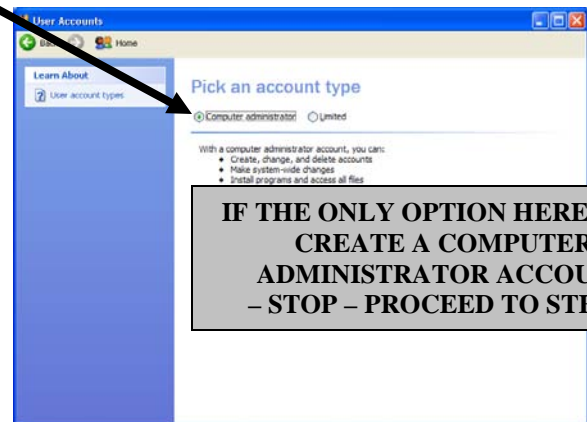
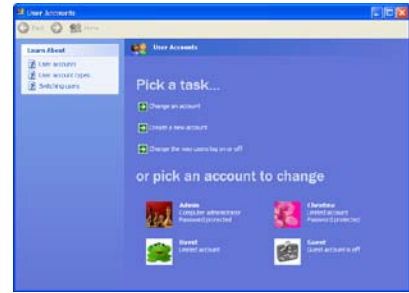
A hardware firewall (an actual external box connected to your computer) adds an additional level of even greater security.

## What to do

## Use a LIMITED account.

### How to do it

- To determine what kind of account you currently have:
  - Start | Control Panel | User Accounts.
  - If necessary, select your account.
  - Under the name of the account, it will say either Limited or Computer Administrator.
  - If the account says Limited, GOOD, you need go no further.
- If the account says Administrator:
  - In the User Accounts Control Panel, select Create a New Account and name the account something such as *[Your Name] Admin*.  
**NOTE: In the next dialog box, if the ONLY option available is to create an Administrator account – in other words, the Limited setting is not selectable, CANCEL, and proceed to step 3.** Otherwise, select Administrator if it is not already selected and click OK.
  - Set a strong password for the account.
  - Open the other account (the one you usually use) select Change Account Type, and change it to Limited.
- If you are not allowed to create an Administrator account OR if the ONLY option is to create an Administrator account:
  - Using the account that you always have, right click the My Documents folder and select Copy. Open My Computer, open the Shared Documents folder and select Edit | Paste. If you have stored files in locations other than My Documents, you will also have to move those files to the Shared Documents folder using copy and paste.
  - Go back to the User's Control Panel.
  - Open the Admin account (the account that you've always used).
  - Change the name of the account to something different than the account you are using now, but not containing "Admin." For example, Christina's User Account.
  - Change the account type to Limited.
  - Go to your original account and change the name so that it does contain the word Admin and set a password, for example "Christina's Admin Account."
  - You should now have at least two accounts, one with an account type of Administrator and one with an account type of Limited. All users should also have Limited user accounts, and they can be created or changed in the User Account Control Panel.
  - Go to Start | Log Off and log off the Administrator account and on to the Limited account.
  - Your new, limited account will need to be re-customized (desktop background, color scheme, folder views, etc.) If you followed the instructions in step 3, all files from the other account will be stored in the Shared Documents folder. New documents should be saved to the My Documents folder on the desktop rather than the Shared Documents folder.



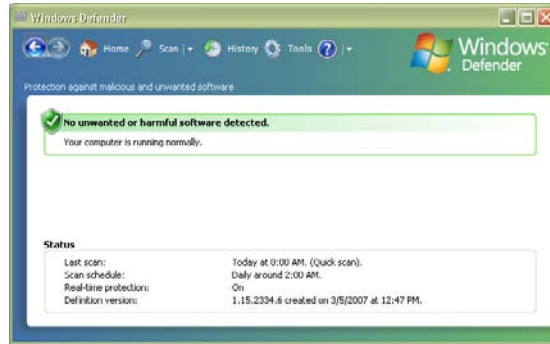
### Comments

Once a Limited account has been created, only use the Administrator account to install new programs or change settings for which you are absolutely certain there is no risk of compromising your machine.

**What to do**      **Use and UPDATE pop-up blockers, spyware and other malicious code protection programs.**

---

- How to do it**
- There are several programs that will assist with this, some free, some for purchase. Microsoft's Windows Defender program is free and a good product and is recommended. Go to Microsoft's web site and follow instructions for downloading and installing. Browsers, antivirus and security centers in operating systems often come with blockers and other detection programs. Review your security center, your antivirus application and your browser options to decide what settings to use.



**Comments**      You must use the Administrator account to install any of these programs.

**What to do**      **Do not use non-secure software.**

---

- How to do it**
- Good examples of non-secure software are peer-to-peer filesharing (KaZaA) programs, QuickTime and RealPlayer. While commonly used and downloaded, people often do not update as often as they should and not all products are as vigilant about developing secure packages. Research a product before you install it – not just at the product's site, but throughout the web, to discover security risks.

**What to do**      **Understand wireless security risks.**

---

- How to do it**
- There are presently two kinds of wireless security: WEP and WPA. WEP uses a static "key," which can be easily defeated. The newest security option is WPA, which uses a dynamic "key," which is much harder to break. Use the highest encryption level that the hardware will let you use (not all options are available on all hardware). Regardless of how high the encryption is set, remember that **everything** is being transmitted in a 300' radius around you and can be captured!

**What to do**      **Turn off/Restart your computer.**

---

- How to do it**
- Usually updates are managed and delivered automatically by your IT professionals; however, users must restart for most changes to be take effect. Therefore, it is best to restart your computer no less than once a week.

## Sites to Explore

---

<http://antivirus.vt.edu/>  
<http://securityresponse.symantec.com/>  
[http://www.zonelabs.com/store/content/catalog/products/sku\\_list\\_za.jsp?lid=pdb\\_za1](http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp?lid=pdb_za1)  
<http://staysafeonline.org/practices/index.html>  
<http://windowsupdate.microsoft.com/>  
<http://www.apple.com/macosx/features/security/>  
<http://www.cit.cornell.edu/computer/security/emailvirus.html>  
<http://www.cit.cornell.edu/computer/security/secure.html>  
<http://www.cit.cornell.edu/helpdesk/mac/kerberos/kerbfirewall.html>  
<http://www.cit.cornell.edu/helpdesk/virus/>  
[http://www.cit.cornell.edu/helpdesk/win/kerb/winxp\\_firewall.html](http://www.cit.cornell.edu/helpdesk/win/kerb/winxp_firewall.html)  
<http://www.cit.cornell.edu/services/nav/>  
<http://www.cit.cornell.edu/services/nav/update.html>  
<http://www.ilr.cornell.edu/techServices/services/desktopSupport/homeComputer/index.html>  
<http://www.lavasoftusa.com/>  
<http://www.microsoft.com/downloads/>  
<http://www.microsoft.com/windowsxp/pro/using/howto/networking/icf.asp>  
<http://www.registry-cleaner.net/pop-up-blocker.htm>  
[http://www.stopzilla.com/download/download\\_select.aspx](http://www.stopzilla.com/download/download_select.aspx)  
<http://www.symantec.com/avcenter/vinfodb.html>  
[http://www.us-cert.gov/reading\\_room/HomeComputerSecurity/](http://www.us-cert.gov/reading_room/HomeComputerSecurity/)