

POINTS OF INTEREST:

- June 10 & 11 - e-Learning Workshop - Learn Adobe Acrobat 6 through Centra. See page 2 for more info!
- June 10 - e-Learning Workshop - Learn PowerPoint 2003 See page 2 for more info!
- The BVMMUG meets June 15, 11:45 a.m.. For more information see page 2!
- County Cost-Share machines arriving. Do those Security Patches **FIRST THING!!!**



eitmail@tam.u.edu 979.845.9689

Regional Specialists:

Bryan - Greg Thomas  
Corpus Christi - Pete Flores  
Lubbock - Steve Paz  
Overton - Aimee Sandifeer  
San Angelo - Jeffrey SoRelle  
Stephenville - Weldon Floyd

TEXAS COOPERATIVE  
EXTENSION

Editors:  
Jim Segers  
Jeffrey SoRelle

We're on the web at  
<http://eit.tamu.edu>

## Bytes & Pieces

### "Five Simple Things" that Computer Users Should do to Prevent Problems: by Paul Sittler

Network Security problems have been very expensive for us all. Viruses and worms have cost us a tremendous amount of time, while creating confusion, lost work, and frustration. Almost all such incidents are easily preventable - by computer users! After reviewing network security incidents over the last six years, there are five simple things that Computer Users should do that would have prevented almost all of them:

User Responsibilities for Security Five Simple Things. . .

1. Maintain Operating System patches to stay current. [6.02]
2. Use Anti-Virus programs as appropriate. Keep it up to date. [6.02]
3. Surf responsibly. [3.01]
4. Use e-mail responsibly. [6.02]
5. Use responsible passwords and safeguard them. [4.02]

The above procedures are the responsibility of each computer user. They are time-tested, reliable, and easy to implement. If we all did these "Five Simple Things", we'd have far fewer problems and wasted time.

By the way, they are not just good ideas; they are actually required by our "INFORMATION SECURITY, COMPUTER USE, AND SOFTWARE INSTALLATION/USE" policies. The numbers in [ ] behind each of the five things reference the policy section that applies. You can find the full

text of the Procedure 21.99.10.A1.01 at: <http://aghr.tamu.edu/xrules/219910X101infosec.htm>, or see Page 6 for applicable excerpts from the "TEXAS COOPERATIVE EXTENSION PROCEDURES" (Ellipses ". . ." are used to indicate omissions). Here's the general concept of the policy from Section 1.00

#### 1.00 GENERAL 1.01

Under the provisions of the Information Resources Management Act, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. These procedures are established to achieve the following:

- \* To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- \* To establish prudent and acceptable practices regarding the use of information resources.
- \* To educate individuals who may use information resources with respect to their responsibilities associated with such use. Violation of these procedures may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to loss of Extension and other Agriculture Program Information Resources access privileges, civil, and criminal prosecution. . . .

## News and Update

### EIT *e-Learning* Opportunity - Intro to PowerPoint 2003 - by Pete Flores and Jeffrey SoRelle

June 10th at 10:00 a.m. to 11:15 a.m. the EIT training team will offer a session introducing PowerPoint 2003. This first session will teach you the basics of PowerPoint such as template design, slide layout, view features, and entering content on a slide. The session will be conducted using Centra Symposium. This session will be limited to 15 participants. To register please go to: <http://centra.tamu.edu/main/tce>. If you do not have an account on Centra Symposium, you can create one. Simply log into Centra Symposium, click on **Events Lists** to view events. Look in the **EIT e-Learning** folder and enroll yourself in the EIT e-Learning - Intro to PowerPoint 2003 event.

### EIT *e-Learning* Opportunity - Adobe Acrobat 6 Professional Session 1 - by Jim Segers and Jeffrey SoRelle

June 10th at 1:30 p.m. to 2:45 p.m. the EIT training team will offer the first session in new series designed to get you up to speed on the advanced features of Adobe Acrobat 6. This first session will introduce you to Acrobat 6, cover some basics, and introduce some of the advanced features. Later sessions will cover additional features. The session will be conducted using Centra Symposium. This session will be limited to 15 participants. To register please go to: <http://centra.tamu.edu/main/tce>. Simply log into Centra Symposium, click on **Events Lists** to view events. Look in the **EIT e-Learning** folder and enroll yourself in the EIT e-Learning - Adobe Acrobat 6 - Session 1 event.

