ISO NEWSLETTER

www.utrgv.edu/is

The University of Texas Rio Grande Valley™

Information Security Office

VOLUME I, ISSUE III

JANUARY 19, 2017

INSIDE THIS ISSUE:

Happy New Year!

The UTRGV Information Security Office (ISO) would like to wish you and your families a happy New Year. Hopefully one of your new years resolution will involve information security at home and work, in the instance that you have not added this to your list don't worry there is still plenty of time.

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

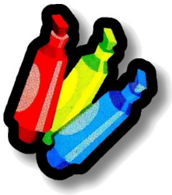
Some basic security reminders to help you start the year:

1. Beware of Tax Scams! The IRS saw an approximate 400 percent surge in phishing and malware incidents in the 2016 tax season. (www.irs.gov/uac/tax-scams-consumer-alerts)
2. System & Data Backups: Ensure you backup important documents, irreplaceable pictures and videos. Do not let hardware failure, malware or cryptoware get your data. Cloud sync services like OneDrive and Dropbox are not suitable backup solutions.
3. Computer Health: Check monthly for Operating System (OS) and program updates. Remove any unsupported or unneeded programs and services.
4. Change your passwords regularly: UTRGV passwords must be changed at least yearly, but you can change it more often if needed. Follow this tip for your banking and social media accounts!
5. 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.
6. Secure your mobile devices (like laptops and tablets) by not leaving them visible in your car, password protecting access to them, and by physically securing them when unattended.

EDITOR

Francisco Tamez

ISO Security Analyst



SECURITY HIGHLIGHTS

Black Friday and Cyber Monday 2016 report

U.S. ecommerce revenue reported that Black Friday 2016 was the first day to "generate more than a billion dollars in online sales from mobile devices, according to Adobe." Similarly Cyber Monday saw an increase of 12.1 percent achieving a new record with "$3.45 billion spent online" (bit.ly/2iLmW4p).

It is clear that this trend will most likely continue for the new year and as the sales event takes place it still remains the possibility of fraudulent sales and fake advertisement.

Despite the threats online by educating ourselves, sharing tips with family, and friends we can combine our efforts to be safe online. In addition the ISO will always stand guard and share with the public any vulnerabilities online and any other topics of interest to you.

Yahoo second data breach

Based on further analysis of data by the forensic experts, Yahoo believes an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts.

Yahoo is notifying potentially affected users by email and posting additional information to Yahoo's website. Additionally, Yahoo is asking potentially affected users to promptly change their passwords and adopt alternate means of account verification. The UTRGV Information Security Office (ISO) highly recommends that any Yahoo user to promptly change their passwords, security questions, and answers.

For potentially affected accounts, the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. (bit.ly/utrgvisonews2YDB)

Pros and cons of your Medical ID in the Health app on your iPhone

If you have the latest version of iOS for your iPhone then you can set up a Medical ID in the Health app in order to access important health information. Medical ID helps first responders access you critical medical information (e.g., medications, medical conditions, and allergies) from the Lock screen, without needing your passcode (apple.co/2jbf7I7).

The questions here would be who really has access to your critical medical information? And what other information is stored in this application? The answers would be: first responders, nosy coworkers, prying family members, or anyone who gets physical access to your iPhone for 15 seconds, and "in addition, the phone numbers and names of your emergency contacts, and their relationship to you, will also be viewable, which introduces identity theft or phishing concerns. You'll therefore need to weigh the risks and benefits of having this information easily accessible via your iPhone." (bit.ly/2j4xmNy)

What to expect this semester?

ISA Trainings

With the help of the academic departments in UTRGV the ISO has founded the Information Security Administrators (ISA) group. The ISA’s will act as a conduit between the ISO and to these departments and colleges. This partnership will help build pathways of communication to ensure both employees and the ISO are kept informed of topics and issues affecting security.

January is the National Stalking Awareness Month (NSAM)

In January 2004, the National Center for Victims of Crime launched NSAM to increase the public’s understanding of the crime of stalking. NSAM emerged from the work of the Stalking Resource Center, a National Center program funded by the Office on Violence Against Women, U.S. Department of Justice, to raise awareness about stalking and help develop and implement multidisciplinary responses to the crime.

