The University of Texas Rio Grande Valley

Information Security Office

All Hands Meeting

Information Security

Thomas Owen
Chief Information Security Officer

Cesar Pastore
Information Security Analyst

Terri Mejia
Program Specialist

Jonas Del Angel
Security Analyst

Francisco Tamez
Security Analyst

7/23/2018

- Why Cybersecurity Is Relevant?
- Security Incidents
- Policies and Standards
- Data Protection

Why IT Matters to Higher Education

EDUCAUSEreview

"The **2018 Top 10 IT Issues** list is a story of the convergence of higher education's biggest concerns with technology's greatest capabilities."

1. Information Security

"In light of recent developments (e.g., the massive data breaches at Equifax and Yahoo), this is now an important issue"

"But also emerging within the Teaching and Learning community is a renewed concern about student privacy"

https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2018

https://er.educause.edu/articles/2018/1/teaching-learning-and-it-issues-points-of-intersection

Why Cybersecurity Is Relevant?

"The core functionality of cybersecurity involves **protecting information and systems from major cyberthreats**. These cyberthreats take many forms (e.g., application attacks, malware, ransomware, phishing, exploit kits).

Unfortunately, cyber adversaries have learned to launch automated and sophisticated attacks using these tactics – at lower and lower costs."

Palo Alto Networks

Information Security #1

EQUIFAX

143 million U.S. consumers impacted from Data Breach

- Social Security Number
- Birth Date
- Addresses
- Driver's License Numbers
- Credit Card Numbers

https://www.equifaxsecurity2017.com/

YAHOO!

3 billion

Yahoo user's:

- Names
- Email Addresses
- Passwords

TARGET

40 million credit and debit cards of shoppers who shopped at U.S. Target stores between November 27 and December 15 2013"

https://www.nbcnews.com/technology/massive-target-credit-card-breach-new-step-security-war-hackers-2D11778083

Information Security #1
For Higher Ed

Newcastle University spoofed in phishing scam

Cybercriminals cloned the Newcastle University website

Data breach at Oklahoma U impacts 30K students

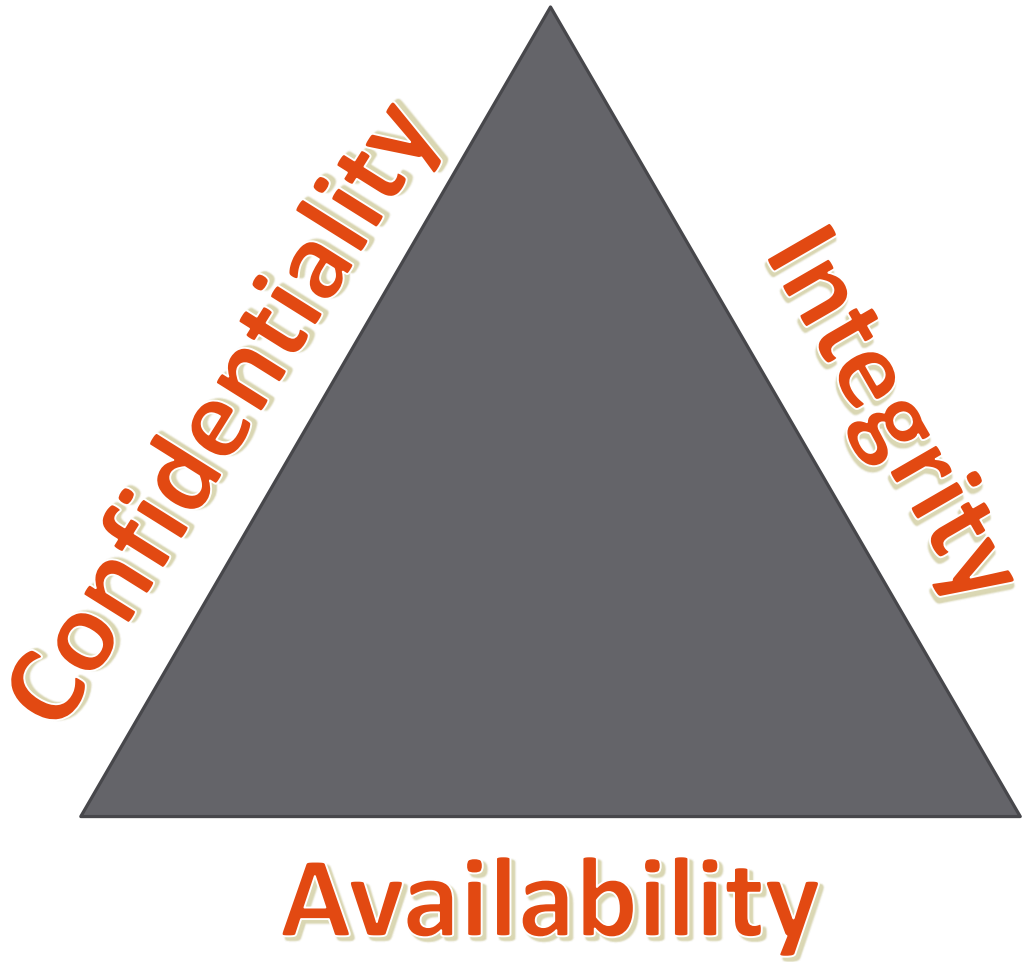
Social Security numbers, financial aid information and grades dating to at least 2002

