THE SHIELD

DECEMBER 8, 2017

VOLUME II, ISSUE III

The University of Texas Rio Grande Valley
Information Security Office

Happy Holidays!

The UTRGV Information Security Office (ISO) hopes that you enjoy the winter break with your family, friends, and pets! We know that for this season there is a lot of online shopping, discounts, special offers, travel, and delicious food. Before we leave to have a pleasant time, we would like to thank you for your support and for reading this newsletter.

As you start to put together that shopping list, please consider the following security tips. Feel free to share them with your family and friends!

- Safe online shopping — Before purchasing any items, make sure your connection to the website is secure. Most browsers show a connection that is secure by having a lock and/or the letters HTTPS in green right before the website's name.
- Tech presents — Thinking of gifting an E-reader, tablet, smartphone, or smart device for home? Don't forget to check how to use the device safely and securely. All devices connected to the internet must be protected.
- Share with care — Think twice about posting your vacation details publicly on social media. You don't want for everyone to know that you are not home.
- Change your password — It's a good practice to change your password every twelve months. In addition, consider having all your passwords unique (specially for your financial accounts). Passwords managers can help you organize your passwords, and easily remember them.

Review your financial statements

Regularly review your credit card statements to identify suspicious charges, especially after you used your cards to make any online purchases or used a new site.

Graphic provided by Stay Safe Online .org

INSIDE THIS ISSUE:

EDITOR

Francisco Tamez
Security Analyst

www.utrgv.edu/is

From SANS Security Awareness. The Monthly Security Awareness Newsletter for Everyone. OUCH! November 2017

Shopping Online Securely

The holiday season is nearing for many of us, and soon millions of people around the world will be looking to buy the perfect gifts. Many of us will choose to shop online in search of great deals and to avoid long lines and impatient crowds. Unfortunately, this is also the time of year many cyber criminals create fake shopping websites to scam and steal from others. Below, we explain the risks of shopping online and how to get that amazing deal safely.

Fake Online Stores

When selecting a website to make a purchase, be wary of websites advertising prices dramatically cheaper than anywhere else or offering products that are sold out nationwide. The reason their products are so cheap or available is because what you will receive is not legitimate, may be counterfeit or stolen, or may never even be delivered.

Protect yourself by doing the following:

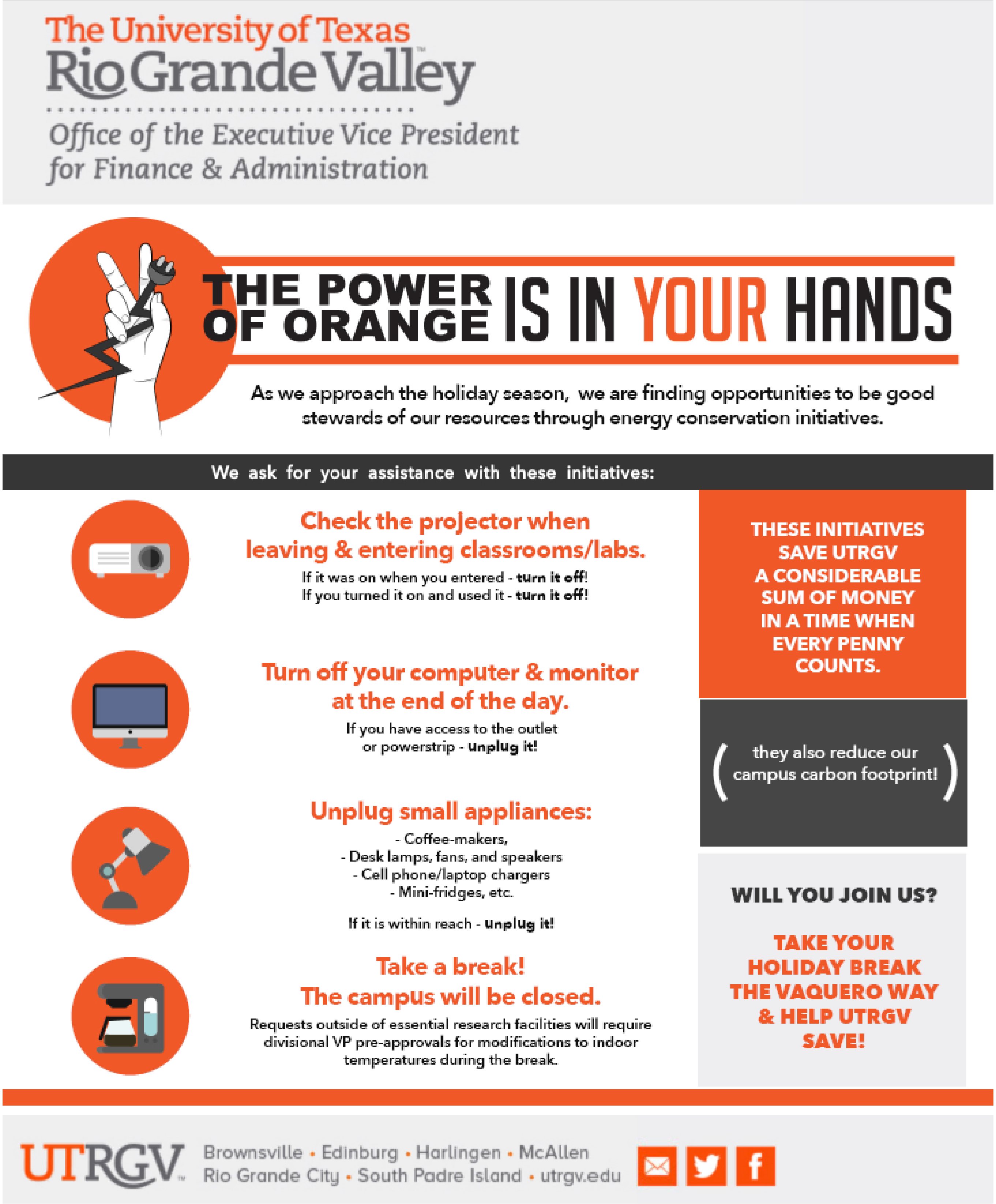
- Be very suspicious if a website appears to be an exact replica of a well-known website you have used in the past, but its domain name or the name of the store is slightly different. For example, you may be used to shopping online at Amazon, whose website is https://www.amazon.com. But be very suspicious if you find yourself at websites pretending to be Amazon, such as http://store-amazoncom.com.
- Type the store's name or URL into a search engine and see what other people have said about the website in the past. Look for terms like "fraud," "scam," "never again," or "fake." A lack of reviews can also be a sign indicating that the website is very new and might not be trustworthy
- Before purchasing any items, make sure your connection to the website is encrypted. Most browsers show a connection is encrypted by having a lock and/or the letters HTTPS in green right before the website's name.

Your Computer/Mobile Device

In addition to shopping at legitimate websites, you want to ensure your computer or mobile device is secure. Cyber criminals will try to infect your devices so they can harvest your bank accounts, credit card information, and passwords. Take the following steps to keep your devices secured:

•If you have children in your house, consider having two devices, one for your kids and one for the adults. Kids are curious and interactive with technology; as a result, they are more likely to infect their own device. By using a separate computer or tablet just for online transactions, such as online banking and shopping, you reduce the chance of becoming infected.
•Always install the latest updates and run up-to-date anti-virus software. This makes it much harder for a cyber criminal to infect your device.

Continue reading in SANS.org : bit.ly/SANS-OUCH-112017



The University of Texas Rio Grande Valley

Office of the Executive Vice President
for Finance & Administration

THE POWER OF ORANGE IS IN YOUR HANDS

As we approach the holiday season, we are finding opportunities to be good stewards of our resources through energy conservation initiatives.

We ask for your assistance with these initiatives:

Check the projector when leaving & entering classrooms/labs.

If it was on when you entered - **turn it off!**
If you turned it on and used it - **turn it off!**

Turn off your computer & monitor at the end of the day.

If you have access to the outlet or powerstrip - **unplug it!**

Unplug small appliances:

- Coffee-makers,
- Desk lamps, fans, and speakers
- Cell phone/laptop chargers
- Mini-fridges, etc.

