OIT - Data and Identity Security Webinar

OIT Behind the Scenes

Webinar Series

Setting Expectations

Lights!

- Camera & Audio

Action!

- Participatory Activities

Camera!

- Recorded Session

Cut!

- Q & A

UNIVERSITY OF CALIFORNIA
MERCED | OFFICE OF INFORMATION TECHNOLOGY

Today's Agenda:

- Current landscape of technology challenges specific to information & identity security
- Why you should care about cybersecurity
- Simple steps to protect yourself and your info
- OIT services that help keep you cybersecure

Cybersecurity: Challenges & Pillars

Tolgay Kizilelma

UC Merced Chief Information Security Officer

A SHIFTING WORLD – CYBERSECURITY CHALLENGES

- Growing threat landscape & attack sophistication
- Growing regulations & privacy concerns
- Digitization of everything
- Remote work
- Operational resiliency
- Managing costs
- Multi-cloud & multi OS
- Scarce skills & talent market

UNIVERSITY OF CALIFORNIA MERCED | OFFICE OF INFORMATION TECHNOLOGY

PROTECT THE PILLARS OF CYBERSECURITY

Identity

Data

Endpoint (Device)

PROTECT THE PILLARS OF CYBERSECURITY

Identity

- Admin role/access
- SSO/2FA - authentication
- Limit access
- Least privilege
- Password resets/managers

PROTECT THE PILLARS OF CYBERSECURITY

Data

- Data Loss Prevention (DLP)
- Backups
- Encryption
- Insider threat

PROTECT THE PILLARS OF CYBERSECURITY

Endpoint (Device)

- Ensure device health
- Use approved devices
- Reduce legacy footprint
- Use managed devices

PROTECT THE PILLARS OF CYBERSECURITY

Identity

- Admin role/access
- SSO/2FA - authentication
- Limit access
- Least privilege
- Password resets/managers

Data

- Data Loss Prevention (DLP)
- Backups
- Encryption
- Insider threat

Endpoint (Device)

- Ensure device health
- Use approved devices
- Reduce legacy footprint
- Use managed devices

PROTECTING DATA & ONLINE IDENTITY: WORK – PERSONAL

Confidentiality: Ensuring only authorized users have access to information.

Integrity: To prevent unauthorized modifications to the data. Ensure that the data is accurate and trustworthy.

Availability: To ensure data is accessible to authorized users whenever it is needed.

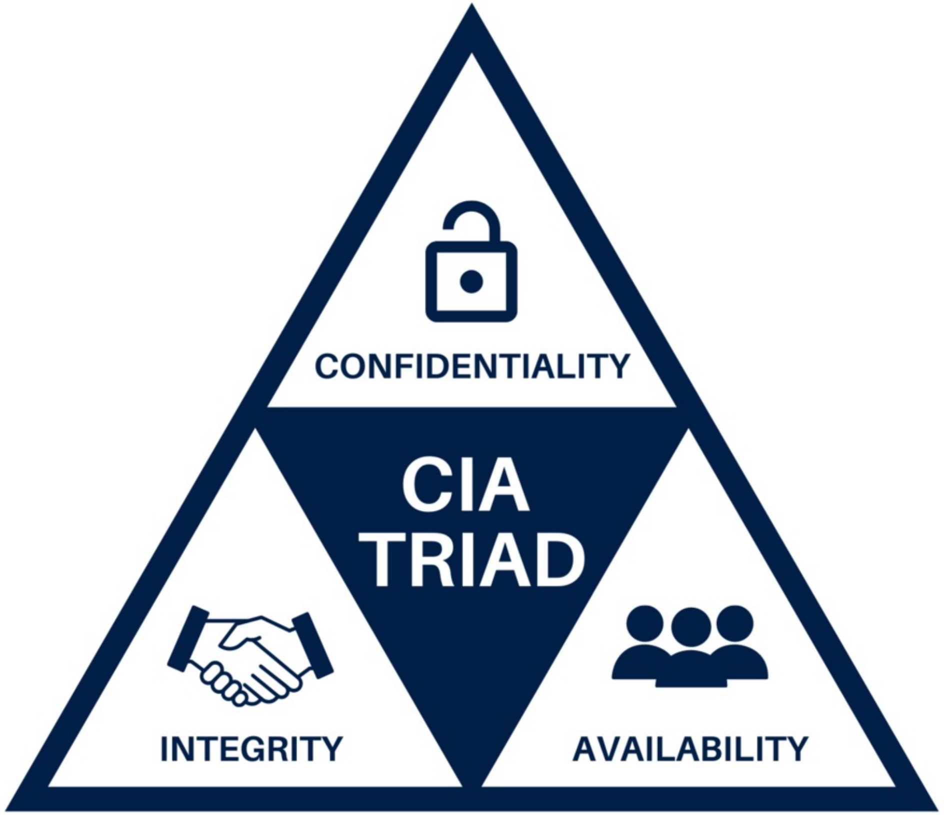


Image by securitymadesimple.org

Making Cybersecurity Personal

Shane Middleton

UC Merced IT Security Analyst

?

