UTRGV ISO NEWSLETTER

www.utrgv.edu/is

The University of Texas Rio Grande Valley™

Information Security Office

VOLUME I, ISSUE VI JUNE 30, 2017

INSIDE THIS ISSUE:

Hot Summer for CyberSecurity

Summer is finally here and for many of us that means it's time to get away! The ending of the Spring semester started with several cybersecurity events, one of these events impacted 99 countries including the United States of America. This summer looks like it's going to be a hot one for cybersecurity.

Please follow these tips that will guide you to refresh you in the summer and luckily, with a little care it's possible to protect yourself and be cyber-aware.

Traveling securely:

- Update your devices — Double check that the latest patches are installed. Your software vendor should notify you whenever an update is available.
- Secure your mobile device — Install a device finder or manager on your device in case it's lost or stolen, and if you are traveling with a laptop or mobile device, remove or encrypt any confidential information. Consider using a laptop or device designated for travel with no personal information, especially when traveling out of the country.
- Social Media — Avoid social media announcements about your travel plans and make sure that you "Don't get **SMACK**ed". It's tempting to share your upcoming vacation plans with family and friends, but consider how this might make you an easy target for local or online thieves. Consider posting those beautiful photos after you return home.

Be secure online:

- Secure your information in transit — Keep an eye out for that lock icon on your browser, or the https in the URL! These are indicators that encryption is currently in use with the site.
- Public computers and open wireless networks — Do not access sensitive accounts (such as banks) or conduct sensitive transactions over public Wi-Fi spots in airports, hotels, coffee shops, and other public places. These public networks can be convenient but they're often not secure and can leave you at risk. Any public Wi-Fi should be considered "unsecured."
- Get two steps ahead — Switch on two-step verification or multi-factor authentication wherever offered to prevent unauthorized access. This can be achieved by a combination of any of the three "Somethings" below:
  - ◊ Something you know — Personal Identification Number (PIN) or Password
  - ◊ Something you have — Smartphone, token or ID badge / smart card
  - ◊ Something you are — Fingerprint, retinal scan, voice pattern, or typing cadence

NOTE: The use of a password in combination with a PIN, for example, is NOT considered two-factor authentication because both pieces of information involve a single factor—something you know.

EDITOR

Francisco Tamez

ISO Security Analyst

SECURITY HIGHLIGHTS

Ensure Your Internet Safety While on Travel this Summer with a VPN!

The spring semester has ended and you may be getting ready to go on travel. If you plan to connect from the outside to UTRGV, you will need to use the Virtual Private Network (VPN). There are a couple of steps that need to be completed before you leave campus to ensure your connectivity. Please take the time to prepare and ensure that all the steps are complete to be VPN ready!

Virtual Private Network (VPN) for UTRGV Employees

The VPN service provides secure (encrypted) off-campus connection to access University resources. Use VPN to access Oracle eBusiness functions such as approving timecards or changing your direct deposit information. VPN is also required to remotely access your office computer and file shares using Remote Desktop Protocol (RDP).

You must complete the following tasks for VPN access.

- Enroll for DUO Mobile two factor authentication. **This step must be completed from the campus network. Visit utrgv.edu/DUO to enroll.**
- Install the DUO Mobile app on your mobile device (recommended).
- Install the FortiClient software on your computer which establishes the secure VPN connection to UTRGV's network.

VPN Instructions (accessible with UTRGV credentials)

- Connect to Virtual Private Network (PDF)
- Connect to Virtual Private Network (iOS iPad)
- Replace Device Enrolled with DuoMobile for VPN
- PowerPoint Presentation with audio

www.utrgv.edu/it/how-to/

Leaving for vacation?

If you are planning on your summer 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!

