ISO
NEWSLETTER

www.utrgv.edu/is

The University of Texas Rio Grande Valley™
Information Security Office

VOLUME I, ISSUE IV MARCH 9, 2017

INSIDE THIS ISSUE:

EDITOR
Francisco Tamez
ISO Security Analyst

Spring Break!

The UTRGV Information Security Office (ISO) would like to wish you a great and safe Spring Break! Prepare yourself for the break and make some educated decisions before you pack your bags and leave.

Please follow these security tips and remember to share them with your friends and family.

Some basic security reminders to help you prepare for Spring Break:

1. **Traveling**
   - For road trips remember: **NEVER** leave any valuables in your car (e.g., laptops, purse, iPad, smartphones, etc.)
   - While waiting for your next airplane to arrive, always be aware of your surroundings and never leave your bags, laptop or iPad unattended.
   - In airports be aware of "juice jacking". Don't trust public phone chargers, the cable might be used to transfer and sync your data to a malicious user! To learn more about juice jacking please visit: www.howtogeek.com/166497/
   - If you connect to the airport Wi-Fi **NEVER** conduct financial transactions, send important emails, etc. Public Wi-Fi most of the time is unsecure and a risk!
   - Keep a list of your passport or Visa, credit, or debit cards numbers at home with their corresponding organization contact information This will make it easier to report these items in case they are stolen.
2. **Staying in a Hotel**
   - Be cautious! Treat your Hotel internet as you would treat any public Wi-Fi. See our newsworthy security article "Free Wi-Fi is it safe?" for more information.
   - Use discretion while checking in at the front desk. No one outside of your group of friends needs to know your room number.
   - In your room remember to check that all of the windows and door locks are secure.
   - Always close your door tightly when entering or leaving your room. Some doors have a slow release and could remain open!
   - Most hotels offer safes. Use them! Store important items or any other easy to steal items (e.g., iPad, jewelry, laptops, passport, etc.) while you are out of the hotel.
3. **Don't get SMACKed!**
   - Check your privacy settings in social media!
   - Be thoughtful about what you post about others and remember that pictures online last a lifetime.

SECURITY HIGHLIGHTS

Tax Scams!

The Internal Revenue Service (IRS), state tax agencies and the tax industry issued an urgent alert to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits. Previously, the W-2 scammers are combining their efforts to steal employee W-2 information such as your Social Security Number (SSN), date of birth, direct deposit, and more!

Here's how the scam works: Cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from an organization executive. The email is sent to an employee in the payroll or human resources departments, requesting a list of all employees and their Forms W-2.

The W-2 scam is just one of several new variations that have appeared in the past year that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies. Individual taxpayers also can be targets of phishing scams, but cybercriminals seem to have evolved their tactics to focus on mass data thefts.
bit.ly/IRS-W2-alert

Are you a Phish?

Phishing is a form of fraud in which the cybercriminal tries to learn information by tricking you as a trustworthy entity or person via email, websites, and phone calls.

Según Microsoft, los delincuentes cibernéticos tratan de convencerlo de que instale software malicioso descargando archivos adjuntos, también buscan persuadirle para que entregue su información personal respondiendo o haciendo clic en un vínculo malicioso en un correo electrónico aparentemente legítimo.

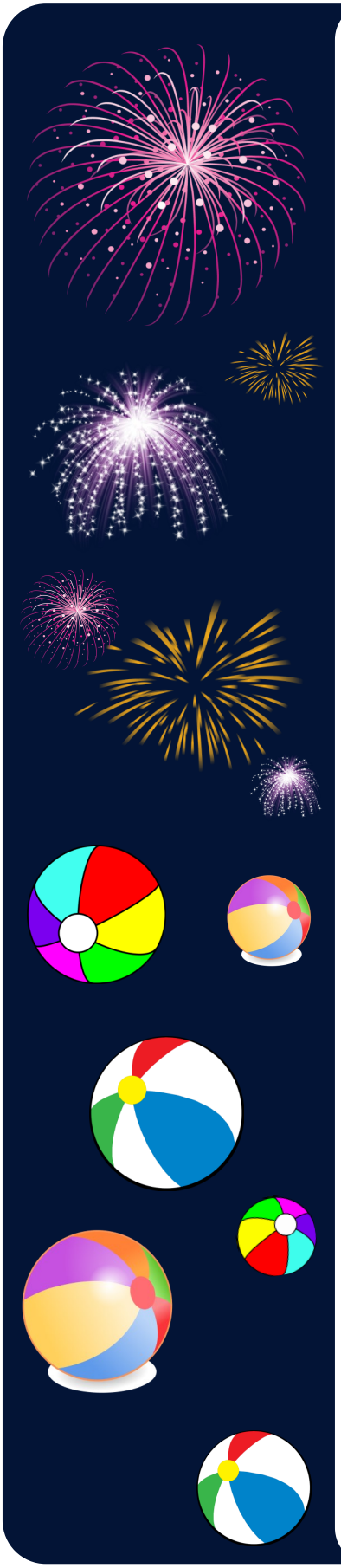
Things to look for in emails:

- Beware of links in emails! **NEVER** click them.
- **NEVER** download or open any attachments.
- **Hover** over links: Simply place your mouse over the link to see the web address. (Links might also lead you to .exe files. These kinds of file are known to spread malicious software.)
- Threats might be included. For example:
  - ◊ "Your account would be closed if you don't respond with your username and password."
- Scam artists use graphics in emails that appear to be connected to legitimate websites.

If you receive an email involving your UTRGV email address that you suspect may be a phishing message please forward email to: itdns@utrgv.edu

For more information on how to report a phishing message please follow these instructions from the IT website: www.utrgv.edu/it/how-to/report-phishing-messages

For more information about phishing please visit: www.utrgv.edu/is/en-us/resources/trainings/phishing-page/



What to expect this semester?

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.

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.

End Of Life Software

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 10.8 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/UTRUTRGVISOComputerSecurityStandard) which requires them to run only vendor supported OS. Vista will be EOL in April of 2017, so plan to upgrade this OS soon.

Apple QuickTime for Windows

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.

Today's EOL products

Please update if you are using the following products with these versions or below.

Product	Version	Product	Version
Windows	8.0	Adobe Acrobat	9.x
Safari for Windows	Any	Adobe Flash Media	4.5
Adobe Acrobat X	10	Adobe Flash Player	19
Adobe Reader	9.x	Java SE	7

For more EOL software please visit: bit.ly/list-EOL2017

ISO Spotlight

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

***Cesar Pastore* MBA**
Information Security Analyst

The University of Texas Rio Grande Valley

1. How did you come into the security field?
I came to the security field through my work as a system administrator, business analyst and data analysis.

2. Top 3 life highlights:
- Getting my first full time job after college.
- Getting down-sized from a job (Believe it or not this teaches you a lot)
- Moving to Texas from California.

3. People would be surprised to know:
I grew-up in the west coast of California.

4. Which CD do you have in your car? Or what radio station do you listen to?
I listen to NPR.

5. If you could interview one person (dead or alive) who would it be?
I would interview my parents or grandparents at my age. In similar fashion I wish I could interview my children or grand-children at my age.

6. If given a chance, who would you like to be for a day?
Any person I have disagreed with – I think gaining perspective is an important thing in life.

7. What is the best advice that you have received and that you have used?
Always keep an eye on the future and try to avoid over reliance on the familiar.

8. What would be your advice for a new security professional?
Concentrate on developing practical skills that will keep you relevant in the workforce. Don't be afraid to try something new or to enter new areas of technology that you don't have a direct background in.

Featured Article

By Jonas Del Angel
UTRGV Security Analyst

Exploit Kits

What is it?

Exploit kits are a relatively unknown term in today's business environments. Put simply, exploit kits are tools used by cyber criminals to exploit vulnerabilities on computer systems. They scan your machine for outdated software and security protection tools. They first became known in 2006 when it was discovered as the delivery method for exploits in Microsoft Windows, Mozilla Firefox, and Java applications to distribute malware. This is generally done by either spam or compromised advertisements on legitimate websites. Websites targeted to compromise include banking, news, web forums, WordPress, and others. Over time exploit kits have evolved and are known for providing updates to their buyers which include: exploits for newly discovered vulnerabilities, improved evasion from anti-virus detection and data analysis metrics to determine infection success rates. Often times the owners of these websites are unaware they have been compromised due to the evasion techniques used by the kits to avoid detection. They are however, generally discovered and fixed within a day so they can no longer infect users.