PASSWORD SECURITY

- **Recent survey concludes the average person has 150 unique online accounts.**

> “…the average American internet user has **150 online accounts** that require a password – in theory, that means you would need to memorize 150 unique, complex passwords for maximum account security.
>
> […] by the year 2022, we predict that number will skyrocket to **300 accounts**.
>
> \- *Dashlane.com*

- **Use a password manager to help you follow best practices.**

?

PASSWORD SECURITY

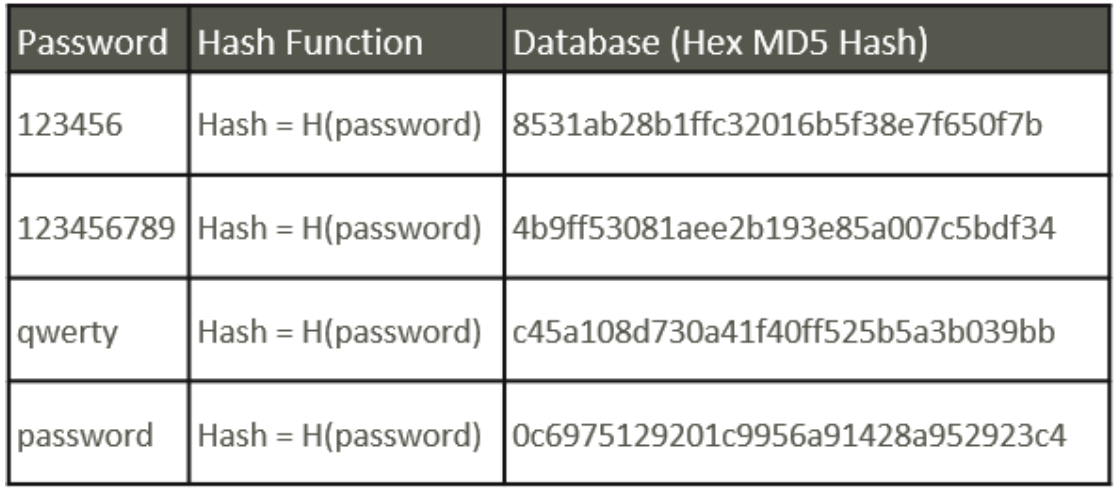
- **Different organizations are held to different standards by way of regulation when it comes to storing your data(including your password).**

yourbank.com != ibuyantiquekitchenknobs.com

- **During a compromise, attackers can obtain unauthorized access to password hashes stored in a user database of some sort.**

PASSWORD SECURITY

- **Password Hash: a one-way transformation on a password, turning the password into a string.**



Password	Hash Function	Database (Hex MD5 Hash)
123456	Hash = H(password)	8531ab28b1ffc32016b5f38e7f650f7b
123456789	Hash = H(password)	4b9ff53081aee2b193e85a007c5bdf34
qwerty	Hash = H(password)	c45a108d730a41f40ff525b5a3b039bb
password	Hash = H(password)	0c6975129201c9956a91428a952923c4

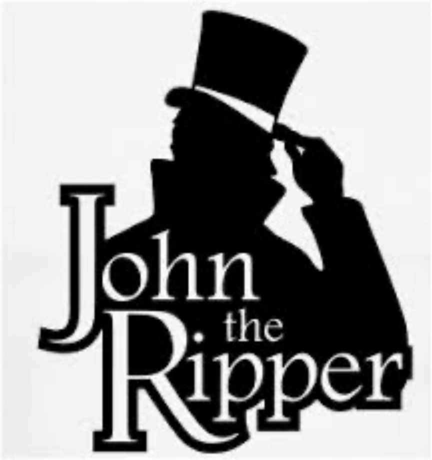
- **Once attackers have a copy of your password hash, they can then begin attempting to "crack" your password using specialized programs.**