UTPA/UTB Email Forwading Permanent Deactivation on August 31, 2017

Attention Legacy Employees:

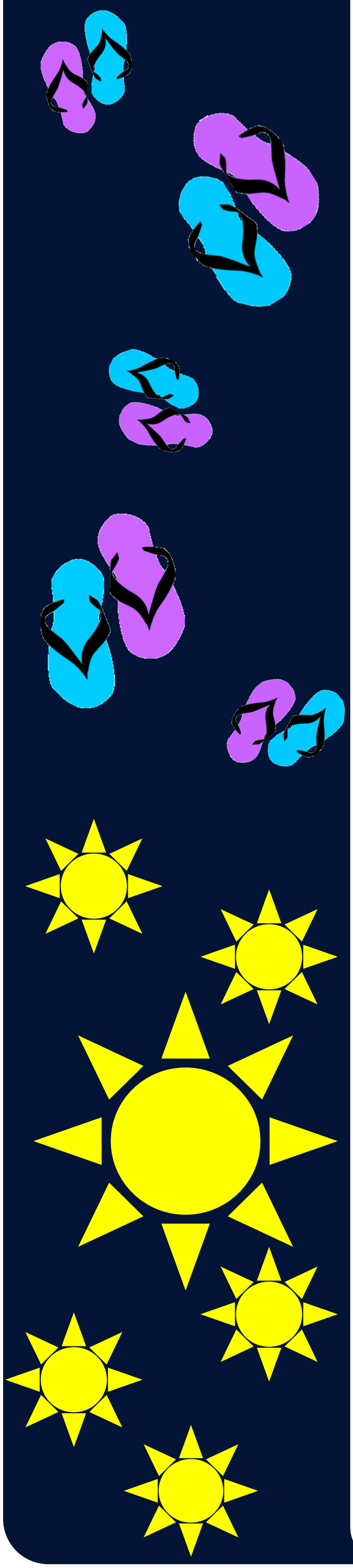
On August 31, 2017, UTPA/UTB (legacy) email forwarding will be permanently deactivated. Currently, email messages sent to UTPA/UTB accounts are being forwarded to UTRGV email accounts. Forwarded messages are denoted by your legacy email address in the "To" section of the message OR include a note indicating the message was forwarded from your UTPA/UTB email address.

You will receive ample notifications between now and the permanent deactivation date of August 31, 2017. We encourage you to **take action now** and inform your contacts that are still using your legacy email to use your UTRGV email address.

Please visit the IT Website FAQ's for more information.

If you have any questions or need technical assistance, please contact the IT Service Desk:
Brownsville / Harlingen / South Padre Island
956-882-2020
Main 1212 (Brownsville)

Edinburg / McAllen / Rio Grande City
956-665-2020
Academic Services Building 1.102
(Edinburg)



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 can lead to no longer receiving security updates that can help protect your PC from harmful viruses, spyware, and other malicious software that can steal your personal information.

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.

Today's EOL products

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

To successfully update to the latest OS you will need the following systems requirements. In the instance that the computer's hardware is not capable to stand the latest OS, then according to the computer security standard that computer will have to go through surplus and a new one with capable hardware will take its place.

If you use for your work activities a university owned computer with an Operating System with EOL, please log in to my.utrgv.edu and submit a ticket through Service Now or contact the IT Service Desk as soon as possible.

Brownsville / Harlingen / South Padre Island	956-882-2020
Edinburg / McAllen / Rio Grande City	956-665-2020

A friendly recommendation for students, faculty, and staff that use personal computers or laptops: Please review the following systems requirements, log in to my.utrgv.edu, visit the vSoftware application, and purchase ($9.95 USD) Windows 10; it is highly recommendable that you back up all of your files, photos, and any other important documents before you upgrade your OS. In the case that your personal computer does not support the OS, please consider upgrading your machine.

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

CLEAN DESK SECURITY BEST PRACTICE

CONFIDENTIAL
CONFIDENTIAL
P@SSWORD

An example of a BAD practice

A clean desk practice ensures that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Please use the checklist below daily to ensure your work (or home) workspace is safe, secure, and compliant.

□ Passwords should not be left written down in any accessible location.

□ Ensure all sensitive/confidential information in hardcopy or electronic form is secure at the end of the workday or when you will be gone for an extended period.

□ Computer (laptops, tablets, phones, etc.) screens should be locked when the workspace is unoccupied.