In 2011, the White House issued the first Presidential Proclamation on National Stalking Awareness Month. President Obama’s proclamation stressed the millions affected by the crime, its often-devastating consequences, the difficulty of identifying and investigating the crime, and the federal government’s strong commitment to combating stalking. (stalkingawarenessmonth.org)

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.

Mac Encryption solution

The currently installed version of SecureDoc, UTRGV’s encryption management solution for Mac OSX, does not support the latest OSX version Sierra. IT is researching a better solution to manage OSX encryption and Mac endpoint management, to include both OSX and iOS.

Retirement of UTB and UTPA domains

The UTB and UTPA legacy domains will be retired this summer. Users with accounts or computers still on these legacy domains run the risk of losing computer and file access. It is critical that computers be migrated to the UTRGV domain as soon as possible. Avoid a last minute rush and submit a service request with the IT Service Desk to get migrated before the summer.

Data privacy day

Respecting Privacy, and Safeguarding Data and Enabling Trust is the theme for Data Privacy Day (DPD), an international effort held annually on January 28 to create awareness about the importance of privacy and protecting personal information.

DPD is the signature event in a greater privacy awareness and education effort. The National Cyber Security Alliance (NCSA) educates consumers on how they can own their online presence. NCSA’s privacy awareness campaign is an integral component of STOP.THINK.CONNECT .-the global online safety, security and privacy campaign. (www.staysafeonline.org/data-privacy-day/about)

ISO Spotlight

The ISO Spotlight interviews an individual that plays a role in UTRGV or information security. In this issue, you will meet *Senior Information Security Analyst* Daniel Ramirez .

Daniel Ramirez
Senior Information Security Analyst
The University of Texas Rio Grande Valley

1. Tell us how information security has changed since you started in your role.
Security is everywhere now because the internet is in everything. As more people and more things become connected to the internet, security becomes increasingly important. A hacker, thousands of miles away, could potentially connect to an internet accessible security camera inside a building and use it to breach security and access restricted areas. This could be someone's home or the nations electrical grid. We live in a new era know than we did just 10 years ago.

2. Who are your customers, and what is one of the most challenging areas for you?
My customers are the students, faculty and staff of UTRGV. One of my most challenging areas is ensuring that each of my customers has the knowledge needed to keep both UTRGV information resources and personal information resources safe and secure.

3. How did you come into the security field?
I grew up with a fascination for computers and programming, before the internet. As computers began to be connected to the internet, I was intrigued by the technologies that were required to secure computers from threats. Threats increased exponentially over the years as the world learned how to hack and this shifted my fascination into ethical hacking and cybersecurity.

4. Top 3 life highlights:
Finding my wife
Births of my kids
Getting a career in Cybersecurity

5. People would be surprised to know:
I like to tinker with woodworking.

6. Which CD do you have in your car? Or what radio station do you listen to?
A self-made mix of over 100 rap and hip-hop songs from the 80s through the new century.

7. If you could interview one person (dead or alive) who would it be?
My great-great-great grandfather. It would be awesome to know about my ancestral history.

8. If given a chance, who would you like to be for a day?
My 6-year-old, to see the world through her eyes, be a kid once more, and see how I am doing as a dad.

9. What is the best advice that you have received and that you have used?
Life is short, enjoy every minute of it.

10. What would be your advice for a new security professional?
Don't do it! LOL. No, in all seriousness security is a great field but it is very dynamic. As technologies change, so do the potential threats and security professionals need to always be learning and vigilant of everything.

Featured Article

By Cesar Pastore
UTRGV Information Security Analyst

Protecting your data in your USB flash drive

As USB flash drives have continued to decrease in price and increase in storage, they have become a popular item to purchase during the holiday season. At the same time, during the last several years, users have become more sensitive about securing information stored in their USB devices. This shift in mentality may be driven by different factors including work related requirements or personal experience with the loss of one of these personal devices. For users looking to secure their USB device there are a number of options available to address USB flash drive security. Generally speaking, even the simplest non-encrypted USB flash drive can be properly secured by taking appropriate steps to encrypt the contents of the drive. Like any other product, options vary on the functionality of USB flash drive security available to users based on simple factors such as price, storage capacity and ease of use. In this short article I will cover three general levels of USB flash drive security including built-in PIN authentication, built-in software based authentication, and finally third-party software based encryption.

