

OIT – Cybersecurity Incidents Webinar

OIT Behind the Scenes

Webinar Series



Setting Expectations



Lights!

- Camera & Audio



Action!

- Participatory Activities



Camera!

- Recorded Session



Cut!

- Q & A

Today's Agenda:

- Overview of cybersecurity & risk management
- Types of cybersecurity incidents
- How we deal with possible cybersecurity incidents
- What to do if you are involved in a cybersecurity incident



Cybersecurity Overview

Shane Middleton

UC Merced IT Cloud Engineer

What is Cybersecurity?

The protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.



INCIDENT RESPONSE

What is Risk Management?

The process of identifying, assessing, and mitigating threats to our organization's assets.



UC Merced Cybersecurity Team



Tolgay Kizilelma
Chief Information
Security Officer



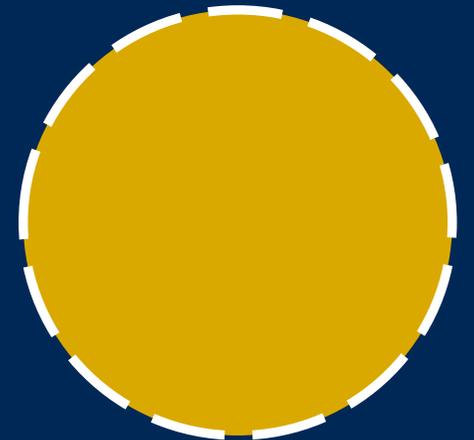
Shane Middleton
Cloud Engineer



Phil Herechski
Security Analyst



James McKenzie
Security Analyst



YOU!