□ Portable computing devices such as laptops, tablets and mobile phones should be secured in locked storage when not attended or at the end of the workday.

□ External storage devices such as CD's, DVD's, or USB drives should be secured in locked storage when not in use or not attended.

□ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.

□ Keys used for access to Confidential or Sensitive information should not be left at an unattended desk

□ All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that Confidential or Sensitive documents are not left behind for the wrong person to pick up.

□ Upon disposal*, Confidential and/or Sensitive documents should be shredded or placed in locked confidential disposal bins.

**Ensure UTRGV record management and retention policies are followed when disposing of any UTRGV official records [HOP ADM-10-102]*

ISO Spotlight

The ISO Spotlight interviews an individual that plays a role in UTRGV and information security. In this issue, you will meet *Network Security Analyst III,* Ramon Hermida.

Ramon Hermida

Network Security Analyst III,

1. Tell us how information security has changed since you started in your role.
Information Security as a field has become more mature and well-defined. This has to do with adversaries figuring out how to monetize their attacks, but it also has to do with how ubiquitous the internet and technology have become in our society. Information Security, and lack thereof, is everywhere you look today. This is ever so apparent when attackers perform a denial-of-service attack on the Minecraft server that your 10-year old is designing their mud-house masterpiece.

2. How did you come into the security field?
Remember that in the early 2000s there was not much of a "security field". My first "official" security title was in 2005 with the university. In previous jobs, I would always be involved with some aspect of Information Security. My first memorable experience with Information Security, and how devastating attacks could be, happened in 2001. No one in the company understood what was bringing the domain controllers down, including several consultants. There were about 80 full-time employees, just sitting there, not being able to log into their accounts and work. What caught my eye were some abnormal entries on my Linux servers, which were later revealed to be the calling card of the Code Red worm.

3. Top 3 life highlights:

- Relocating to Texas with pretty much whatever I could pack on an airplane
- Getting married to Irma
- Deeper understanding about life through meditative practices

4. People would be surprised to know:
I have actually ridden my bicycle from Houston to Austin. I always make it a point to ride a bicycle whenever I travel. I have a goal to ride my bicycle in every single state, and as many countries as I can.

5. Which CD do you have in your car? Or what radio station do you listen to?
I actually don't own a car. However, I am a firm believer in listening to background noise generators and binaural beats. Do a google search for NOISLI to get a better understanding of it. And no, they did not pay me for that.

6. If you could interview one person (dead or alive) who would it be?
Albert Einstein. Not so much to talk about physics or relativity, but more to understand his overall perspective in life. Such things as: what time did he get up every day? what were his daily rituals? what were his life goals? what did he think his life purpose was? how did he manage projects and deadlines at work? how did he did manage his Work-Life balance?

7. What is the best advice that you have received and that you have used?
The advice given to me by my English teacher in High School. He wanted me to take AP classes, instead of regular classes. Naturally, I objected. To which his answer was: "evaluate which of the options and the direction that you can easily fall back on, and choose the more difficult (and often more rewarding) one". So in this example, I could take the AP classes, and if I did not cut it, I could easily fall back to regular courses. However, going the other direction would not have been as easy, or rewarding for that matter.

8. What would be your advice for a new security professional?
Always nurture a healthy level of curiosity and get "hands-on" practical experience in whichever aspect of Information Security you are involved with, or you want to be involved with. Do note that our field is in constant flux, and that you will need to get this "hands-on" experience outside of work or school. I have seen plenty of folks with an Information Security degree that are unable to answer basic security questions.

WannaCry Ransomware and Lessons

By Department of Information Resources
DIR.texas.gov

A vulnerability first uncovered by the National Security Agency and then released by hackers on the internet is now being used in one of the most prolific cyberattacks ever around the globe.
On May 12, 2017, tech blogs and IS news feeds ignited with the news of a new ransomware attack that was spreading like wildfire through both private- and public-sector networks, locking people out of their data and demanding they pay a ransom or lose everything. Agencies like the British National Health Service (NHS) and Telefonia, Spain's largest telecommunications provider, were affected. Even private companies like Fedex felt the toll of this malicious software. In the first few hours alone, somewhere between 230,000 to 390,000 computers in more than 150 countries were infected with this newly-discovered ransomware. Its name was WannaCry (WNCRY/WannaCrypt).