If it is within reach - **unplug it!**

Take a break! The campus will be closed.

Requests outside of essential research facilities will require divisional VP pre-approvals for modifications to indoor temperatures during the break.

THESE INITIATIVES SAVE UTRGV A CONSIDERABLE SUM OF MONEY IN A TIME WHEN EVERY PENNY COUNTS.

(they also reduce our campus carbon footprint!)

WILL YOU JOIN US?

TAKE YOUR HOLIDAY BREAK THE VAQUERO WAY & HELP UTRGV SAVE!

UTRGV

Brownsville • Edinburg • Harlingen • McAllen
Rio Grande City • South Padre Island • utrgv.edu

From Stay Safe Online . org

Happy Online *Holiday* Shopping

According to a Pew Research Center survey, Americans use a wide range of digital tools and platforms to shop, and roughly 80 percent of adults purchase products online. Mobile has taken over holiday gift giving: last year, half of website visits and 30 percent of online sales were conducted via mobile devices. Gift givers are going mobile to conveniently compare products, read reviews and make purchasing decisions while out and about. Technology also ranks high on shopping lists – from new laptops and gaming systems to tablets, the latest phones and Internet of Things (IoT) devices like video cameras, toys and appliances.

"All tech users – especially vulnerable audiences like teens and seniors – need to take responsibility and protect themselves against cyber threats, scams and identity theft – not only during prime shopping time, but every day," said Michael Kaiser, NCSA's executive director. "In past years, we have seen that scammers, hackers and cybercriminals are actively on the prowl during the holidays. Stay alert for phishing emails, deals that look to good to be true and warnings about packages that can't be delivered or orders that have problems. Continually learn about and always initiate basic safety and security practices, and you will connect with more peace of mind during the holidays and year-round."

'Tis the season for many teenagers to receive their first smartphones, tablets or other devices. When giving the gift of technology, parents should also give the gift of safety. While most young people have grown up with technology and are comfortable navigating their online lives, the Keeping Up with Generation App: NCSA Parent/Teen Online Safety Survey revealed that teens and parents are aligned on their top three concerns (ranked as thing they are "very concerned" about), which are:

- Someone accessing a teen's account without permission (teens, 41%, vs. parents, 41%)
- Someone sharing a teen's personal information about them online (teens, 39%, vs. parents, 42)
- Having a teen's photo or video shared that they wanted private (teens, 36%. vs. parents, 34%)

The good news is that teens turn to their parents for help, with almost half (47%) saying their parents are among their top three sources for learning how to stay safe online, compared with 40 percent who say their friends are top sources. With this is mind, giving a tech-inspired gift may offer the opportune time to begin the internet safety and security dialogue.

Continue reading in Stay Safe Online .org : bit.ly/staysafeonline-NCSA-Holiday2017

ISO Spotlight

The ISO Spotlight interviews an individual that plays a role in UTRGV or information security. In this issue, you will meet Eloy Alaniz, who is UTRGV's Chief Audit Officer.

Eloy Alaniz
Chief Audit Officer
The University of Texas Rio Grande Valley

1. **Tell us how information security has changed since you started in your role.**
   Many things have changed since I started my role as an internal auditor. Technology has advanced creating innovative ways of doing business. Business is more mobile than ever. Smart phones and iPad/ Tablets have consumed our daily lives. Confidential and/or sensitive information is traversing through, and in some cases, being stored on these devices. Therefore, information security is more important than ever.

2. **Who are your customers, and what is one of the most challenging areas for you?**
   Through our internal audit activity, we not only serve internal customers such as executive management, students, faculty and staff of UTRGV, but also external parties such as taxpayers and funding agencies.

3. **How did you come into the security field?**
   As an internal auditor focusing on enterprise wide risks, I have an appreciation and an obligation to assist in protecting the assets of the institution. And that includes information security.

