ISO NEWSLETTER

www.utrgv.edu/is

The University of Texas Rio Grande Valley™

Information Security Office

VOLUME I, ISSUE II NOVEMBER 23, 2016

INSIDE THIS ISSUE:

EDITOR

Francisco Tamez

ISO Security Analyst

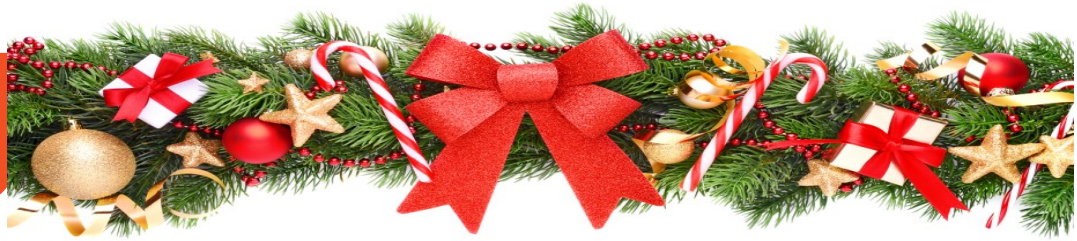
Happy Holidays!

The UTRGV Information Security Office (ISO) would like to wish you a safe and happy holidays. It is November and as you are getting started for your holidays shopping or planning to visit your loved ones, we would like to thank you for your support, for reading this newsletter, and for taking an interest in Information Security.

The ISO would also like to share a few security tips and hopefully you will share them with friends and family.

Some basic security reminders to help you start the holidays:

1. While shopping online look for the "s" in https:// due to the fact that these sites take extra security measures. It will protect you against many forms of surveillance and account hijacking, and some forms of censorship.
2. Share with care and do not broadcast your location on social media. This tells thieves you are not home. Visit our Social Media Access Controls campaign 'Don't get SMACked' (bit.ly/2fTPJSc) to learn more about privacy.
3. Stop. Think. Connect. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. (bit.ly/2fDvn0p)
4. Start organizing your passwords with a password manager (e.g., www.lastpass.com) where you can easily remember your password and everything is kept secure.
5. Update your banking information and password, also ask your bank if they offer two factor authentication in order to add an extra layer of security to your account.



ANNOUNCEMENTS

EOL Software
Software applications have a lifecycle. The lifecycle begins when the software is released and ends when it is no longer supported by the vendor, also called End Of Life (EOL). When software stops being supported by the vendor, it no longer receives security updates.

EOL OS
Windows XP and Apple OSX 10.6 and below are EOL. If you are currently using an EOL Operating System (OS) you should upgrade your OS to maintain the security of your computer and data. Computers owned, leased or managed by UTRGV must adhere to the Computer Security Standard, (bit.ly/2fgljsz) which requires them to run only vendor supported OS. Vista will be EOL in April of 2017, so plan to upgrade this OS soon.

QuickTime EOL
Apple announced that it will no longer support QuickTime for Windows. Windows computers installed with QuickTime can be vulnerable to malware. The ISO strongly recommends that all Windows users uninstall QuickTime.

UTRGV Computer Domain Migration Project Update
This project entails transitioning all University computers from the legacy domains to the UTRGV domain.

If your computer is still pending migration, you must submit a Service Request through ServiceNow to schedule an appointment. When submitting the Service Request, please make sure to include the following information:

- UTRGV email address
- Computer Tag number(s)
- Location
- Phone number(s) and/or cellphone
- Available times and dates for IT to contact you

Contact IT Service Desk for any technical issues.
956-665-2020 (Edinburg)
956-882-2020 (Brownsville/Harlingen)