Going Phishing

James McKinzie
IT Security Analyst

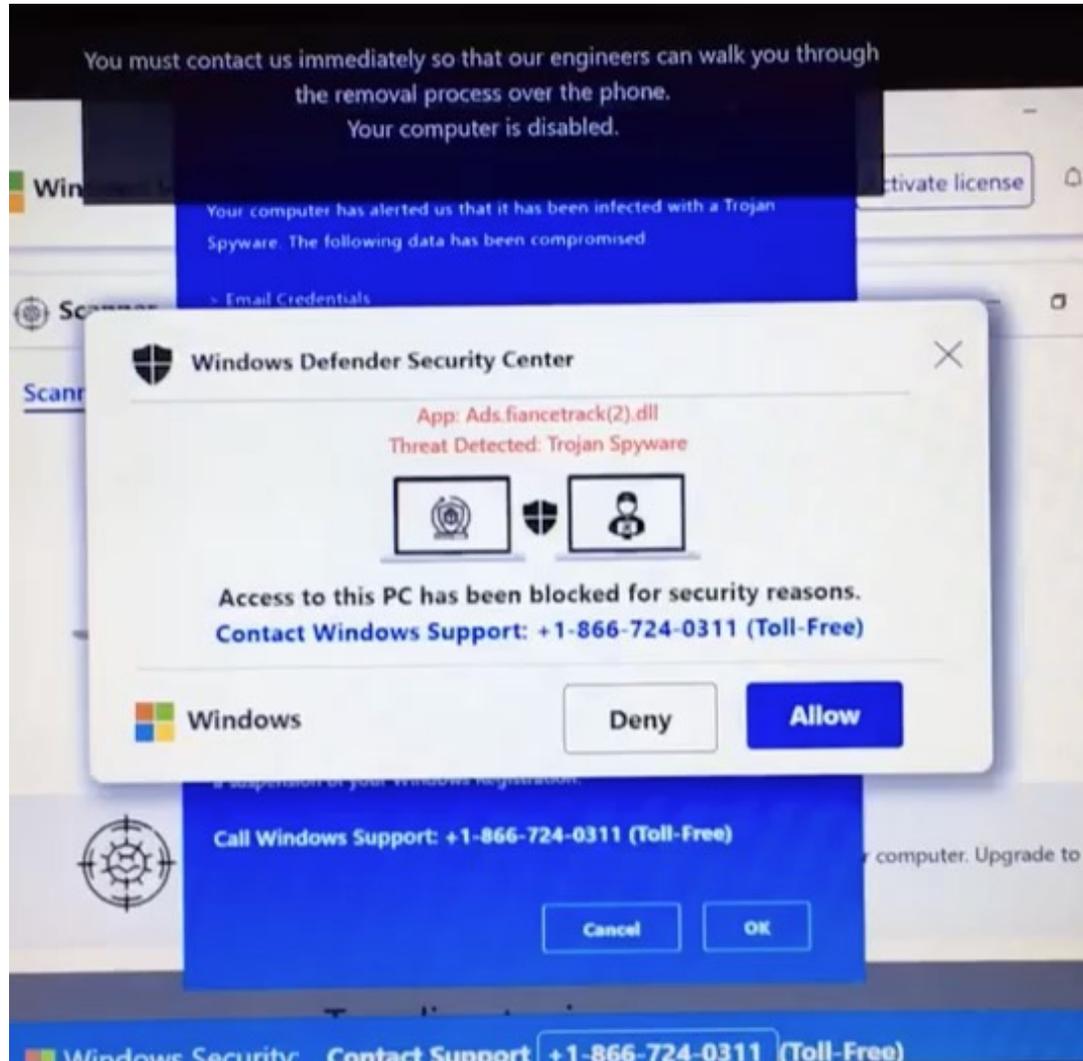
GOING PHISHING

What is Phishing?

- Target(s) typically contacted by 'bad actor' posing as legitimate institution/person
 - Can happen by email, phone, or text
- Attempting to lure you into providing sensitive data
 - personally identifiable info, banking/credit card details/passwords



GOING PHISHING



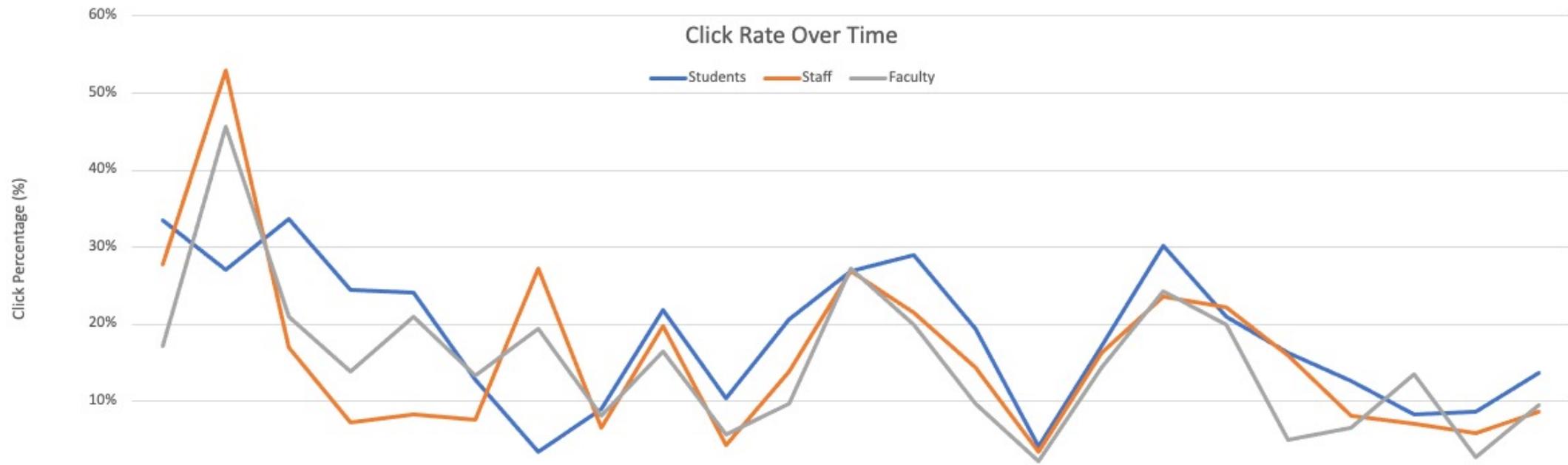
Types of Phishing

- Email
- Website
- 'Vishing' (video phishing)
- 'Smishing' (SMS phishing)

؟

GOING PHISHING

UC Merced Self-Phishing Campaigns



More than 1 million self-phishing emails sent since 2018

GOING PHISHING

How Phishing Works

- Impersonates a person or entity you know/are familiar with
- Vague or unrealistic details
- Sense of criticality/time sensitivity
- Asks that you provide information that should already have on file



Investigate the Display Name/Email Address:

Changing the "From" name is a classic phishing play for hackers, known as Spoofing.

Make sure the name and email address make sense.

Spelling Mistakes:

Legitimate emails rarely have major spelling mistakes or poor grammar – brands and corporations wouldn't allow that. Can you catch the typos?

