

*KEEPING YOUR  
COMPUTER SAFE*

REFERENCE GUIDE



1 8 6 4

UNIVERSITY TECHNOLOGY SERVICES  
COMPUTER TRAINING

**Table of Contents**

Viruses .....1

Spyware .....4

Passwords.....5

Operating System and Application Updates .....7

Firewalls .....9

Pop-up Ads .....10

Encryption.....12

Spam .....13

Phishing.....15

## Viruses


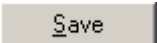
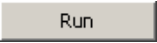



A computer virus is a program written to enter your computer system surreptitiously and "infect" it by installing or modifying files or establishing itself in memory. Viruses can spread via any of the methods used to get information into your computer: network connections, shared folders, e-mail, and shared media such as flash memory, CDs, and diskettes. Once they are established on your computer, viruses work at transferring themselves to other computers.


Sometimes people differentiate viruses by the methods they use to spread. Worms are viruses that self-replicate and spread via e-mail or networks. Trojans are seemingly legitimate computer programs that have been intentionally designed to disrupt your computing activity or use your computer for something you did not intend.

### What should I do?


- A. Never open an attachment of any type from a person you do not know.
- B. Never open an executable file from any e-mail (.exe).
- C. Install free DU-provided antivirus software, Symantec version 10.

NOTE: Before completing these steps, be sure to **remove any other antivirus programs** you may have on your computer. If you have an earlier version of Symantec, you do not have to remove it first.

1. Go to <https://taurus.cair.du.edu/downloads/savce.html>
2. Type **yes** in the Legal confirmation box.
3. Enter your **DU ID** and **passcode** and click .
4. Click  to copy savce.exe.
5. Click  to unzip the compressed file.
6. Click  and choose **Desktop** as the file location and click .
7. Click **OK** when notified that 7 files were extracted successfully.
8. Click .
9. View your **Desktop**.

10. Double-click  Setup.exe
11. **Accept** the license agreement and click **Next**.
12. Mark **Client Install** and click **Next**.
13. Mark **Complete** and click **Next**.
14. Mark **Managed** and click **Next**.
15. Enter **HYGEIA** for Server Name and click **Next**.
16. Click **Install**.
17. Click **Finish** to end the installation.
18. In the **LiveUpdate Options** window, click **Next** to begin installation of current virus definitions.
19. Click **Finish**.

**Important:** After you have installed Symantec Antivirus, install Symantec's "point patch" to correct a decomposition buffer overflow vulnerability. The patch is available at <https://taurus.cair.du.edu/downloads/savce.html>

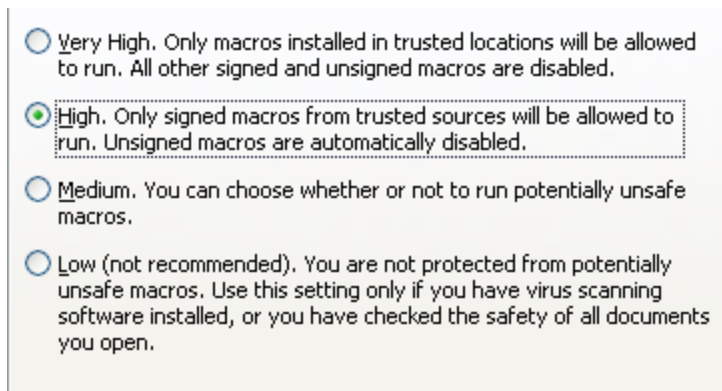
- D. If you choose **Unmanaged** client, you need to schedule daily automatic live updates and weekly automatic system scans.
  1. Start Symantec AntiVirus by Choosing Start...Programs... Symantec Client Security...Symantec Antivirus or double-click the Symantec Antivirus Icon  on the Windows taskbar.
  2. Click on File on the Menu bar.
  3. Click Schedule Updates and check Enable Scheduled Automatic Updates box.
  4. Click on Schedule, select Daily for Frequency setting and select the time for live update to run.
  5. In the left pane, click Scheduled Scans.
  6. In the right pane, click New Scheduled Scan.
  7. Select Full Scan. Click Next.
  8. Type a name and description for the scan. For example, call the scan "Friday at " Click Next.

9. Specify weekly as the frequency and select a time when your computer is usually signed on to the network. Click Next.
10. In the Symantec AntiVirus main window, click Save. The new scan is added to the list in the Scheduled Scans folder.

NOTE: Your computer must be turned on when the scan is scheduled to take place.

E. Make sure that **Macro Virus Protection** is enabled in all Microsoft applications, and you should NEVER run macros in a document unless you know what they do. There is seldom a good reason to add macros to a document, so avoiding all macros is a great policy.

1. Open Microsoft Word.
2. From the menu, choose **Tools. Options.**
3. Click the **Security** tab.
4. Click the **Macro Security** button.



