



***Guide to  
Safer Computing***

# **Staying Safe: Steps for Safer Computing**

Your personal computer is a popular target for intruders on the Internet. Why? Because intruders want what you've stored there. They look for credit card numbers, bank account information, and anything else they can find. By stealing that information, intruders can use your money to buy themselves goods and services.

But it's not just money-related information they're after. Intruders also want your computer's resources, meaning your hard drive space, your fast processor, and your Internet connection. They use these resources to attack other computers on the Internet and your local network. If they are able to infect enough computers, they can bring an entire network quickly to its knees. And the more computers an intruder uses, the harder it is for law enforcement (and University Technology) to figure out where the attack is really coming from. If they can't be found, they can't be caught.

This can sound very frightening, but by taking the basic steps included in this booklet, you can start protecting yourself and your computer.

It is the responsibility of each student to maintain their computer. This includes keeping Windows or Mac OS updated with critical security patches, regularly updating anti-virus protection, and running anti-spyware programs. Take steps to protect yourself today!

## **Activate Your Windows XP Firewall**

A network firewall is a device that protects your computer from malicious network traffic. It examines all incoming network information as it arrives, and decides whether to allow it to reach your computer.

You can create an added layer of protection for your computer by enabling a software firewall — a program that runs in the background on your computer, silently monitoring network traffic.

If you have Windows XP, follow these steps to enable the firewall.

1. Click on the Start menu, and open the "Control Panel."
2. In the next window, click on the "Security Center" category.
3. At the next screen, select "Windows Firewall".
4. Select the radio button "On (recommended)".

\*\*If you notice that your firewall is blocking legitimate traffic, don't turn it off! Repeat steps 1 through 3 above, and click on the "Exceptions" tab. Check the box next to the program you want to allow through the firewall.

## **Disable Windows File Sharing**

### ***Why Should I Disable Windows File Sharing?***

Have you ever hit print and had it print out in a room down the hall? This probably happened because the owner of the printer left file sharing on. When file sharing is active on your computer, you risk unintentionally sharing the information and resources on your machine with strangers. If

you leave file sharing active on your computer and don't specify a password, Windows is also more vulnerable to viruses.

### ***How to Disable File Sharing in Windows XP/2000***

1. To disable file sharing, start by opening your Control Panel from the Start menu.
2. Click on Network and Internet Connections. If you are using Windows 2000, skip to the next step.
3. Click on Network Connections.
4. Right-click on the icon marked Local Area Connection and select Properties from the menu that appears.
5. In the window that appears, make sure that the box for File and Print Sharing for Microsoft Networks is unchecked. Click OK to complete the process.

## **Run Windows Update**

Microsoft periodically releases security patches for its Windows OS. Downloading and installing these updates help protect your computer from viruses and threats such as Blaster, Nachia, and Sasser!

We strongly encourage students with Windows XP to update to Service Pack 2, as it is considered safer and much more stable.

### ***How to Download Critical Updates***

1. Open Internet Explorer and go to [www.windowsupdate.com](http://www.windowsupdate.com). There might also be a link to it in the Start menu or Programs menu.
2. If a "Security Warning" or a prompt to install software appears, confirm it is from Microsoft, and then click "Yes."
3. Click the link titled "Express Install (Recommended)" next to the green arrow.
4. Wait briefly while the site scans your computer to see what updates are needed.
5. At the next screen, click the "Install" button on the right-hand side of the screen.

A grey window will appear with a dialog box and a progress bar. The updates you selected will be downloaded and installed. If you are prompted to restart after the updates have been installed, do so.

### ***How to Schedule Automatic Updates***

It is essential to download new updates as soon they are available, as hackers exploit some vulnerabilities almost as soon as they are detected. Scheduling Windows to automatically download and install updates will make sure your computer has the most current defenses.

1. Right-click on your "My Computer" icon and choose "Properties." The icon might be on your desktop or in your Start menu.
2. In the row of tabs at the top, click on the one labeled "Automatic Updates."
3. Check the radio button saying "Automatic (recommended)" You can also schedule what time the updates will be downloaded if you wish.

## Run Up-to-Date Anti-Virus Software

Getting online without anti-virus software is like walking into a hurricane without a raincoat. You're going to get wet, and your clothes (or in this case computer) will probably be ruined.