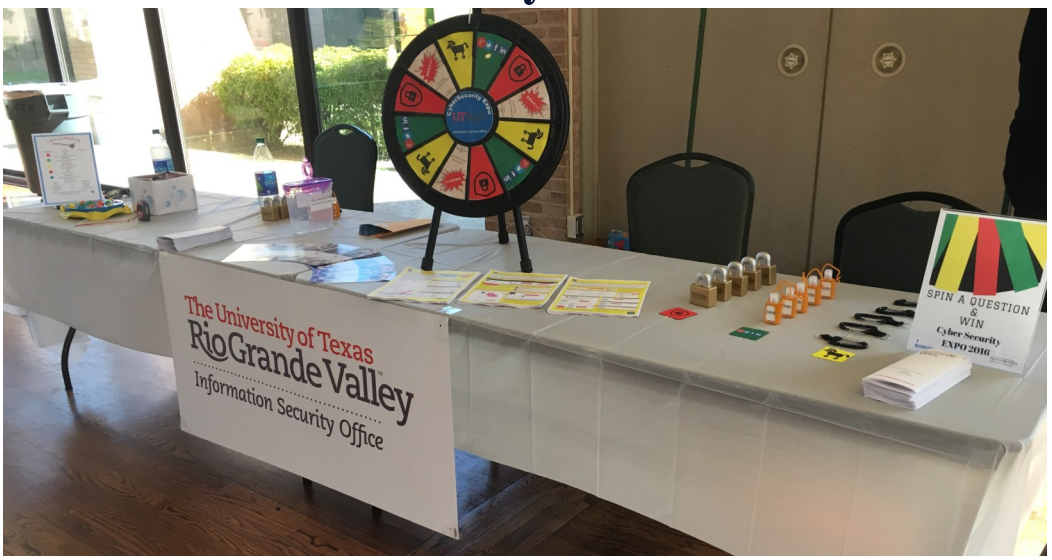
Office 365: Security and Compliance Data Loss Prevention (DLP) Feature

On November 15, a new security feature was implemented to enhance Data Loss Prevention (DLP) efforts at UTRGV. This security feature provides warning file icons and email notifications when personal information such as credit card numbers and/or social security numbers are being shared through OneDrive, Office 365, or email.
The files are not read but scanned to see if data matches social security number and/or credit card number patterns. This does not occur immediately. The time needed for warning icons to appear and email notifications to be received vary since OneDrive, SharePoint and email are hosted offsite by Microsoft.

Today's EOL products
Please update if you are using the following products with these versions or below.

Product	Version	Product	Version
Adobe Acrobat X	10	Adobe Flash Player	19
Adobe Reader	9.x	Java SE	5
Adobe Flash Media	4.5		

What did you miss?



October NCSAM

October was the National Cyber Security Awareness Month (NCSAM), administered by the Department of Homeland Security.

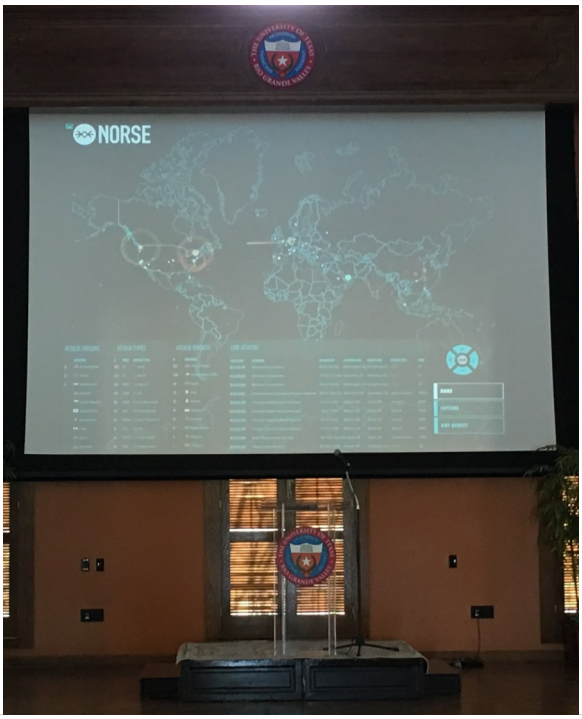
Throughout the month of October the ISO discussed several cyber security topics such as the use of malware by online criminals, theft of intellectual property, internet fraud, identity fraud, cyberstalking, and more. Our office provided weekly cyber tips in October through our News Blog, feel free to check our website and social media!

