THE SHIELD

OCTOBER 1, 2017

VOLUME II, ISSUE II

The University of Texas Rio Grande Valley
Information Security Office

THE BEGINNING OF FALL

The UTRGV Information Security Office (ISO) hopes that the start of the new semester and academic year is going great for you! Since the beginning of the Fall semester the cyber security field has been terribly busy. The number of scams and malware taking advantage of social media users and platforms is on the rise. Similarly, phishing attacks and data breaches took place earlier in September.

Below we will examine some ways that you can keep your school, personal, and social media accounts safer through smart online practices.

How to Identify Attacks

- Opportunists — There can be malicious cyber activity that seeks to capitalize on interest in hurricanes, earthquakes, or other natural disasters (e.g., Hurricane Harvey)
- Shortened URLs — These are a common tactic used by scammers to conceal where malicious links lead since some social media sites have a character limit. The links will use a URL shortening services to hide the true link destination—a malicious site that can infect your device.
- Fake coupons — The scammers create a fake coupon requiring you to click a link to download it and put the coupon on a malicious website that can infect your device with malware.
- Click bait — Click baiting is when there is a "teaser" to get you to click on the link. For example, it might suggest a promise a "giveaway". This is another way a scammer can get your information or install malware on your computer

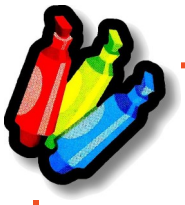
How to Prevent Attacks

If you receive a suspicious email or encounter a questionable post in social media please:

- Do not click on any links or shortened links
- Never reply with personal information (e.g., usernames, passwords, etc.)
- Use caution when opening email attachments
- Verify the legitimacy of any email solicitation by contacting the organization directly through a trusted contact number.

INSIDE THIS ISSUE:

EDITOR
Francisco Tamez
Security Analyst



SECURITY HIGHLIGHTS

The U.S. Department of Homeland Security (DHS) Issues Binding Operational Directive on Kaspersky Products

On September 13, 2017, the U.S. Department of Homeland Security (DHS) released Binding Operational Directive (BOD) 17-01 directing federal agencies to remove/ discontinue use of products, solutions, and services provided by AO Kaspersky Lab or related entities. The BOD mandates that federal agencies identify Kaspersky Lab products on federal information systems within the next 30 days, develop detailed plans to remove and discontinue use of the products within 60 days and implement those removal/discontinuation plans within 90 days. This follows the July 11, 2017, General Services Administration (GSA) decision to remove Kaspersky Lab from its list of approved vendors due to alleged ties between the company and Russian intelligence services. bit.ly/CISecurity-DHS-BOD

SANS OUCH! September Newsletter: Password Managers

One of the most important steps you can take to protect yourself online is to use a unique, strong password for every one of your accounts and apps. Unfortunately, it is most likely impossible for you to remember all your different passwords for all your different accounts.

This is why so many people reuse the same password. Unfortunately, reusing the same password for different accounts is dangerous, because once someone compromises your password, they can access all your accounts that use the same password. A simple solution is to use a password manager, sometimes called a password vault. These are programs that securely store all your passwords, making it easy to have a different password for each account. Password managers make this simple, because instead of having to remember all your passwords, you only have to remember the master password to your password manager. bit.ly/SANSSeptemberN

Potential Hurricane Harvey Phishing Scams

US-CERT warns users to remain vigilant for malicious cyber activity seeking to capitalize on interest in Hurricane Harvey. Users are advised to exercise caution in handling any email with subject line, attachments, or hyperlinks related to Hurricane Harvey, even if it appears to originate from a trusted source. Fraudulent emails will often contain links or attachments that direct users to phishing or malware-infected websites. Emails requesting donations from duplicitous charitable organizations commonly appear after major natural disasters. bit.ly/US-CERT-HarveyPhishing

Equifax Data Breach: 143 U.S. consumers affected

During the Equifax Data Breach the information that was accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Criminals also accessed credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers. www.equifaxsecurity2017.com/

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 **previous** 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	60.2
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 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]*

Cyber Security Expo 2017

October is the National Cyber Security Awareness Month (NCSAM).

In support of the Department of Homeland Security's (DHS) and the Stop.Think.Connect. campaign, the University of Texas Rio Grande Valley and the Information Security Office are proud to promote NCSAM and the importance of online safety.

Throughout the month of October, we will highlight cybersecurity in our website and in our social media posts. We hope you will join our efforts to promote this issue and hopefully you can attend our Cyber Security Expo that is going to take place on:

- October 17, 2017 – Edinburg Student Union from 11:00 am to 2:00 pm
- October 19, 2017 – Brownsville Salon Cassia (BMAIN 2.402) from 11:00 am to 2:00 pm

In the Cyber Security Expo, you will find:

- Helpful tips and resources that will help to raise awareness about cybersecurity
- Live map of cyber security attacks
- Games + free prizes
- Presentations and webinars

In order to register you will need to:

1. Click the 'register' button
2. If you are:
3. Affiliated to the university, then sign in with your UTRGV username and password
4. Not affiliated to the university, then click on 'sign up for a New Account'
5. Search for the Cyber Security Expo 2017

NOTE: Make sure that you register on the campus that you can attend

REGISTER

https://webapps.utrgv.edu/it/training/

Save the date and don't forget to bring your UTRGV ID card!
Thank You,

The Information Security Office

Cont'd from page 5

IDENTITY THEFT

Identity Theft (ID)

is a **crime** where a thief steals your personal information, such as your Social Security Number, to commit fraud. The identity thief can use your information to:

- Fraudulently apply for credit
- File taxes
- Get medical services

These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you are a victim of ID theft until you experience a financial consequence (mystery bills, credit collections, denied loans) down the road from actions that the thief has

Protecting Your Identity

Active Duty Alerts— add an extra layer of protection to the credit records of service members while they are deployed.

Credit Freeze FAQs

Identity Theft Protection Services— Other services that you can buy.

www.consumer.ftc.gov/topics/identity-theft

Prevent Identity Theft

Take steps to protect yourself from identity theft:

- Secure your Social Security Number (SSN). Don't carry your social security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.
- Don't respond to unsolicited request for personal information (your name, birthdate, SSN, or bank account number) by phone, mail, or online.
- Store personal information in a safe place at home.
- Review your credit card and bank account statements. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- Crate a strong password that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases.
- Review your credit report once a year to be certain that it doesn't include accounts that you have not opened. You can order it for free from www.annualcreditreport.com
  ⇒ Federal law allows you to get a free copy of your credit report every 12 month from each credit reporting company.

DATA BREACH

If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.

There are steps to take to help protect your information from being misused. Visit Equifax's website, www.equifax.com

- ♦ Click on the "Potential Impact" tab and enter your last name and the last six digits of your Social Security number.

Here are some other steps to take to help protect yourself after a data breach:

- **Check your credit reports**
- **Consider placing a credit freeze on your files**. A credit freeze makes it harder for someone else to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for changes you don't recognize
- **Place a fraud alert on your files.** A fraud alert warns creditors that you may be an identity theft victim

Helpful links

Federal Trade Commission (FTC)
www.ftc.gov
www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
www.consumer.ftc.gov/topics/identity-theft
www.consumer.ftc.gov/features/feature-0014-identity-theft

USA.gov
www.usa.gov/identity-theft
IdentityTheft.gov
www.identitytheft.gov/

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


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


CyberAware
HAPPY
#CYBERAWARE
MONTH
STAYSAFEONLINE.ORG/NCSAM
National Cyber Security
Awareness Month
STOP | THINK | CONNECT

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