From: Jobandinternshipfair <beygivens.w@gmail.com>

Sent: Monday, September 23, 2019 10:28AM

To: Xxxxx Xxxx; Yyyy Yyyyy; Zzzz Zzzz

Subject: Part Time Job Fair, Monday September 23rd

Review the Salutation:

Is the salutation to a vague "Valued Customer?" or "Dear User"? Legitimate businesses will often use your first and last name, so beware if it doesn't.

Good Morning! Hope you're enjoying you summer.

Seeking a job or internship this fall? Mark you calendar- the UNICEF Fall Part Time Job and Internship Fair is coming up September! This is the perfect opportunity to connect with both on and off campus employers seeking ALL majors to fill part-time and internship positions! |

If you looking <http://www.badguys-hq.xyz> please (see attached). If you want to register, go to our website at

<https://www.unicef-jobs.org>

Act soon since we fill up fast!!!

Feel free to pass along the application to anyone that maybe a good candidate.

Best, Terry

Attachments can be Dangerous Too!

Hackers can embed attachments with viruses and malware that can steal your passwords, damage files on your computer, or even spy on you.

The Signature Line

Are you able to contact the company? Does the email provide details about the signer? Legitimate businesses always provide contact information.

Look But Don't Click

Hackers love to embed malicious links with fake link text. To expose this fraud, hover your mouse over the link.

Urgent or Threatening Language

Beware of emails that promote a sense of urgency or fear. Hackers know people will act without thinking if they feel rushed.

Ways to Circumvent Phish Attempts

1

Read
carefully

2

Investigate
links before
you click

3

Don't click,
enter the
URL yourself

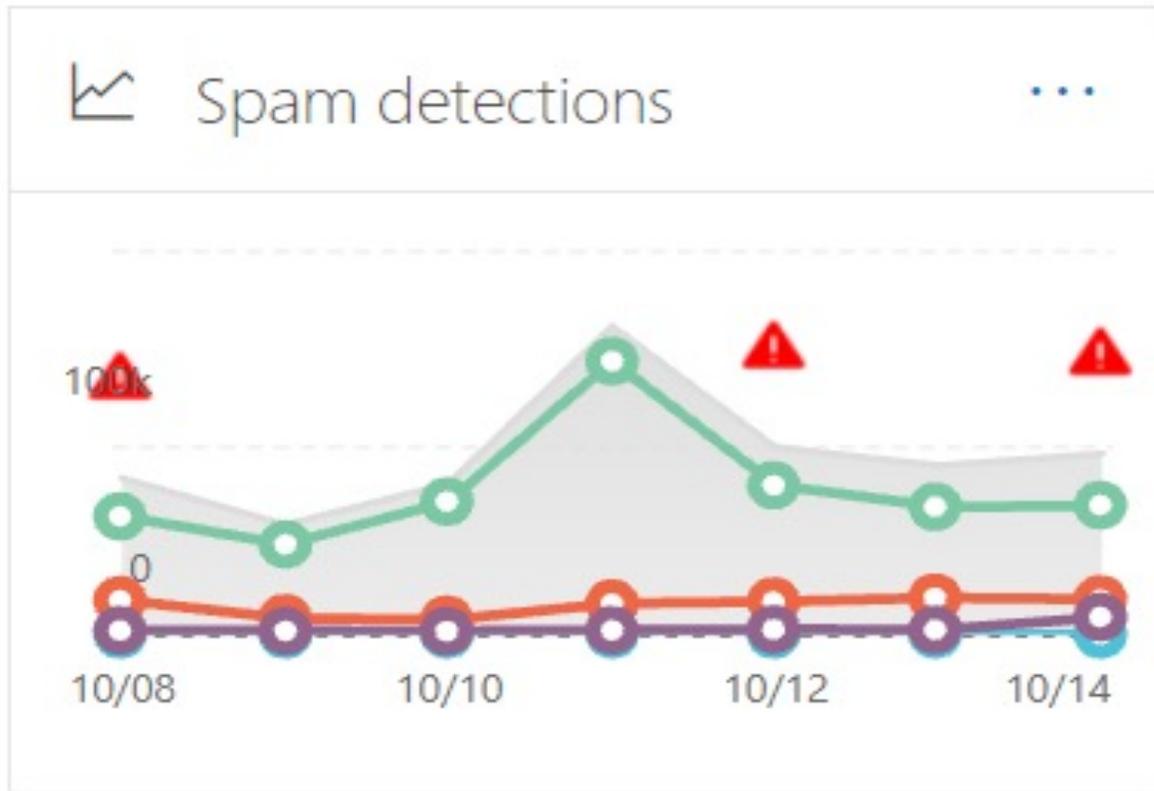
4

Give the
wrong
information

5

Think and
trust your
instincts

GOING PHISHING – SPAM/PHISH DETECTIONS



Total Email	161805	Percent blocked
Phishing rules blocked	16222	10.026%
Blacked listed site blocked	143399	88.625%

