Fraud & Cybersecurity: How to Protect RSCCD

RSCCD

Management Council

May 7, 2019

Learning Objectives

1. Why is RSCCD a target of fraud schemes?
2. How do we respond as managers?
3. Known fraud attempts against RSCCD and how we responded
4. Best Practices to Protect RSCCD

Learning Objective #1

- Why is RSCCD a target of fraud schemes?

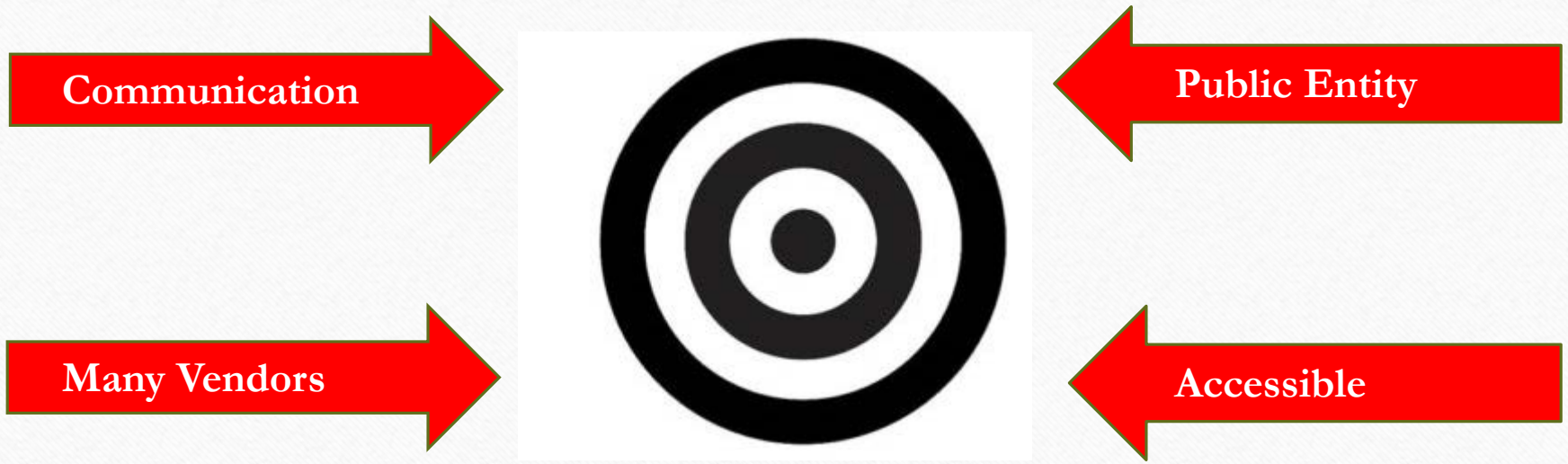
NATURE OF RSCCD

- Public Entity / Higher Education
- How we do business
  - Long-term employees / Confidence and Trust
  - Accessible
  - Communication internally
  - Vendor relationships

NATURE OF FRAUDSTERS

- Creative thinkers to invent scams, willing to take a chance with crime, fearless
- Scams now go well beyond hacking
- Impersonation of an employee by Business Email Compromise
- Social Engineering
- Use vendors to get at customers – RSCCD is a customer of each of our vendors

Why is RSCCD a target of fraud schemes?



The question is not **IF** it is happening … the answer is **WHAT** are we doing about it!

Questions – Stop 1

- Open discussion & questions

Learning Objective #2

- How do we respond as managers?

The answer is **WHAT** are we doing about it!

- The very nature of our business creates some unavoidable vulnerabilities
- Recognize that threats exist
- Maintain AWARENESS & VIGILANCE in our departments for all team members

Maintain Awareness & Vigilance

The question is not **IF** it is happening … the answer is **WHAT** are we doing about it!

Awareness and Vigilance need to be higher than our baseline level of risk

Learning Objectives #3

- Known fraud attempts against RSCCD and how we responded

Fraud Attempts

- Walkthrough recent examples that have already occurred
- Demonstrate how RSCCD responded correctly

The question is not **IF** it is happening … the answer is **WHAT** are we doing about it!

Example #1 – Email

Easter, Candi

From: Erika Almaraz <almaraz_erika@rsccd.edu>
Sent: Thursday, November 29, 2018 11:06 AM
To: Easter, Candi
Subject: Info

Are you available? Reply as soon as possible.