Image by bmc.com

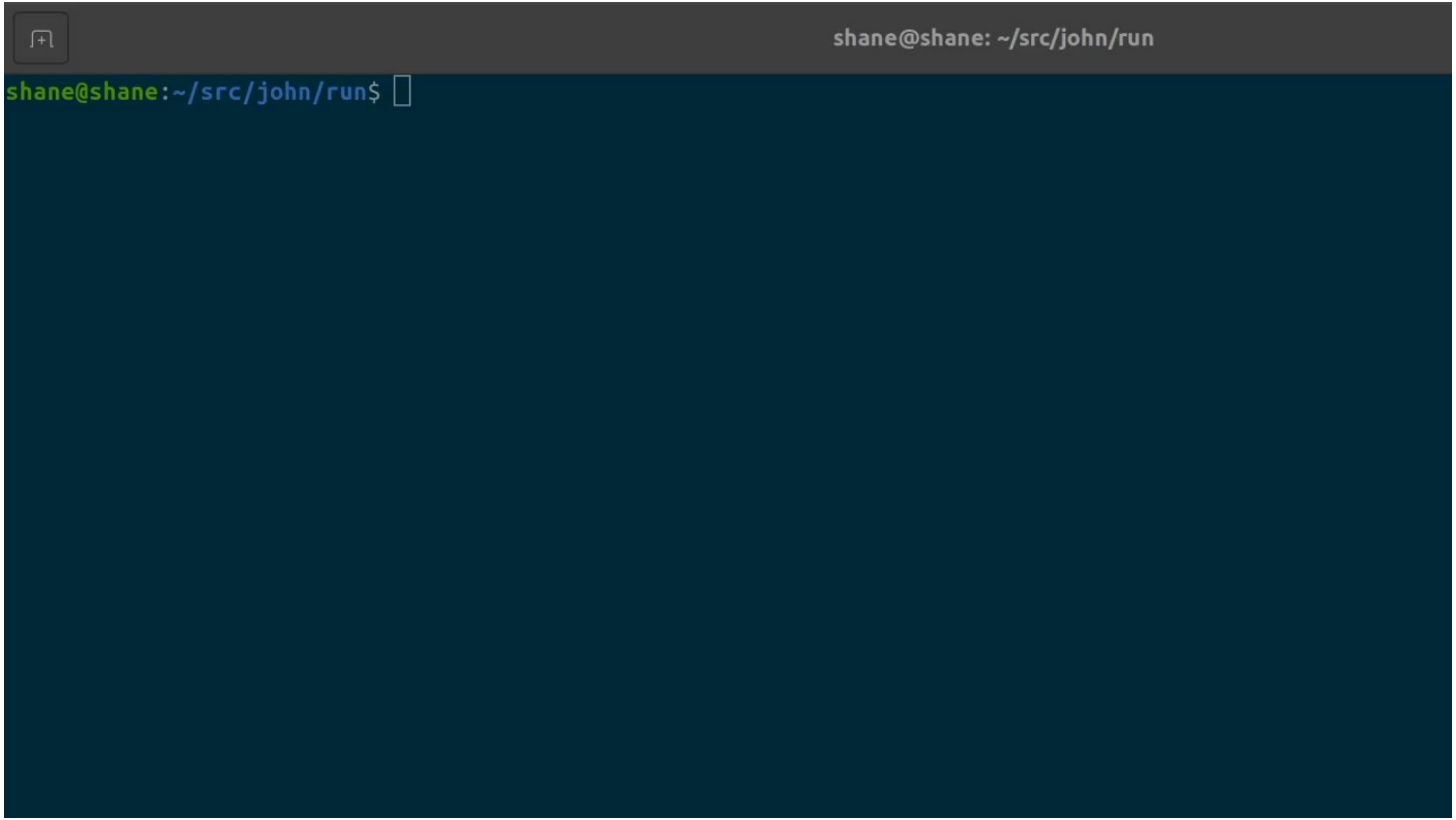
PASSWORD SECURITY

- **"John the Ripper"**
  - **open source security auditing and password recovery program**
  - **freely available (https://www.openwall.com/john/)**