Los Angeles college pays $28,000 in ransomware

University of Calgary paid $20K in ransomware attack

http://www.cbc.ca/player/play/701283395504/

C.I.A



Why Cybersecurity Is Relevant?

- Security Incidents
- Policies and Standards
- Data Protection

Security Incident

Lost/Theft of computing device

- All University owned and personal computing devices (storing University data)
- For example: computer, laptop, tablet, smartphone

Lost/Theft of external digital storage device

- Thumb/USB drive, DVD, CD, etc.

Unauthorized or Unintended disclosure of Confidential or Sensitive information

- Credit Card Number
- SSN

Compromised Credentials

- UTRGV accounts and password

Cyberstalking, Bullying, or Harassment

Security Incident Cont'd

Compromised University Website

Virus, Worm, or Malware Infection

- Damage, disrupt, steal data or networks

Cryptoware or Ransomware Infection

- Trojan that encrypts certain types of files, then it would ask for ransom

Phishing

- The fraudulent practice of sending emails claiming to be from a known source in order to convince individuals to reveal personal information

05/18/2016

From: Frank Tamez [frank.tamez@utrgv.edu]
Subject: Very Urgent

To: noreply@utrgv.edu

I received this message from your mailbox and I have upload the documents via Microsoft Exchange Portal just Get Started and sign in with your email address to vire documents.

Best Regards

viruswebsite.net/inc/.s/

Frank Tamez

Admin Guy / Department of College

University of Texas – Rio Grande Valley

Edinburg // Brownsville

From: University of Memphis Webmail Management [webmaster@memphis.edu]

Sent: Thursday, May 19 2016 3:52 PM

Subject: VERIFY YOUR EMAIL ACCOUNT

Attention Outlook Web User

This message is to all University of Memphis Webmail Users

We are currently upgrading our data base and webmail network.

All inactive email accounts will be deleted, as we intend to create more space for registration of new users (Staff and Students).

To prevent your account from being deleted, we kindly request that you confirm your account information for update, by providing the information below.

Username:
Password:

Warning! Failure to o this will render your email permanently.

Thanks for your understanding

Warning Code: VX2G99AAJ

University of Memphis Webmail Management

Sneak Peek

Phish Alert Button (PAB)

- A safe way to forward potentially malicious emails to information security personnel for their review.
- This feature will also automatically remove the suspicious email from your inbox to prevent future exposure.