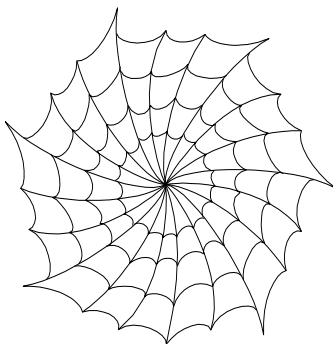
### EIT *e-Learning* Opportunity - Adobe Acrobat 6 Professional Session 2 - by Jim Segers and Jeffrey SoRelle

June 11th at 10:00 a.m. to 11:15 a.m. the EIT training team will offer the second session in a new series designed to get you up to speed on the advanced features of Adobe Acrobat 6. This second session will teach you to create interactive forms and review and modify PDF documents. The session will be conducted using Centra Symposium. This session will be limited to 15 participants. To register please go to: <http://centra.tamu.edu/main/tce>. Simply log into Centra Symposium, click on **Events Lists** to view events. Look in the **EIT e-Learning** folder and enroll yourself in the EIT e-Learning - Adobe Acrobat 6 - Session 2 event.

### The Brazos Valley Macromedia Users Group - by Summer Wilson

The Brazos Valley Macromedia Users Group will meet on June 15 at MicroAge from 11:45 to 1:00. Diann Mitchell, Website Administrator for Texas Cooperative Extension, will be discussing JAWS and ADA compliance. For information about BVMMUG, visit their website at: <http://bvmmug.tamu.edu>

## The Bottom Half - Website Info



### Possible URLs to link from your Websites this Month!

#### FCS

National Men's Health Week - <http://www.menshealthweek.org/>

#### AG and Natural Resource

Africanized Honey Bee - <http://agnews.tamu.edu/bees/>

Reference Guide for Texas Rancher's - <http://texnat.tamu.edu/ranchref/guide/index.htm>

#### 4H

2004 Texas 4H Roundup - <http://texas4-h.tamu.edu/roundup/>

### Tricks, Tips, and Dirty Cheats for Webmasters - Diann Mitchell

Spacing Your Images - You can specify the spacing between your images by using the horizontal and vertical space tags.

```
<IMG SRC="yourimage.jpg" VSPACE="10" HSPACE="10">
```

You can specify the horizontal and vertical spacing by editing the VSPACE and HSPACE values.

## Tip of the Month: Creating a WP Mail Merge from DataMaster

by Pete Flores

From DataMaster, after requesting a mail merge, an ASCII Delimited file named DMMail.dat is going to be created in the C:\ckv\dm\files\ directory. It is important to remember where the file is located.

**Using WordPerfect 10 and creating a mail merge use the following steps:**

1. Click on **Insert** from menu bar. (See Figure 8)
2. Go to **Spreadsheet/Databases** and select **Import**. A dialog box will be displayed as seen in Figure 9.
3. From the Dialog box as seen in Figure 9, Change the Data Type to **ASCII Delimited Text** and Import as Field to **Merge Data File**.
4. Click on the Filename and browse to the **C:\ckv\dm\files\** folder and select the **DMMail.dat** file.
5. The delimiters, Field is a **Comma**, Record is **[CR][LF]**, and Characters are **quotes**, at this point click on **OK** and the date file will be created.
6. **Save** the dat file and proceed with the Mail merge from WordPerfect 10.