- **Let's see it in action!**



PASSWORD SECURITY



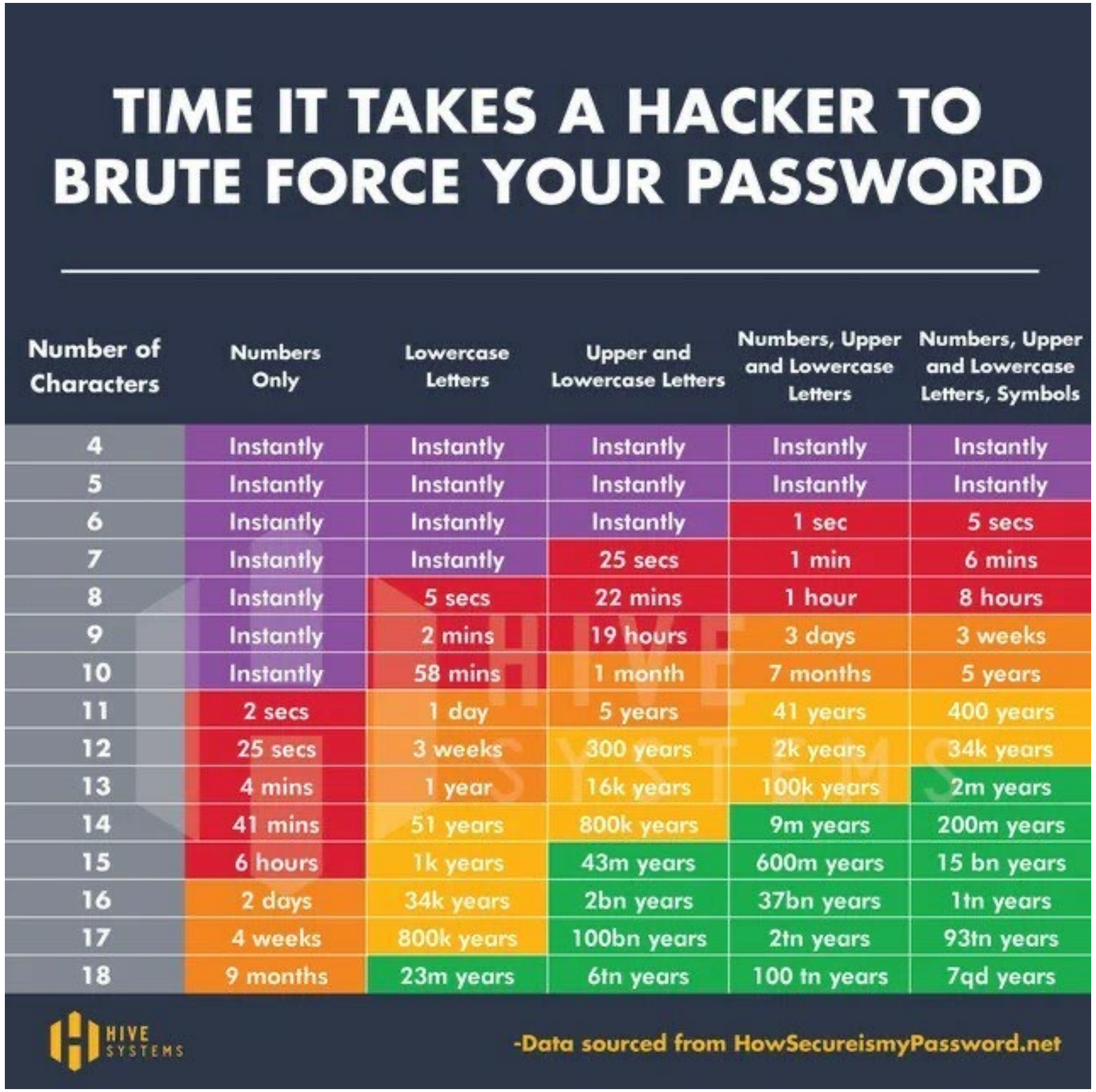
```
shane@shane:~/src/john/run$ 
```

PASSWORD SECURITY

Password reuse is risky!

- Once attackers "crack" your password, they can then use it to attempt to get into other sites. If you reuse passwords, you’re vulnerable!

PASSWORD SECURITY



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

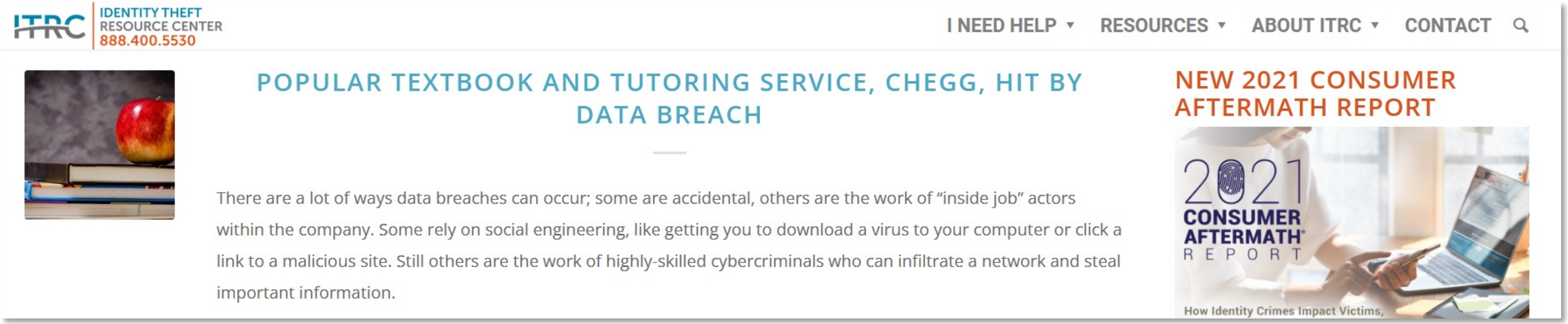
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

CYBERSECURITY BREACHES: REAL-WORLD EFFECTS

- Chegg Data Breach
  - Affected 40 million users
  - Hackers didn't access financial or SSN data
  - Password hashes were obtained


ITRC
IDENTITY THEFT RESOURCE CENTER
888.400.5530
I NEED HELP ▾
RESOURCES ▾
ABOUT ITRC ▾
CONTACT
2021 CONSUMER AFTERMATH REPORT
How Identity Crimes Impact Victims,