Sent from my iPhone

Thank you,

Erika Almaraz, CPA, CIA
Fiscal Services Manager
Accounting and Accounts Payable
Rancho Santiago Community College District
Office: (714) 480-7349

Timeline & Team Response

November 29 – Candi received suspicious email

November 29 – Candi discussed email with Erika

November 29 – Management Response - Erika emailed her full team to "Be Aware" of a suspicious email going around. Redistributed ITS literature as a reminder, "How To Spot A Phish"

November 29 – Manager informed ITS and ITS sent a reminder of online training to RSCCD

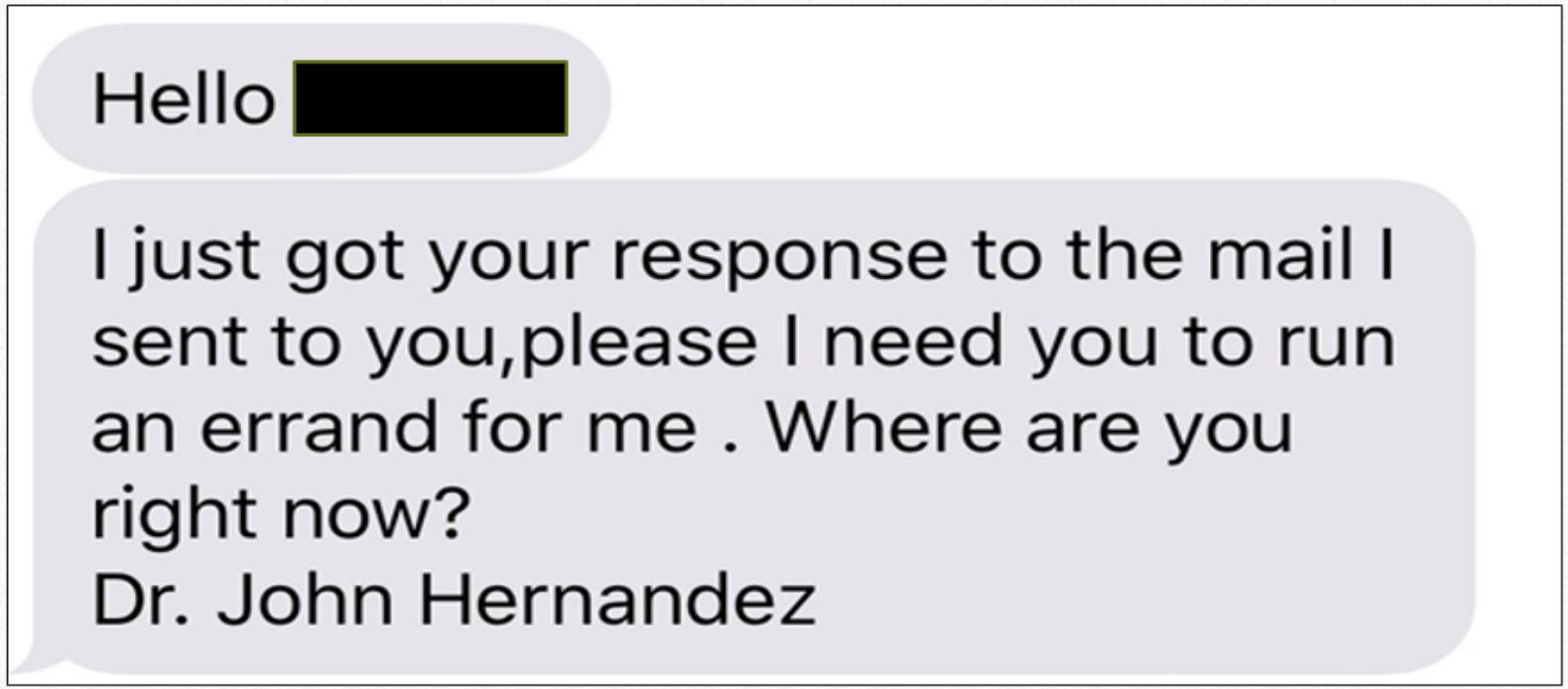
Example #2 – Email & Text

From: John C. Hernandez <president030030@gmail.com>
Sent: Wednesday, April 3, 2019 1:18 PM
To: [redacted]
Subject:

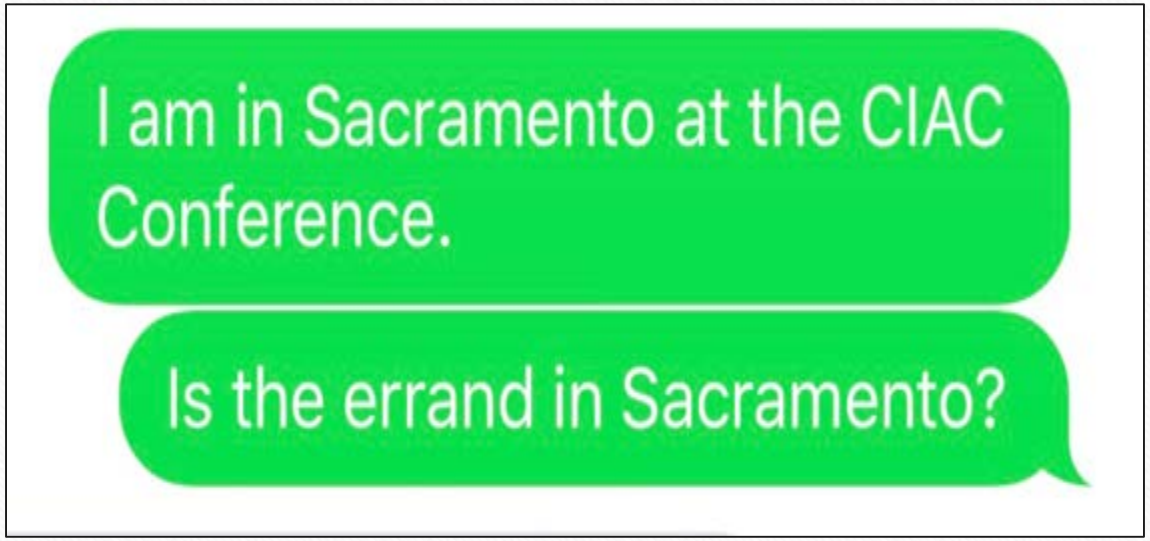
Good day,
I'm stuck in a seminar right now and i need your assistance which i will appreciate your help a lot.Kindly drop your cellphone number to send text message.
Thanks