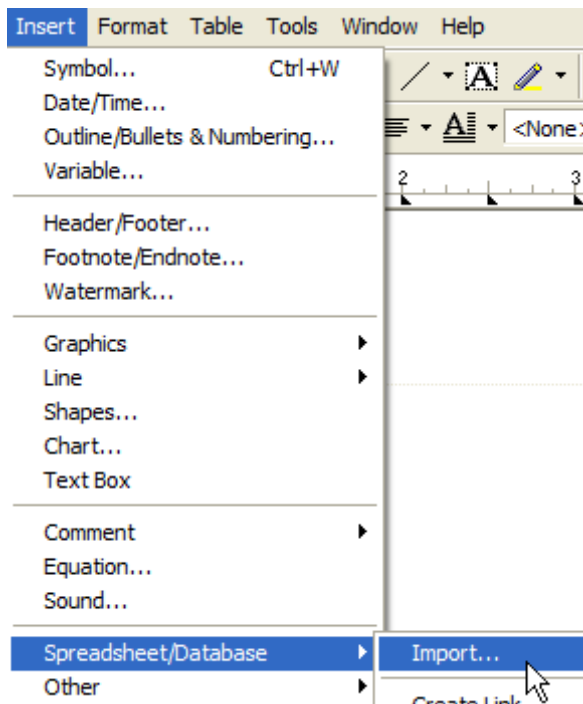


Figure 8: Insert Menu

**Using WordPerfect 11 and creating a mail merge use the following steps:**

1. Click on **Insert** from menu bar. (See Figure 8)
2. Go to **Spreadsheet/Databases** and select **Import**. A dialog box will be displayed as Figure 9
3. From the Dialog box as seen in Figure 9, Change the Data Type to **ASCII Delimited Text** and Import as Field to **Merge Data File**.
4. Click on the Filename and browse to the **C:\ckv\dm\files\** folder and select the **DMMail.dat** file.
5. The delimiters, Field is a **Comma**, Record is **[CR][LF]**, and Characters are **quotes**, at this point click on **OK** and the date file will be created.
6. **Save** the dat file and proceed with the Mail merge from WordPerfect 11.

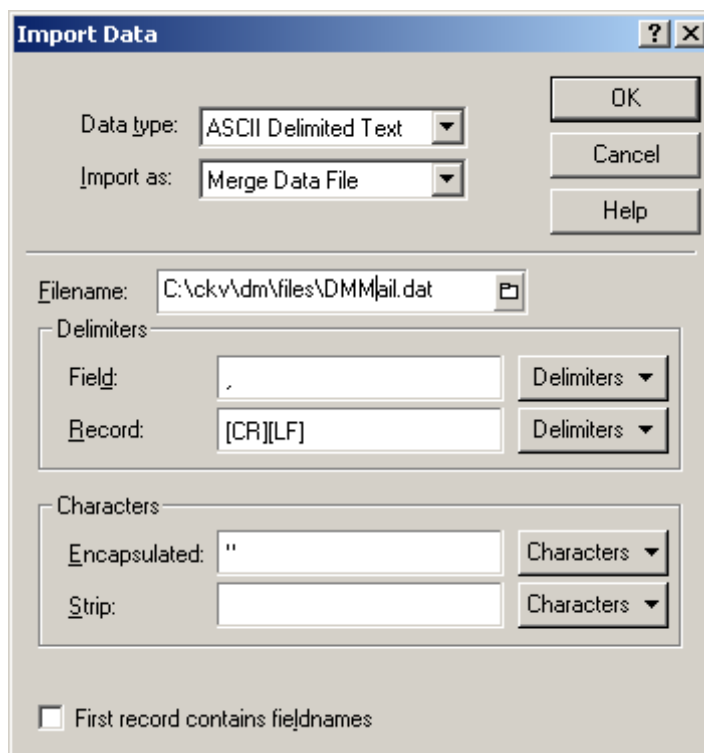


Figure 9: Import Data Dialog Box

## Tip of the Month: How to Install and Use Spybot version 1.3

by Jeffrey SoRelle

As many of you know, spyware is becoming ever more of a problem. Fortunately, there are some very simple solutions to protect yourself and your machine. For a better understanding of what spyware is, and why you should be concerned, please read "Spyware do you have it?" by Robert S. Cohen, <http://eit.tamu.edu/EITDOCS/TnT/Volume1/Volume1Issue4.pdf>. This tip will help you install one solution -- Spybot 1.3 -- and help you learn to use it.

### Step 1: Installing Spybot version 1.3

1. **Download** the file **spybotsd13** from the EIT website at <http://eit.tamu.edu/download/spybotsd13> to **your Computer's Desktop**. After download, double-click on the icon labeled **spybotsd13**. (See Figure 1)



Figure 1: spybotsd13 Icon

OR

If you receive the **Spring 2004 County Support CD**, insert the CD in the CDROM drive of your computer. At the menu click **Security Tools > Spybot**.

2. The first dialog box to pop-up is the Select Setup Language, choose **English** and click **Ok**. (See Figure 2)
3. At the *Welcome Screen*, click the **Next** button.
4. At the *License Agreement* dialog box, select **I accept the agreement** and click **Next**.
5. On the *Select Destination Location* dialog box, leave the default installation folder as is and click **Next**.
6. On the *Select Components* dialog box, accept defaults and click **Next**.
7. Click **Next** on the *Select Start Menu Folder* dialog box.
8. At the *Select Additional Tasks* dialog box, accept the defaults and click **Next**. (See Figure 3)
9. Finally, on the *Ready to Install* dialog box, click **Install**.
10. You may be prompted to **Restart** your computer. Please restart if prompted.