4. **Top 3 life highlights:**
   - Birth of my boys
   - Birth of my boys
   - Birth of my boys

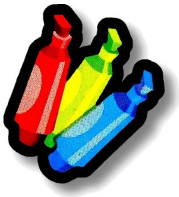
5. **People would be surprised to know:**
   I like heavy metal music and I'm funny

6. **Which CD do you have in your car? Or what radio station do you listen to?**
   CDs? Really? I stream music through either Pandora or Spotify. Pandora 80's hairbands.

7. **If given a chance, who would you like to be for a day?**
   No one else but ME.

8. **What is the best advice that you have received and that you have used?**
   Surround yourself with good people.

9. **What would be your advice for a new professional?**
   I have several pieces of advice…surround yourself with good people, give people the benefit of the doubt, balance work life with personal life, work on things only you can control.



SECURITY HIGHLIGHTS

Forever 21 reports data breach, failed to turn on POS encryption

The clothing retailer Forever 21 reported that unauthorized access to its payment card system when the encryption installed on some of those systems was not operational.

The Los Angeles-based chain said in a statement that it was informed of the problem by a third-party vendor and that the issue took place between March and October 2017. The 600-store chain noted that only a limited number of point-of-sale payment systems were affected, although the company did not issue say how many could be involved. The retailer had rolled an encryption and tokenization solution to secure its POS stations in 2015, but for an as yet unstated reason this was not in operation in all of its locations.

The fact that encryption was turned off on some of the company's payment card readers is indicative of poor cybersecurity hygiene, said Mike Kail, CTO of Cybric.
bit.ly/Forever21-databreach

WannaCry ransomware: Hospitals were warned to patch system to protect against cyber-attack—but didn't

The National Health Service (NHS) was left vulnerable to the WannaCry ransomware attack because, despite local health trusts being warned to patch their systems, many had failed to do so.

A National Audit Office (NAO) investigation into May's global cyber-attack -- which took down IT systems at many NHS organizations -- has found that the impact of WannaCry could have been prevented if basic security best practice had been applied.

Locked out of systems by the file-encrypting malware, many NHS bodies had to resort to pen and paper and thousands of operations and appointments were cancelled.
bit.ly/WCry-Hospitals-nopatch

Uber concealed hack of 57 million accounts for more than a year

Hackers stole names, email addresses, and phone numbers of 57 million Uber riders around the world in a breach dating back to October 2016. Data on more than 7 million drivers was also stolen, including over 600,000 drivers' license records.
bit.ly/Uber-databreach2017

Up to 5 million people fell for fake WhatsApp application

A sneaky app called 'Update WhatsApp Messenger' has been downloaded by users on the Google Play store, who were fooled by a developer title with hidden characters.

Once downloaded, users realized that the app was a fake version that served users with adverts to download other apps.

A spokesperson for Google said: 'I can confirm that the app was removed from Google Play and the developer account was suspended for violating our program polices.'

Experts warned that the malicious apps can take control of devices without the user's knowledge.
bit.ly/5million-fall-FakeWhatsApp

New scam targets Netflix customers

Scam or "phishing" emails that look like they're coming straight from Netflix are asking customers to update their payment information. Customers are told there was a billing error, and are asked to either email their billing information, or click on a link to enter it. The email even includes "copyright" dates -- but the notice is not coming from Netflix.
bit.ly/Phishing-Netflix

Graphic provided by Stop Think Connect .org

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	Product	Version
Windows	7	OS X 10.11	El Capitan	Adobe Flash Player	26.0	Android	Jelly Bean	Java SE	8
Windows	8	OS X 10.12	Sierra	Adobe Reader	2017.012	iPhone	iOS 9.1	Internet Explorer	11
Windows	8.1	OS X 10.13	High Sierra	Adobe Acrobat X	2017.012			Google Chrome	60.2
Windows	10							Firefox	55.0.2

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@$$WORD

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.