Dr. John C. Hernandez, PH.D.
President
Santiago Canyon College

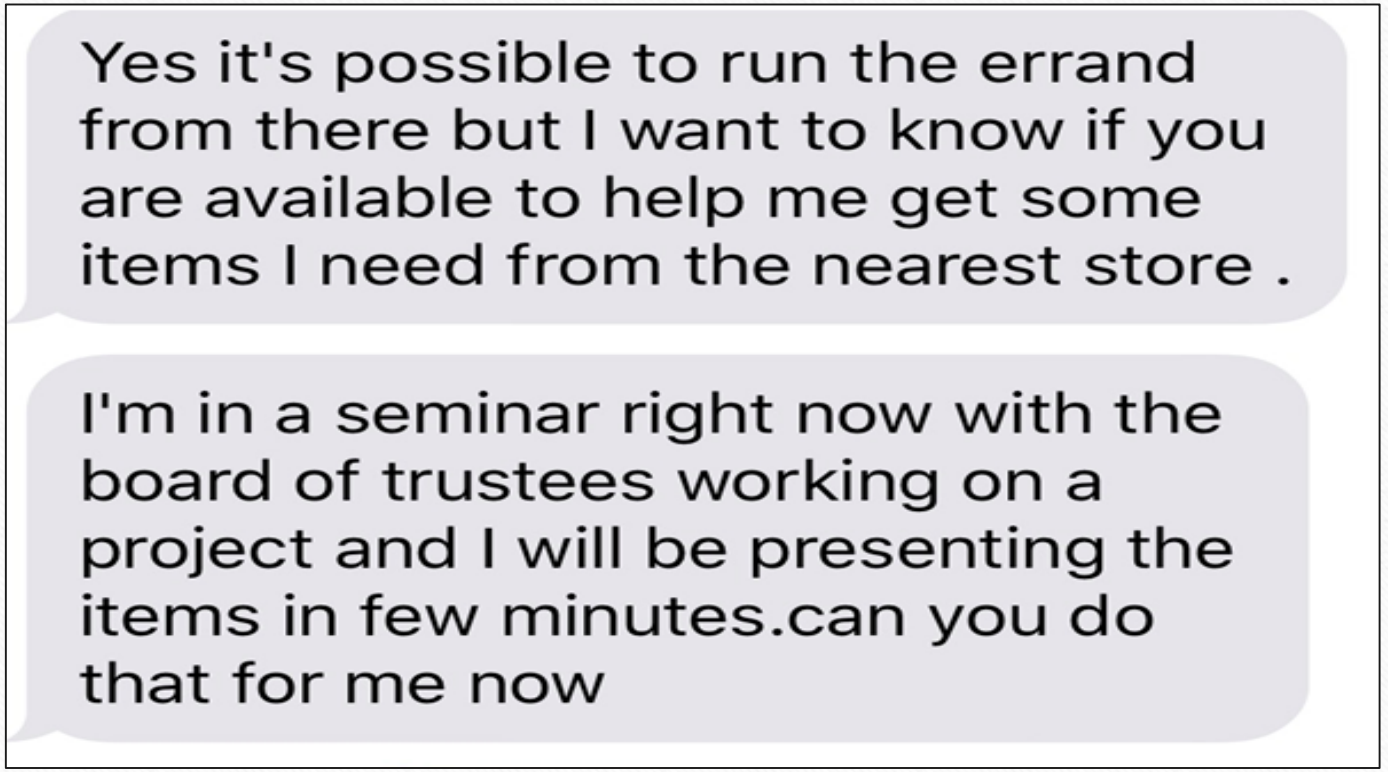
Example #2 – Email & Text



Example #2 – Email & Text



Example #2 – Email & Text



Example #2 – Email & Text

Example #2 – Email & Text

Timeline & Team Response

- This is an example of a specific scam, CEO Fraud Attack
- Campus employee received "personal" email from Dr. Hernandez
- Quickly transitioned to phone texting
- Red flags: Gmail account; Urgency; Odd request
- Employee escalated communications to ITS

Heads Up

- CEO Fraud Attack
- Impersonating an executive in “urgent” communications
- RSCCD will be a target when a new Chancellor is named

Questions – Stop 2

- Open discussion and questions

Example # 3 – Payroll Fraud

From: Email Address "appeared" as a valid system address
Sent: Friday, September 21, 2018 8:43 AM
To: Basham, Sherri <Basham_Sherri@rsccd.edu>
Subject: Direct Deposit Update

Sherri ,

I intend to update my current direct deposit to a new information , Kindly walk me through the Process and what is the deadline for Direct deposit change and will this change effect in my next pay.

Thanks

Employee Name Redacted

Timeline & Team Response

Sept 21 – An email from the employee's RSCCD email account was sent to Payroll to request a change in the direct deposit bank. Payroll responded to email providing the authorization form. On the same day, Payroll received the signed authorization in PDF from the employee's RSCCD email account. Payroll processed the request for the Sept 30 paycheck.

Oct 11 – Payroll implemented a new process requiring **in-person** authorizations only based on Orange County Dept of Education notification of a widespread fraud; this process change was done as a proactive measure.

Timeline & Team Response

Nov 29 – Employee called and said current check and past 2 checks had not been received in their credit union bank account.

Nov 29 – Payroll Manager prioritized this fraud immediately and recovered the funds for the current paycheck as a pending banking transaction; payroll started the research with employee and determined it was fraud.

Timeline & Team Response

Nov 29 - ITS was informed of the fraud and started an internal investigation. It was identified that the RSCCD email account had been compromised for over 3 months due to an OLD password (over 5 years old).

The corrective action was to change the password. Employee was using SAME password in their District & personal accounts. ITS recommended to change passwords in all sites and to monitor all personal accounts closely.

Dec 3 – Manual check was issued to the employee for all 3 missing paychecks.