How does it targets systems?

Ransomware has become the favored payload in today's use of exploit kits because of its ability to remain undetected by anti-virus software and its extremely high success rate at infecting user machines. When scanning a machine, exploit kits search for the version of the browser, browser plugins and even out dated software. When vulnerable plugins are detected it will find an exploit to use against the specific vulnerability it found and deliver a payload which can contain malware, trojans, or ransomware. Favored software targets to scan for tend to include out dated Adobe Flash Player, Adobe Reader, and Java plugins. This entire process occurs without the user's knowledge because the download and installation of the payload occurs in the background through the use of a hidden web frame after a vulnerability has been found. If no vulnerabilities are found or if security software tools are sufficient, the exploit kit will ignore the machine and look for another target. (bit.ly/2lV908J)

Awareness

One of the primary reasons exploit kits continue to evolve is due to the analytic data collected from exploit kits indicating that users continue to fall victim to ransomware which is seen as highly profitable. The stealth method of downloading and installing the malware when performed as a drive-by download also add to it's success since it occurs without the user ever being aware.

What about Mac OS X and Linux Users?

One would normally think that the chances would be significantly lower if either of these are your preferred operating systems (OS). However, because exploit kits are leveraging web browsers to scan machines and deliver malware, any OS is a potential target. Adobe Flash Player vulnerabilities rank among the highest for most success according to trend reports from 2015 and 2016. (bit.ly/23wr6C3)

Prevention

So how can we take better precautions to not fall victim to ransomware that was delivered with an exploit kit? Some basic security minded tips to be aware of it would be to:

- Keep all your software, browsers, and plugins up to date.
- Back up your data regularly to an external hard drive that you don't regularly leave attached to your machine.
- Install ad blocking software for your web browser of choice. Exploit kits often find ways in to machines because they use website ads as a means of scanning the target machine.

Exploit kits are a growing problem that's been on the rise over the last several years and continues to grow. The reason for this is because of their key use in the delivery of malware and ransomware. It's no longer just about being suspicious of e-mails or attachments. Vigilance against phishing emails is only one way to prevent falling victim to a cyber crime, the other means staying true to the common practice of keeping our software up to date. More information on safeguarding against security threats like this can be found here: (bit.ly/2lZZ5iV)

ISO GUEST

About UTRGV Emergency Preparedness

The Office of Emergency Preparedness is committed to the continuous process of preparing for, responding to, recovering from, and mitigating potential losses from natural, technological or human-caused disasters that may negatively impact students, faculty, staff, visitors, and facilities at The University of Texas Rio Grande Valley.

Emergency Alert Notification

Rapid and timely communication to the university community during emergencies is critical. The UTRGV Emergency Alert System (EAS) provides mass, urgent and timely communication using multiple methods to promptly notify students, faculty and staff of an active major campus emergency or high risk incident through:

- Emails
- Text messages
- Voice messages
- University owned personal computer alerts
- University Police Facebook page @UTRGVPoliceDepartment

Students, faculty and staff are automatically registered to UTRGV Emergency Alerts with the contact information contained in Banner (students) and Oracle (faculty and staff).

Emergency Alert Notification

When University Police or Campus Safety and Security determines there is an active emergency in which the public safety of the campus may be at risk, an urgent notification through the UTRGV Emergency Alert System will be initiated. Examples are:

- When a person actively shooting a weapon is on the loose
- When a tornado or severe thunderstorm with expected winds greater than 70 miles per hour is predicted to impact a campus area
- When a major hazardous material spill or together high risk emergency impacts a large portion of campus

Coastal Environment

- If you are caught in a rip current, stay calm and don't fight the current
- Swim parallel to the shore until you are out of the current. Once you are free, turn and swim toward shore
- Stay at least 100 feet away from piers and jetties. Permanent rip currents often exist near these structures
- When at the beach, check conditions before entering the water. Check to see if any warning flags are up or ask a lifeguard about water conditions, beach conditions, or any potential hazards