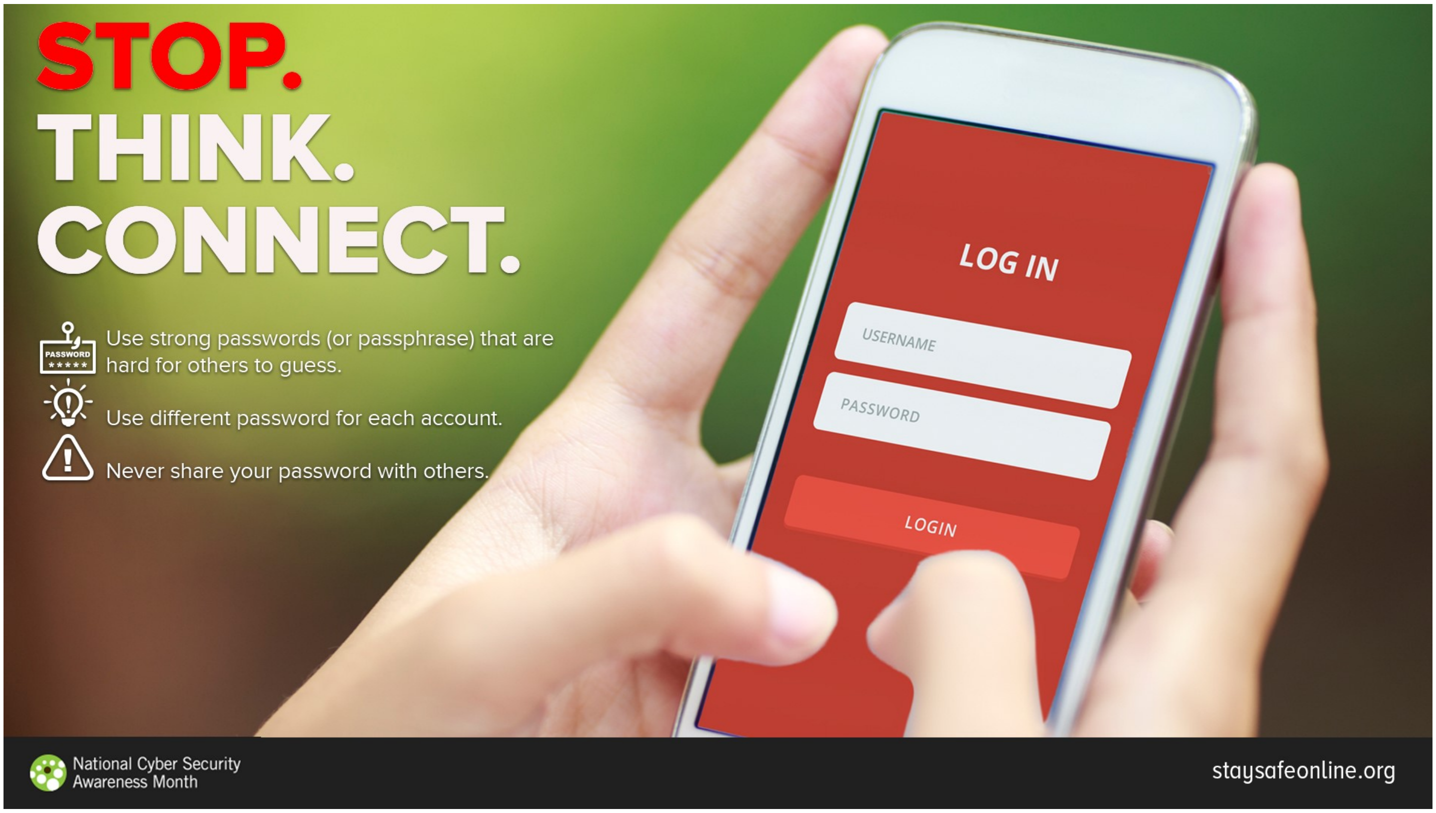
□ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.

□ 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]*



STOP. THINK. CONNECT.

