THE SHIELD

AUGUST 28, 2017

VOLUME II, ISSUE I

The University of Texas Rio Grande Valley
Information Security Office

Welcome back to school!

The UTRGV Information Security Office (ISO) is proud to introduce the new look and name to our newsletter. This 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 2017 and the start of another great academic year!

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

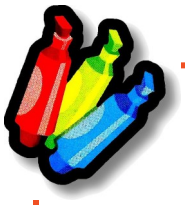
- Check your UTRGV email — nowadays most professors and classmates will communicate via email. UTRGV employees should use their UTRGV email for conducting official university business.
- Don't get Phished — Use caution when clicking on email links and opening any attachments from suspicious emails; remember to **always** place your mouse over the link, this technique will reveal the real web address. If you are not expecting an email or if it just doesn't look right, **don't** click on any links or download any attachments! It could be a phishing attempt. For more information feel free to visit our website: www.utrgv.edu/is/en-us/resources/training/phishing-page
- Update your devices — Double check that the latest patches are installed. 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 Microsoft Office products (e.g., Word, Excel, etc.).
- Back it up — Start protecting your valuable work and other digital information by making an electronic copy in One Drive for Business. One Drive for Business is a **FREE** cloud storage service provided by UTRGV to students and employees, you can rely on 1 Terabyte (TB) of cloud storage.
- Connect with care — When shopping online, check to be sure the site has security enabled. Look for web addresses with "https://", which means the site takes extra measures to help secure your information.

INSIDE THIS ISSUE:

EDITOR

Francisco Tamez
Security Analyst

www.utrgv.edu/is



SECURITY HIGHLIGHTS

NCSAM

October is the National Cyber Security Awareness Month (NCSAM), administered by the Department of Homeland Security. NCSAM was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

NCSAM 2017 also marks the 7th anniversary of the STOP. THINK. CONNECT.™ campaign. Each year, NCSAM highlights the overall message of STOP. THINK. CONNECT.™ and the capstone concepts of the campaign, like "Keep a Clean Machine," "Protect Your Personal Information," "Connect with Care," "Be Web Wise," "Be a Good Online Citizen," "Own Your Online Presence" and "Lock Down Your Login."

Social Engineering Fraud Warning

A state organization uses SpawGlass as for construction projects. In June, someone registered a domain Spawglasscontractors.com and sent emails to the business office and eventually social engineered them to change the bank routing number to another account. They sent large payments to this other account and didn't realize it was fraudulent until the real SpawGlass contacted them for their payments.

This is one of several incidents over the past few months involving the changing of bank routing numbers. Please make your business offices aware of this so that no other organizations fall victim to this exploit, and that you have good controls in place for changing these numbers.

Permanent Deactivation Date for Legacy (UTPA/UTB) Email Forwarding Set for August 31, 2017

ATTENTION ALL LEGACY EMPLOYEES:
On August 31, 2017, email forwarding from UTPA/UTB (legacy) accounts **will be permanently deactivated.** Currently, email messages sent to UTPA/UTB accounts are being forwarded to UTRGV email accounts. Forwarded messages are denoted by the use of **your legacy email address** in the "**To**" section of the message. They also include a note in the subject line and the **note below in the body** of the message indicating it was forwarded from UTPA/UTB.

****Email Forwarding from UTPA/UTB****
Please read message below:
Email Forwarding from UTPA/UTB (legacy) accounts to UTRGV accounts will be permanently deactivated on August 31, 2017. Please take action now and inform your contacts that are still using your legacy email to use your UTRGV email address.

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

If you have any questions or need technical assistance, please contact the IT Service Desk.
Brownsville / Harlingen / South Padre Island
956-882-2020
Main 1.212 (Brownsville)

Edinburg / McAllen / Rio Grande City
956-665-2020
Academic Services Building 1.102 (Edinburg)
Thank you,
End User Support
Information Technology

Cybersecurity Expo 2017

We will be conducting our second Cybersecurity Expo in the Brownsville and Edinburg campus!

Throughout the month of October the ISO will be discussing several cyber security topics such as the use of malware by online criminals, theft of intellectual property, phishing, cyberstalking, and more. Our office will be providing weekly cyber tips in October through our website and social media!

