TEXAS TECH UNIVERSITY
Office of the
Chief Information Officer™

From Here, It's Possible

Information Technology Division | Bulletin

vol.12 no. 9 | June 2016

MESSAGE FROM THE CIO

TTU has completed another successful spring culminating in graduation celebrations. As we approach the summer vacation months, Internet criminals remain active during this time. In this bulletin, we highlight **Dell inventory scams**, and **Ransomware**. We also provide information on **"free" Internet services that pose risk to TTU data and information resources - Weebly and Cloud-hosted storage sites.** Finally, please review IT Security risks associated with **the discontinuation of Apple QuickTime for Windows**. Remember to practice cybersecurity as you enjoy the summer!

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

WEEBLY WEBSITES COMPROMISED

Websites hosted at weebly.com were recently compromised by Internet criminals, and some TTU faculty, staff, and students who were using the site had their account credentials stolen. The criminals used these credentials to send "phishing" emails to TTU mail servers. Although the TTU IT Division blocked the service as quickly as possible, some members of the campus community still received these email messages, responded, and had their account credentials stolen.

Because of attacks from these public, unregulated, and anonymous websites, access to the weebly.com domain has been blocked from the TTU network. As an alternative, TTU provides secure, centrally-supported tools for faculty to use.

Here are some popular tools used by faculty and students:

- Blackboard Learning Management System – a learning environment, with assessment and collaboration tools;
- Microsoft SharePoint – a collaboration environment with secure document sharing features;
- TTU Websites – areas and departments use OmniUpdate to create, maintain, and protect university web materials;
- Confluence Wiki – a blogging and collaboration tool that aids peer review, team editing, and document delivery;
- Mediasite – a solution for video-delivered content;
- Personal TTU Website (MyWeb) – campus-hosted webspace; and
- Skype for Business – a collaboration and communication tool – many instructors use this medium for office hours.

RANSOMWARE

Ransomware is malware (malicious software) used for extortion. Using ransomware, Internet criminals can take control of a computer, including the files and information stored on it, and hold them hostage until a ransom is paid. Cyber criminals hold your information and system hostage by either blocking access to the computer or encrypting the files.

As with most spam and phishing schemes, ransomware is usually introduced through email, enticing the reader to visit a website or open an attachment. Ransomware can also be distributed by pop-up windows on public websites that have been compromised. Some Internet criminals cleverly impersonate credible authorities or organizations. Other ransomware scams trick the user into thinking they have done something illegal and are being contacted by law enforcement or other authority.

Once a system or device is infected with ransomware, the user receives a hostile communication outlining the terms of the ransom. Unfortunately, those that pay the ransom often do not get full system and data access returned, and they could be subject to further identity theft.

<u>Be on guard and protect yourself against ransomware and other Internet-based criminal activities:</u>

- IMPORTANT! Backup your system regularly (automate backups to another location);
- If the data is very important, keep a second copy on offline media (maintain required compliance, e.g. encrypted if required);
- Install anti-virus and anti-malware software, and keep them updated;
- Be aware of current trends in scams and malware;
- If an email, pop-up, or website seems suspicious, or if you have doubts about its validity, do not open the email or click on the pop-up;
- Do not install software, plugins, or extensions unless you know they are from a reputable, legitimate source;
- Be aware of phone calls purporting to be from Microsoft, Apple, or Dell, offering to "fix" your computer;
- Maintain operating system and application updates - it is recommended that you configure your system to install automatic updates. If your Windows system is on the domain, it will have the automatic updates already configured for security:
  - » Windows Users: Select "Windows Update" from your Windows Control Panel. Additional information for installing Windows Updates is available at: *http://www.askit.ttu.edu/windowsupdate*; and
  - » Mac Users: Use Software Update in System Preferences.

If you believe that your system is infected with ransomware, shut down your computer and contact your area or department IT professional. For more information or questions about ransomware on TTU-owned systems, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu. You can find additional cybersecurity tips at *www.cybersecurity.ttu.edu*.

APPLE ENDS SUPPORT OF QUICKTIME FOR WINDOWS

Apple announced that they will no longer provide security patches for QuickTime for Windows software. Additionally, the United States Computer Emergency Readiness Team (US-CERT) recently discovered two new vulnerabilities within QuickTime (*source: https://www.us-cert.gov/ncas/alerts/TA16-105A*). This does not affect QuickTime for Mac.

The TTU IT Division recommends uninstalling QuickTime for Windows from your system immediately to protect your personal data, and TTU data and information resources. Instructions for uninstalling software from a Windows system may be found at *www.askit.ttu.edu*.

