

## Cyber Security Awareness Month

Apple iOS  
Vulnerability

We are all  
Responsible

IT Spotlight -  
Red Raider Shred

TTU IT -  
Social Media

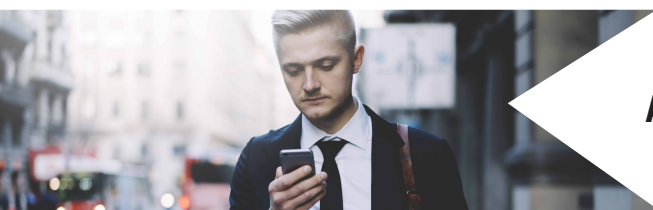
Like-farming

Encrypt to Secure

### Message from the CIO

The Department of Homeland Security, the National Cyber Security Awareness Alliance, and other government, education, and industries designate October as “Cyber Security Awareness Month.” The TTU Office of the CIO has been participating since the inaugural campaign 12 years ago, and this year we dedicate this bulletin to cybersecurity for “everyday” activities. As the threat to our personal and institutional data continue to rise, we provide practical information to help you navigate safely. **We are all responsible** for protecting ourselves, our families, and our businesses online, as well as keeping our personal and business information secure.

—Sam Segran, Associate Vice President for IT and Chief Information Officer



### Apple iOS Vulnerability

[askit.ttu.edu/iosupdate](http://askit.ttu.edu/iosupdate)

Apple has announced a serious vulnerability in Apple iOS (iPhones, iPads, iPod touch) recently. This vulnerability can be exploited if you access a malicious webpage, typically through a link sent through email or text message. If successfully exploited, an attacker could gain access to sensitive information on the device, including passwords, documents, or photos. In addition, if the device has applications that access sensitive information, the vulnerability puts any information accessed by that application also at risk. Criminals could also obtain access to the device's camera and microphone, giving the perpetrator the ability to record audio and/or video calls.

Apple has released a patch to correct this vulnerability in their latest update, iOS 9.3.5. You may find instructions for updating your iOS devices online at [www.askit.ttu.edu/iosupdate](http://www.askit.ttu.edu/iosupdate). The TTU IT Division recommends updating your

iOS devices as soon as possible to keep your information safe!

As a reminder the following cybersecurity practices can help protect your information, TTU data, and information resources:

- Do not click on links or open attachments contained within an email unless you are certain of the sender's identity and expecting the information;
- Delete and do not reply to any of these emails;
- Update your desktop, laptop, and/or mobile device anti-virus software;
- Do not download and install applications from unknown or untrusted sources; and
- Keep current on critical system updates:
  - » Windows: [www.askit.ttu.edu/windowsupdate](http://www.askit.ttu.edu/windowsupdate)
  - » Mac: [www.askit.ttu.edu/macupdate](http://www.askit.ttu.edu/macupdate)
  - » iOS: [www.askit.ttu.edu/iosupdate](http://www.askit.ttu.edu/iosupdate)

### We are all Responsible

[depts.ttu.edu/infotech/security](http://depts.ttu.edu/infotech/security)



As employees of a state institution and in the course of our work duties, we all have a responsibility to protect institutional information resources and data, especially confidential information, such as social security numbers, student grades, home addresses, financial information, etc.

Please review the relevant TTU IT Security policies at [www.depts.ttu.edu/infotech/security](http://www.depts.ttu.edu/infotech/security), specifically, the policies on Acceptable Use, Information/Data Classification, and Privacy that address individual responsibility to safeguard confidential data.



## IT Spotlight – Red Raider Shred

[depts.ttu.edu/services/redraidershred/](https://depts.ttu.edu/services/redraidershred/)

For the past several years the TTU Information Technology Division and TTU Operations Division has partnered to provide the TTU campus with affordable, on-campus document shredding – Red Raider Shred. A big Double T thank you to the Operations Division for collaborating with us, and providing this valuable service to the TTU community. Call Red Raider Shred at (806) 742- 8327 (TEAR) to schedule a pickup or regular service.

For additional information and service details, please visit [www.depts.ttu.edu/services/redraidershred/](https://www.depts.ttu.edu/services/redraidershred/). Go Team, Go Tech, Go Green!

Pictured above left-to-right: John Thomas and Jeff Barrington (IT Division); Danny Chavira and Evan Putnam (Operations Division).

## TTU IT - Social Media

[cybersecurity.ttu.edu](https://cybersecurity.ttu.edu)



To complement our cybersecurity website, we have designed a social media presence on Facebook, Twitter, and Instagram. Follow us and share our pages to help spread awareness during cybersecurity month and keep up-to-date on all of the events we are hosting this month. You can find our social networking links at [www.cybersecurity.ttu.edu](https://www.cybersecurity.ttu.edu).



## Trend in Online Scamming: Like-farming

Facebook users may unknowingly be promoting malicious content due to a new trend amongst Internet scammers called “like-farming.” Liking pages on Facebook may now have some unintended consequences. Criminals create posts that play on emotions or grab your attention with free deals and click-bait articles. It’s important to check your “Activity Log” for any suspicious content, that you can “unlike”, delete, and report to Facebook.

Other common characteristics of “like-farming” attempts:

- Posts that promise to raffle off expensive gifts if it is “shared” and “liked”;
- Invitations that ask a user to “like” or “share” to show appreciation;
- Any solicitations that thrive on the good nature of people and to play to their emotions; and
- Sites that appear on your news feed identifying people that have also “liked.”

## Encrypt to Secure



Mobile computing devices are easy targets for theft. When mobile devices containing confidential and sensitive data are stolen or compromised, institutional data, information resources, and individual identity are placed at risk.

If you have a business need to store and/or transfer confidential or sensitive information on your mobile device and have no viable alternative, the TTU IT Division offers the following

resources for the TTU Community:

- **Mobile Phones/Tablets:** Use one of the devices with internal security features - contact ITHC for a recommended list.
- **Laptops:** TTU IT provides Symantec’s PGP Whole Disk Encryption software for Windows and Mac operating systems. Contact your departmental IT support or ITHC at (806) 742-4357 (HELP) or via email at [ithelpcentral@ttu.edu](mailto:ithelpcentral@ttu.edu).

Mail | Mail Stop 2008

Phone | 742-5151

Fax | 742-5155

**View IT Bulletins online at**  
[infotech.ttu.edu/itbulletin](https://infotech.ttu.edu/itbulletin)

**Need IT assistance?**

IT Help Central  
(806) 742-4357 (HELP)  
[ithelpcentral@ttu.edu](mailto:ithelpcentral@ttu.edu)



Copyright 2016 Texas Tech University

**Computer-Based Training (CBT):**  
[www.cbt.ttu.edu](https://www.cbt.ttu.edu)