Office Outlook

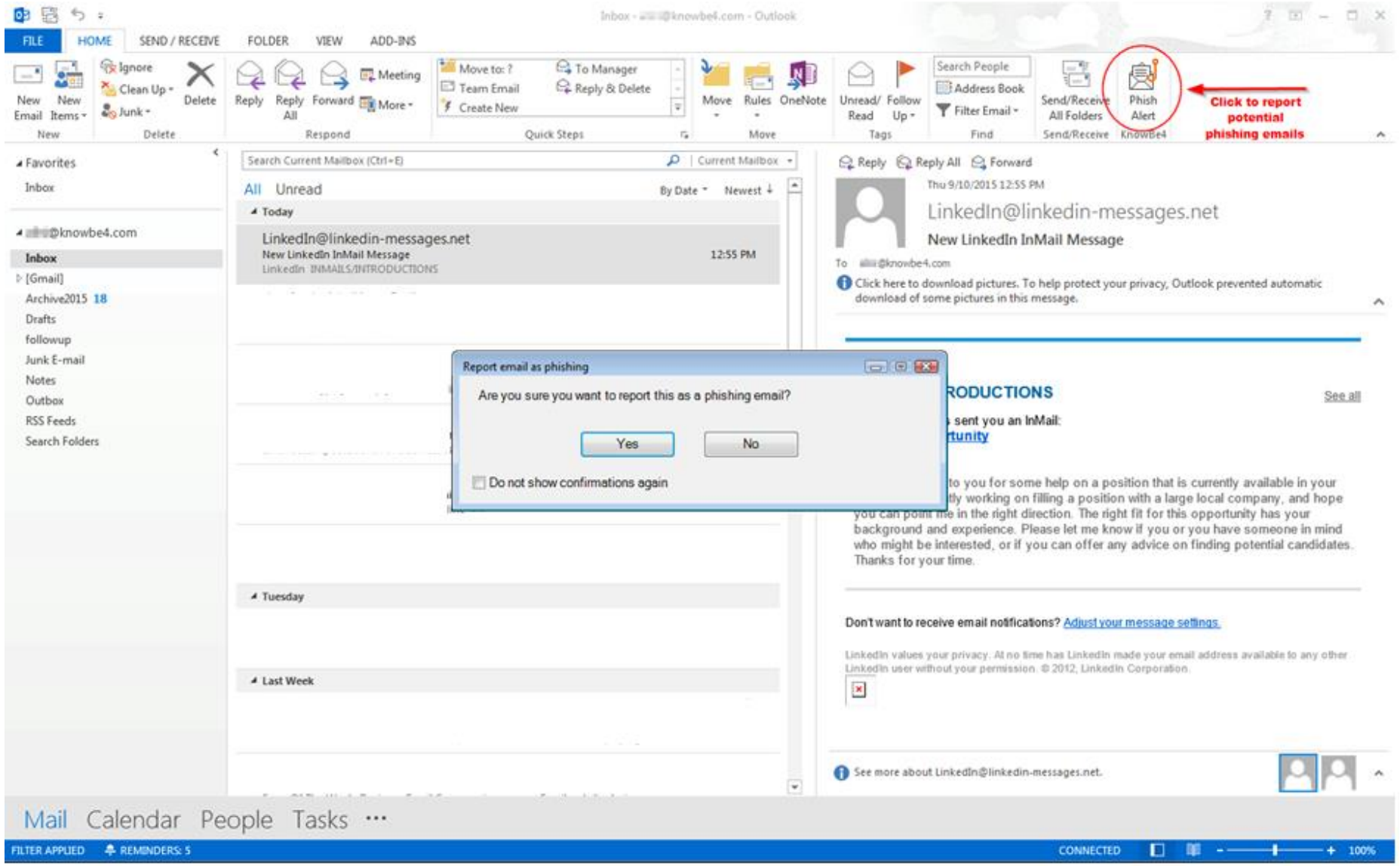
Phish Alert

Phish Alert Button add-in for Outlook in Office 365

Phish Alert Button add-in for Outlook 2016

Sneak Peek

Phish Alert Button (PAB)

