



Student Help Desk

St. Mary's College of Maryland
at Historic St. Mary's City

COMPUTER SECURITY

Security is a very important thing for everyone who owns a computer to know and understand. Five main areas that you should focus on are described below.

Network/Email Passwords

As part of the St. Mary's network, students are given access to several services that require authentication in order to protect sensitive data. Due to state policies, St. Mary's College requires and enforces complex password policies on all network accounts that must be changed every 90 days. The required guidelines for complex network passwords are below:

- Cannot contain your name or your user name
- Must contain at least eight characters
- Must contain at least three from the following four groups of characters:
 - Uppercase letters
 - Lowercase letters
 - Numerals
 - Symbols - for example, ! @ % * & ^ - _ #

To change your password via Outlook Web Access (webmail):

1. Login to your email account via the web.
2. Click on the **Options** button located in the window to the left of your screen. (If your view is set up to show folders, the options button can be found on the left of your screen at the bottom. It is the last button on the right in this window.)
3. Scroll down and click on **Change Password**. The Internet Service Manager window will appear.
4. Enter your Domain, SMCM, and press the tab key.
5. Enter your Account (username i.e. jdsmith), and press the tab key. (Note: If the domain field is not available, use your entire email address, i. e. jdsmith@smcm.edu)
6. Enter your old password, and press the tab key.
7. Enter your new password, and press the tab key.
8. Confirm your new password.
9. Click **OK**. You will receive the message "Password Successfully Changed". It will take about 10-15 minutes for your new password to propagate through the network and become active. During this time, you may have to use your old password.

Password Regulations:

- You cannot reuse the same password for at least 6 months.
- You must change your password at least every 90 days.
- The system will keep track of when you change your password.
- You will receive a notification when your password is due to expire in 14 days. When you receive this notification, it is a good practice to go ahead and change your password. You can log on once after your password expires. If you don't change your password then, a

COMPUTER SECURITY

System Administrator will have to reset it for you. This will require you to contact the Student Help Desk for assistance.

Firewalls

On the Internet, hackers use malicious code, such as viruses, worms, and Trojan Horses, to try to find unlocked doors—an unprotected computer. A firewall can help protect your computer against these and other security attacks.

While connected to the St. Mary's network, it is not necessary for you to have a firewall enabled on your computer. In fact, while connected to ResNet, students **MUST** disable all firewall systems on their computer to be properly accepted onto the network. While you are connected to the St. Mary's network, you are safe from the outside world; we have a system wide firewall that protects all network users.

Most modern operating systems have a firewall option. The following directions will tell you how to enable and disable the system firewall in Windows XP and in Mac OS X (10.2 or greater). Earlier versions of Windows and Mac OS do not have a system based firewall option.

Windows XP & XP Service Pack 1:

- Click on the **Start** button.
- Go to **Settings**, click on **Control Panel**.
- Double click on **Network Connections**.
- Right click on the **Local Area Connection** icon.
- On the quick menu, click on **Properties**.
- Click on the tab titled **Advanced**.
- Make sure the box for the **Internet Connection Firewall** is unchecked to turn it off, and checked to turn it on.
- Click **OK**.
- Close the **Network Connections** window.

Windows XP Service Pack 2:

- Click on the **Start** button.
- Go to **Settings**, click on **Control Panel**.
- Double click on **Network Connections**.
- Right click on the **Local Area Connection** icon.
- On the quick menu, click on **Properties**.
- Click on the tab titled **Advanced**.
- Click on the **Settings** button under "Windows Firewall".
- Select "**Off (not recommended)**" to turn it off and "**On (recommended)**" to turn it on.
- Click **OK**.
- Close the **Network Connections** window.

Mac OS X Firewall:

- Click on the **Apple** in the top left corner of your screen.
- Go to **System Preferences**, Click on **Sharing**.