Questions – Stop 3

- Open discussion & questions

Learning Objective #4

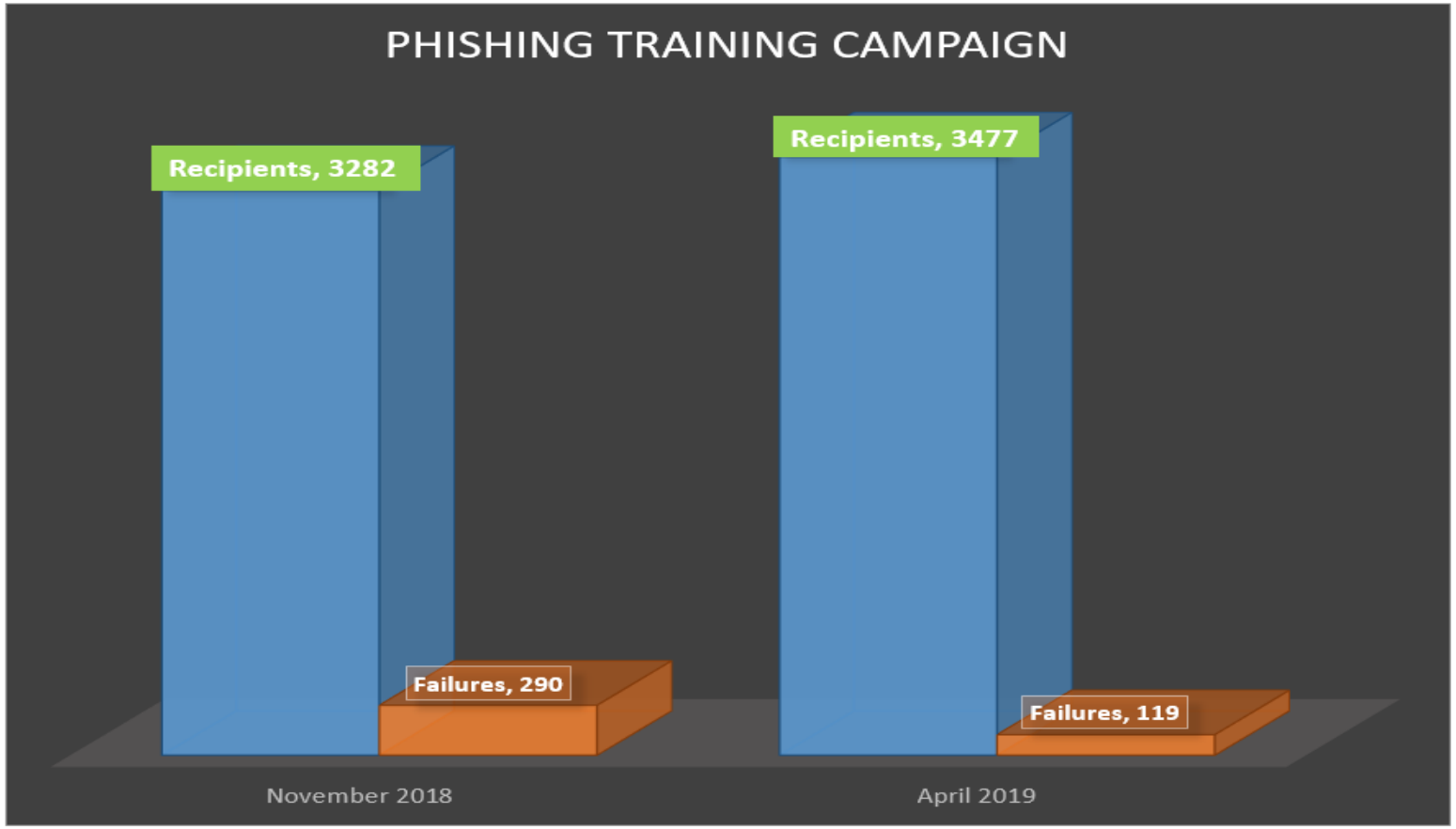
Best practices to protect RSCCD

- Co-create a culture of awareness and vigilance for all employees by reinforcing training
- Pay attention to alerts and DISCUSS with your teams on a regular basis
- Communicate to your teams the importance of changing passwords on a regular basis
- Alert your teams of the need to communicate ODD REQUESTS
- Management should keep employees informed on a continuous basis

ITS Literature

- ITS literature as a reminder, “How To Spot A Phish”
- CCCCO newsletter as a reminder, “Ransomware”

ITS Security Training Update



	November 2018	April 2019
Recipients	3282	3477
Failures	290	119
Phish Prone	8.84%	3.42%

Next Steps

- Voluntary Change Password Campaign
- ITS will conduct recurring quarterly security awareness training sessions for management on a drop-in basis to attend as schedule allows. Current topics such as cybersecurity, announcements for updates to online courses, and other related subjects will be covered.
- ITS is uploading online courses for employees. Certificates are issued upon completion.

Questions – Stop 4

- Final Questions