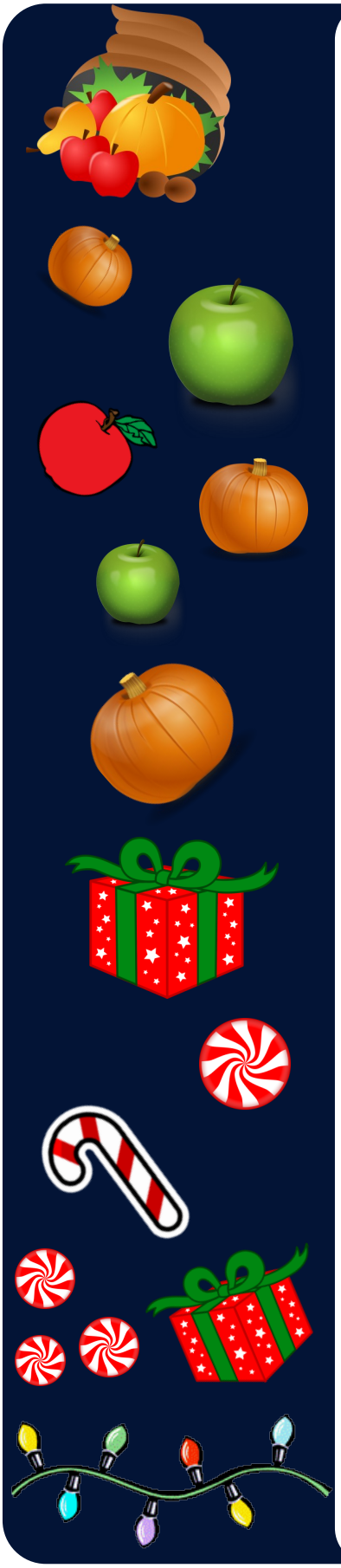
Cyber Security Expo

On October 11 the ISO conducted the first Cyber Security Expo in the campus of Edinburg at the ballroom. More than 110 UTRGV students, faculty, and staff attended the event.

Similarly the ISO conducted the first Cyber Security Expo in the Brownsville Campus at Plains Capital El Gran Salon on October 31.

More than 70 UTRGV students, faculty, and staff attended this event, 13 students from Instituto Tecnológico De Matamoros were able to take part of the Expo as well.





What to expect next year 2017?

ISA Trainings

The ISO will begin to search for Information Security Administrators (ISA) for each academic department in UTRGV. ISA's will act as a conduit between the ISO and all the departments and colleges. This will help build pathways of communication to ensure both employees and the ISO are kept informed of topics and issues affecting security.

Current ISO Projects

Our office is currently working on several projects that will enhance asset and vulnerability management for computers in our University. The ISO is currently improving methods of asset discovery, inventory, classification of data, and data loss prevention.

Leaving for vacation?

If you are planning on your winter vacation and you will not be using your office computer, then don't forget to turn it off. By leaving your computer off you are protecting your information and you are saving energy at the same time!

Online Holiday shopping is here!

Being safer and more secure while shopping online is a high priority during the holiday season, a key time for online gift buying. This year's Cyber Monday—which falls on November 28—is predicted to be the biggest and busiest ever, generating $3.36 billion in sales with 9.4 percent growth compared to 2015.

Read more: bit.ly/2fi50wu

New computer, smartphone or tablet?

Please take into consideration the following ISO tips:

- Update your device and enable automatic updating.
- Pay attention when configuring your new device for the first time, especially the privacy options
- Be carful of what apps or features you allow to synchronize.
- Try to understand what personal information the device collects, how is being used and how it is stored.
- Keep your antivirus updated.
- Change the password on the device before using it.

Passwords are like...

- **Riddles:** Should be hard for others to guess.
- **Passphrases:** The longer the better.
- **Toothbrush:** Use different passwords for each account.
- **Underwear:** Never share your password with others.

ISO Spotlight

The ISO Spotlight interviews an individual that plays a role in UTRGV or information security. In this issue, you will meet Dr. Jeffery A. Graham, who is UTRGV's Chief Information Officer.