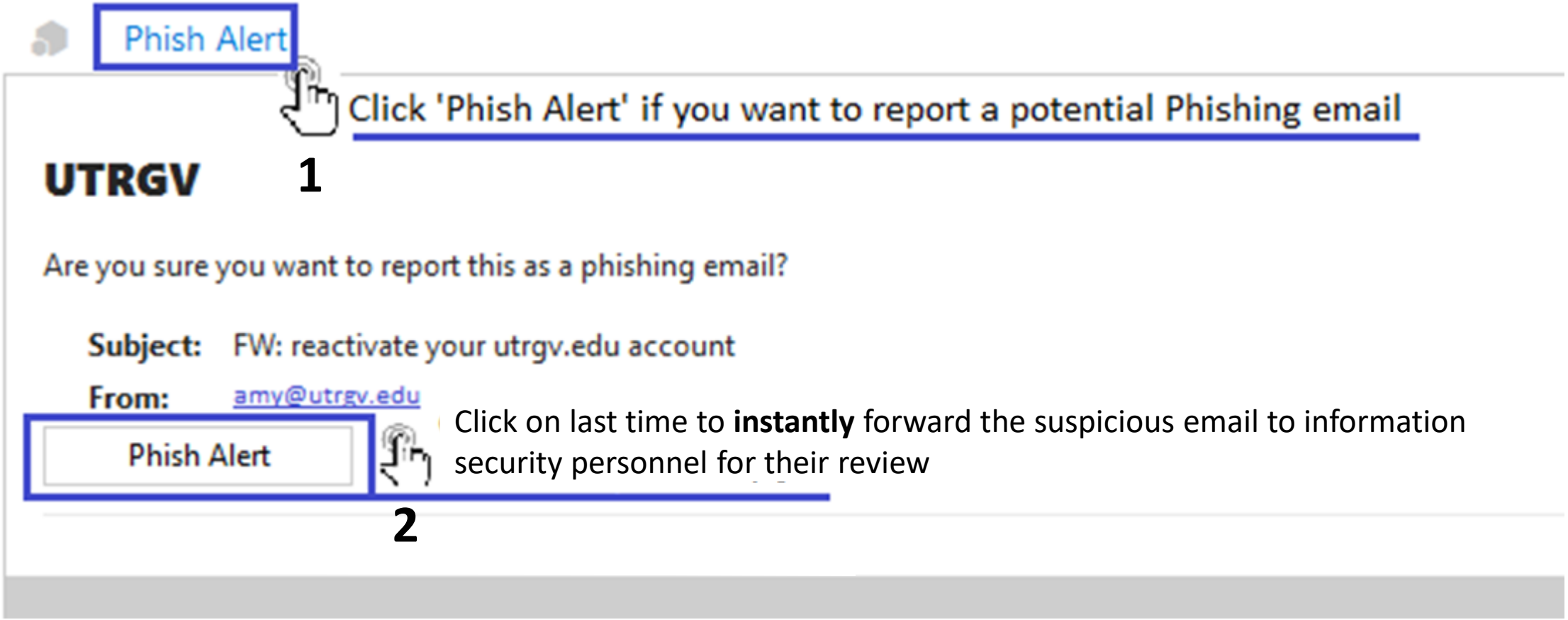


Sneak Peek

Phish Alert Button (PAB)

Office

Outlook



Why Cybersecurity Is Relevant?

Security Incidents

Policies and Standards

Data Protection

Policy Reviews

TAC 202

- Establish information Security Standards for Institutions of Higher Education
- States the rules for: Responsibilities of the Institution Head, Information Security Officer, and Staff.

UTS 165

- It is the policy of The UT System to protect Information Resources based on Risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of these resources.