Anti-virus software protects your computer from viruses and worms, malicious software explicitly designed to damage your computer, steal your personal information, and infect others. The worst viruses and worms can make your computer inoperable, and when too many computers on the Lesley Network are infected, the whole network can be brought down. To prevent this from happening, installing and maintaining anti-virus software is essential.

### ***How to Get Anti-Virus Software***

A free version of **Symantec Anti-Virus 9** is available to Lesley's *residential* students at <http://www.lesley.edu/ut/resnet/antivirus.html>. Follow the onscreen instructions to download and install the software.

We encourage all residential students to use the Lesley-provided anti-virus software to protect their computers and avoid the cost and hassle of keeping anti-virus subscriptions up-to-date.

## Rid Your Computer of Spyware, Adware, & Other Malware

"Lavasoft Ad-Aware" and "Spybot – Search and Destroy" are Windows programs that take an active approach to removing spyware from your computer. Spyware is often installed without your knowledge when you install other programs, and it can be responsible for a wide range of problems, including pop-ups, system slow-down, and network failure. These two programs complement each other, and each find spyware the other will not. Using them can drastically reduce the number of spyware problems you suffer.

### ***How to Set Up Ad-Aware***

#### **Download**

1. Open your web browser to Lavasoft's web site at <http://www.lavasoftusa.com/software/adaware/>.
2. Click on the "Download.com Rated Top 5" icon in the upper-right corner.
3. Click "Download Now!" in the Window that appears, and save the file.

#### **Install**

1. Open the file you downloaded. It should be named "aawsepersonal.exe" or something similar.
2. Click "Next" on the first screen that appears.
3. At the next screen, read the EULA, click "I accept the license agreement," and click the "Next" button.
4. Click "Next" on the several following screens.

5. Once the progress bars are complete and a new screen is presented, click the "Finish" button.

### **Maintain**

It is a good idea to run Ad-Aware at least once a week to remove spyware as it accumulates. Ad-Aware should remain on your computer, so that you can run scans at any time. Before running Ad-Aware, make sure to update to the latest definition files. You can do this by clicking the "Check for Updates Now" button before running a scan.

### ***How to Set Up Spybot***

#### **Download**

1. Open Internet Explorer and go to [www.download.com](http://www.download.com). Search for "spybot" using the search field at the top of the page.
2. You should see "Spybot – Search and Destroy" listed in the search results.
3. Click on the green "Download" icon and save the file to your hard drive.

#### **Install**

1. Open the Spybot installer. It should be named "spybotsd14.exe" or something similar.
2. In the dialog box that appears, select the appropriate language, and click "OK."
3. Click "Next" after reading through each of the several dialog boxes that appear.
4. At the final screen, make sure the "Run SpybotSD.exe" box is checked, then click "Finish."

#### **Maintain**

Whenever you run Ad-Aware, it is a good idea to run Spybot as well, to pick up anything Ad-Aware misses. Before running Spybot, make sure to update the program. You can do this by clicking the "Search for Updates" button on the main screen when you first open the program.

## **Simple Steps to Combat Spam**

### **Never make a purchase from an unsolicited email.**

If spam wasn't economically viable, it would be obsolete. By purchasing the products advertised in spam, you can not only fall prey to a potentially fraudulent sales scheme, but your email address is often added to the numerous email lists that are sold within the spamming community, further compounding the number of junk email you receive.

### **Don't open attachments unless you are expecting them!**

Even if the message is from someone you know and trust, don't open an attachment you are not expecting to receive. Many virus emails cloak themselves as friends or relatives in your inbox. Don't be fooled!

### **If you do not know the sender of an unsolicited email message, delete it.**

While most spam is just annoying text, a spam email message could actually contain a virus and/or other malicious code that could damage your computer.

### **Never respond to spam & never click on links in spam messages.**

Replying to spam – even to "unsubscribe" or be "removed" from the email list – only confirms to the sender that you are a valid recipient and a perfect target for future spam.

### **Avoid using the preview functionality of your email software.**

Some spammers use advertising techniques that can track when a message is viewed, even if you don't click on the message. If you use Lesley email through myLesley, see the online email FAQs for instructions on how to turn off preview mode.

