ISO NEWSLETTER

www.utrgv.edu/is

The University of Texas Rio Grande Valley™

Information Security Office

VOLUME 1, ISSUE 1 SEPTEMBER 02, 2016

Welcome back to school!

The UTRGV Information Security Office (ISO) is proud to introduce its inaugural newsletter. This bi-monthly newsletter will strive to keep you informed about important security news and topics that will help you remain safe and secure both at work (for employees), at school (for students), or at home (for everyone). Your comments, ideas and critiques are welcome in order to ensure this newsletter serves the UTRGV community in the best way possible. Welcome to the Fall of 2016 and the start of another great academic year!

Some basic security reminders to help you start the new Fall semester:

1. Keep your computer software up-to-date. Check to make sure your Operating System (OS) is updated as well as any applications you have installed, especially Adobe Readers, web browsers (IE, Edge, Safari, Chrome, Firefox, etc.) and office products (word, excel, etc.).
2. Don't forget to update your antivirus and to run a full scan at least once a month. You don't need to spend your hard earned money to stay protected, there are many great antivirus products available for free! Using a computer with no virus protection is like driving a car with no windshield on the highway, your guaranteed to get hit with something and its going to hurt. (http://bit.ly/25BuJ7i)
3. Check your UTRGV email— nowadays most professors and classmates will communicate via email. UTRGV employees should use their UTRGV email for conducting official university business.
4. Don't be a phish— use caution when clicking on email links and opening any attachments. If you are not expecting an email or if it just doesn't look right, don't open it! It could be a phishing attempt.
5. Use strong passwords for all your accounts. They should be at least 14 characters long and contain upper and lowercase letters, numbers and symbols. Use different password for each of your accounts. Don't use your banking or UTRGV passwords on social media sites. A good password manager can help you stay on top of all your passwords. (http://bit.ly/2aEeO6i)
6. Minimize (or eliminate) the use of USB drives to transfer data between computers. They can be easily lost or stolen and the hardware often fails. All UTRGV users are given a Microsoft OneDrive account, so use it instead.

INSIDE THIS ISSUE:

EDITOR

Francisco Tamez

ISO Security Analyst

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, 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.

PowerBroker

Throughout the summer, the Information Security Office (ISO) and Information Technology (IT) have implemented a privileged access solution called PowerBroker for all UTRGV owned computers. The PoweBroker solution has already been deployed to all Windows computers. Apple computers running OSX can request PowerBroker by submitting an IT Service Request with the IT Service Desk.

PowerBroker is an application that enables UTRGV employees to perform limited administrative tasks such as installing and updating software, adding or removing printers, without requiring privileged access or assistance from IT. To learn more about PowerBroker, visit how to use PowerBrower in the IT website (www.utrgv.edu/it/how-to).

What to expect this Fall 2016

October NCSAM

October is National Cyber Security Awareness Month (NCSAM), administered by the Department of Homeland Security. The ISO will discuss 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 will be providing weekly cyber tips in October through our News Blog, so don't forget to check our website and social media!

ISA Trainings

The ISO will begin to search for Information Security Administrators (ISA) for each department. 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.

Stay tuned! Follow us on social media www.facebook.com/utrgviso and visit our website www.utrgv.edu/is for more information

Ransomware: The Bad and The Ugly

by Daniel Ramirez (UTRGV Sr. Information Security Analyst)

Javier Jaén

The basics, what is Ransomware? Ransomware is a form of malware that targets your data and systems for the purpose of extortion. Ransomware targets specific file types like: .doc, .pdf, .xls, .jpeg, .mov, .zip, and many others. Files that are known to contain important data such as personal pictures, memorable videos, important work projects, or any data that a threat actor (criminal/hacker/attacker) may determine is important enough to you that you would pay money to get it back. The last two years of pictures you took with your smart phone or the past years' worth of research you had stored on your computer, gone in a blink! Would you pay to get this back? And how much would you be willing to pay? And if you pay, does this guarantee that you get your data back?

Ransomware is frequently delivered through malicious emails, where threat actors trick you into opening an infected attachment or clicking on a link that takes you to a malicious website. Computers with no anti-virus or out-of-date software are easily infected with ransomware (and other malware). Once a computer is infected with ransomware, the ransomware will target specific files on the victim computer and encrypts them, or locks them so that the owner can no longer access them. After the user has been locked out of the data, the ransomware will display a notification informing the victim that the files are now being held hostage, how much it will cost to recover them and how much time before the files are lost forever. After receiving the ransomware payment, the threat actor will purportedly provide an avenue to the victim to regain access to the data.

