

Protect yourself on-line.

- (cont.)
online with a virtual credit card number or a limited credit card from your banking institution.
- Do not respond to any emails requesting credit card, bank account or password information. Don't fall prey to anyone requesting you cash a check or money order for them.

WHAT SHOULD I DO IN THE EVENT OF SUSPECTED IDENTITY THEFT?

- First educate yourself by going to: <http://www.ftc.gov/bcp/edu/microsites/idtheft/> or at <http://privacyrights.org> before it happens.
- Contact your Credit Card Company and bank.
- Contact local law enforcement.
- Notify credit bureaus and establish fraud alerts. Immediately report the situation to the fraud department of the three credit reporting companies -- Experian, Equifax, and TransUnion. When you notify one bureau that you are at risk of being a victim of identity

theft, it will notify the other two for you. Placing the fraud alert means that your file will be flagged and that creditors are required to call you before extending credit. Consider using a cell phone number if you have one.

Equifax: P.O. Box 740250, Atlanta, GA 30374-0241.

Report fraud: Call (888) 766-0008 and write to address above.

Experian: PO Box 9532
Allen TX, 75013

Report fraud: Call (888) EXPERIAN (888-397-3742) and write to address above.

TransUnion: P.O. Box 6790, Fullerton, CA 92834-6790.

Report fraud: (800) 680-7289 and write to address above.

Call the FTC's Identity Theft Hotline: (877) IDTHEFT (877-438-4338)

¹ All student projects are supervised and conform to laws within Shelbyville, Tennessee. Informational statistics were gathered May 2007. This brochure is for informational use only and may be distributed and copied without notice to the Tennessee Technology Center at Shelbyville.

TTC Shelbyville
1405 Madison Street
Shelbyville, Tennessee 37160
Phone (931) 685-5013
Fax (931) 685-5016
www.ttcshelbyville.edu

Steve Mallard, IT Manager

A partnership with the Shelbyville Police Department
Austin Swing, Chief of Police
Mike Rogers, Asst. Chief of Police
Lt. Det. Pat Mathis



How to Protect Your Identity and Your Home Computer



How to Protect Your Identity and Your Home Computer

FACTS

Technology in Shelbyville is growing at an unprecedented rate. Recent studies and research at the Tennessee Technology Center at Shelbyville shows that 90% of home computers have spyware or viruses imbedded on the computer. 80% of home computers have expired antivirus software or have no antivirus software installed. Greater than 90% of work orders handled by more than 50 Computer Operations Technology students were missing critical updates. Almost all of the computers repaired had their software firewall turned off. A recent student project showed more than 100 open wireless network routers or devices were left unsecured that could be accessed from over 1000 feet from their homes. ¹

DANGER

If you have filed your taxes on your computer, have critical documents such as memos or emails to creditors, personal documents, personal health information, or other valuable information on your computer, you may be unprotected and at risk. P2P file sharing programs such as music sharing programs are often illegal and leave your computer open. A recent search on a major file sharing software program used to download music, showed open

computers where tax information could be downloaded from thousands of computers on these networks.

The information gained by leaving your computer unsecured could leave your personal identity and personal information at risk.

PROTECT YOUR PC AND IDENTITY

In order to protect information follow these steps to protect your computer and data.

- Remove any P2P file sharing programs (music sharing) that has not been paid for.. If you must have this software on your computer, make sure it meets any RIAA approval. Remember you could be sharing out sensitive data.
- Turn on your Windows firewall. Go to the security center under the control panel and activate the firewall. Did you know, if you keep music downloading software on your computer, the firewall can remain 'open' even if it is turned on? This could allow sensitive data exposure on your computer.
- Update your antivirus software. Check daily. Yes, daily. Download antispysware software such as Adaware or Spybot's Search and Destroy. These can be found at www.download.com.
- Click on start and go to the Windows Update site at least weekly. Even if you have automatic updates on, you could be missing

important updates. Download and install any critical updates to your computer.

- If you have a wireless router or WAP for your internet connection, follow the manufacturers' suggestions on securing this device. You are generating a signal that can go hundreds of feet from your home. Change the Admin password on the device. Remember, even if you lock the device with WEP or WPA as the manufacturer suggests, you could leave yourself vulnerable by not changing the password.
- Use complex passwords on your computer. Require a login username and password. This setting is under 'users' found in the control panel. Use letters, symbols and numbers. Use a pass-phrase such as Th3 doG! . This makes guessing passwords difficult. A few seconds typing in your password could save you a great deal of time and money.
- Test your system by going to www.grc.com and clicking on "Sheilds Up!". This test is free and it tests your firewall for open ports.
- Get updates for any software you may have such as Microsoft Office, QuickTime and any third party software.
- Do not shop untrustworthy websites. Make sure they are Better Business Bureau members or shop