TEXAS A&M UNIVERSITY

IT

Summer 2010

Crossword for Cookies
See back page.

What's Inside

PossibilITies Away from the Office

During the summer months, you may be traveling to fun vacation destinations or working at home while classes are not in session. We'll tell you about technology resources for staying productive while away from campus or enjoying your time off safely and securely.

If you have questions about an IT service, please contact Help Desk Central, anytime day or night, at 979.845.8300 or **helpdesk@tamu.edu**.

Tell us what you think about this newsletter by emailing **tamu-it@tamu.edu**.

WORKING SECURELY ANYWHERE

Any place can become your "office" with a computer or mobile device and an Internet connection — at home, on the road, or even on vacation. When using laptops or smart phones to work remotely, good IT security practices are critical. Not only are they important to safeguard university confidential information, they help protect your personal data as well.

Here on campus we rely on IT professionals to keep university assets safe with a campus firewall, spam filters, and other security measures. However, even the strongest campus security measures can't protect your home computer.
(continued on Page 2)

Let's get together. Use video, audio, or webconferencing to collaborate with your colleagues. Learn more at **IT.tamu.edu/Connecting/Conferencing.php**.

Staying Connected

Using VPN to Connect to Texas A&M

If you've ever accidentally left something at work, you know that feeling of wishing you could be on campus without driving back. VPN cannot magically transport you to the Texas A&M campus, but using VPN is like having your computer or mobile phone on campus even when you are at home, on vacation, or on the go.

What is VPN?

VPN creates a tunnel to the Texas A&M Network so that you can be "on campus" from anywhere including your mobile phone or your off-campus computer.

When should I use VPN?

Some IT services at Texas A&M are only available on campus. You should use VPN to access these services when you are away from the office. One campus-wide example is managing your **people.tamu.edu** web site. Departments also use VPN for internal web sites, file storage, and more. Ask your departmental IT staff about the services you can access using VPN.

How does VPN work?

VPN creates a link between your computer or mobile phone and the VPN server on campus. This link allows you to access the on-campus resources you need through the VPN server.

Want to learn more?

Learn more about VPN including complete set-up instructions at **it.tamu.edu/VPN.php**.

Surfing Securely on Public Wi-Fi

You may enjoy the convenience of public Wi-Fi in many places including cafes, airports, and hotels. But did you know that most public Wi-Fi hotspots are not secure? While you surf the Internet, someone nearby may be fishing for your dollars.

Hackers use sniffer programs to spy on data traveling through the air. They can see almost anything you do on public Wi-Fi — the sites you visit, forms you complete, or emails and instant messages you send and receive. This information can be used to steal passwords and other sensitive information.

To read more about how to be secure on public Wi-Fi, visit **url.tamu.edu/publicwifi**.

Preventive steps to stay secure while on public Wi-Fi

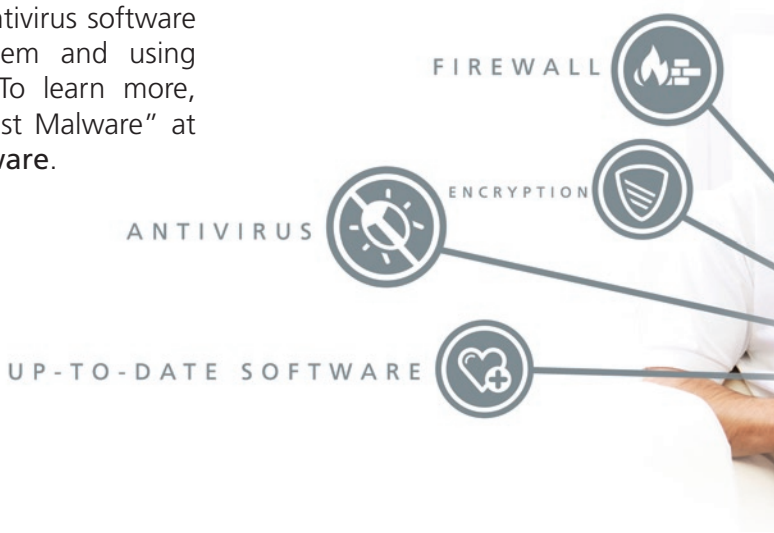
- Do your online banking and shopping at home, not on public Wi-Fi.
- Remember "***S***" for security. If logging in to a site, look for ***https*** in the web address, indicating a secure site.
- Use Virtual Private Network (VPN) to safely connect to the Texas A&M Network.
- Beware of the "Evil Twin." Confirm the exact spelling of the Wi-Fi network before connecting to avoid slightly misspelled fakes.
- Encrypt confidential files to make it more difficult to steal personal information.
- Turn off the wireless connection when you don't need to be on the Internet.

Working Securely Anywhere

continued from page 1

In fact, personally owned computers are among the favorite targets of cyber criminals looking to steal identities and plunder bank accounts. You also may be sharing the same computer with your family, making online safety precautions even more important.

- Beef up security on your computer by updating your antivirus software and operating system and using strong passwords. To learn more, read "Protect Against Malware" at **url.tamu.edu/malware**.
- Take steps to safeguard personal information online. See "Staying Safe" at **url.tamu.edu/stayingsafe**.
- Read more tips in this newsletter to learn how to work securely wherever you are.



