

Manage security settings for: Automatic Updates

1. Check here when you have enabled Automatic updates: _____

Enable Screen Saver Timeout

1. Right-click anywhere on the Desktop and select Properties
2. Select the Screen Saver tab
3. Set a time interval for the computer to wait before enabling the screen saver (recommended: 10 minutes)
4. Make sure the "On resume, password protect" box is checked and click OK.

Disable AutoRun (aka AutoPlay)

1. Download the file located at www.besekure.ku.edu/files/disable_autorun.reg (You may need to click File→Save As... in your browser if the file does not download automatically.)
2. Double-click the file. When you see a popup that says "Are you sure you want to add the information in C:\...\disable_autorun.reg into your registry?" Click Yes.
3. A second popup message should appear saying "Information in C:\...\disable_autorun.reg has been successfully entered into the registry." Click OK

Start→Control Panel→Security Center

Manage security settings for: Windows Firewall

(Note: If you are using a third party firewall product, it will disable the Windows ICF. This is fine! Manage your firewall options within your third party firewall's settings instead.)

1. *(General tab)* Check here when you've ensured that the Windows ICF is enabled: _____
2. *(Exceptions tab)* Check here when you have unchecked the following:
 - File and Printer Sharing: _____ *(Note: if you are sharing files or a printer with other computers on your home network, leave this enabled. If you are **not** sharing a printer or files on your home network, disable it.)*
 - UPnP Framework: _____
3. *(Exceptions tab)* You may opt to disable other firewall exceptions. Note which ones you disabled here in case applications associated with those exceptions stop working:
 - _____
 - _____
 - _____
 - _____

Disable Windows File and Print Sharing

Note: If you share a printer on your home network, skip this section.

1. Click Start→Control Panel and select Network Connections
2. Right-click on Local Area Connection (this may be followed by a number) and select Properties
3. Click File and Printer Sharing for Microsoft Networks and click “Uninstall,” then click OK.

Configure an account to run as a “Limited User”

Note: You will still need an account with Administrator privileges to install most software and make changes to the system. If you are changing your own account to be a Limited User account, make sure you create an account with administrator privileges for installing software and making other system changes!

1. Click Start→Control Panel and select User Accounts
2. If you are converting an existing account to run as a Limited User, click “Change an account.” If you are creating a new account, click “Create a new account.”
3. If you are creating a new account, select “Limited” on the “Pick an account type” screen, then follow the steps to configure that account to use a password.
4. If you are modifying a current account, click the account name and then click “Change the account type.” Make sure “Limited” is selected and then click the “Change Account Type” button.
5. If the account doesn’t have a password, follow the steps below to configure it to use a password.
6. Log out and then log back in under your new limited user account.

Configure an account to use a password

1. Click Start→Control Panel and select User Accounts
2. Click on the account on which you wish to use a password
3. Click “Create a password”
4. Type in your new password and click “Create Password.”
5. The use of password hints is *not recommended*.

Important Programs

Note that “more” does not always equal “better.” You should never install more than one antivirus or firewall product at one time.

Antivirus

1. Are you using an antivirus software package? ____ Yes ____ No
 - a. Note its name here: _____
2. Go to Start→Control Panel→Security Center. Does it indicate that it is monitoring your antivirus software? ____ Yes ____ No
 - If your answer was “No,” open up your antivirus software and ensure that it is up to date and running. If you use a product that requires you to pay an annual subscription fee, make sure you are paid up on your subscription.
 - If you are using Sophos Anti-Virus and it is malfunctioning, contact the KU Customer Service Center at (785)864-8080. If you use another antivirus product, contact its vendor.
3. If you are not using an antivirus software package or your subscription ran out, you **must** remove your old antivirus software prior to installing a new antivirus software package. The easiest way to do this is by going to Start→Control Panel→Add/Remove Programs.
 - Symantec has its own removal tool for removing its products when Add/Remove programs is unsuccessful. It is located at www.symantec.com/symnrt.
4. You have several options when it comes to antivirus software:
 - Sophos Anti-virus (free to KU students, faculty, and staff, **REQUIRED** for ResNet users) www.security.ku.edu/antivirus
 - AVG (free, must be registered) www.avg.com
 - Avast (free, must be registered) www.avast.com
 - ClamWin (free) www.clamwin.com
 - Kaspersky (\$\$\$) www.kaspersky.com
 - Symantec/Norton (\$\$\$) www.symantec.com
 - Trend Micro (\$\$\$) www.trendmicro.com

Anti-spyware

If you are using an antivirus software package that also works to prevent spyware, check with your vendor prior to installing any of these programs. If you are using Sophos, AVG, or Avast, however, these will help give you an additional layer of protection without adversely affecting your system's performance.

1. Spybot Search & Destroy (free) includes both passive protection and cleaning tools. It is available for download at www.safer-networking.org
2. Spyware Blaster (free) includes passive protection only, no removal. It is available at www.javacoolsoftware.com/spywareblaster.html
3. Ad-Aware (free) includes removal tools only. Paid version (Ad-Aware Plus/Pro) includes on-access scanning. www.lavasoftusa.com/products/ad_aware_free.php
4. Microsoft Windows Defender (free) includes active protection and removal capabilities—and is pretty unobtrusive to boot. www.microsoft.com/downloads/
5. Malwarebytes is available (free/paid) at <http://www.malwarebytes.org/>
6. CCleaner (free) is not specifically a spyware removal tool, however it removes cookies, temp files, and other “junk files” where spyware may try to hide. www.ccleaner.com

Patch/update management

1. Allow add-on programs like iTunes, Adobe Reader, etc. to automatically update themselves.
2. Install Secunia PSI (available at http://secunia.com/vulnerability_scanning/personal/) to help keep your software up to date.

Web browsers

One of the easiest ways to surf safer is to move away from using Internet Explorer as your day-to-day browser. Installing Firefox, changing a few settings, and installing a few add-ons can go a long way towards keeping you and your computer safe when you're surfing the web.

1. Firefox (free) is available at www.mozilla.com
2. Launch Firefox and go to Tools→Options.
 - a. *(Main tab)* Make sure "Always check to see if Firefox is the default browser on startup" is checked.
 - b. *(Content tab)* Make sure "Block pop-up windows" is checked.
 - c. *(Security tab)* Make sure that "Warn me when sites try to install add-ons" is checked.
 - d. *(Security tab)* Make sure that "Tell me if the site I'm visiting is a suspected forgery" is checked, then decide if you wish to use the list Firefox downloads or the anti-phishing service provided by Google.
 - e. *(Security tab)* Uncheck "Remember passwords for sites."
3. Visit addons.mozilla.com and consider the following add-ons (also called "plug-ins") for the Firefox browser:
 - a. Adblock Plus: <https://addons.mozilla.org/en-US/firefox/addon/1865> hides ads, but can also potentially help prevent malicious page elements from displaying on the websites you visit. The Adblock
 - b. NoScript: <https://addons.mozilla.org/en-US/firefox/addon/722> Allows active (scripts, Flash, etc) content only to run from sites you trust. Can help protect your system in the event you stumble upon a malicious site.
4. McAfee SiteAdvisor (free) www.siteadvisor.com is an add-on that can help prevent you from clicking malicious links and/or maliciously crafted websites. Use it in conjunction with Firefox's built-in anti-phishing features for added protection.

Sometimes use of Internet Explorer is unavoidable. Here are some steps you can take to make using IE a bit safer:

1. Upgrade to IE 8.
2. Install the IE version of McAfee SiteAdvisor.
3. Ensure that the immunization and signatures for both Spybot Search & Destroy and Spyware Blaster are up to date.