### **Never provide your email address on web pages, newsgroup lists, or other online public forums.**

Many spammers utilize "web bots" that automatically surf the internet to harvest email addresses from public web pages.

### **Have & use one or two secondary email addresses.**

If you need to fill out web registration forms, or surveys at sites from which you don't want to receive further information, consider using secondary addresses to protect primary email accounts from spam abuse. Also, always look for a box that solicits future information/offers, and be sure to select or deselect as appropriate.

## **Don't Fall Prey To Phishing Scams**

Phishing is an increasingly common type of spam that can lead to theft of your personal information, such as credit card numbers or online banking passwords.

Phishing attacks are "spoofed" emails that appear to come from a legitimate web site that you have online dealings with, such as a bank, credit card company or Internet service provider (ISP). The message may ask you to reply with your account details in order to "update security" or for some other reason. The phishing email may also direct you to a spoofed website or pop-up window which looks exactly like the real site, but has been set up for the sole purpose of stealing personal information. Unsuspecting people are then often fooled into handing over credit card numbers, passwords or other details.

Legitimate financial institutions will rarely if ever send such an email request. If you are in doubt about the veracity of such an email, try typing the company's URL (e.g. [www.paypal.com](http://www.paypal.com)) directly into your web browser's address bar, rather than clicking on the suspect email.

## **Good Password Habits**

In general, a good password should be difficult to guess and easy for you to remember. Below are additional tips on creating passwords that protect your information from prying eyes.

### **A few good general password practices:**

- **Never share your password.**

Your account is assigned to you. You will be held responsible for the activities of the account. By sharing a password, you make it possible for someone else to use your email account to send harassing email. Don't let this happen to you.

- **Never write down a password.**

Passwords that are written down can be easily stolen.

- **Change your password with some frequency.**

The longer that you have used your password, the more likely it is that someone else can figure it out. How frequently you change your password depends on how frequently you use it and the nature of what you are protecting. For example, you may wish to change the password you use for online banking more frequently than the password you use to read The Boston Globe.

- **Never store your password in your software.**

Many e-mail clients, web browsers, and web services will offer to store your password for you so that you don't need to type it in each time you want to use it. This is a bad idea – it is possible for someone to recover your password from inside one of these programs if they have access to your computer (and sometimes even if they don't).

It is also possible for some computer viruses to recover your password from such stores and e-mail them to random people or post them publicly on the Internet. Such viruses may even distribute the password before anti-virus software is able to locate and remove the virus.

### **A few tips when setting a password:**

- **When choosing a password, avoid using *dictionary words*.**

Dictionary words are any common words, names, dates, or number, including words in foreign language words. One standard method that is used frequently when attackers attempt to guess passwords is a *brute force attack*. This basically tries possible passwords over and over again until they manage to break into the account.

Also, avoid using words or names, regardless of the language.

- **Don't use common misspellings of dictionary words (such as replacing "l" with "1" ).**

Many of the dictionaries include both common misspellings and words with letters replaced with similar looking numbers.

- **Don't use personal information.**

It is alarmingly easy for hackers to find basic information about you, such as your birthday, address, or phone number.

- **Don't use the name of your computer or your account.**

- **Don't use sample passwords, such as "1234."**

- **Use a mixture of upper and lower case letters, numbers, and punctuation.**

## **Back Up Your Files!**

Not backing up your files on your computer is like getting into a car accident and not having any insurance. It's something you just don't want to do.

Too many people fail to make backups of their important files until after a disaster strikes. Don't let this happen to you! Disaster can strike in so many ways, and always when you least expect it.

For example:

- You might shut off your computer one night, only to find that in the morning it refuses to come back on.
- Your computer might crash right after you finished that 20-page midterm you spent all night writing.
- That flash drive you've saved your whole life to might get lost, corrupted, or stuck in the machine. Sometimes drives get corrupted for no good reason – even the most reliable drives can have flaws in them.

Everything on your computer that's important to you should be saved in at least two places – save one copy on your hard drive, and another on a flash drive (or other removable storage media device).

## **Finding More Information**

The following web sites contain additional information on how to keep your computer and personal information safe.

<http://www.microsoft.com/athome/security/>

<http://www.securityawareness.com/secnews.htm>

<http://www.consumer.gov/idtheft/>

<http://www.computersecurityday.org/>