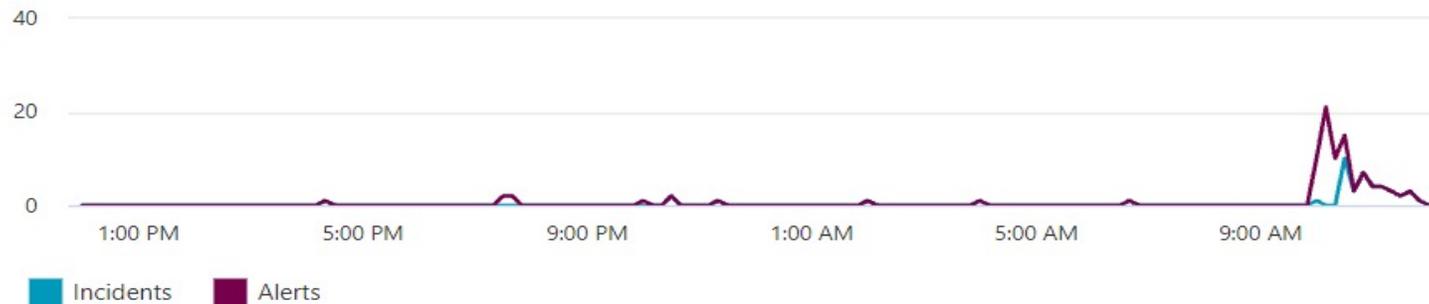
GOING PHISHING – PHISHING REPORTING

Active incidents

247 active incidents

Relevant for last 30 days

Most recent incidents and alerts



Incident name	Tags	Severity	Last activity	Scope
Email reported by user as malware c		Low	Oct 15, 2021 11:47 ...	0 0 1
Email reported by user as malware c		Low	Oct 15, 2021 11:45 ...	0 0 1
Email reported by user as malware c		Low	Oct 15, 2021 11:41 ...	0 0 1
Email reported by user as malware c		Low	Oct 15, 2021 11:40 ...	0 0 1

GOING PHISHING – OIT PHISHING RESOURCES

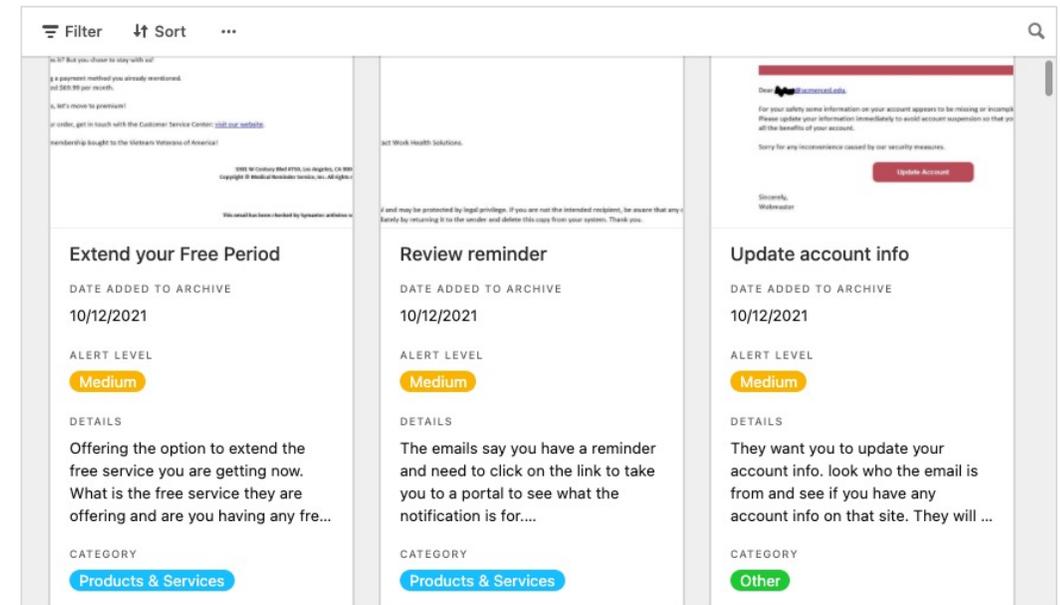
 <https://it.ucmerced.edu/phishing>

- Phishing Archive
- Ways to Spot a Phish Explainer
- Self-phishing campaign information
- Report a Phish