Water Safety

- Swim in designated areas supervised by lifeguards
- Never leave a young child unattended near water and do not trust a child's life to another child; teach children to always ask permission to go near water
- If you have a pool, secure it with appropriate barriers. Many children who drown in home pools were out of sight for less than five minutes and in the care of one or both parents at the time
- Have appropriate equipment, such as reaching or throwing equipment, a cell phone, life jackets and a first aid kit

The Office of Emergency Preparedness

Promotes a foundation for emergency management and provides the framework for effective preparedness efforts through the Emergency Operations Plan and related annexes;

- Maintains, develops and aligns achievable emergency management goals and objectives with the vision, mission, and purpose of The University of Texas Rio Grande Valley;
- Defines procedures pertinent to the execution of the Emergency Management Program;
- Identifies, and maintains good working relationships with internal and external emergency management partners and stakeholders; and
- Strengths program continuity and viability by providing training and exercises.

Office of Emergency Preparedness Contact Info

Phone: (956)665-2658
Email: emergencypreparedness@utrgv.edu
Website: www.utrgv.edu/emergencypreparedness

Emergency Contacts

University Police
Brownsville:
(956)882-8232 (main)
(956)882-2222 (emergency)

Edinburg:
(956)665-7151

Harlingen:
(956)882-8232(main)
(956)882-2222 (emergency)

Env. Health, Safety & Risk Management
(956)882-5930 (Brownsville)
(956)665-3690 (Edinburg)

Facilities Operations
(956)665-2770

Emergency 911

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 (AITP) 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 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 (www.facebook.com/UTRGV.AITP)
All majors are welcomed to join.

Protect Yourself from Cyber Criminals this Spring Break

By: AITP

Spring break is fast approaching, which means vacation time for millions of college students across the country. Unfortunately, this gives opportunity for hackers and scammers to prey on unsuspecting students and their families. We list 3 popular methods attackers use to scam students, and simple ways to protect yourself this spring break.

1. **Card Skimmers** – Card skimmers are malicious card readers that steal data from the card's magnetic stripe attached to the payment terminals most commonly on ATM's. Card skimmers have accounted for more than 80 percent of ATM fraud dating back to 2008. The best way to protect yourself is to do a little investigation on any ATM machine you end up using. Always check for tampering, if you see that something looks different, such as a different color, material or strange looking graphics, do NOT use that ATM. Also, don't be afraid to wiggle the card reader, as it should be constructed very sturdy and unable to break apart easily.

2. **Infected USB's** – This is an old method scammers have been using for a while, especially in popular spring break vacation spots. Scammers will leave a malware infected USB in a parking lot, lobby or even in an entertainment venue, hoping that someone will pick it up and plug it into their laptop. The consequence of this is unintentionally installing malware on your computer. This can very damaging as you can unknowingly install a remote access Trojan that can enable cyber criminals to remotely control and spy on your PC. The best way to avoid this is to ignore any stray USB's you find even if they are labeled with something enticing like "Bathing Suit Photos" or "Top Secret Don't Open".

3. **Phishing** – (also known as Message Baiting) is a popular scam that attackers use to gain personal info such as credit card numbers, passwords, usernames etc. This is done by disguising themselves as a trustworthy entity usually through email. So if you get emails by popular hotel chains offering special spring break discounts that seem too good to be true, they probably are. Remember that most reputable organizations will never use email to request you to reply with your password, social security or other confidential information. Always be suspicious of any email message that asks you to verify personal information. Never reply to these messages, and of course, never click on the link.


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

Texas hospital penalized $3.2 Million for HIPAA violations
It was determined that the Children's Medical Center of Dallas used unencrypted mobile devices, among other noncompliance in efforts to protect customer health data. (bit.ly/TEXAShospital-penalized)

New website is clearing house for medical device vulnerabilities
A website run by the National Health ISAC will serve as a clearing house for information on security vulnerabilities in medical devices. (bit.ly/NEWwebsite-NationalHealthISAC)

Protect your portable devices
Protect your portable devices such as laptops, iPads, or smartphones from loss or theft. (www.utrgv.edu/is/en-us/resources/how-to/protect-devices)

Free Wi-Fi: Is It safe?
Did you know that 82% of travelers connect to free but unsecured Wi-Fi networks in public places such as airports, coffee shops, and hotels? Unfortunately, this common practice may put travelers at risk! (er.educause.edu/blogs/2016/10/free-wi-fi-is-it-safe)

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