Keeping Your Information Safe
Encryption

Did you know that if you lose your computer, the information on that computer can be used by whomever finds it? Even if you password protect your system, the data stored on your hard drive can still be taken. So, if you store valuable information, such as student records or personal financial information on your computer, you need to protect it with more than just a password. What should you use? Encryption.

What is encryption?

Encryption is a way to increase security for sensitive information. It scrambles the content of files so that it can be read only if you have the correct encryption key to unscramble it.

When should I use encryption?

Texas A&M employees who work with confidential or sensitive information must protect it. A common way to lose confidential information is losing a portable device on which it is stored. SAP 29.01.99.M1.16 requires confidential information stored on portable computing devices to be encrypted.

What encryption tools are provided by the university?

PGP Desktop is provided by the university to departments. One advantage of using ***PGP Desktop*** is that we can recover your data in the event of a lost encryption key. ***PGP Desktop*** is not currently offered as a tool to individual users. Please contact your departmental IT personnel if you are interested in using this resource.

What other tools are available?

Most operating systems have a built-in way to encrypt files. Windows provides ***BitLocker*** (**http://windows.microsoft.com/en-US/windows7/products/features/bitlocker**). Apple has ***FileVault*** (**http://docs.info.apple.com/article.html?path=Mac/10.6/en/8727.html**). But beware! If you use one of these methods and forget your encryption key, you won't be able to log in and your files will be lost forever.

Where can I find out more?

See **url.tamu.edu/portabledevices**.

Follow TAMU_IT on Twitter!

What to Do if it **Happens to You!**

Identity Theft

According to the Federal Trade Commission (FTC), identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission to commit fraud or other crimes. If you suspect identity fraud, take steps to protect yourself as quickly as possible:

1. Contact the fraud departments of the three major US credit bureaus to place fraud alerts on your credit reports. See **ftc.gov/idtheft**.
2. Close any accounts that you know or suspect have been compromised or opened fraudulently.
3. File a complaint with the FTC. This helps you receive certain protections such as blocking fraudulent information from appearing on your credit report.
4. If you believe your Social Security number has been used illegally, contact the Social Security Administration (**www.ssa.gov**).

To find out more about staying safe online, visit **security.tamu.edu**.

Security **Tip**

Using Antivirus Software

Use an up-to-date antivirus program to protect your computer from infection by email attachments and downloaded files.

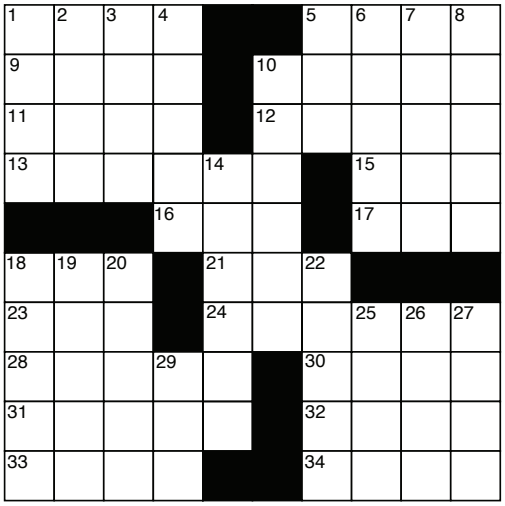
Visit **software.tamu.edu** to get antivirus software at no charge for home computers and laptops.

sell@tamu.edu | 979.862.4104

Texas A&M **Information Technology**
Security Crossword

ACROSS
1. Smell
5. Curved roof
9. Surface a road
10. Out of shape
11. Wields
12. Downloadable fix for software
13. Crafty
15. Before, poetically
16. British drink
17. Neither's partner
18. Password to never send in email
21. Estimated time of arrival
23. Poet Edgar Allen
24. Lacking entirely
28. Where actors work
30. Upon
31. Unusual ____ messages are a sign of viruses
32. Chilled
33. Never ___ your password in email
34. Demonstration

DOWN
1. Musical composition
2. Hurry
3. Ended
4. Can't log in? ____ your password ASAP.
5. Genetic code
6. Many times
7. Opp. of macro
8. Vanish into the___
10. Use auto___to protect your computer
14. Garden caretaker
18. Recesses
19. "__ Dame"
20. Desire
22. ___ listing private info on Facebook
25. __ upon a time
26. Object
27. Extinct bird
29. Deity



For crossword solution and coupon details, go to http://security.tamu.edu/Crossword.php

Sponsored by

IT'S A GRIND COFFEE HOUSE

FREE DESSERT

Take completed crossword to **IT'S A GRIND** for a free cookie, brownie, or dessert bar with the purchase of a 16 oz. drink.

Did You **Know?**

Keeping In Touch

Phones and Voice Mail

Phone and voice mail options make it simple for you to stay in touch — at the office, at home, or on the road.

- Forward calls from your office to another telephone, such as your home phone or cell phone.
- Check your office voice mail from any phone on or off campus.
- Forward your voice mail to your email account and receive an email alert when you receive a message.

For step-by-step instructions, visit url.tamu.edu/userguides.

IT Recipe

Set Up TAMU Email Mobile on Your Smart Phone

1. Your mobile device
2. Your TAMU Email (Neo) account
3. Follow the instructions at **url.tamu.edu/emailmobile**

Now your Texas A&M email, calendar, and contacts will sync to your mobile device.

Featured **Service**

Instructional Technology Services

No-cost, hands-on training for integrating technology into teaching.

itsinfo.tamu.edu | its@tamu.edu | 979.862.3977