Don’t Let Identity Theft Spoil Your Vacation

Vacationers are at an increased risk for identity theft because they often carry credit cards, passports, and other official forms of personal identification. As a result, tourists are routinely targeted by criminals. Travelers must be careful in their efforts to protect themselves and take extra precaution with items most likely to be stolen while traveling. Thieves are just as likely to target your personal information as your expensive camera or laptop. The TTU IT Division offers these tips to help protect your identity while vacationing:

• Don’t travel with all your credit cards -- carrying limited credit cards reduces the chance of loss or theft.
• Don’t leave personal information in your hotel room; we suggest that you store valuables in the hotel safe.
• Avoid accessing personal information from public computers. Most public wireless connections are not secure, so avoid using them for important transactions; for example, transactions requiring a login.
• Stay alert! It is easy to let your guard down while relaxing on vacation, but it’s important to be aware of your surroundings and the people around you.

Mobile Safety on the Go

Many travelers use smartphones as a vacation planning tool to book flights or hotels. If you make travel arrangements using your mobile phone, be careful about the information you input and store in the application, such as saving your login information, credit card number, or billing address. Remember, connecting to public Wi-Fi networks to access the Internet can expose your information and data. The IT Division offers a few tips to keep in mind when you’re vacationing:

• Avoid connecting to an unsecured wireless network.
• Before downloading an “app,” read the privacy policies and make sure you are comfortable with how your information will be used.
• Always be mindful and cautious with the information the “app” stores, such as login credentials, as well as personal and financial information.
• Make a record of your Electronic Serial Number (ESN) and/or your International Mobile Equipment Identity (IMEI) number in case you lose your cell phone. You can find your IMEI number by pressing *#06# on most mobile phone keypads, and it will display your 15-digit IMEI number. You may also physically inspect your phone and check under the battery for this serial number.
• If your phone is lost or stolen, report it to your local police station immediately.

Protecting Your Identity

For most services at Texas Tech University, we have transitioned from using Social Security Numbers (SSN) to eRaider or Banner IDs (R numbers). While providing your SSN is still required for access to certain services at TTU, as well as for access to Federal loan programs, you should always be vigilant about providing your personally identifiable information. The TTU IT Division suggests the following tips when you are required to provide your SSN or other personally identifiable information:

• Ask About Alternatives – Although you may be asked to provide your SSN, it may not be the only acceptable form of identification. Note that you may be required to provide your SSN in situations that require identity verification or that involve IRS matters. Make a practice of always asking if another form of identification is acceptable.

• Control the Circumstances - Don’t give out your SSN or other personal information to someone who initiates contact by phone or email. For example, if you receive an email that claims that you must provide your SSN or other personal information to someone who initiates contact by phone or email. For example, if you receive an email that claims that you must provide your SSN in situations that require identity verification or that involve IRS matters. Make a practice of always asking if another form of identification is acceptable.

• Lock It Up – Consider keeping your Social Security card locked up in a safe at home, not in your wallet or purse. Public academic settings, where students often leave backpacks and wallets containing personal information unattended, are particularly vulnerable to theft.

• Stay Up To Date – Keeping your anti-virus software up-to-date goes a long way in avoiding online identity theft. You can download Symantec Endpoint Protection free-of-charge at http://eraider.ttu.edu.

• Change passwords for online accounts regularly – do not use the same passwords for your financial, social networking, or email accounts.

• Be In Charge of Your Information – Being proactive does not completely eliminate the chance that you will become a victim of identity theft. However, taking a few minutes daily to monitor your online bank accounts and other financial services allows you to catch unauthorized transactions and report them quickly to your financial institution and credit bureaus.

(continued on back)
If your Social Security or credit card is stolen, contact the police and make a report. With a police report, you can place an extended fraud alert on your credit report, and you'll have documentation to bolster your case if you become a victim of identity theft.

Do Not Share your eRaider Password - As a reminder, the TTU IT Division will NEVER ask for your eRaider password, nor will any other authorized affiliate. Remember that sharing your eRaider password with anyone is a violation of TTU IT Security Policies and state law.

Social Networking Safety While You Are on Vacation

Sharing vacation plans with friends, family, and co-workers using social networks is a wonderful way to communicate excitement about upcoming trips. Due to the public nature of social networking, we encourage you to wait until you return home to post your vacation details and photos. The TTU IT Division suggests these social networking safety tips for when you are on vacation:

• Do not post trip updates while you are away -- such information “advertises” that you are not home, possibly making your unoccupied home more vulnerable to criminals prowling the web for personal information.

• Have a family discussion and agree on rules about sharing information while on vacation.

• Never share vacation details, including dates, times, or any information about family members that remain at your home while you are gone.

• While on vacation, turn off location service applications on your phone unless you need to use one.

• If possible, take a break – vacations are a great time to disconnect from the social networking and technology world for a while.

For more safe computing information, please visit: http://www.safecomputing.ttu.edu.

Computer Educational Training

The TTU IT Division offers a variety of educational resources for all Texas Tech University students, faculty, and staff at no charge. We encourage all members of the Texas Tech community to take advantage of these opportunities.

Every semester, including summer semesters, Technology Support offers instructor-led computing ShortCourses. To accommodate a wide variety of schedules, we offer morning, afternoon, and evening classes. All Technology Support ShortCourses are taught by professional IT staff members and are held in the main ATLC facility, located in the west basement of the University Library building. Class sizes are limited, so we ask that you register in advance. To view the current ShortCourse schedule and to register, please visit http://www.itts.ttu.edu/training/shortcourses. If you have questions, please email ITeducation@ttu.edu or contact Technology Support at (806)742- 1650.

The TTU IT Division offers learning and professional development “anytime, anywhere” for the TTU community with free online Computer Based Training (CBT), a service TTU contracts from SkillSoft. CBT courses are online, self-paced and interactive. TTU hosts an inventory of over 4,000 courses, covering basic computer skills, advanced technology topics, financial training, customer service development, project management methodologies, and general management skills. CBT courses can be used as professional development for a wide variety of skills or to prepare students for technology required in their coursework at TTU.

Visit http://www.cbt.ttu.edu to view the listing of available courses. Start building your skills today!

Contributions by: Katherine Austin Beltz, Ph.D., Mark Holwerda, Ron Nail, Britta Tye, Laura Webb, and Allen Young.
Safe Computing Practices Committee: Sam Segran, Katherine Austin Beltz, Ph.D., Jeff Barrington, Darrell Bateman, Pulin Bhatt, Shannon Cepica, Paco Diaz, Scott Hall, Mark Holwerda, Michael Horton, Danny Mar, Ron Nail, Yung Ng, Randall Osborne, Mike Simmons, Phil Smith, Ph.D., J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.

Past copies of TTU IT Division Bulletins may be found online at http://www.infotech.ttu.edu/itbulletin
Copyright 2011 Texas Tech University