UTRGV AUP

- Acceptable Use Policy for users and computers accessing UTRGV information resources as defined by UTS 165

Laws & Standard

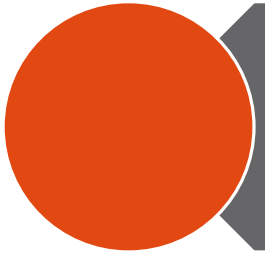
UTRGV Standards

- Computer Security Standard
- Data Classification Standard
- Two-Factor Authentication Standard

Why Cybersecurity Is Relevant?

Security Incidents

Policies and Standards



Data Protection

Data Protection

Personally Identifiable Information (PII)

Type: Data that uniquely identifies a person (SSN, DOB, Credit Card, Name, Address)

Who wants it: Identity thieves

Reason: Financial gain, to commit fraud

Intellectual Property (IP)

Type: Research, Inventions, literary and artistic works, design, images

Who wants it: Competitors, opportunists

Reason: Personal credit, patents, technological advance, financial gain

So how do we protect data at rest?

Encrypt

Transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.

Whole disk encryption to prevent unauthorized access to data storage.

To properly encrypt sensitive digital files you can use SPIRION/Identity Finder.

Remember that encryption does not protects you from virus/malware it protects you from unintended disclosure due to loss or theft.

SPIRION

Formerly Identity Finder

Will allow you to:

a. Delete (Shred) digital files

- Delete the files for PERMANENT disposal
- Encrypt and password protect the files, if you MUST have them on your computer

b. Find files in your computer that contain protected data

- SSN, Credit Card Number, Password

c. Should be pre-installed on all University owned computers.

- If not, contact the IT Service Desk

SPIRION
formerly Identity Finder

Protect data in motion

Because email messages are sent over the internet and might be intercepted by an attacker, it is important to add an additional layer of security to sensitive information.

To send an encrypted email just include [secure] at the beginning of the subject field of your email.

Example:

Subject: [secure] Monthly Report

www.utrgv.edu/it/how-to/email-encrypt-decrypt

Approved Storage Devices
Transport Media

APRICORN

Passwords

Why are passwords important?

- They provide validation
- They allow access and authorization
- They protect our data/information

Your UTRGV password allows access to

- Email
- Student records (FERPA) – subject to role
- Network access (Wired and WiFi)
- Confidential Files / Research papers (IP)
- Employee Data (Your SSN, Direct Deposit, Contact Info, Home Address)

Passwords (Cont'd)

The 5 Best Password Practices

1. **You Shall Choose One Wisely**

   Password123 VS #eY7453AB!! VS MyPassphraseRocks2!

2. **You Will Never Write It Down**

   NEVER!

3. **You Will Never Share It With Anyone**

   Not even your supervisor, IT, or Security (ISO)

   UTRGV personnel will never ask for it

4. **You Can Change It Often**

   Default policy is once per year

   The policy for Privileged users is more frequent

5. **You Will Be Mindful of Where You Use It!**

   Be careful of fake emails and websites that are made to look real

Passwords (Cont'd)

Multi Factor

Multi Factor Authentication

1. Something you know (e.g. passphrase)
2. Something you have (e.g. bank card, mobile phone, token)
3. Something you are(Biometrics: Fingerprint, voice, retina)

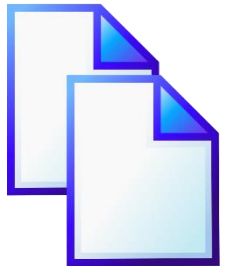
UTRGV

Uses DUO-Security for two factor authentication when accessing secure sites or establishing a VPN connection to the campus

https://www.utrgv.edu/is/en-us/resources/how-to/duo/

The University of Texas Rio Grande Valley™

Information Security Office



www.utrgv.edu/is

www.facebook.com/UTRGVISO

www.twitter.com/UTRGVISO

Additional Information

Why Cybersecurity Is Relevant?

Security Incidents

Policies and Standards

Data Protection

The University of Texas Rio Grande Valley™

Information Security Office

All Hands Meeting

Information Security

Francisco Tamez
Security Analyst

Cesar Pastore
Information Security Analyst

6/22/2018