Dr. Jeffery A. Graham
Chief Information Officer
The University of Texas Rio Grande Valley

1. Who are your customers, and what is one of the most challenging areas for you?
Faculty, students, staff and visitors. It creates a challenge to give them ubiquitous services they expect when each have different needs and abilities.

2. What do you like best of your job?
The chance to solve problems, the harder the more satisfying.

3. Tell us how information security has changed since you started in your role.
Information security's importance is much more recognized and taken more seriously at the same time the complexity of the attacks has increased.

4. Top 3 life highlights:
- My marriage to Rosario
- The birth of my 3 daughters
- And moving to the valley in 1988, as none of it would have been possible if I hadn't taken that chance.

5. People would be surprised to know:
That I was married in Mexico and hadn't yet learned Spanish, so I didn't understand most of what went on in the ceremony :J

6. Which CD do you have in your car? Or what radio station do you listen to?
Band A of my radio is set to scan the local ham repeaters and Band B scans the local Air Traffic control frequencies.

7. If you could interview one person (dead or alive) who would it be?
Steven Hawkins, I am fascinated with astrophysics, quantum physics, relativity, etc. I wouldn't understand the conversation but I would enjoy it.

8. If given a chance, who would you like to be for a day?
One of the lunar astronauts, when I was a child I always assumed I would one day walk on the Moon.

9. What is the best advice that you have received and that you have used?
Dress and act to the job you want, not the job you have.

10. What is one thing you couldn't live without?
My coffee cup!

11. What would be your advice for a new IT professional?
Technology changes very rapidly and if you need to keep learning there will always be lots of opportunities.

Student Association Spotlight

Student Association Spotlight features a student association in UTRGV. In this issue, you will meet the Association of Information Technology Professionals.

If you or your student association is interested in appearing in this newsletter feel free to contact the ISO.

Association of Information Technology Professionals

Association of Information Technology Professionals is an organization that is committed to providing its members with experience that will enhance their academic and professional careers; with activities such as community engagement, hands on training, and competitions. As an organization here at The University of Texas - Rio Grande Valley, we provide our members with topics of discussion during our general meetings to inform them about the most common and interesting items relating to our major such as protocol analysis, port scanning, google hacking, malware removal, and command lines.

Visit our Facebook for contact or questions (http://bit.ly/2g3TzZT)
All majors are welcomed to join.

Protect Yourself

By: AITP

When entering college, it's a whole new world, filled with excitement and danger… through the internet.
As college students we go to Starbucks or any place where there is free Wi-Fi to do homework, projects, read or surf the internet. Yet, most of us are not aware of the risks we go through when connecting to public networks. Exposures that can affect you are theft, fraud, stalking and/or harassment, these are categorized as major risks that can harm you in every aspect of your life. It is important to keep in mind of the dangers that can happen when surfing the web. Here are a few dos and don'ts that can help you stay safe!

DOS	DONTS
Strong Pa$$w0rd5	Download free media
Get Virus and Spyware protection	Store payment information online
Get Pop-Up Blocking	Overshare personal information
Account Monitoring	Click unfamiliar links
Backups	Give out bank account info
	Give out social security number

Featured Article

By Thomas Owen
UTRGV CISO

With the explosion in new communication platforms, hackers are moving swiftly to capitalize in every way they can. While Facebook, MySpace, Twitter and other social networking/blogging sites used to be the domain of Generation Y, the trend is now for people of all ages to use these sites to keep in touch and spread information. However, the problem is you never know exactly what information is being spread and to whom.

For instance, consider the case of two employees of a large US financial firm that made news a few months ago. For simplicity's sake, we will call them Jack and Jill. Both had Facebook accounts, were Facebook friends, and sometimes communicated outside of work. Sounds like an innocent friendship, right? It was, until hackers were able to take control of Jack's Facebook account. The hackers then sent Jill a simple message, "Look at the pictures I took of us at the company picnic." Jill clicked on the link, expecting to see pictures from the picnic. Instead, she downloaded malicious software, allowing the hackers to take control of her company laptop. I'm sure you can see where this is headed: The attackers were then able to use her credentials to access the company's network. The breach went undetected for approximately two weeks.