OR

After installation, you may see a *Completing Spybot Wizard* dialog box. **Uncheck** Run SpybotSD.exe and click **Finish**.

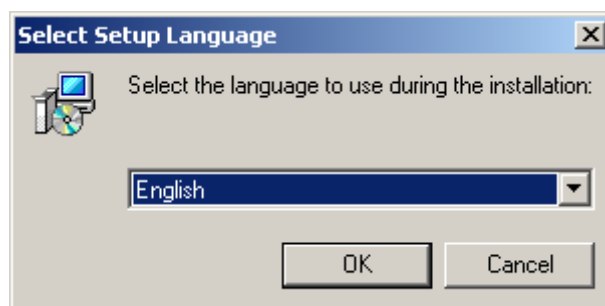


Figure 2: Select Setup Language

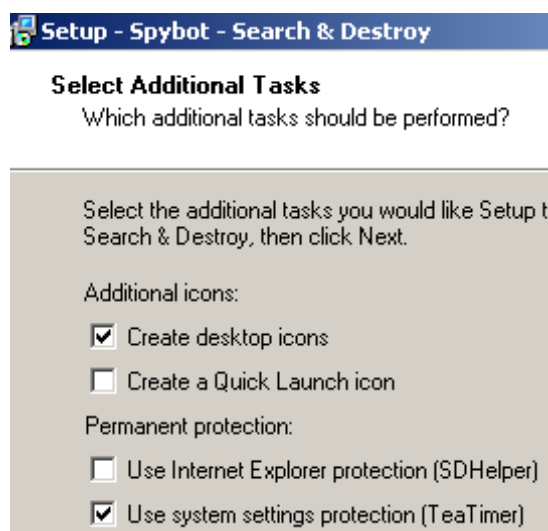


Figure 3: Select Additional Tasks

[Step 2. Using Spybot is Continued on Page 5!](#)

## Tip of the Month Continued: How to Install and Use Spybot 1.3

### Step 2: Using Spybot

1. **Double-click** on the **Spybot Search and Destroy** icon on the desktop of your computer. (See Figure 4)
2. When Spybot starts for the first time, you will see a **Create registry backup** option button, click the **button** to backup the registry.
3. Then click **Next**.
4. On the *Search for Update* dialog box, click the **Search for update** button. If updates are available, click on the **Download all updates available**.
5. Then click **Next**.
6. On the *Immunize this system* dialog box, click the **Immunize this system** button. **\*\*NOTE\*\* Bad products blocked will vary depending on the Operating System**
7. Then click **Next**.
8. Click the **Start Using this program** button.
9. Click on the **Search and Destroy** icon in the top left corner
10. Then click on the **Check for problems** button. (See Figure 5) **\*\*NOTE\*\* A scan will start. The progress of the scan can be monitored in the lower left corner.**
11. Once the scan is complete, a list of problems will be displayed. (See Figure 6)
12. Click **Fix Selected problems** button. (See Figure 5)
13. At the *Confirmation* dialog box to remove checked entries, click **Yes**
14. At the *Confirmation* dialog box that the problems were fixed, click **Ok**.

**\*\*NOTE\*\* For future scans make sure you Search for Updates. Also, if updates are available, make sure you Immunize your machine against these new threats. Then do a full Check for problems. (See Figure 7) I update and scan my machine, at least once a month.**

