ID Theft

Identity theft is one of the nation’s fastest growing crimes. According to the Federal Trade Commission (FTC), 9.9 million Americans were victims in 2003. Identity theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another’s personal data in some way that involves fraud or deception, typically for economic gain. The Identity Theft and Assumption Deterrence Act (1998) prohibits “knowing, transferring, or using without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”

Interestingly enough, most security professionals believe that the biggest danger of identity theft does not come from online transactions but from paper ones. The thefts of traditional mail or “dumpster-diving” through trash are common methods used to obtain private information. One traditional solution is to shred all documents (including credit card solicitation) before they leave your residence. Reports of camera phones used to take photos of credit card transactions in stores remind us to be aware of our surroundings.

Technology can assist in the prevention of identity theft through the proliferation of online bill notification and payment. Many financial institutions offer partnerships allowing the payment of your bills through one central location. Other banks and creditors offer the ability to receive your bills electronically. An e-mail is sent notifying you of a bill, and the next time you are online you may schedule payment. Remember to use a different, hard-to-guess password for all online financial accounts. Should someone crack your standard password (that you may use for e-mail), there is no danger this will allow access to your online financial information.

Obviously there are still online threats; do not tell anyone on the Internet anything you would not tell someone on the street. When shopping online, verify through the Better Business Bureau the credibility of the online merchant, or limit shopping to well-known Internet vendors, such as, www.amazon.com, www.bn.com, and organizations that guarantee your transactions such as www.ebay.com.

Some general guidelines for protecting your identity:

- Adopt a “need to know” policy about your personal information.
- Be “stingy” with your personal data.
- If you are traveling, have your mail held at the Post Office.
- Check your financial information regularly; online banking facilitates timely and accurate information.
- Obtain a copy of your credit report periodically.

VPN: Secure Remote Access

VPN stands for Virtual Private Networking and is a technology that is used to allow remote computers on the Internet to connect to campus servers securely. The essence of VPN technology is that your home PC or traveling laptop appears exactly the same as a PC that is physically on campus. The IT Division provides this service at no additional cost to the University community. A VPN connection allows you to access file servers, printers, e-mail systems, and applications, just as you can from your campus location. For instance, you can use Outlook to connect to TechMail and to access your e-mail exactly the same from home as you would from the office. Forgot to copy that file onto your laptop before heading off to a conference? With a VPN connection you can connect to your file server and access the files directly.

In a time of escalating Internet threats and attacks, VPN connections provide highly secure access to University resources. All transmissions between your PC and TTUnet are encrypted to prevent interception by an unauthorized individual. Since the University’s VPN service uses your eRaider username and password to authenticate the connection, configuring your VPN connection is simple. Once you have set up your VPN connection on your computer, you are ready to authenticate to TTUnet and to access your resources.

Our current statistical trend analysis indicates that usage has increased from a monthly average of 27 sessions in 2003 to a monthly average of approximately 80 sessions in 2004. While usage is still very low compared to the University community size and technical capacity, we are encouraged by the increasing averages. To assist with configuring your home or traveling laptop for VPN, we have provided comprehensive instructions on the IT Help Central Web site (www.helpdesk.ttu.edu). If you need further assistance with your VPN connection, you can contact IT Help Central at 742-HELP.

Message from TTU Chief Information Officer

As the academic year commences, I am initiating a vital Safe Computing Practices Campaign for the University. In each bulletin, we plan to highlight various measures and tools to heighten our awareness and security practices related to information technology both at Texas Tech and at home. In this issue, we have selected three key areas that impact a majority of our TTU community: Identity Theft, Secure Remote Access (VPN), and Wireless Networking in the home environment. Our IT Staff has compiled information to empower and protect you in each of these scenarios. In each edition, we will also include some simple Safe Computing Tips that target key problems and issues that arise during the course of daily operations. As the Internet computing environment escalates with security threats and attacks, we must work together as a professional community to protect our information and resources.

If you have been a victim or believe identity theft has happened to you, contact your local law enforcement and the FTC at www.consumer.gov/idtheft for more information. At the FTC site, you will find the ID Theft Affidavit created for you to certify that your identity was used without your knowledge. Identity theft is not the end of the world, but it can be a long and expensive issue from which to recover. Protection of vital information is your best prevention tool.

-Sam Segran
TTU Chief Information Officer
Minimum Precaution to be Taken

1. **Change the System ID**: Wireless routers and access points come with a default system ID called the SSID or ESSID. It is easy for a hacker to find out what the default identifier is for each manufacturer of wireless equipment, so you need to change this to a unique name (not your family name or something easily guessed).

2. **Disable Identifier Broadcasting**: Announcing that you have a wireless connection to the world is an invitation to hackers. Check the instruction manual of your access point for steps to disable broadcasting.

3. **Enable Encryption**: Enabling encryption (such as WEP or WPA) allows your data only to be read by the intended recipient. By using encryption, you will keep the casual hackers out of your systems. If possible, you should use WPA encryption because it fixes some security flaws found in WEP.

4. **Change the Default Administrator Password**: This is a good practice for ALL hardware and software. The default passwords are easily obtained, and many people simply do not change them. Be sure to change the default password on your wireless router/access point to something that is not easily guessed.

5. **Patch and Protect Your PCs**: As a last line of defense, you should have personal firewall software and anti-virus software installed on your computer and update this software regularly. The University provides Norton AntiVirus for free to students, faculty, and staff for use at the University and at home. Also keep your computer updated with operating system patches and service packs. For those with Microsoft operating systems, visit www.windowsupdate.com to help keep you current with patches.

For added protection:

6. **Restrict Unnecessary Traffic**: Many wireless routers have built-in firewalls. Router firewalls help create one more line of defense. Refer to your manual to learn how to configure your router only to allow approved incoming or outgoing traffic.

7. **MAC Address Authentication**: The MAC (Media Access Control) Address is a unique identifier that is specific to every network card. In order to find the MAC Address on a Windows machine, go to “Start,” “Run Command,” and type “ipconfig /all.” The MAC Address will be listed as a physical address. We recommend that you enable and use MAC address authentication. Once enabled, whenever the router receives a request to join the LAN, it compares the MAC address of the client against a list of allowed MAC addresses. Clients on the list authenticate as normal, but clients not on the list are denied access.

For further support questions, please contact IT Help Central at (806)742-HELP.