This example illustrates how the growth of social media, coupled with a lack of awareness among employees and employers regarding personal and potential business use, can increase an institution's reputational, liability, and operational risk exposures. This increase can be attributed to the institution having a social networking presence to reach customers, employees accessing social networking sites at work, and employees accessing social networking sites on institution-owned computers at home.

How can organizations manage this risk?

Treat social media as any other type of risk: Include social media in a formal risk assessment process. This risk assessment should help you gauge the level of risk, identify existing controls, evaluate the need for additional controls and ultimately, help the bank determine its approach to the use of social media by employees. All decisions should be based on this risk-based process.

What types of controls are available?

Controls will vary by organization, but some examples include technical restrictions, addressing social media in the Acceptable Use Policy (AUP) or as a specific policy, and security awareness training for employees.

Technical controls usually provide the greatest (but sometimes a false) peace of mind. Hardware appliances or software can be used to filter websites by web address, content, or category. Organizations can also set up a proxy server to force users through a filtering process even when users are physically offsite.

Identifying social media use in the AUP or a specific policy will help organizations provide guidelines for employees and mitigate risks, especially reputational risk. The policy framework should address whether social media can be used on organization-controlled systems (both at work and at home) and what information an employee is allowed to disclose regarding the organization and organizational activities.

Security awareness training for employees regarding social media is an ongoing process. It is not adequate to expect users to sit in a room for 8 hours once a year and retain that knowledge until the next annual training. Posters, memos, and emails regarding the evolving social media landscape can serve as reminders to be vigilant both at the workplace and at home. If there is a virus outbreak on frequently-visited sites (such as the Koobface worm on Facebook), use the occasion to inform employees about the hazards.

NEWSWORTHY SECURITY ARTICLES

Cyber Monday: Be aware of "phantom stores" with these 5 tips
AS you shop for the perfect holiday gift, hackers are shopping for you. This time of year is rife with email scams, deceptive advertising and criminals lurking to steal information from vulnerable devices and unwary shoppers.
(cbsn.ws/1y4cfcS)

Beware, iPhone Users: Fake Retail Apps Are Surging Before Holidays
Hundreds of fake retail and product apps have popped up in Apple's App Store in recent weeks — just in time to deceive holiday shoppers.
(nyti.ms/2fBmbtY)

Arizona man arrested for hacking email accounts at universities
An Arizona man was arrested on charges that he hacked into over 1,000 email accounts for students and others at two universities, including Pace University in New York, and tried to do the same at 75 other higher-education institutions.
(reut.rs/2eCPEIZ)

These and other articles can be found at: www.utrgv.edu/is/en-us/news-and-alerts/

If you need to report an incident

Visit our website (www.utrgv.edu/is) if you need to report a security incident. Some incidents may require you to report them to both the ISO and the UTRGV Police Department (PD) or to Information Technology (IT). For example any loss or theft of a University owned computer (e.g. workstation, laptop, smartphone, tablet) has to be reported to the ISO and the UTRGV PD. Similarly, ransomware infected UTRGV owned computers must be reported to ISO and IT.

REPORT INCIDENT

The University of Texas Rio Grande Valley™

Information Security Office

1201 W. University Drive
Sugar Road Annex (ESRAX) Building
Edinburg, TX 78539

Phone: (956)665-7823
Fax: (956)665-3154
Email: is@utrgv.edu

Visit us on the web and social media!
www.utrgv.edu/is www.facebook.com/utrgviso

The mission of the Information Security Office is to provide support to the University in achieving its goals by ensuring the security, integrity, confidentiality, and availability of information resources. The role of the Chief Information Security Officer (CISO) is to maintain oversight and control of the enterprise information security program for the University.

Services We Provide

GOVERNANCE, RISK AND COMPLIANCE

ASSET AND VULNERABILITY MANAGEMENT

ENGINEERING AND INCIDENT RESPONSE

AWARENESS, COMMUNICATION AND OUTREACH