POSSIBILITIES

Texas A&M **Information Technology**

Fall 2010

TEXAS A&M UNIVERSITY

PossibilITies Online

As social networking grows and personal information online proliferates, Internet fraud risk and privacy concerns also increase. We'll tell you about steps you can take to stay safe online.

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

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

REAL VILLAINS OF CYBERCRIME

When you think of "Hackers," you may remember a 1995 movie where teenagers harmlessly competed to prove their skills. However, hackers have evolved into a world of cybercrime with highly organized, well-funded crime syndicates launching sophisticated attacks from around the globe.

This new generation of cybercriminals dedicates immense quantities of time and resources to building better viruses and online scams. From fake Rolex watches to bogus software and phony discount pharmacies, cybercriminals reap billions of dollars every year through scams planted in emails, pop-up windows, Twitter and Facebook messages, and even links inserted on legitimate sites.[1]

continued on page 2

[1] www.sophos.com/security/topic/threat-report-jan2010/

October is IT Security Awareness Month. Visit **mystery.tamu.edu** and solve cases for weekly rewards (coupon offers) and a chance to win $50 gift cards.

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

Spam

Spam is unsolicited junk email, often generated for criminal or fraudulent schemes such as identity theft. To combat spam, delete unsolicited email or move it into the Junk folder. Use the junk mail handling tools in your email program, such as block lists. To protect your @tamu.edu email, obtain a free account, such as Gmail or Yahoo Mail, for filling out web registration forms.

Reporting Spam

See the Spam section of the Information Security web site (**http://url.tamu.edu/stayingsafe**) to learn more.

Real Villains of Cybercrime

continued

Some cons target individuals, tricking them into revealing credit card numbers. Others infect personal computers to build zombie networks used in coordinated attacks on university, corporate, and government databases.

Cybercriminals are running smarter scams and producing more ingenious software. No longer are hoaxes easy to spot through bad grammar or poorly constructed web sites. Scammers have honed their skills to develop sites and emails that closely resemble legitimate businesses. Improved viruses have been designed to mask symptoms, such as programs running slowly or closing unexpectedly.

What can we do to protect ourselves?

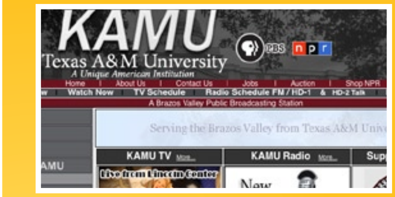
- Keep your computer's software and operating system updated.
- Do not click links in an email or open attachments unless they are from a trusted source.
- Be suspicious anytime a web site or email asks for your personal information.
- Never click Internet pop-up ads.
- Do not use Facebook games or applications that require downloads.

Learn more about how to stay safe at **security.tamu.edu**.

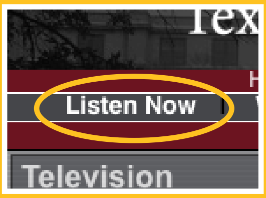
A special IT Forum on October 27th from 3:00 – 4:30 p.m. in Rudder 601 will be dedicated to discussing the new generation of cybercrime. See the back page for more details.

IT Recipe

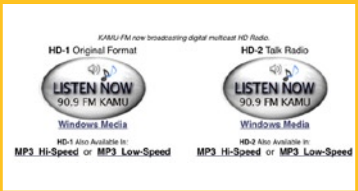
Listen to KAMU Streaming Radio


KAMU
Texas A&M University
A Unique American Institution
PBS
npr
Home | About Us | Contact Us | Jobs | Auction | Shop NPR
Watch Now | TV Schedule | Radio Schedule FM / HD-1 & HD-2 Talk
A Brazos Valley Public Broadcasting Station
Serving the Brazos Valley from Texas A&M Univ
KAMU TV More...
KAMU Radio More...
Sup
Live from Lincoln Center
Now

1. Go to **http://kamu.tamu.edu**



2. Click "Listen Now"



KAMU-FM now broadcasting digital multicast HD Radio.