This bad business taught us all some hard lessons.

1. **Patch…. PATCH!!** Everyone always says it but clearly not everyone did it. This ransomware successfully attacked so many systems due to unsupported or unpatched operating systems. Like I said, PATCH!

2. **Forgetfulness is no excuse.** Systems left in the past often mean unmonitored access points. WannaCry demonstrated just how important consistent asset management is. Bad actors prey on your human error. It is critical to take a step back and look at your system from the outside. If you were trying to sneak into your systems, where would you look first?

3. **Build some walls with network segmentation**. Patching old systems often comes with a slew of technical challenges. For this reason, new systems are often built on top of the old and unsupported. Many do not realize the risk of unpatched systems and a lack of network segmentation. Network segmentation and well-planned network architecture could have saved some organizations a world of pain.

4. **Cybersecurity protects real life**. It is important to remember while cybersecurity is digital and you may be fighting the good fight behind a computer screen, people's lives hang in the balance. WannaCry's attack on health care services in the UK, was a clear display that there are consequences that go far beyond bitcoin.

5. **Don't forget about Availability!** WannaCry gave organizations a swift kick in the rear and reminded them that availability in the CIA (Confidentiality, Integrity, and Availability) three-legged stool, is essential to the success of everyday business. The cost of this ransomware is estimated to be over $8 billion dollars due to business interruption, lost income and timed spent restoring.

ISO Guest

Environmental Health, Safety & Risk Management

Management and Disposal of: Hazardous Waste, Biological Waste and Radioactive Waste

Batteries are managed as "Universal Waste" and we have a program in place to recycle specific batteries that includes the following;

A. Lead Acid Batteries (car batteries)
B. Most rechargeable batteries (e.g. NiCad)

Note: Common consumer batteries, including alkaline (AA, AAA, C, D, 9 volt) are non-hazardous and may be discarded with solid waste (trash) without special requirements.

Toners are also non-hazardous and may be discarded with regular trash but we also have a recycling program in place to minimize the impact on our landfills.

The departments who generate these two types of wastes can submit a pickup request to waste@utrgv.edu, pickups of these items are usually conducted on Fridays.

UTRGV Safety
Is In Everybody's Job Description

Office of Emergency Preparedness Contact Information

Phone: (956)665-3690
Email: EHSRM@utrgv.edu
Website: www.utrgv.edu/ehsm

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

I Million Gmail Users Impacted by Google Docs Phishing Attack

"We were able to stop the campaign within approximately one hour," a Google spokesperson said in a statement. "While contact information was accessed and used by the campaign, our investigations show that no other data was exposed. There's no further action users need to take regarding this event."

bit.ly/googlephishingattack

Chipotle breach affected restaurants across 47 states

Shortly after Chipotle reported a breach on April 25 that affected more than 2,000 restaurant locations and an undisclosed number of individuals across 47 states, an investigation concluded the point-of-sale (POS) malware attack lasted from March 24 to April 18 and searched for "track data" which sometimes includes card numbers, expiration dates, and internal verification codes, according to Chipotle's security alert.

bit.ly/chipotlebreach2017

Sensitive Pentagon Files on Amazon Server With No Password

A cache of more than 60,000 files was discovered last week on a publicly accessible Amazon server, including passwords to a US government system containing sensitive information, and the security credentials of a lead senior engineer. What's more, the roughly 28GB of data contained at least a half dozen unencrypted passwords belonging to government contractors with Top Secret Facility Clearance.

bit.ly/pfileswnopassword

SANS OUCH! June Newsketter: Lessons From WannaCry

Recently, you most likely watched widespread news coverage of a new cyber attack called WannaCry. It infected over 200,000 computers worldwide and locked numerous organizations out of their data, including hospitals in the United Kingdom.

