



Securing Your Computer

[About Barret](#)

[Research Sources](#)

[Library Services](#)

[Technology Services](#)

[Need Help?](#)

[Ask Us!](#)

[Search](#)

As computer systems get more complex, the need to keep them up to date is crucial for preventing data loss and maintaining the security and privacy of your information.

A compromised computer affects all the other computers on campus because we are connected to the same network. The speed of and reliability of our network can be affected because compromised computers may cause large amounts of network traffic and often attack computers on and off the campus network.

Therefore it is important that you keep your computer up to date.

1) Patch & Update Your Operating System

Computer operating systems need regular updating with security patches and "bug fixes." Windows XP and OS X are the currently supported systems on campus and details are provided here. If you use another OS, such as Linux, be sure you know how to update it.

Windows Update helps you keep your computer up-to-date with the latest security patches and updates. If your computer is not up-to-date, you are at risk from viruses and worms taking over your computer to use it for illegal purposes without your knowledge. As part of your **Certification Process** you should have set your computer to **run Windows Updates automatically**. Make sure you keep that setting!

Macintosh Software Updates fix bugs and security holes in applications and the operating system and in general help make your computer more secure and function better. From the Apple menu, select Software Update. Check the boxes for all available updates for Macintosh OS, Security Updates, or Quicktime updates. Check any other updates in the list you wish to install. Then press the Install button and follow all instructions.

2) Protect Your Computer from Viruses and Worms

Viruses and Worms are two of the biggest CyberSecurity threats. They spread by infecting insecure computers that, in turn, infect other insecure computers.

For protection from dangerous e-mail, Rhodes ITS scans all incoming and outgoing e-mail for suspicious attachments. Some attachments, such as .exe or .com files, are not allowed to be received in e-mail from the Internet because they are frequently used for spreading viruses.

Infected and compromised computers may have their network access disabled to isolate network problems. This is done to keep the entirety of the network secure while infected computers are repaired. Don't let this happen to you! To prevent and eliminate viruses, use an anti-virus program in combination with regular security updates for your operating system. Rhodes provides anti-virus software and virus-definition updates free for College-owned computers and for student computers which have been **certified by the Computer Depot**.

3) Check for Adware & Spyware

Anyone who browses the Web or uses instant messaging software with a Windows computer is very likely to have software installed on their computer without their knowledge. Such software, called spyware and adware, will slow down the computer or even, in some cases, cause the computer to stop working. Even a small program as seemingly innocuous as WeatherBug can be a conduit for malicious software.

For recommendations on how to limit your vulnerability to spyware and adware, see our instructions titled [Prevent or Remove Spyware](#).

4) Back Up Your Data

If your computer is compromised, your data backup will be your best friend. Files missing? Corrupted? If you have a recent back up of your documents, you will be able to restore them after your computer gets cleaned up, or be able to work on your documents elsewhere while your computer is being cleaned up.

Copy your essential files to CD or a USB flash drive. Each time you make changes to those files, be sure you copy the changes to your backup.

NOTE: One of the safest places to store your documents is to your Student Folder on the Student Community fileserver. Files stored on the fileserver are backed up regularly. If you accidentally delete or overwrite your document, you can [Ask Us](#) to restore the file.

5) Protect Your Computer with a Firewall

A firewall is set up to protect a computer or network from intrusion. This can be done with a firewall box or with software. If you have a computer on the Rhodes network, some protection is provided by a campus firewall box between our network and the Internet. In addition, you should use firewall software on your own computer.

Having firewall software on a Windows computer is a smart idea. Connecting your computer to the Internet can be equated to leaving your front door unlocked and open all the time. On the Internet, hackers can delete information from your computer, access private information, or even crash your computer. Having a firewall in place to protect your computer helps prevent hackers from being able to access your computer in the first place.

Included in Service Pack 2 for Windows XP is the Windows Firewall. Firewall software for Windows protects your computer by monitoring (and restricting in some cases) any information that travels between your computer and the Internet, and also the information that travels between your computer and other computers on your network. Should a network worm somehow make its way onto campus, having the Windows XP firewall enabled helps protect a computer from infection.

As part of your [Certification Process](#) you should have set your computer to **run the Windows XP Firewall**. Make sure you keep that setting!

If you have a firewall installed from another vendor (such as Norton or McAfee) at home, it is recommended that you disable it so it does not counteract the Windows XP Firewall. This makes it more likely that ITS staff will be able to identify problems you may have with firewall software interfering with legitimate programs on your computer being unable to access the network properly.

6) Use Strong Passwords

In this electronic age, most of us have many, many passwords for various electronic accounts, at Rhodes College and elsewhere. At Rhodes, most of us have a password for our network/email account and a PIN for Banner Web. At home you might have a PIN for your electronic banking, a PayPal account, your home e-mail password, perhaps an eBay account.

How do you remember them all? Are you one of those people who uses the same password for all of your accounts? Do you write them down? What should you do?

Philosophies vary somewhat, but the bottom line is this: make sure your passwords are secure. If you must write them down, you need to find a way to secure your list so that you and only you can get to that list. If you write them down, where is the piece of paper? If you store a list electronically, how do you secure the file?

A strong password is at least 8 characters long (using numbers, uppercase and lowercase letters, and symbols) and is never shared with anyone or written down in an easily found location. Try using two numbers interspersed among the characters, for example: ca3nar8y or redc74at. You can substitute symbols for letters such as changing an "o" to (). The use of mnemonics is often useful in remembering a password. For example, the phrase "Route 9 was too slow this morning" can become Rt9WtsTm.

Instructions on changing your network/email password and Banner PIN are located here:

- [Changing Your Network Password](#)
- [BannerWeb Username & Password](#)

Also, please keep in mind that the web browsers on your computer are often set up to assume you prefer convenience to security, and the browsers save not only usernames but passwords. This may not be a security risk for something like your hotmail account, but it is a risk for something like your PIN for your online banking or for access to secure data here at Rhodes. If you use the web to access information that needs to be kept secure, be sure to set up your browser so that it does not save secure passwords and PINs to your computer. When working on a computing lab computer, make sure to properly log out of any websites that you log into during your session instead of just closing the browser. If you are working on a shared computer, remember to clear the browser cache if you used the computer to access secure data.

7) Protect Yourself from Phishing and Identity Theft

Phishing is a type of information collection scheme using fraudulent emails that specifically target users with online accounts of some kind (i.e. banking, PayPal, etc.) The information that they collect is then used to perform various acts of identity theft.

Consumer Reports recommends the following steps to outwit online ID thieves:

- Never directly respond to e-mail asking for personal information
- Questionable messages should be verified by contacting the institution itself
- When prompted for a password, give an incorrect one first. A phishing site will accept it; a legitimate one won't.
- Don't follow links within emails you receive. Instead, avoid spoofed sites by entering Web addresses directly into the browser yourself or by using bookmarks you create.

For more information about phishing and identity theft, please visit:

<http://www.millersmiles.co.uk/> and <http://www.consumer.gov/idtheft/>

8) Remember: Computers Can Be Stolen!

In addition to protecting your data electronically, don't forget the obvious: physical security.

Portable computers are much easier to steal than bulky desktop computers, but both can be targets of thieves. While such thefts are rare at a place like Rhodes College, how would you feel if yours was the rare exception?

Use common sense:

- Lock your dorm room when you leave it.
- Ask a friend to watch your laptop if you must leave it for a moment in the library or elsewhere.
- Use a Windows password on your computer, so if it is stolen, it will be harder for the thief to retrieve your sensitive data.

[Adapted, with grateful acknowledgement, from content developed by [Wellesley College](#).]