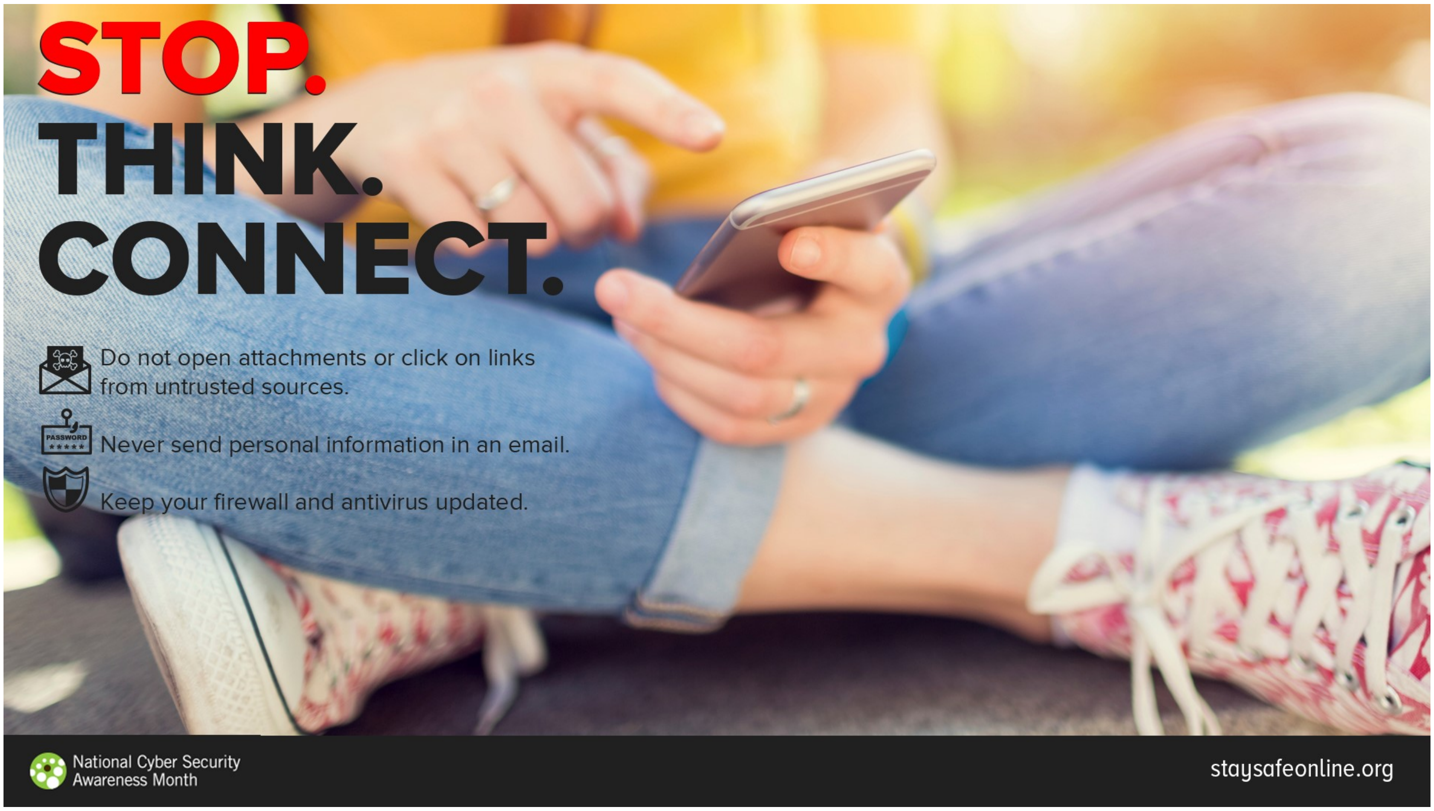
Use strong passwords (or passphrase) that are hard for others to guess.

Use different password for each account.

Never share your password with others.

National Cyber Security Awareness Month

staysafeonline.org



STOP. THINK. CONNECT.

Do not open attachments or click on links from untrusted sources.

Never send personal information in an email.

Keep your firewall and antivirus updated.