In addition, users hosting QuickTime videos online (.mov format) should convert these videos to a different file format. A good alternative is the .mp4 (MPEG-4) format — this software offers the same functionality as QuickTime.

DELL SERVICE TAG SCAMS

The TTU IT Division warns the TTU Community of an active phone-based scam targeting Dell computers purchased between 8/15/15 and 11/15/15. Due to a security flaw that Dell has disclosed, scammers are able to obtain technical information identifying a computer, such as a Dell Service Tag or Express Service Code. Currently, Dell has no evidence that credit card information is implicated in this scam.

Once a scammer has obtained system information, they will call a system owner, posing as a Dell employee, and state that their computer is infected, at risk of infection, or is exhibiting suspicious behavior. The scammer claims that they can correct the problem by installing software or tools on the system. If the user questions the authenticity of the call, the scammer will provide stolen information about the computer as proof that they are legitimate.

Please note that this vulnerability only affects systems with operating systems installed by Dell. If you have reformatted or re-imaged your computer, then the vulnerability has been removed. Additionally, as TTU IT images all computers before distributing them, any system that has been set up by ITHC Desktop Services will not be vulnerable. The TTU IT Division recommends these steps to protect yourself from this scam:

- Scan your computer to determine if your system is vulnerable at *https://zmap.io/dell/*. Note: You will need to perform this scan on all web browsers on your system;
- If your system is vulnerable (contains the faulty certificate), Dell has provided instructions for you to follow at *https://dellupdater.dell.com/Downloads/APP009/eDellRootCertRemovalInstructions.docx*; and
- If you receive a call that matches the description above, hang up immediately and report the scam to Dell at *https://marketing.dell.com/reportscams*.

STORING INSTITUTIONAL DATA IN UNAUTHORIZED CLOUD SERVICES

State and federal regulations restrict certain types of institutional and/or personally identifiable information (PII) from being stored in and/or transmitted over public networks and commercial/cloud storage facilities, such as Dropbox, without sufficient protections and access controls. The restricted data types include, but are not limited to:

- Data designated by the University data owner as "Confidential", such as:
  - » Student data protected by FERPA;
  - » Personally identifiable information (PII) such as SSN, date of birth, and driver's license numbers;
  - » Payment card information; and
  - » Data or media files subject to copyright protections.
- Data designated by the University as "Sensitive", such as:
  - » TTU proprietary data, intellectual property, or sensitive research data; and
  - » Security information such as account/access profiles.

TTU faculty, staff, and researchers often have authorized access to restricted data, and it is their responsibility to protect it from unauthorized release. Examples include:

- Emailing restricted data to unauthorized individuals;
- Losing unencrypted restricted data stored on a mobile or portable storage device;
- Storing unencrypted restricted data on a public/commercial website or service (such as Dropbox, GoogleDocs, etc.);
- Sharing of eRaider account credentials in response to phishing emails, or with colleagues, peers, or assistants; and
- The use of peer-to-peer file sharing services to distribute copyright protected materials.

To protect institutional data and resources, the TTU Office of the CIO must review and approve the use of any cloud-based services or third parties to store, transmit, or process restricted data.

We Are All Responsible

www.cybersecurity.ttu.edu

TEXAS TECH UNIVERSITY
Office *of the*
Chief Information Officer™

Mail Stop 2008
Phone: 742-5151
Fax: 742-5155

cybersecurity.ttu.edu

Contributions by: Sam Segran, Katherine Austin Beltz, Ph.D., Jeff Barrington, Logan Beaty, Devyn Bracken, Kailyn Cox, Scott Hall, Brandon Navarre, Yung Ng, Randall Osborne, Adrianna Robertson, Amanda Salazar, and John Thomas.
Cybersecurity Practices Committee: Sam Segran, Katherine Austin Beltz, Ph.D., Jeff Barrington, Daniel East, Scott Hall, Carlene Kelly, Brandon Navarre, Yung Ng, Chris Oglesby, Randall Osborne, Nathan Rogers, Amanda Salazar, Mike Simmons, Alan Sill, Ph.D., J Stalcup, John Thomas, and assistance from IT Division staff.

Scan the barcode to
view IT Bulletins online
www.infotech.ttu.edu/itbulletin

IT Website:
www.infotech.ttu.edu

Texas Tech University Website:
www.ttu.edu

Computer-Based Training (CBT):
www.cbt.ttu.edu

Cybersecurity Practices:
www.cybersecurity.ttu.edu