Adobe to Stop Supporting Flash Player in 2020

As open standards like HTML5, WebGL and WebAssembly have matured over the past several years, most now provide many of the capabilities and functionalities that plugins pioneered and have become a viable alternative for content on the web. Over time, Adobe have seen helper apps evolve to become plugins, and more recently, have seen many of these plugin capabilities get incorporated into open web standards. Today, most browser vendors are integrating capabilities once provided by plugins directly into browsers and deprecating plugins.

Adobe is planning to end-of-life Flash. Specifically, we will stop updating and distributing the Flash Player at the end of 2020 and encourage content creators to migrate any existing Flash content to these new open formats.
bit.ly/Adobe-EOLFlashP

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.
For example, Apple QuickTime 7 for Windows is no longer being supported.

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.

Please update if you are using **older** versions of any of the following products:

Supported products							
Product	**Version**	**Product**	**Version**	**Product**	**Version**	**Product**	**Version**
Windows	8	MacBook Pro	OS X 10.7	Java SE	8	Firefox	55.0.2
Windows	8.1	Adobe Flash Player	26.0	iPhone	iOS 8.1	Google Chrome	6.2
Windows	7	Adobe Reader	2017.012	Android	Jelly Bean	Internet Explorer	11
Windows	10	Adobe Acrobat X	2017.012				
iMac	OS X 10.7						

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

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 work-place. 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 unoc-cupied.
- ☐ 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,* Jennifer Avila.

Jennifer Avila
Network Security Analyst III,

1. Tell us how information security has changed since you started in your role.
The prioritization on cybersecurity, since now everything is cloud based. It has definitely increased due to the high rise of cybercrime, and the high price on personal data.

2. Who are your customers, and what is one of the most challenging areas for you?
UTRGV IT staff, senior management, legal affairs, PD, HR. According to the task in forensics and vulnerability scanning for applications. The challenging part is getting the data that they need, the deliverables; every task can be unique, half of the time it feels that you need to reinvent the wheel.

3. How did you come into the security field?
I started (around 2001) I was an IT director for a small organization, and I was involved with access control, server admin (exchange admin) with assistance from consultants. From all the different roles the security field was of a great interest to me.

4. Top 3 life highlights:
- Getting married
- Getting my undergraduate degree and graduate (MSIT)
- -reserving this one for future highlights-

5. People would be surprised to know:
- Usually when I'm not at work, I'm taking dance classes
- Love to cook (pastries and anything in general)
- I've been to a LOT of concerts and tons festivals

6. Which CD do you have in your car? Or what radio station do you listen to?
I have in my vehicle Sirius XM (Hard rock, Latin, 80's music)

7. If you could interview one person (dead or alive) who would it be?
- My judge –the guy who created silicon valley-
- Tool (the main singer)

8. If given a chance, who would you like to be for a day?
Somebody who is super rich and I'll give it to charity.

9. What is the best advice you have received and that you have used?
Stay true to yourself and your first instinct is most of the time the correct way to go.

10. What would be your advice for a new security professional?
Get your certifications, be open to learning different concepts and people skills.

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 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

U.S. DEPARTMENT OF STATE
OVERSEAS SECURITY ADVISORY COUNCIL

Hacking Happens

Case Study: Dendroid Malware

Malicious functions include:

- Make and record calls
- Delete call logs
- Intercept text messages
- Take pictures with the phone's camera
- Download existing pictures
- Record and upload audio and video
- Open applications and web pages
- Initiate denial of service

In the first few months of 2015, 5,000 new strands of Android malware were discovered *daily*. Just one of those was "Dendroid," a dynamic and difficult-to-detect remote access too, which as at one time easily available in malware forums for a meager fee of $300. Dendroid hides inside these applications and evades Google Play's malware detector, allowing it to potentially operate for extended periods of time. Its various capabilities—like turning on the microphone at will—could be used to hefty bills from premium-rate numbers, or allow malicious actors to gather intelligence on the Android owner's business and personal contacts/ Users should be suspicious of apps requesting a wide variety of permissions, and can download mobile-security apps to protect against various malware threats.