There are several reasons this attack gained so much attention. First, it spread rapidly from computer to computer by attacking a known weakness in Windows computers. Second, the attack was a type of malware called Ransomware, which meant that once it infected your computer it encrypted all your files, locking you out of your data. The only way you could recover your data was from backups or by paying the attacker a $300 ransom to decrypt all of your data. The third and most important reason this attack gained so much attention was because it never should have happened.

The weakness that WannaCry attacked in Windows computers was well known by Microsoft, which had released a fix months earlier. But many organizations failed to install the fix, or were still using operating systems that are no longer supported by Microsoft.

securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201706_en.pdf

Hackers hosted tools on a Stanford University website for months

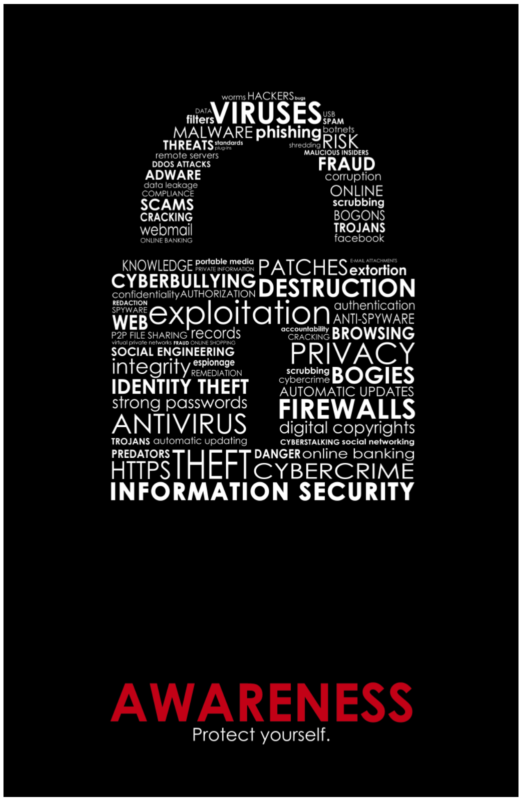
Compromising legitimate websites and the web servers that store and deliver them is a time-honoured tactic of opportunistic hackers, and a failure to keep them out can result in the servers hosting phishing and scam pages, spam mailers, exploit kits, or malware.

bit.ly/hackerstoolsstanforduni

Data breach at Oklahoma University impacts 30,000 students

Lack of privacy settings in a campus file-sharing network led to an unintentional exposure of the educational records of thousands of students at Oklahoma University.

bit.ly/databreachOklahomaU


worms HACKERS bugs
DATA filters VIRUSES USB SPAM
MALWARE phishing botnets
THREATS standards plug-ins shredding RISK
remote servers MALICIOUS INSIDERS
DDOS ATTACKS FRAUD
ADWARE corruption
data leakage
COMPLIANCE ONLINE
SCAMS scrubbing
CRACKING BOGONS
webmail TROJANS
ONLINE BANKING facebook
KNOWLEDGE portable media PRIVATE INFORMATION PATCHES E-MAIL ATTACHMENTS extortion
CYBERBULLYING DESTRUCTION
confidentiality AUTHORIZATION
REDACTION SPYWARE WEB exploitation authentication ANTI-SPYWARE
P2P FILE SHARING records accountability CRACKING BROWSING
virtual private networks FRAUD ONLINE SHOPPING
SOCIAL ENGINEERING PRIVACY
integrity espionage REMEDIATION scrubbing cybercrime BOGIES
IDENTITY THEFT AUTOMATIC UPDATES
strong passwords FIREWALLS
ANTIVIRUS digital copyrights
TROJANS automatic updating CYBERSTALKING social networking
PREDATORS THEFT DANGER online banking
HTTPS CYBERCRIME
INFORMATION SECURITY
AWARENESS
Protect yourself.

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

Special Thanks To:

Information Technology	**Environmental Health, Safety & Risk Management**
Irma Hermida and Hilda Gonzalez	Dr. Richard Costello and Liza Dimas