5. Mark **High** and click **OK.**
6. Click **OK** to close the Options box.

## Spyware

Spyware is a relatively new kind of threat that common anti-virus applications do not comprehensively cover. If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if your browser start page has changed without your knowing, you most probably have spyware. But even if you don't see anything, you may be infected, because more and more spyware is emerging that is silently tracking your surfing behavior to create a marketing profile of you that will be sold to advertisement companies.

### What should I do?

A. Install Spybot Search and Destroy software (free)

1. Follow the detailed installation and operating instructions at [www.safer-networking.org/en/tutorial/index.html](http://www.safer-networking.org/en/tutorial/index.html)

B. Install Ad-Aware SE Personal software (free)

1. Go to <http://www.lavasoftusa.com/>.
2. Under the **Products** heading on the left, click **Ad-Aware Personal**.

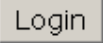

3. Click  , then  again!
4. From the Download File Security Window, choose **Run**, then **Run** again (if necessary) to verify the publisher.
5. Click **Next** to begin the installation process.
6. Accept the license agreement and click **Next**.
7. Accept the destination folder location and click **Next**.
8. Choose **Only for me** and click **Next**.
9. For Start Installation, click **Next**.
10. Click **Finish** to complete the installation and run a scan.

C. Run Spybot and Ad-Aware weekly.

## Passwords

A more dangerous form of Spyware is silently looking for your internet and computer passwords in order to steal your personal information such as bank and credit card account numbers or social security number. Password-cracking software could be attempting to match your passwords to words found in the dictionary, or could be logging your keystrokes.

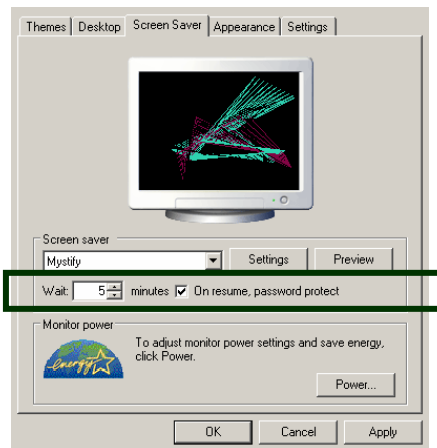
For these reasons, you must create passwords that will be hard for this password-cracking software to detect. Therefore, follow these rules when working with passwords:

- A. Do not use passwords that could be found in the dictionary. Use a combination of upper and lower case characters, numbers, and symbols.
- B. If you have to write down your passwords to remember them, do not post them in clear view at your desk or on your monitor. Don't store a list of your passwords in a file on your computer.
- C. Never share your passwords
- D. Change any passwords that could be vulnerable.
  1. To change the 6-digit password associated with your "87" DU ID number (used for access to Webmail, myWeb, WebCentral, etc.):
    - a. Go to [www.du.edu](http://www.du.edu).
    - b. Click **MyWeb** on the bottom of the page.
    - c. Choose **Enter Secure Area**.
    - d. Enter your "87" ID number and current password and click .
    - e. Choose the **Personal Information** category.
    - f. Select **Change your Passcode**.
    - g. Enter the old and new passcodes and click .
    - h. Choose **Exit** to logoff of MyWeb.
  2. To change the computer password used when logging into your local computer or a DU network (e.g., CAIR).
    - a. Login to your computer as usual.
    - b. Press Ctrl+Alt+Delete to access the Windows Security box.
    - c. Click the Change Password button.

- d. Enter your old and new passwords and click OK.
3. To add a password to your Windows Screen Saver:
  - a. Choose Start...Settings...Control Panel.



- b. Double-click **Display**.
- c. Choose the Screen Saver tab.



- d. Enter **5** minutes in the Wait box.
- e. Mark the box **On resume, password protect**.
- f. Click **OK**.
4. To change the password that you use to access and edit [www.du.edu](http://www.du.edu) web pages on DU's agora server:
  - a. Go to **<http://www.du.edu/uts/webwork/>**
  - b. In the **Quick Links** box, click **Web Account Manager**.
  - c. Login to you account with your agora login (the name before the @ in your DU e-mail address) and your current agora password. (If you don't know your agora password, contact the Help Desk at 303.871.4700)
  - d. Under **Services**, click **[Change your password](#)**.
  - e. Enter the new and old passwords and click the **Change Password** button.
  - f. Click **Logout** to exit Web Account Manager.

## Operating System and Application Updates


Windows computers at DU are required to run Windows XP Professional. In addition, most faculty and staff members use Microsoft Office 2003 for daily activities.