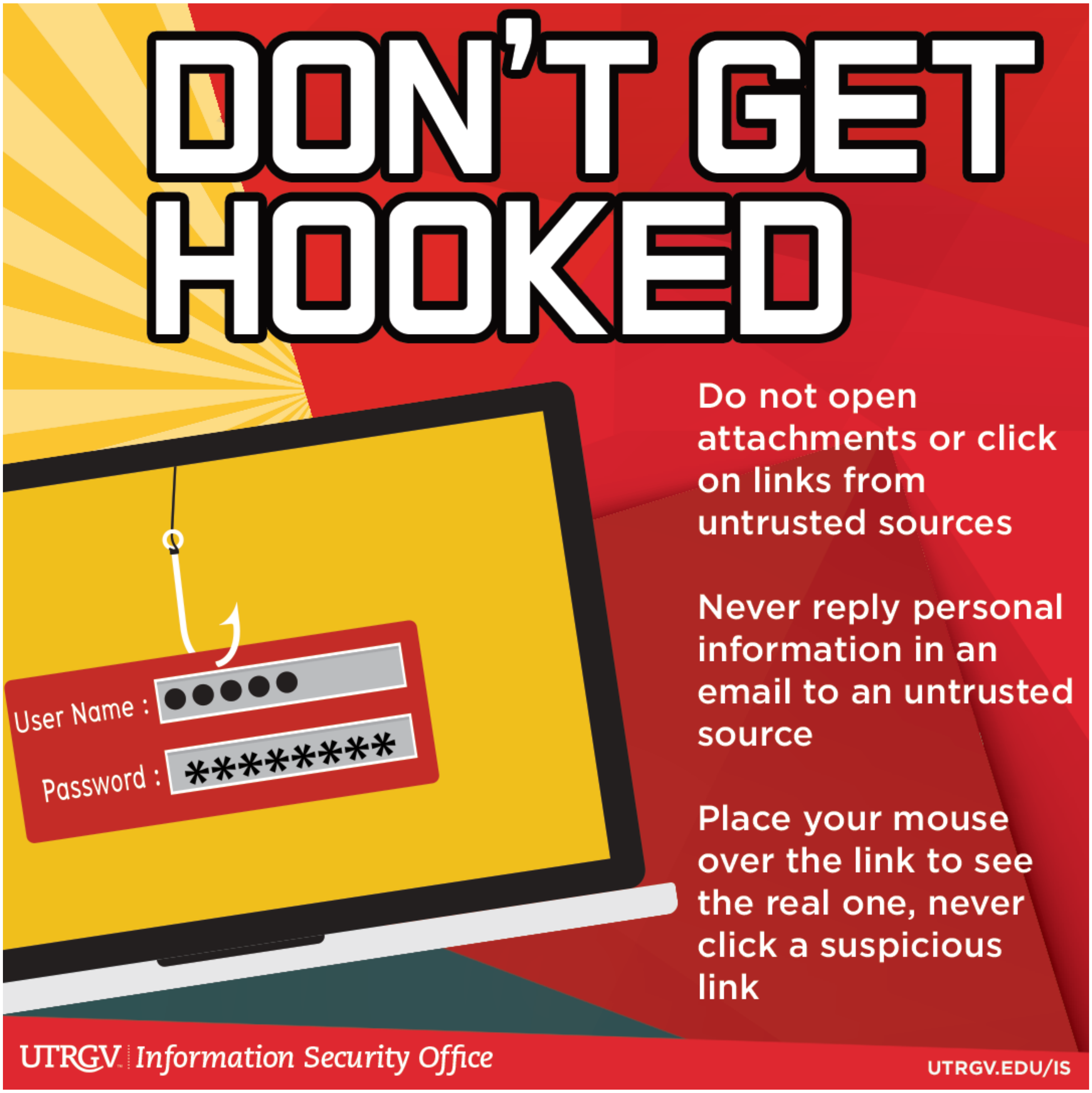
National Cyber Security Awareness Month

staysafeonline.org

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 HOOKED

Do not open attachments or click on links from untrusted sources

Never reply personal information in an email to an untrusted source

Place your mouse over the link to see the real one, never click a suspicious link

UTRGV Information Security Office

UTRGV.EDU/IS

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

#CyberAware
LOOK FOR
THE "S"
IN HTTPS://
THESE SITES TAKE
EXTRA SECURITY MEASURES
STAYSAFEONLINE.ORG
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

Special Thanks To:

University Auditor
Eloy Alaniz
Chief Audit Officer