The preferred method for both encryption and password protection is hardware based encryption with a built-in security keypad. These devices are normally the most expensive in the market because of their high level of security and cross-platform compatibility. These devices can run in Windows based systems, Mac based OS or any other USB enabled device. These USB flash devices require the unlocking of the USB key with a programmable security PIN before the stored data can be accessed. An example of one of these USB flash drive devices would be the Apricorn Aegis Secure Key USB flash drive. The downside to these USB flash drive devices is the higher price of the drive when compared to simple un-encrypted drives. This price differentiation becomes more pronounced as the capacity of the USB flash drive increases.

A second set of devices offer an equivalent level of hardware based encryption but do so at lower cost, especially for devices at higher storage capacities. These USB flash drives provide no visible key-pad, and must instead be plugged into a compatible computer in order to enter a device password and unlock the drive. The main difference between these devices is that the drive must be plugged into a compatible PC/Mac computer in order for the password authentication program to execute and validate the correct password. These devices tend to be lower in price from their security PIN / key-pad counterparts, however they may not be as compatible.   Some examples of these type of USB flash drives include the Kingston Digital Data Traveler or the Integral Crypto Drive.

Finally, if you find yourself in possession of a USB flash drive with no built-in security features, encryption and password protection can still be obtained via operating system based functionality or third party application software. Depending on what type of operating system you are running, you may be able to utilize the built-in encryption functionality provided by Microsoft or Apple. Microsoft utilizes bitlocker for their drive encryption and Apple utilizes FileVault. The main drawback to these tools is that you are restricted on to using a Windows or Mac based system. Once the data has been encrypted the drive is not cross platform compatible. The upside is that these encryption applications come at no additional cost provided that you have a version of Microsoft or Mac OS supporting the functionality. Finally, if you do not have operating system based encryption support like bitlocker or FileVault, you may choose to use an open-sourced third party application such as VeraCrypt or, for a fee, any number of third-party applications that will offer software based encryption protection for your USB flash drives.

These three general levels of USB flash drive encryption should give users a general idea of the different levels of USB flash drive security currently available. Given the different choices to protect your flash drive data from loss or exposure, it is easier than ever to encrypt your USB flash drive and rest assured that your data is protected and secured.

ISO GUEST

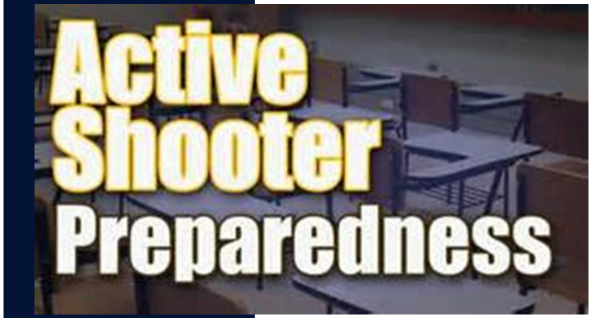
THE UNIVERSITY OF TEXAS RIO GRANDE VALLEY

POLICE DEPARTMENT

About UTRGV PD:

Protects and serves the campus community of students, faculty, staff and visitors throughout the Rio Grande Valley Region by providing professional law enforcement services and actively promoting community involvement through progressive community policing partnership strategies and a commitment to education. We are open 24 hours a day, 7 days a week.

Important Personal Safety Info!



CIVILIAN RESPONSE TO

ACTIVE SHOOTER EVENTS

Are you Prepared? The possibility of being involved in an active shooter situation is a high risk threat. This workshop provides the knowledge, skills and attitudes required for effective responses to such threats. We'll teach you what to do and how to respond safely and decisively if you are caught in the cross fire.

Training Dates to be announced soon! For more information contact Officer Antonio Zarzoza, 956 665-2988.

Some Ways UTRGV PD Can Help Me!?

Police Escort:

Police escorts to vehicles/dorms on campus available 24/7 for students, faculty and staff.

Vehicle Assistance:

The University Police has special equipped units to provide **jump starts** and **assistance to unlock a vehicle**. A valid UTRGV Parking Permit entitles you to these services, give us a call at 956-665-7151 or 956 882-8232. We are Open 24/7 365 days year.

Additional ways UTRGV PD Can Help Me!?