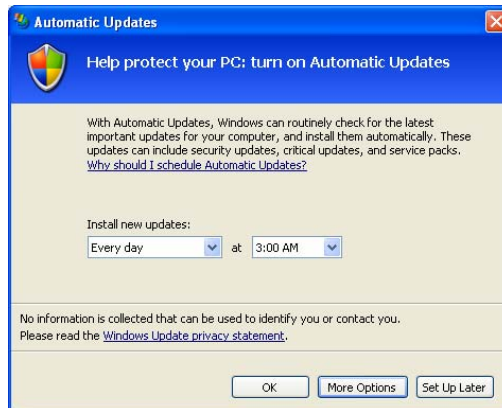
Microsoft frequently issues program updates that are required for you to keep your computer safe.

### What should I do?

A. Register with Microsoft to automatically receive system updates to Microsoft Windows XP Professional and to Microsoft Office 2003.

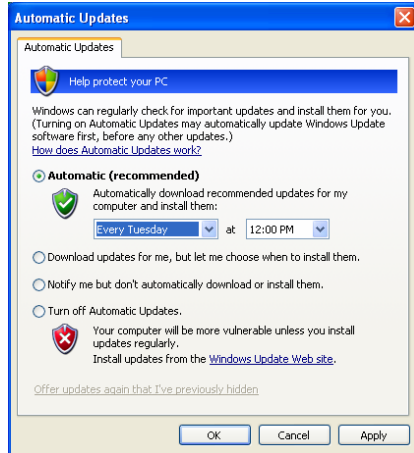
1. Go to [update.microsoft.com](http://update.microsoft.com)

2. Click  in the Help Protect your PC box. The Automatic Updates window will appear.



3. Click the More Options button.

4. Mark Automatic (recommended) and choose the day and time for weekly updates to be identified and installed (NOTE: This must be a time when your computer is turned on.) and click OK.



5. Click the Express button to get High-Priority updates.
6. Click the Install Updates button to install any necessary information.

## Firewalls

A firewall is a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.<sup>1</sup>

### What should I do?

- A. Turn on the Windows firewall on your computer.
  1. Click **Start** and then click **Control Panel**.
  2. In the control panel, click **Windows Security Center**.
  3. Click **Windows Firewall**.
  4. In the **General** tab and Mark **On (recommended)** and click **OK**.



---

<sup>1</sup> Tyson, Jeff, "How Firewalls Work", <http://computer.howstuffworks.com/firewall1.htm>, May 11, 2006.

## Pop-up Ads

A pop-up ad is an ad that "pops up" in its own window when you go to a page. It obscures the Web page that you are trying to read, so you have to close the window or move it out of the way. Pop-under ads are similar, but place themselves under the content you are trying to read and are therefore less intrusive.

Pop-up and pop-under ads annoy many users because they clutter up the desktop and take time to close. However, they are much more effective than banner ads. Whereas a banner ad might get two to five clicks per 1,000 impressions, a pop-up ad might average 30 clicks. Therefore, advertisers are willing to pay more for pop-up and pop-under ads. Typically, a pop-up ad will pay the Web site four to 10 times more than a banner ad. That is why you see so many pop-up ads on the Web today.

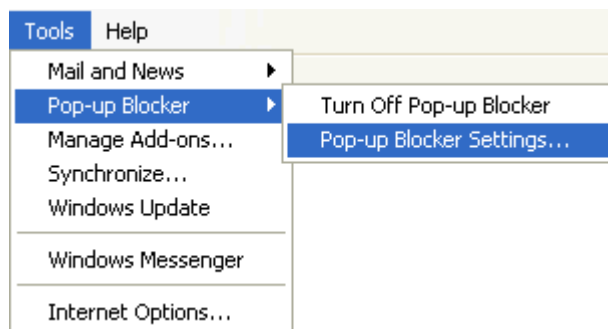
Some pop-up windows can contain inappropriate content or can be a way for you to accidentally download dangerous software (spyware or adware) onto your computer.

### What should I do?

- A. Don't click on pop-up windows.
- B. Use a Pop-up Blocker

In Windows XP Professional SP2, Pop-up Blocker is turned on in Internet Explorer and set to the medium setting, which means it will block most automatic pop-ups. The default settings for the pop-up blocker allow you to see pop-ups that are opened when you click a link or button on a Web site. Pop-up Blocker will also play a sound and show the Information Bar when a pop-up is blocked. You can adjust these settings so that Pop-up Blocker works the way you want it to.

1. To change Pop-up Blocker settings
  - a. Open Internet Explorer.
  - b. On the **Tools** menu, point to **Pop-up Blocker**, and then click **Pop-up Blocker Settings**.





- c. If you want to see pop-up windows from a specific Web site, type the address (or URL) of the site in the Address **of Web site to allow** box, and then click **Add**.

**Tip** To temporarily allow a site to display pop-ups, click the Information Bar when it notifies you that a pop-up has been blocked. Then click **Temporarily Allow Pop-ups**.

## Encryption

Encryption is the process of taking all of the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.