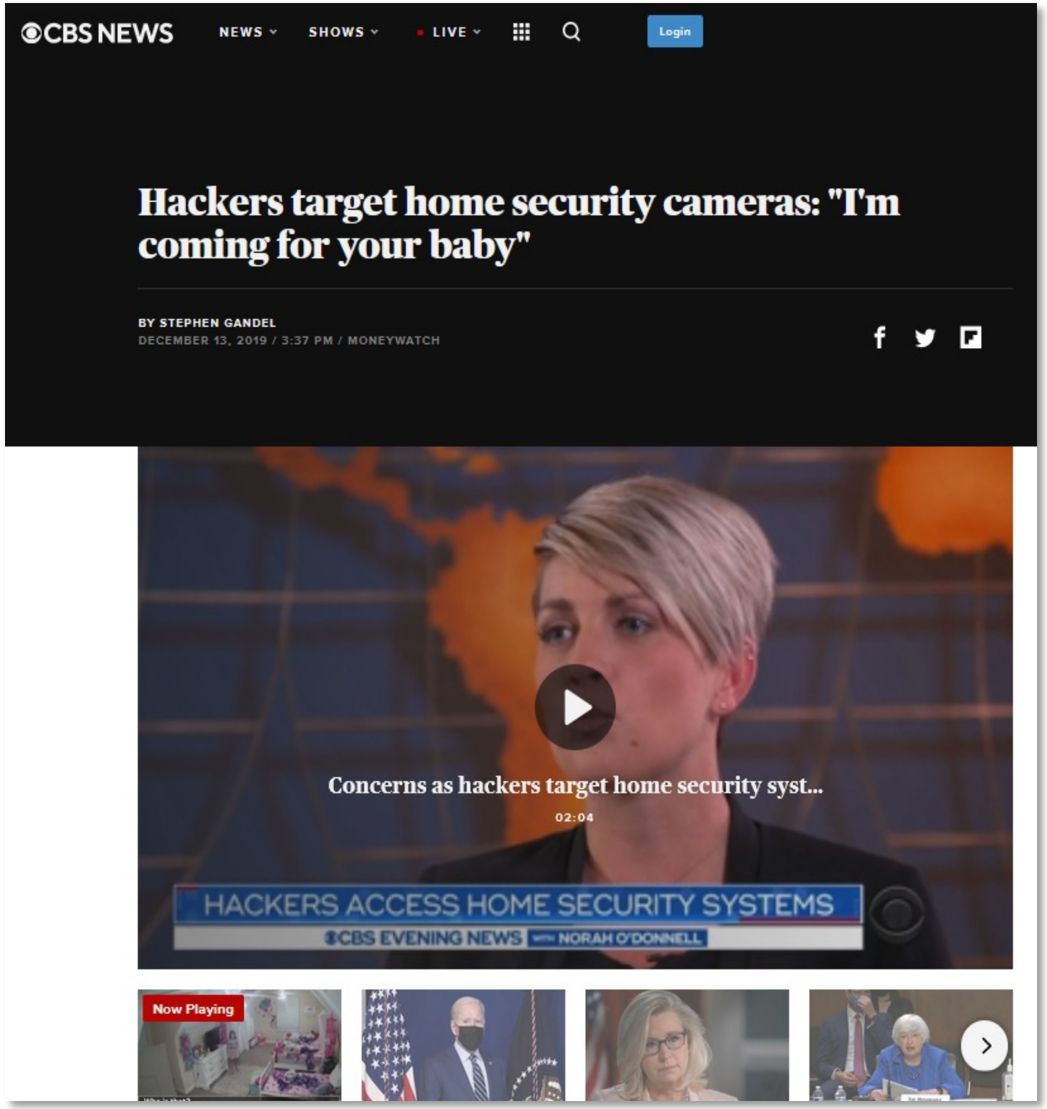
POPULAR TEXTBOOK AND TUTORING SERVICE, CHEGG, HIT BY DATA BREACH

There are a lot of ways data breaches can occur; some are accidental, others are the work of “inside job” actors within the company. Some rely on social engineering, like getting you to download a virus to your computer or click a link to a malicious site. Still others are the work of highly-skilled cybercriminals who can infiltrate a network and steal important information.

NEW 2021 CONSUMER AFTERMATH REPORT

CYBERSECURITY BREACHES: REAL-WORLD EFFECTS

- **Thermostats and Security Cameras, oh my!**
  - **IoT devices hacked due to password reuse**
  - **The use of 2FA could have prevented attacks**
  - **Digital threats impact our daily lives**


CBS NEWS
NEWS
SHOWS
LIVE
Login

Hackers target home security cameras: "I'm coming for your baby"

BY STEPHEN GANDEL
DECEMBER 13, 2019 / 3:37 PM / MONEYWATCH

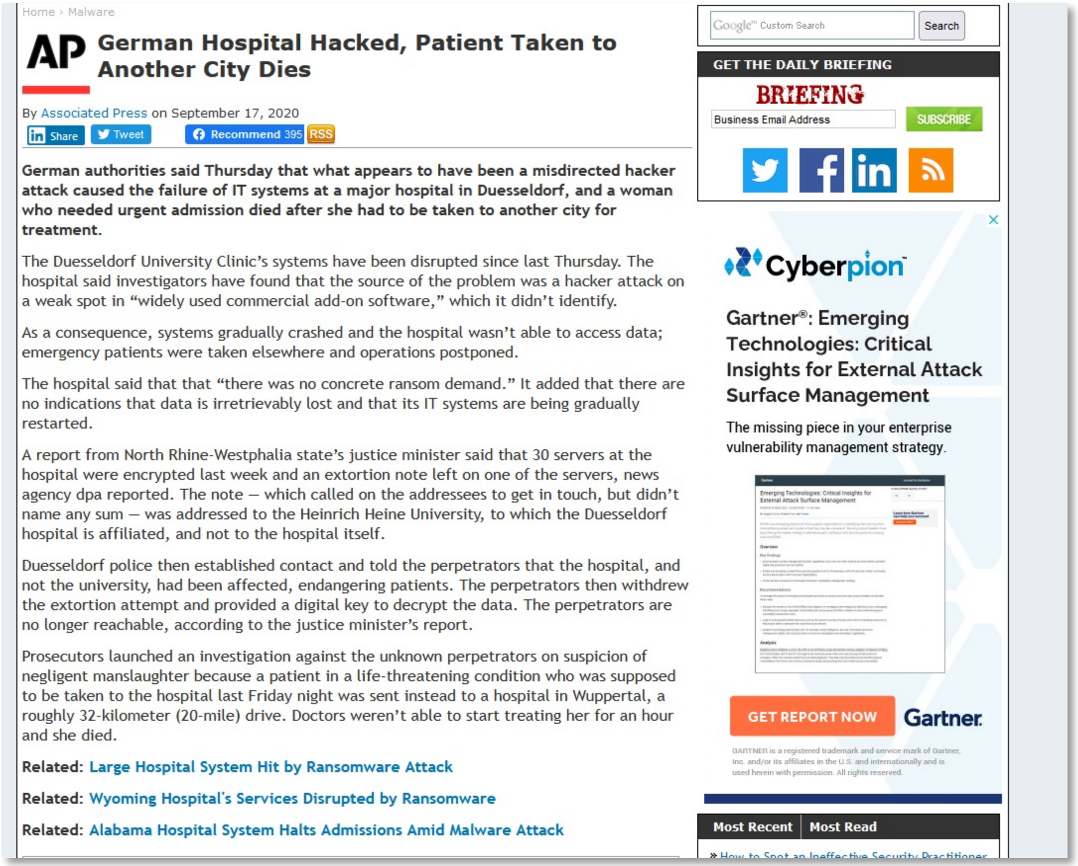
Concerns as hackers target home security syst...

