



Preparing Your Personal Computer to Connect to the VPN

(Protecting Your Personal Computer Running Windows)

Using the VPN to connect your computer to the campus network is the same as bringing your computer to campus and using it on the network. Once connected to the VPN, your computer “bypasses” the defenses of the campus network (i.e., the University’s firewall). If your computer is infected with malware or viruses, it puts the entire campus network at risk. Before you connect to the VPN, follow the steps below which help protect and clean your computer.

These steps will also help safeguard your personal identity. Safeguarding your personal information and the computer itself against hackers, phishing attempts, spyware and viruses can be daunting! You must avoid falling for email scams (called phishing), detect and remove unwanted malware (called spyware), prevent (or remove) virus infections and stop hackers from turning your machine into a zombie slave by applying Microsoft patches on a regular basis.

If you decide to get rid of your PC someday, it doesn’t end there. Your old computer may have personal information that is still retrievable (even if you deleted that information). That, however, is beyond the scope of this document.

There are four categories of protection that you should implement to protect and clean your computer (Virus Protection, Personal Firewalls, Spyware detection and removal, and Microsoft Windows Updates). Each of these is discussed below.

STEP 1: Virus Protection

Regardless of whether your computer is connected to the Internet, virus protection is a must!

- Cal Maritime employees and students may obtain CDs from the IT Help Desk to install Kaspersky Antivirus on their personally-owned computers at no charge. This is the same software used to protect all computers on campus from virus infections.
- As an alternative, you can download the **AVG Free Edition** from <http://free.avg.com/>. It scans computers for viruses and removes them if they are present. Another free anti-virus software program recommended by Microsoft is **Easy Armor** (but some people have reported that they found it difficult to configure).

STEP 2: Personal Firewalls

Firewalls prevent hackers and malicious programs from gaining access to your computer through the Internet. It also can prevent malware on your computer from accessing the Internet to compromise your personal information.

There are two types of firewalls— software and hardware. Although some people will run than one firewall, only one is necessary. Also note that installing a firewall will help protect your computer against future attacks... but they are not generally intended to detect malware or spyware that may already exist on your computer (we'll deal with that threat in section 3 below).

A) Software Firewalls

- 1) **ZoneAlarm** offers both commercial and free versions of their software firewall at <http://www.zonealarm.com>. (I recommend starting with their free version. It is easy to install and configure.)
- 2) If you are running **Windows XP SP2**, Microsoft provides a built-in software firewall with the operating system. Unlike ZoneAlarm, Microsoft's firewall only protects against incoming traffic. It does not monitor outgoing traffic. To turn on the firewall, click on the Start button and select "Control Panel." When the window opens, locate the "Windows Firewall" icon and click on it.

B) Hardware Firewalls

A router that has built-in firewall features is relatively inexpensive. The device is put between your cable modem (or DSL modem) and your computers network interface card (abbreviated as NIC). Make certain that the router you purchase has both stateful inspection (sometimes referred to as stateless inspection) and NAT (network address translation) capabilities. Most of these routers will have NAT but not all of them have stateful inspection.

Please note that routers do not support dial-up connections (i.e., you must have a broadband connection such as DSL or Cable). Also, after installing the router, make sure that you change the default administrative password for the device and periodically check the manufacturer's website for firmware updates.

An advantage of a router is that you will be able to connect more than one computer to the Internet. You can also run a wireless access point behind the firewall. Once a firewall router has been configured and you are able to access the Internet, little or no maintenance of the router is required. However, you should make a backup of the routers configuration in case you need to reload it in the future.

STEP 3: Spyware Detection and Removal

Spyware detection and removal programs can help insure that your computer is free of malware or other pests... and keep it that way. Free software applications that detect and remove uninvited Spyware are available for download from the Internet. These applications will scan your hard drive for Spyware and remove it.

You should use at least two of anti-spyware programs. Often, one will detect a problem that another fails to detect. The addresses to download them, as well as instructions for running some of those listed below, are found in the Appendix.

- A) Spybot – Search and Destroy
- B) Ad-Aware
- C) Windows Defender

Run anti-spyware programs before you do online banking or use a credit card on the web (or enter any personal information online) to help protect your identity and personal information.

STEP 4: Microsoft Windows Updates

Windows updates, patches and fixes are periodically made available for download and installation from Microsoft. These updates close known vulnerabilities in your operating system. To check for updates, click the Start button and select “Help and Support.” Then click on the “Keep your computer up-to-date with Windows Update” link. You should configure the update to be run automatically.


APPENDIX

Spyware Detection & Removal

The following four programs are among my favorites. Because these programs are regularly enhanced, some of these instructions may be outdated.

Each of these programs includes a web update feature that you should use frequently in order to protect against new variants of Spyware and other malware.


1. **SpyBot Search & Destroy**

- ❖ Go to <http://spybot.safer-networking.de> to download the installation program for SpyBot Search & Destroy. It is free but you can choose to make a contribution. Install the product on your computer. (Once you download and run the installation program, you do not need to repeat this step.)
- Each time you run the program, make sure that your computer has access to the Internet.
- Launch the Spybot Search & Destroy program by clicking on the  icon. (As an alternative, you can click on Start → All Programs → Spybot – Search & Destroy → Spybot – Search & Destroy.
-



After the program is loaded, always click on the **Update** icon to check for new updates. If updates are available, you will be prompted to select a site from which to download the updates. Select one that is closest to your location and then click the **Continue** button. A list of updates will then be displayed... click the **Download** button. After the update is finished, click **Exit**.



If new updates were downloaded (in the step above), click on the **Immunize** icon... if it indicates that there are “*additional protections possible,*” click on the  **Immunize** icon.



Now you are ready to do a scan—which takes some time. Click on the **Search & Destroy** icon and then click on the



icon.

When the scan finishes, detected problems will be displayed in the large white panel... and a “Fix Selected Problems” button will appear... click it.

2. **Ad-Aware**, from Lavasoft (<http://www.lavasoft.nu>), is another free Spyware detection and removal program that is great for those of use who are first-time Spyware detectives. It will detect many types of Spyware and remove most infections. As noted above, you

should frequently use the update feature to protect against new variants of Spyware and other malware.

3. How to Perform the Windows Update

- Periodically (at least once a week), check for operating and application patches and updates from Microsoft. An easy way to do this is to launch Internet Explorer, click on **Tools -> Windows Update**. (Another way to do this is to click: **Start → Help and Support → Keep you computer up-to-date with Windows Update**.)
- When the “Welcome to Windows Update” screen appears, click on the **Express** button. Wait and be patient... this can take a short while. If there are any critical updates to apply, make sure they are selected and install them... just follow the instructions on the screen.

4. ZoneAlarm (a software firewall)

ZoneAlarm is a software program that acts as a firewall to prevent hackers and malware from gaining access to your computer from the Internet. It also can prevent malware from passing information to the Internet without your knowledge. If a program that ZoneAlarm is unfamiliar with tries to access the Internet, it will pop up a dialog box in the lower, right-hand corner of the screen and give you a chance to allow or deny access for that particular program.

NOTE: Every once in a great while, ZoneAlarm comes out with a new update to the program. Be sure to obtain the latest updates as they become available.

A free version of ZoneAlarm is available from www.zonealarm.com .

5. Scan for Viruses

Cal Maritime faculty, staff and students are encouraged to use Kaspersky Antivirus which is available from the Help Desk during regular business hours.