Phishing Email Archive

UC Merced Information Security encourages faculty, staff, and students to exercise caution when opening emails that contain links or attachments. We want our campus community to report phishing scams and to contact us when they aren't sure if an email is a phishing scam.

As part of our campus user education and awareness program for phishing scams, we have created an archive of known phishing attacks currently active on our campus. We hope this will help users to better identify and avoid these pesky and annoying emails! Browse the archive below to see examples of what to look out for.



Filter	Sort	...
Extend your Free Period DATE ADDED TO ARCHIVE 10/12/2021 ALERT LEVEL Medium DETAILS Offering the option to extend the free service you are getting now. What is the free service they are offering and are you having any fre... CATEGORY Products & Services	Review reminder DATE ADDED TO ARCHIVE 10/12/2021 ALERT LEVEL Medium DETAILS The emails say you have a reminder and need to click on the link to take you to a portal to see what the notification is for... CATEGORY Products & Services	Update account info DATE ADDED TO ARCHIVE 10/12/2021 ALERT LEVEL Medium DETAILS They want you to update your account info. look who the email is from and see if you have any account info on that site. They will ... CATEGORY Other





Other Kinds of Cybersecurity Incidents

Phil Herechski

UC Merced IT Security Analyst

؟

Social Engineering

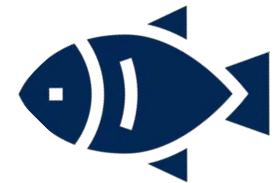
SOCIAL ENGINEERING

What is Social Engineering?

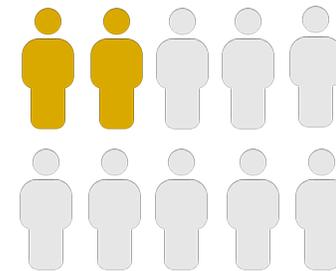
- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes
- Phishing is the most common social engineering attack
- Phone Calls masquerading as Microsoft or the IRS demanding information
- Dressing up as an employee to gain access



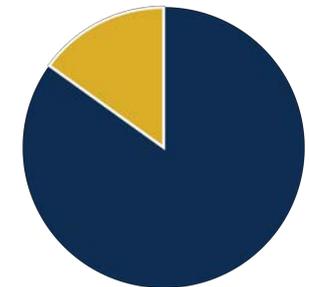
Happening 24/7



Phishing is most common



2/10 employees have been compromised



Involved in 85% of data breaches in 2019

SOCIAL ENGINEERING

- O365 Spam and Spoofing Protection
- AI and heuristic detection of fraudulent emails
- Security Education and Cybersecurity Training
- Awareness when something is wrong

IMPACT

- Involved in most UC Merced attacks
- 15 incidents per week
- 5-25 password resets per day
- Security education through our cybersecurity and phishing programs

Denial of Service

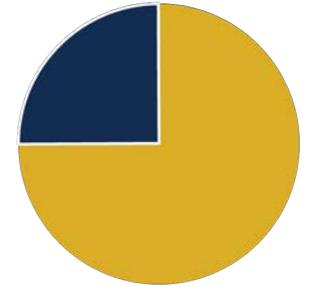
DENIAL OF SERVICE

What is Denial of Service?

- Seeks to shut down a machine or network, making it inaccessible to its intended users
- DoS attacks flood the target with traffic, overloading the network and bringing speeds to a crawl

7K

DDoS-style attacks on UC Merced each day



Uses up to to 25% of a nation's entire bandwidth



Victim of DoS attack in 2020



Happening worldwide 24/7

DENIAL OF SERVICE

- Load balancing, firewalls, and automated systems
- “Black Hole” malicious traffic
- Intelligent routing and traffic shaping

IMPACT

- Automated systems take care of most attacks
- No serious attacks in the last 5 years
- No noticeable impact on UC Merced community

Malware & Ransomware

MALWARE & RANSOMWARE

What is Malware & Ransomware?