02:04

HACKERS ACCESS HOME SECURITY SYSTEMS
CBS EVENING NEWS WITH NORAH O'DONNELL
Now Playing

CYBERSECURITY BREACHES: REAL-WORLD EFFECTS

- German Hospital infected w/ ransomware results in patient dying.
  - Ransomware-based attack locked up hospital's computer systems.
  - Hospital turned away patients as a result.
  - Patient who needed immediate care wasn't able to get the care they needed. As a result, the patient died.



German Hospital Hacked, Patient Taken to Another City Dies

By Associated Press on September 17, 2020

German authorities said Thursday that what appears to have been a misdirected hacker attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.

The Duesseldorf University Clinic's systems have been disrupted since last Thursday. The hospital said investigators have found that the source of the problem was a hacker attack on a weak spot in "widely used commercial add-on software," which it didn't identify.

As a consequence, systems gradually crashed and the hospital wasn't able to access data; emergency patients were taken elsewhere and operations postponed.

The hospital said that that "there was no concrete ransom demand." It added that there are no indications that data is irretrievably lost and that its IT systems are being gradually restarted.

A report from North Rhine-Westphalia state's justice minister said that 30 servers at the hospital were encrypted last week and an extortion note left on one of the servers, news agency dpa reported. The note — which called on the addressees to get in touch, but didn't name any sum — was addressed to the Heinrich Heine University, to which the Duesseldorf hospital is affiliated, and not to the hospital itself.

Duesseldorf police then established contact and told the perpetrators that the hospital, and not the university, had been affected, endangering patients. The perpetrators then withdrew the extortion attempt and provided a digital key to decrypt the data. The perpetrators are no longer reachable, according to the justice minister's report.

Prosecutors launched an investigation against the unknown perpetrators on suspicion of negligent manslaughter because a patient in a life-threatening condition who was supposed to be taken to the hospital last Friday night was sent instead to a hospital in Wuppertal, a roughly 32-kilometer (20-mile) drive. Doctors weren't able to start treating her for an hour and she died.

Related: Large Hospital System Hit by Ransomware Attack

Related: Wyoming Hospital's Services Disrupted by Ransomware

Related: Alabama Hospital System Halts Admissions Amid Malware Attack

?

OIT Services

Phil Herechski

UC Merced IT Security Analyst

DEVICE MANAGEMENT, INVENTORY, AND CONTROL

Microsoft

jamf PRO

Available for:

UNIVERSITY OWNED DEVICES

- Enroll and manage devices from a central location
- Enforce configuration standards and secure devices
- Enrolled devices: remote wipe, remote imaging, and remote lock
- Software installations, updates, patches, and inventory management
- For More Information: https://ucm.edu/Device_Setup

ENCRYPTION – WINDOWS, OS X, LINUX, & (MOST) MOBILE DEVICES

Available for:

FACULTY
STAFF
STUDENTS

- Available for almost every device
- Protects your devices and data from unauthorized access and snooping
- Most devices offer encryption, including computers, mobile devices, and tablets
- Setup is simple and can be done in minutes*
- For more information - https://it.ucmerced.edu/security-services

UNIVERSITY OF CALIFORNIA MERCED | OFFICE OF INFORMATION TECHNOLOGY

ANTI-VIRUS PROTECTION

FIREEYE

- Realtime protection, kill threats as they happen!
- Protection against ransomware, malware, and other nasty on-line threats
- Works with Windows, OS X, and Linux
- For More information - https://it.ucmerced.edu/FireEyeHX

Available for:

FACULTY
STAFF

DEVICE BACKUP AND RECOVERY

CODE42

Available for:

FACULTY
STAFF

- Automatically back up key folders and files quietly in the background
- Cloud based recovery anywhere in the world
- Protects your files against theft, loss of data, and ransomware
- For More Information - https://it.ucmerced.edu/crashplan-install

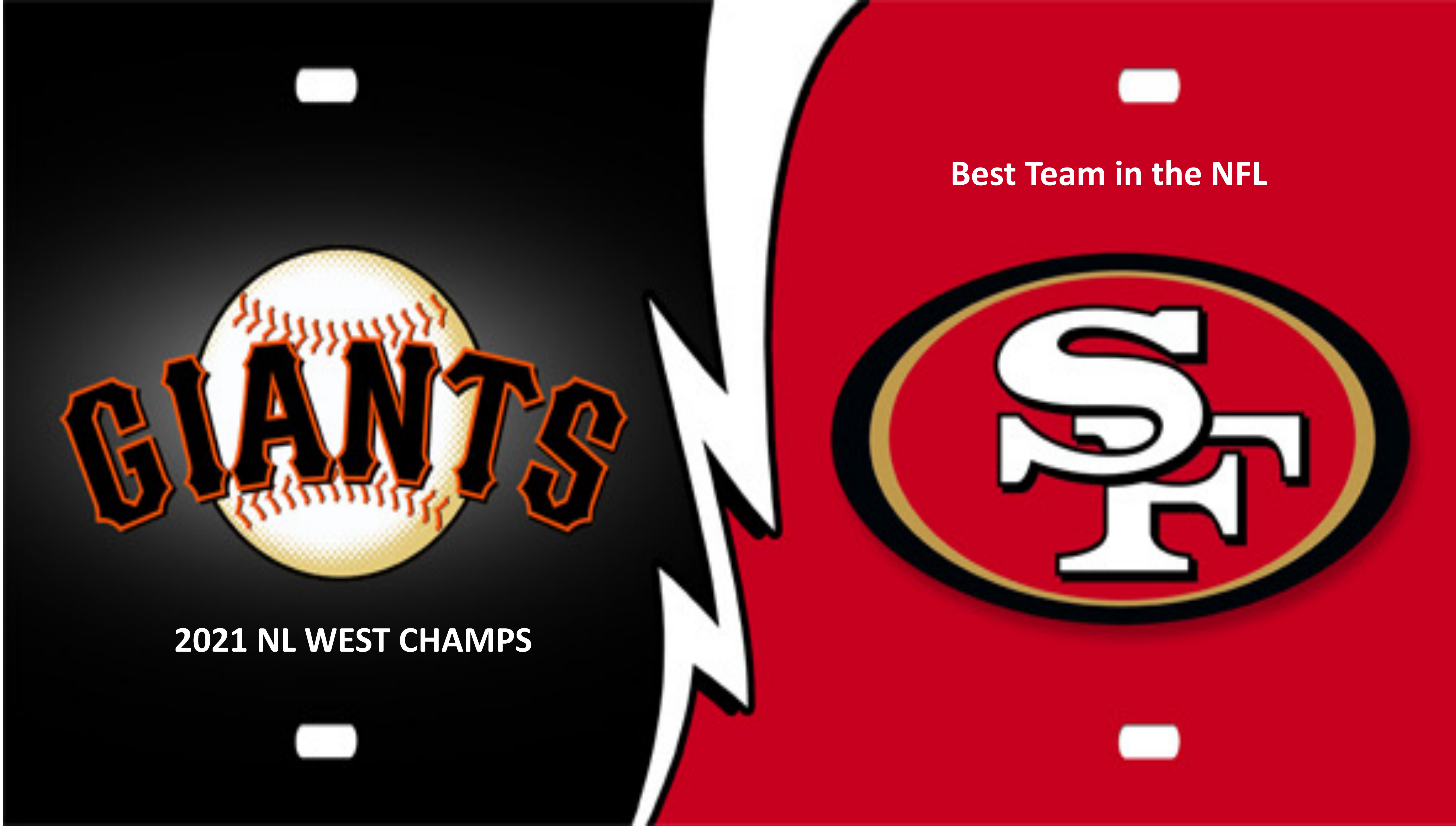
TWO-FACTOR AUTHENTICATION

Available for:

FACULTY
STAFF
STUDENTS

- Second factor of authentication, additional layer of security for your account
- Runs on iOS and Android devices
- “Hardware Token” available if you don’t have a phone.

- For more information - https://it.ucmerced.edu/2FA



Best Team in the NFL

2021 NL WEST CHAMPS

VIRTUAL PRIVATE NETWORK (VPN)

Available for:

FACULTY
STAFF
STUDENTS

- Establishes a secure tunnel, and encrypts your data to protect your connection from hijacking
- Allows access to UC Merced services, labs, and offices while off campus
- Send a print job from the field, print when you get back to the campus!
- For More Information- https://it.ucmerced.edu/VPN_Changeover