The key in public-key encryption is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. Essentially, the hash value is a summary of the original value. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value. Here's a simple example:

Input number	Hashing algorithm	Hash value
10,667	Input # x 143	1,525,381

Public keys generally use complex algorithms and very large hash values for encrypting, including 40-bit or even 128-bit numbers. A 128-bit number has a possible  $2^{128}$  or 3,402,823,669,209,384,634,633,746,074,300,000,000,000,000,000,000,000,000,000,000,000,000 different combinations!

### What should I do?

A. Before entering personal information on a website

1. Look for the "s" after "http" in the address whenever you are about to enter sensitive information, such as a credit-card number, into a form on a Web site.
2. The padlock symbol lets you know that you are using encryption.



## Spam

SPAM is unsolicited marketing e-mail.

### What should I do?

To help combat spam, follow these recommendations: <sup>2</sup>

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

If spamming weren't economically viable, it would be obsolete. Not only can an email user fall prey to a potentially fraudulent sales scheme, but his or her email address can also be added to the numerous email lists that are sold within the spamming community, further compounding the number of junk emails received.

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

While most spam is usually just annoying text, a spam email message could actually contain a virus and/or other exploit that could damage the computers of all who open it.

#### **Never respond to any spam messages or click on any links in the message**

Replying to any spam message, even to "unsubscribe" or be "removed" from the email list only confirms to the spammer that you are a valid recipient and a perfect target for future spamming.

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

Many spammers use advertising techniques that can track when a message is viewed, even if you don't click on the message or reply. Using the preview functionality essentially opens an email and tells spammers you are a valid recipient, which can result in even more spam.

#### **When sending email messages to a large number of recipients, use the blind copy (BCC) field to conceal their email addresses**

Sending email where all recipient addresses are "exposed" in the "To" field makes it vulnerable to harvesting by a spammer's traps.

#### **Think carefully before you provide your email address on websites, newsgroup lists or other online public forum**

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

#### **Never give your primary email address to anyone or any site you don't trust**

Share it only with your close friends and business colleagues.

---

<sup>2</sup> "Minimizing spam", Sophos Plc.,  
<http://www.sophos.com/spaminfo/bestpractice/spam.html>, May 11, 2006.

**Have and 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.

## Phishing

Phishing<sup>3</sup> is a method of online identity theft. In addition to stealing personal and financial data, phishers can infect computers with viruses and convince people to participate unwittingly in money laundering.

Phishers often use real company logos and copy legitimate e-mail messages, replacing the links with ones that direct the victim to a fraudulent page. They use **spoofed**, or fake, e-mail addresses in the "From:" and "Reply-to" fields of the message, and they obfuscate links to make them look legitimate.

Most phishing messages give the victim a reason to take immediate action, prompting him to act first and think later. Messages often threaten the victim with account cancellation if he doesn't reply promptly. Some thank the victim for making a purchase he never made. Since the victim doesn't want to lose money he didn't really spend, he follows the message's link and winds up giving the phisher exactly the sort of information he was afraid they had in the first place.

In addition, a lot of people trust automatic processes, believing them to be free from human error. That's why many messages claim that a computerized audit or other automated process has revealed that something is amiss with the victim's account. The victim is more likely to believe that someone has been trying to break into his account than believe that the computer doing the audit made a mistake.

E-mail is the most common way to distribute phishing lures, but some scammers seek out victims through:

- Instant messages
- Cell phone text (SMS) messages
- Chat rooms
- Fake banner ads
- Message boards and mailing lists
- Fake job search sites and job offers
- Fake browser toolbars

### What should I do?

A. Phishers tend to leave some telltale signs in their e-mail messages and web pages. When you read your e-mail, you should be on the lookout for:

1. Generic greetings, like "Dear Customer." If your bank sends you an official correspondence, it should have your full name on it. (Some phishers have moved on to **spear phishing**, which can include personalized information.)

---

<sup>3</sup> Wilson, Tracy V., "How Phishing Works",  
<http://www.howstuffworks.com/phishing.htm>, May 11, 2006.

2. Threats to your account and requests for immediate action, such as "Please reply within five business days or we will cancel your account." Most companies want you as a customer and are not likely to be so quick to lose your business.
  3. Requests for personal information. Most businesses didn't ask for personal information by phone or through e-mail even before phishing became a widespread practice.
  4. Suspicious links. Links that are longer than normal, contain the @ symbol or are misspelled could be signs of phishing. It's safer to type the business's URL into your browser than to click on any link sent in e-mail.
  5. Misspellings and poor grammar.
- B. Report phishing emails to **[phishing-report@us-cert.gov](mailto:phishing-report@us-cert.gov)** and/or **[reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org)**.

For more information on security visit **[www.du.edu/uts/security](http://www.du.edu/uts/security)**