COMPUTER SECURITY

- Click on the **Firewall** tab.
- Enable the firewall by clicking the '**Start**' button, disable the firewall by clicking the '**Stop**' button.
- Close the **Sharing Preferences** window.

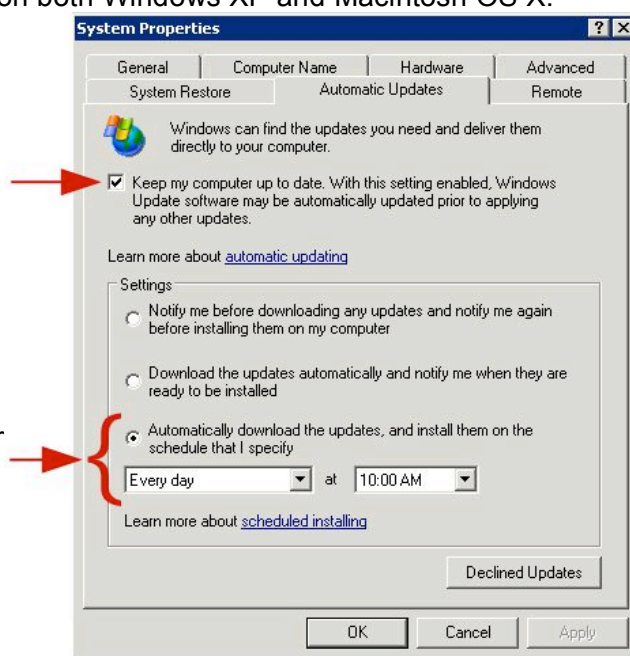
If you're still having problems after following the above directions, make sure your computer has the latest system updates, antivirus, and anti-spyware (Windows only) software installed. Then contact the Student Help Desk for more assistance.

Critical Updates

These are the security updates that Microsoft and Apple release when new threats are found. They are available through Windows Update or Software Update respectively. Below you will find instructions on how to enable automatic updating on both Windows XP and Macintosh OS X.

Windows XP:

1. Click **Start**
2. Right click **My Computer**
3. Click **Properties**
4. The System Properties Property Sheet will open.
5. Click the **Automatic Updates** tab and choose how you want to set your updates. We recommend that you select to automatically download and install the updates during a time when your computer is usually on, but not in use.
6. Click **Apply** and **OK**.



Macintosh OS X:

- Choose **System Preferences**, (Or Software Update directly if you're using 10.3 or later) from the Apple menu.
- Choose **Software Update**.
- Select your options for Software Update. We recommend that you select to automatically download updates during a time when your computer is usually on, but not in use.
- Close the System Preferences window.



COMPUTER SECURITY

Spyware Programs

Spyware is computer software that gathers information about a computer user without the user's knowledge or informed consent, and then transmits this information to an organization (that usually expects to be able to profit from it in some way). Data-collecting programs installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.

More broadly, the term spyware is applied to a wide range of related adware products which are not spyware in the strict sense. These products perform many different functions, including the delivery of unsolicited advertising, harvesting private information, re-routing page requests to illegally claim commercial site referral fees, and installing stealth phone dialers.

While spyware and adware usually won't affect your network settings, they can hog system resources and considerably slow down your system. We recommend that you keep anti-spyware and anti-adware software on your computer and up-to-date at all times. This can ensure that your computer will keep running smoothly and also acts to help prevent future problems. Currently only Windows users are affected by spyware. Mac and Linux users are not affected and therefore do not need to install these programs.

Two programs that we recommend for finding and deleting spyware and adware on your computer are Ad-aware and Spybot Search & Destroy for Windows. Both are available on the [Downloads](#) page of the Student Help Desk website.

Physical Security

This is a commonly overlooked aspect of personal computing. Your computer is most likely one of your more valuable possessions. It is important that you take care in protecting it. There are a few simple guidelines you can follow to protect your computer.

- Lock your room door when ever you leave your room
- Never leave a laptop unattended
- Take you computer home over long breaks
- Lock your computer to your desk