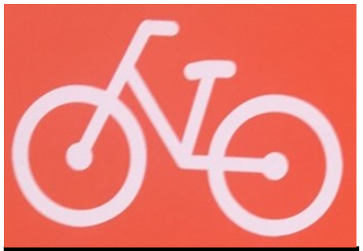
Lost and Found Information:

If you've lost something, please report it using our lost and found form. (www.utrgv.edu/police/services/lost-and-found) You may report lost items by telephone, but will **receive a swifter response reporting online**. Please be detailed in describing the item you have lost so we can tell your keys, for example, from the 30 other sets of keys turned in each month. Details that are helpful include: brand name, color, size, shape, model number, quantity, material (leather, plastic, fabric, metal,

Good Info to Know!

Preventing Bicycle Theft

- Register the bicycle with the Office of Parking and Transportation, 665-2738 (Edinburg) or 882-7051 (Brownsville)
- Keep bicycles locked any time they are unattended with a good "U" type lock. Second choice would be a good case- hardened padlock and cable. Be sure the "U" lock or cable goes through the front wheel and frame or rear wheel and frame, and secure it to a fixed object.
- Check the lock by pulling on it to make sure it is secure.
- Use an engraver to place an identifying mark on unpainted major bicycle components.
- During the day at home, keep the bicycle out of sight, or at least at the rear of the house.
- At night and when not at home, keep the bicycle inside a locked structure.
- Be sure to retain all evidence of purchase including the serial number.
- Be able to identify the bicycle…not only by its color, but by its features.
- Have one or more close up color photographs of the bicycle and its owner on hand.
- Never loan a bike to strangers.
- Try to avoid parking in deserted or poorly lit areas.



OPERATION ID

For the security of your bike a bicycle decal is required on your bike (FREE). Park only at available bike rack locations. For more information please contact the UTRGV Police Department (956)665-7151

Contact UTRGV PD

Edinburg Campus

On Campus HELP: 4357
On Campus Emergency: 911
Dispatch and Emergency:
(956) 665-7151

Police Station
Academic Services Facility
Bldg.
501 N. Sugar Road

Harlingen Campus

Emergency, Dispatch: (956)
882-8232

Police Station
2102 Treasure Hills Blvd.
Harlingen, TX 78550

Brownsville Campus

Dispatch: (956) 882-8232
Emergency: (956) 882-2222

Police Station
One W. University Boulevard
Brownsville, TX 78520

Email: police@utrgv.edu

Website: www.utrgv.edu/police

Facebook:
www.facebook.com/UTRGVPoliceDepartment

Twitter: www.twitter.com/utrgvpolice

DON'T
GET
SMACked
Check your
Social Media
Access Controls
utrgv.edu/is/en-us/
resources/social-media

WE
ARE
SOCIAL!
www.utrgv.edu/is
www.facebook.com/utrgviso

NEWSWORTHY SECURITY ARTICLES

FDA issues final guidance for medical device security.
With all the current concern over IoT being insecure from cyberattacks, the U.S. Food & Drug Administration (FDA) has posted the agency's final guidance for medical device safety. (bit.ly/2j8tGwE)

The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities.
These could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks, the FDA said. (bit.ly/2jvlU0f)

Los Angeles college pays $28,000 in ransomware.
Los Angeles Valley College in Valley Glen said it paid $28,000 in bitcoins to the hackers, who had used malicious software to commandeer a variety of systems, including key computers and emails. (bit.ly/2j5Afjj)

Ransomware– restoring your files the nasty way
Hackers are stealing people's computer files and only giving them back if they pay money or accept to infect two other users with the malicious virus, cybersecurity researchers have found. (cnb.cx/2ikI8QM)

These and other articles can be found at: bit.ly/UTRGVISOnewsnalerts

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

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.

Locations:

- Sugar Road Annex (ESRAX) Building
- R-167 Rusteberg Hall (BRUST) Building (*by appointment*)

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

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

Services We Provide

GOVERNANCE, RISK AND COMPLIANCE

ASSET AND VULNERABILITY MANAGEMENT

ENGINEERING AND INCIDENT RESPONSE

AWARENESS, COMMUNICATION AND OUTREACH

Give us YOUR FEEDBACK!
bit.ly/utrgvisonewsletterfeedback