Cont'd from page 7

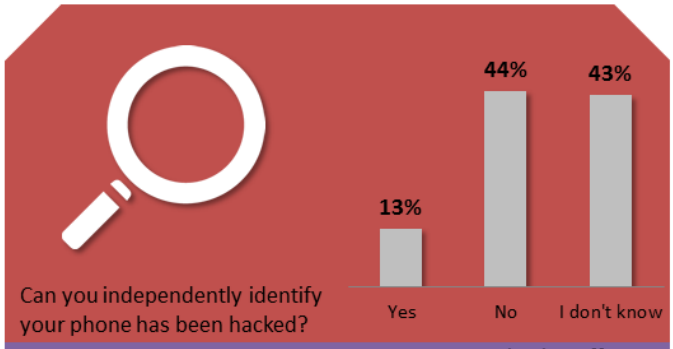
Detecting an Intrusion

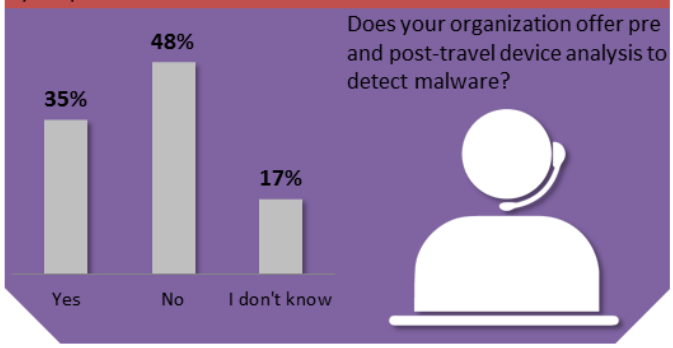
How do you know when you've been hacked?

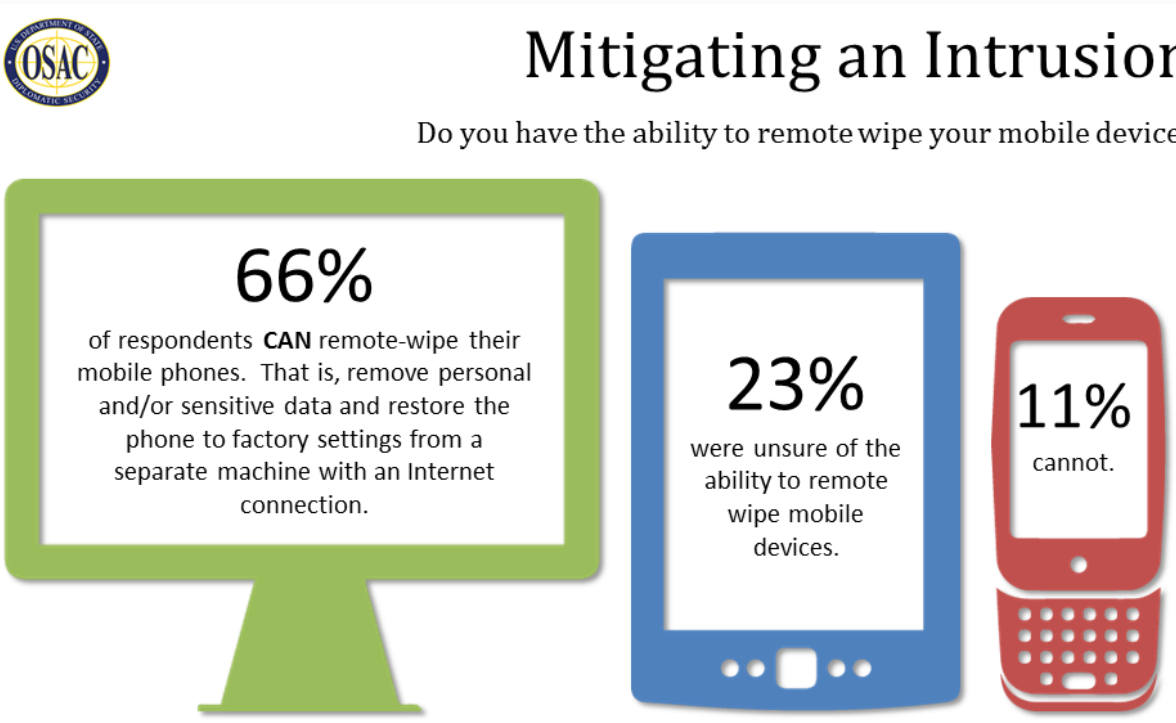
The majority of survey respondents were unsure or unable to identify a compromise on the their mobile devices. This again heightens the information risk, especially if employees continue to use their phones for business purposes after a device is hacked. Often, smartphone malware is extremely difficult to detect. Some signs of compromise may include:

- Latency
- Frequently drained battery
- Increased data usage
- Appearing apps
- Disappearing apps

Unfortunately, many of the symptoms of compromise can also be confused with connecting through a foreign service provider while traveling overseas. Offering employees a loaner device or technical assistance may be the best way to mitigate undetected hacks of mobile phones.







All major smartphone providers offer the ability to remote-wipe devices—a virtual kill switch that allows sensitive data to be erased in the event a phone is lost or stolen. Although remote—wipe won't execute if the phone battery dies, a signal isn't available, or a hacker disables network connections, it is nonetheless a mitigation tactic that all employees should enable and use as soon as a phone disappears. The following links offer step-by-step guides on remote wiping Android (support.google.com/a/answer/173390) and Apple (support.apple.com/kb/PH2701)

Feel free to continue reading the "Traveling with Mobile Devices: Trends & Best Practices" report by visiting the OSAC website: https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=17989

Do **YOU** have an idea for a topic? Would you like to include something in particular to this newsletter? Any comments or suggestions are **ALWAYS** welcome!

Feel free to submit your thoughts by visiting our website:
bit.ly/utrgvisonewsletterfeedback

er.educause.edu/blogs/2015/12/january-guard-your-privacy-online

WELCOME TO UTRGV

FREE BAG & GOODIES

Get a chance to WIN
one of our popular drawstring bag WITH goodies!

LIKE ● SHARE ● TAG 3 FRIENDS

@UTRGViso

NEWSWORTHY SECURITY ARTICLES

5,300 University of Iowa Health Care records exposed for two years
Thousands of University of Iowa Health Care (UIHC) patients had some of their private information inadvertently posted for more than two years on a web application development site.

In May 2015 the unencrypted patient information was saved by a UIHC employee to a public file-sharing site that was part of an open-source web application creation program being used by the organization. The files were left on the site unprotected after the project was completed. The files were spotted on April 29 by a cybersecurity professional and reported to UIHC's privacy officer. The files were removed from the file-sharing site by May 1. On June 22 UIHC began sending letters informing those affected of what happened.
bit.ly/UICHDB

SANS OUCH! August Newsletter: Backup & Recovery
If you use a computer or mobile device long enough, sooner or later something will go wrong, resulting in you losing your personal files, documents, or photos. For example, you may accidently delete the wrong files, have a hardware failure, lose a device, or become infected with malware, such as ransomware. At times like these, backups are often the only way you can rebuild your digital life. In this newsletter, SANS explain what backups are, how to back up your data, and how to develop a simple strategy that's right for you.
bit.ly/SANSAugustN

New York Supreme Court Justice fell for $1M phishing attack
New York State Supreme Court Justice Lori Sattler was duped out of more than $1 million while trying to sell her Upper East Side apartment and purchase another.
bit.ly/1MillionPhish

Newcastle University spoofed in phishing scam
Cybercriminals went to extreme lengths to clone the Newcastle University website going as far as to create dozens of sub-pages explaining different programs offered by the university

While the fraudsters committed a few errors in phony site, those unfamiliar with the actual site, such as foreign exchange students might easily mistake it for real. The hackers incorrectly referred to the school on the phishing site as the "Newcastle International University" instead of as "Newcastle University" in both the URL and throughout the site.
bit.ly/UNewcastleSpoofed

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 the 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

Jennifer Avila

The Overseas Security Advisory Council (OSAC)

www.osac.gov