- Malware: software specifically designed to disrupt, damage, or gain unauthorized access to a computer system
- Ransomware: malicious software designed to block access to a computer system until a ransom is paid
- Costs the industry an average of \$4.62 million per incident



Attacks are constant



Fake files



Phishing



Ads on legitimate websites

DENIAL OF SERVICE

- Firewalls, AI, and automated systems filter most of it
- Keep system up to date to secure against security vulnerabilities
- Endpoint protection through FireEye HX
- Automatic backups using Crashplan to protect data

IMPACT

- Properly configured systems with running backups are quickly restored
- Data recovery difficult or impossible without a backup
- Malware and ransomware account
- Information security can assist in vulnerability scanning, hardening, and monitoring

Global Ransomware Damage Costs*

- **2015: \$325 Million**
- **2017: \$5 Billion**
- **2021: \$20 Billion**
- **2024: \$42 Billion**
- **2026: \$71.5 Billion**
- **2028: \$157 Billion**
- **2031: \$265 Billion**



Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

Data Breach

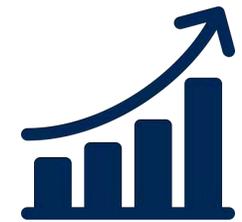
DATA BREACHES

What is a data breach?

- Security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so
- Lost data includes personal identifiable information (PII), passwords, research data



Often due to
vulnerable systems



38% increase over
previous year

Frequently Targeted:



Healthcare



Education



Military

DATA BREACHES

- Follow best practices
- Encryption at Rest / Encryption in Transit
- AI and traffic analysis detects errant data streams
- Auditing and review of security policy

IMPACT

- No data breaches at UC Merced
- UC Merced OIT scans our environment routinely for vulnerabilities and flaws
- Continued monitoring and review of policies

HOW TO REPORT A CYBERSECURITY INCIDENT



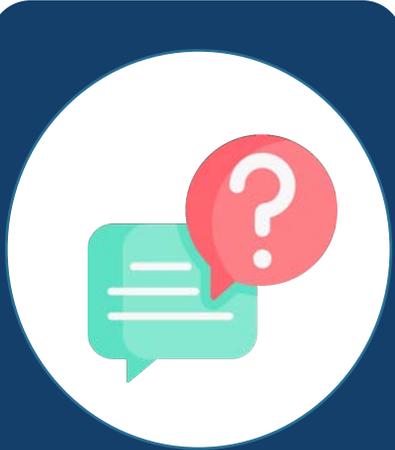


Cybersecurity: A Day In the Life

Shane Middleton

UC Merced IT Cloud Engineer

INCIDENT RESPONSE – A TYPICAL DAY



Incidents or
requests



Projects



Environment
Monitoring



Maintenance

INCIDENT RESPONSE

3 Phases of Incident Response



INCIDENT RESPONSE- EXAMPLE INCIDENT



INCIDENT RESPONSE- EXAMPLE INCIDENT

8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.

Dear Customer,
This is your bank. We forgot your
social security number and password.
Why don't you send them to us so
we can protect your
money.

Sincerely,
I. B. Banker

LOOKS
LEGIT.



INCIDENT RESPONSE- EXAMPLE INCIDENT

Uh oh, he clicked!



INCIDENT RESPONSE - REPORTING

- In doubt?
 - Open a ticket: <https://ucmerced.service-now.com/servicehub/>
- Have a general question, need guidance, or need help deciding if you need a ticket?
 - Email infosecurity@ucmerced.edu



INCIDENT RESPONSE- EXAMPLE INCIDENT



INCIDENT RESPONSE - IDENTIFICATION

Identify Scope

- Location
- Device
- Breadth
- Method of Entry



INCIDENT RESPONSE - REMEDIATION

Isolate, then remediate

- Restore from a backup / fresh install
- Apply relevant patches
- Close off unnecessary points of entry
- Monitor