3. Choose "Original Format" or "Talk Radio"

Now you can listen to the "Computer Tip of the Week" on Wednesday at 7:30 a.m.

979.845.5611 | penny@kamu.tamu.edu

Take Charge of Your Online Reputation

An online reputation is the public perception of a person based on their online behavior and what is shared about that person by others.

From keeping in touch with friends and family, investigating a job applicant, to seeking information about a potential date, searching online about other people is a common occurrence. As online information about us proliferates, the effects of your online reputation on your personal and professional lives may increase.[1] Also, your information may be harvested for all the wrong reasons – such as identity theft and online fraud. Taking charge of your online reputation is important not only to avert misunderstandings or embarrassment – it helps thwart online thieves.

How can you manage your online reputation?

- Safeguard personal information online. Do not publically reveal your full birth date, address, or phone number.
- Be aware of how you are perceived online by searching for your name.
- Use privacy settings on social networking sites to limit who can view your full profile.
- Be diligent about removing embarrassing or false information by deleting unwanted comments or untagging photos.
- Separate your personal and professional online profiles, such as using Facebook and LinkedIn.

[1] Reputation Management and Social Media, Pew Internet & American Life Project, May 26, 2010 (**http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx**)

Featured **Service**

Help Desk Repair

Hands-on computer diagnostic, troubleshooting, virus removal services.

url.tamu.edu/helpdeskrepair | helpdesk@tamu.edu | 979.845.8300

Follow TAMU_IT on Twitter!

Facebook **Privacy Settings**

Facebook's recommended privacy settings reveal personal information that can be used by thieves to steal your identity. By default, anyone in a network you are a part of, including people who are not your friends, can see your full profile. To protect yourself, restrict your profile information to be viewable by only friends.

- Under "Settings," go to the "Privacy" section.
- Click "Profile."
- Change to "Friends Only."

Default settings allow Facebook to release information about you to all site sponsors, including what you like or find interesting, your location, and email address. Default settings also make your profile searchable by Google and other search engines.

Facebook does provide many options to customize privacy settings. However, these options can be difficult to understand by the average user. Sophos, a leading IT security firm, provides an online guide to walk you through setting up secure settings on Facebook (**www.sophos.com/security/best-practice/facebook/**).

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

1	2	3	■	■	■	4	5	6	7
8			9	■	10				
11				■	12				
13				14		■	15		
■	■	16				■	■	17	
18	19	■	■	20		21	22	■	■
23		24	■	25				26	27
28			29		■	30			
31					■	32			
33				■	■	■	34		

ACROSS

1. Secure wireless Internet
4. Avoid personal___ in your passwords
8. Direction
10. Gets dirty
11. Sore
12. Cloak
13. Protector
15. Environmental Protection Agency (abbr)
16. Taboo
17. Jr.'s Dad
18. Dad
20. Chew
23. Alternative (abbr.)
25. Make less pretty
28. After shower need
30. Guilty or not
31. Boss
32. Thick soup
33. Execute
34. National ID number you should protect

DOWN

1. Password made of real words or personal info
2. Walk back and forth
3. Pale
4. Note of debt
5. Before ten
6. What a pancake does
7. Movie award
9. Common sign of phishing email
10. Passwords with letters, symbols and numbers
14. Immerse
18. Download to fix vulnerable software
19. Hawaiian 'hello'
21. Swiss mountains
22. Droops
24. Bed size
26. Fines
27. Show boredom
29. Medical test

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

Mark Your **Calendar**

IT Forum

October 27, 2010

3:00 – 4:30 p.m.

Rudder 601

Mark your calendar for IT Forum. Chet Wisniewski from Sophos will present "How Hackers Become Millionaires." This unique presentation will describe the ways cybercriminals attack and how you can protect yourself.

Chet Wisniewski is a Senior Security Adviser for Sophos with 15 years of network security consulting experience. He works with the SophosLabs to develop in-depth analyses of network security threats.