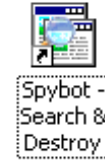


Figure 4: Search and Destroy Icon

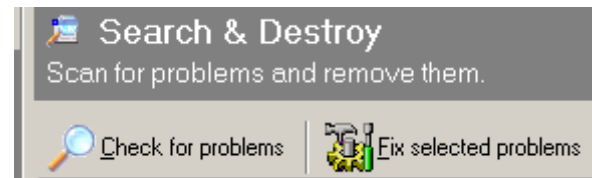


Figure 5: Check and Fix Problems

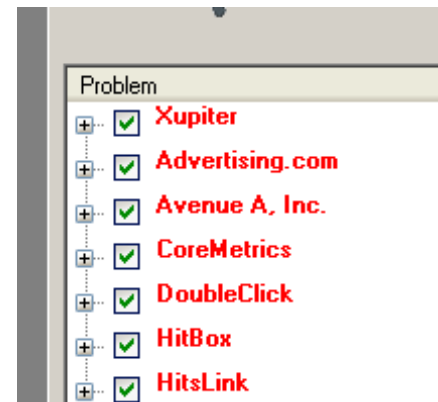


Figure 6: Problems Found

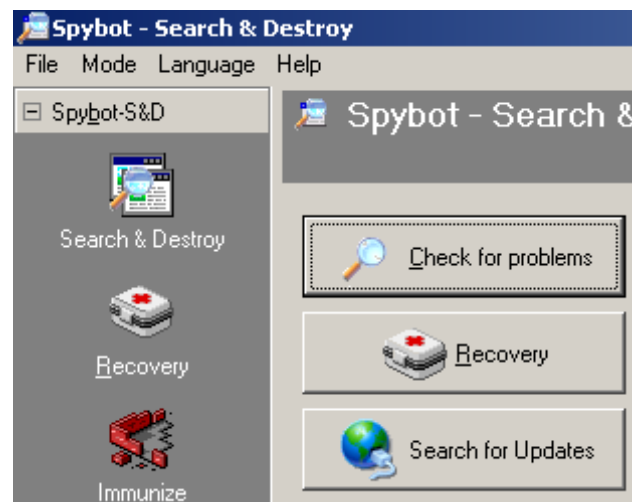


Figure 7: Future Use Icons

## **Selected Excerpts from the TCE Procedures 21.99.10.X.1.01 Information Security, Computer Use, and Software Installation/Use**

### 3.01 Employees Shall:

- A. Install on agency computers only that software which is licensed to or owned by Extension, and the license covers installation on the employee's specific computer.
- B. Copy software only if authorized by the specific license agreement governing that software.
- C. Install on agency computers only software which has a business or computer maintenance purpose. As such, use of certain screen savers, internet chat, and other software which has a personal purpose should be avoided. . . .

### 4.02. Password Standards

- A. All passwords should be constructed and maintained according to the following guidelines:
  - 1. be routinely changed
  - 2. be at least 8 characters in length
  - 3. be a combination of alpha and numeric characters
  - 4. not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relatives' names, birth date
  - 5. not be dictionary words or acronyms
  - 6. not be the same passwords used for personal accounts with services like Yahoo, MSN, AOL, Hotmail, etc.
- B. User account passwords should not be divulged to anyone nor displayed in a publicly accessible area. IT support personnel will only ask for user account passwords when necessary to resolve a specific problem.
- C. If the security of a password is in doubt, the password must be changed immediately.
- D. System administrators must not circumvent the password guidelines for the sake of ease of use.
- E. Users should not circumvent password entry with such means as auto logon, password remembering, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup).
- F. Computing devices should not be left unattended without enabling a password protected screen saver or logging off of the device. . . .

6.00 COMPUTER VIRUS PROTECTION Computer viruses are programs designed to make unauthorized changes to programs and data, therefore, viruses can cause destruction of corporate resources. It is important to know that:

- A. Computer viruses are much easier to prevent than to cure.
- B. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

### 6.01 Extension Information Technology (EIT) shall:

- A. Assist employees with the acquisition, installation, and maintenance of appropriate antivirus software on all computers.
- B. Notify all employees of imminent virus attacks, providing them guidance on how to respond, destroy any virus detected, and document each incident

### 6.02 Employees Shall:

- A. not knowingly introduce a computer virus into Extension computers.
- B. not load diskettes of unknown origin.
- C. scan incoming diskettes for viruses before they are read.
- D. IMMEDIATELY disconnect workstations from any network to which they may be connected, run available up-to-date virus scanning software, and notify appropriate computer support personnel if it is suspected that their workstations have been infected by viruses.
- E. not connect any web or file servers to the network until they are reasonably certain that they have applied all available software patches and have configured all security settings in the software to the most secure level possible given the purpose and function of the server. If possible, isolated security screening of these servers should be done prior to connecting them to the network.
- F. not use nor access any e-mail system other than the GroupWise system administered by Extension Information Technology unless they have installed and keep up to date the latest virus scanning software and security patches available for this alternative e-mail system.
- G. not use any internet chat software capable of transferring files unless they have installed and keep up to date the latest virus scanning software and security patches available for that software.