INCIDENT RESPONSE- EXAMPLE INCIDENT

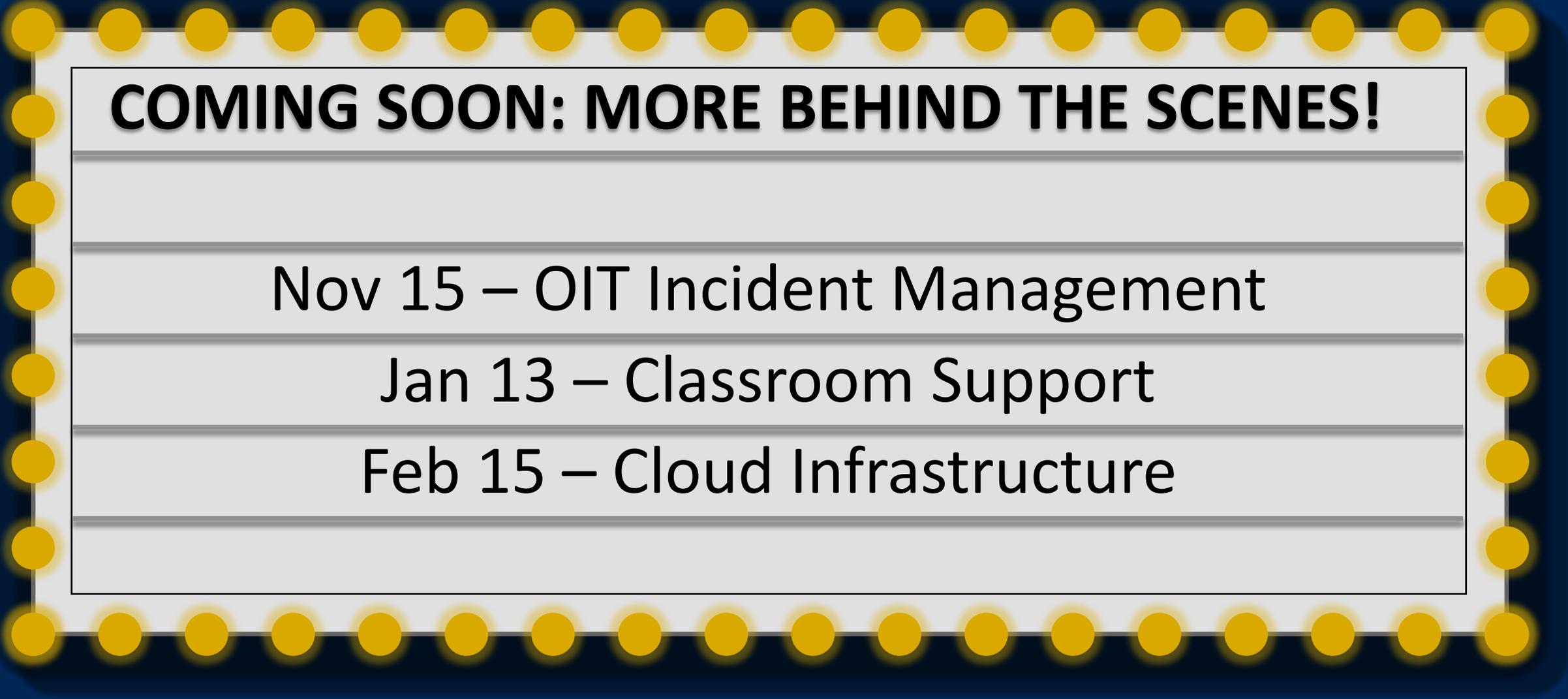


Resources OIT Provides

- **Report Problems via the ServiceHub**
- **FireEye Endpoint and Network Monitoring**
- **Managed Desktop & Backups (Crashplan)**
- **Service Desk Support**
- **Access to Security Professionals when needed**



Q&A



COMING SOON: MORE BEHIND THE SCENES!

Nov 15 – OIT Incident Management

Jan 13 – Classroom Support

Feb 15 – Cloud Infrastructure



<http://ucm.edu/v/oitbehindthescenes>

OIT Behind the Scenes: Cybersecurity Incidents was created on location at the University of California, Merced in Merced, California!

Thanks to all the participants
who put hard work into this webinar!

Katie Adams Arca, Webinar Coordinator

Edson Gonzales, Webinar Support

Phil Herechski, Subject Matter Expert

Jennifer Howze-Owens, Instructional Designer

James McKinzie, Subject Matter Expert

Shane Middleton, Subject Matter Expert

Preethi Merugumala, Student Technology Consultant

Christian Ortiz, Student Technology Consultant

Rachel Peters, Webinar Support

Quinncie Reider, Student Technology Consultant

Christy Snyder, Communications & Promotional Support



That's all, folks!