Javier Jaén

Ransomware is the fastest growing malware threat, targeting users of all types, from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. (Source: fbi.org How to Protect Your Networks from Ransomware). The University of Calgary was victim to a ransomware attack in May of 2016. The ransomware attack crippled multiple critical systems and forced the University to pay $20,000 dollars in order to regain access to its systems. A chain of hospitals in Washington, D.C., was hit in March 2016, while a Los Angeles medical center paid out $17,000 this year to hackers following a ransomware attack. (Source: http://bit.ly/2bZF7o2).

Ransomware Myths

A problem for only corporations or organizations.

Alina Simone wrote an article about how her mom's home PC fell victim to a ransomware attack in which she was forced to pay $500 to retrieve her files. (Source: http://nyti.ms/1xnYhpP). Ransomware is an opportunistic crime in which threat actors will target anyone they think will pay their ransom.

I only use a Mac (OS X) and so I am immune to malware.

KeRanger is a ransomware variant that has been seen in the wild and infects only OSX. (Source: http://bit.ly/2blco7G)

An ounce of prevention is worth a pound of bitcoins and a lighter wallet.
How to keep from falling victim to ransomware.

Awareness and education: Know the threat and that it exists. Understand how it works and learn how to prevent it. Share your knowledge with co-workers, family and friends.

Prevention: As with any malware, keeping your computer updated regularly is the number one method of prevention. This includes your Operating System, your Anti-Virus software, and all your applications especially Java, Adobe Flash, Adobe Reader and your web browsers. Uninstall any software that is no longer supported by the manufacturer (Apple ended support for Windows QuickTime: http://www.utrgv.edu/is/en-us/news-and-alerts/quicktime-eol/). Users should use computer accounts on the principle of least privilege: administrative access should be used only when absolutely necessary.

Internet habits: Don't click on email links from untrustworthy emails or open attachments that you were not expecting. Install only trusted software from a reputable source. Stay away from shady websites!

When it comes to computer malware, the computer user is the weakest link in defense.

If you have questions or comments about this article, please send them to is@utrgv.edu.

ISO Spotlight

The ISO Spotlight interviews an individual that plays a role in information security for UTRGV. In this issue, you will meet Thomas Owen, who is UTRGV's Chief Information Security Officer.

Thomas Owen, CISSP, CRISC, CISA, CISM, CGEIT, C|CISO, CEH, CHFI, MCSA: Security, MCTS, MCITP
Chief Information Security Officer
The University of Texas Rio Grande Valley

Tell us how information security has changed since you started in your role.
One of the main things is awareness. Information security is becoming more commonplace not just in businesses, but in personal lives as well. Individuals are becoming more cognizant they need to protect their sensitive information and that malicious attacks could happen to them, too.

Who are your customers, and what is one of the most challenging areas for you?
Internally, my customers are students, faculty, and staff of the university. One of the most challenging areas is trying to find the right balance between security and usability – we want to enable business and learning but do it safely. In essence, we want be a road map to get there safely instead of a road block. Finding that balance can be difficult depending on the processes involved.

How did you come into the security field?
I grew up on a farm and moved from tinkering with mechanical devices to electronic devices to network-connected devices.

Top 3 life highlights

Becoming a Christian
Births of my children
Marriage

People would be surprised to know:
I can speak Irish Gaelic.

Which CD do you have in your car? Or what radio station do you listen to?
Reckless Kelly – Wicked Twisted Road

If you could interview one person (dead or alive) who would it be?
Jesus

If given a chance, who would you like to be for a day?
My wife so I could better understand her.

What is the best advice you have received and that you have used?
"Learn how to read a manual. You can fix anything." – My grandfather told me that and it has proved to be immensely valuable. It works for anything from electronics to tractors.

What would be your advice for a new security professional?
Never stop learning. It's not up to your employer or coworkers to push you to learn, it is up to yourself so make it a priority. The field is changing rapidly, and knowledge is never wasted.

Newsworthy Security Articles

Dropbox massive data breach involving 68M users
What started out last week as a warning by Dropbox to its users that some login data may have been compromised has exploded into a massive data breach with an estimated 68 million Dropbox user credentials being exposed on the web.

Cyber Threats and Opportunities—by The University of Texas System Chancellor William H. McRaven
Cyber attacks take place all day, every day – on people, businesses, government agencies, national political parties, you name it – and the consequences of just one attack succeeding can be devastating. This vulnerability poses a serious threat to our economy, our way of life, and to our collective security.

University of Calgary Ransomware
The University of Calgary paid a $20,000 ransom in untraceable Bitcoins to shadowy hackers after a devastating malware attack. University officials agreed to pay the ransom to ensure critical systems could be restored, but noted it will take some time for the university's IT staff to apply the encryption keys to the infected machines.

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

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.

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

Services We Provide

GOVERNANCE, RISK AND COMPLIANCE

ASSET AND VULNERABILITY MANAGEMENT

ENGINEERING AND INCIDENT RESPONSE

AWARENESS, COMMUNICATION AND OUTREACH