Simple Best Practices

James McKinzie

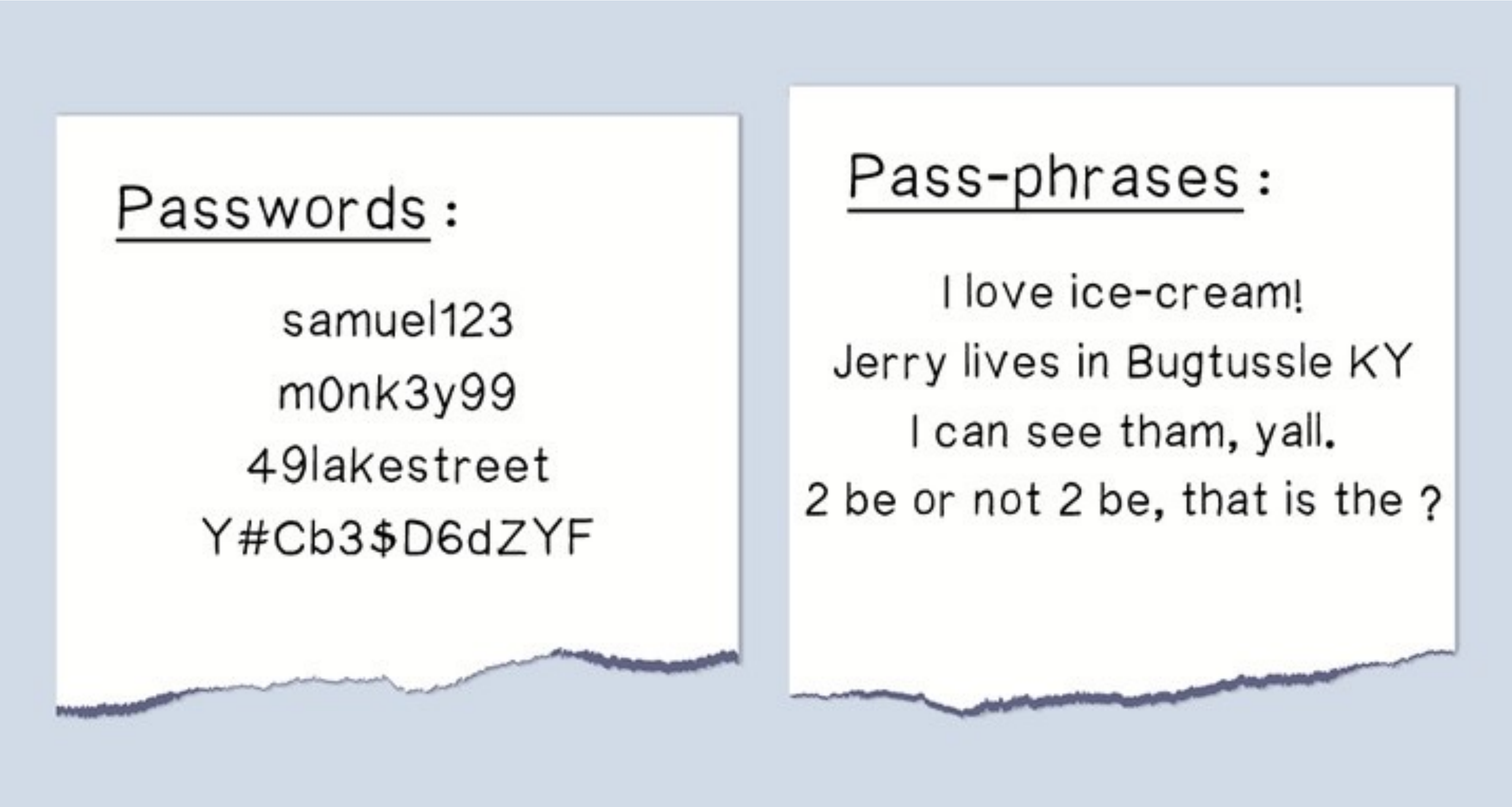
IT Security Analyst

CYBERSECURITY: SIMPLE BEST PRACTICES IN GENERAL

1. Use an anti-virus program that is always scanning
   - Good options are:
     - Norton
     - McAfee
     - MalwareBytes
2. Back up your data
3. Enable multi-factor authentication
4. Change your password regularly
     - Don’t make predictable changes
5. Adhere to strong password standards or use passphrases

?

PASSWORD VS. PASSPHRASES



Passwords:

samuel123

m0nk3y99

49lakestreet

Y#Cb3$D6dZYF

Pass-phrases:

I love ice-cream!

Jerry lives in Bugtussle KY

I can see tham, yall.

2 be or not 2 be, that is the ?

Image courtesy of CyberHoot

CYBERSECURITY: SIMPLE BEST PRACTICES AT HOME

Think about how much information you share on social media!

1. Vacation details - wait until you're back at home
   - Smart devices can help make it look like you're home
   - Make sure to keep them updated!
2. Avoid sharing a lot of photos & video of your home
3. Those silly social media quizzes
   - Are you giving away your password hints?

CYBERSECURITY: SIMPLE BEST PRACTICES AT WORK

1. Enable Auto Updates
   - This installs critical updates as soon as they are released
2. Make sure your operating system is up to date
   - Apple: https://support.apple.com/en-ph/HT201222
   - Windows: https://docs.microsoft.com/en-us/windows/release-health/release-information
3. Inventory your system regularly
   - Remove or disable programs you don’t need
4. Lock your system when you’re away from your desk

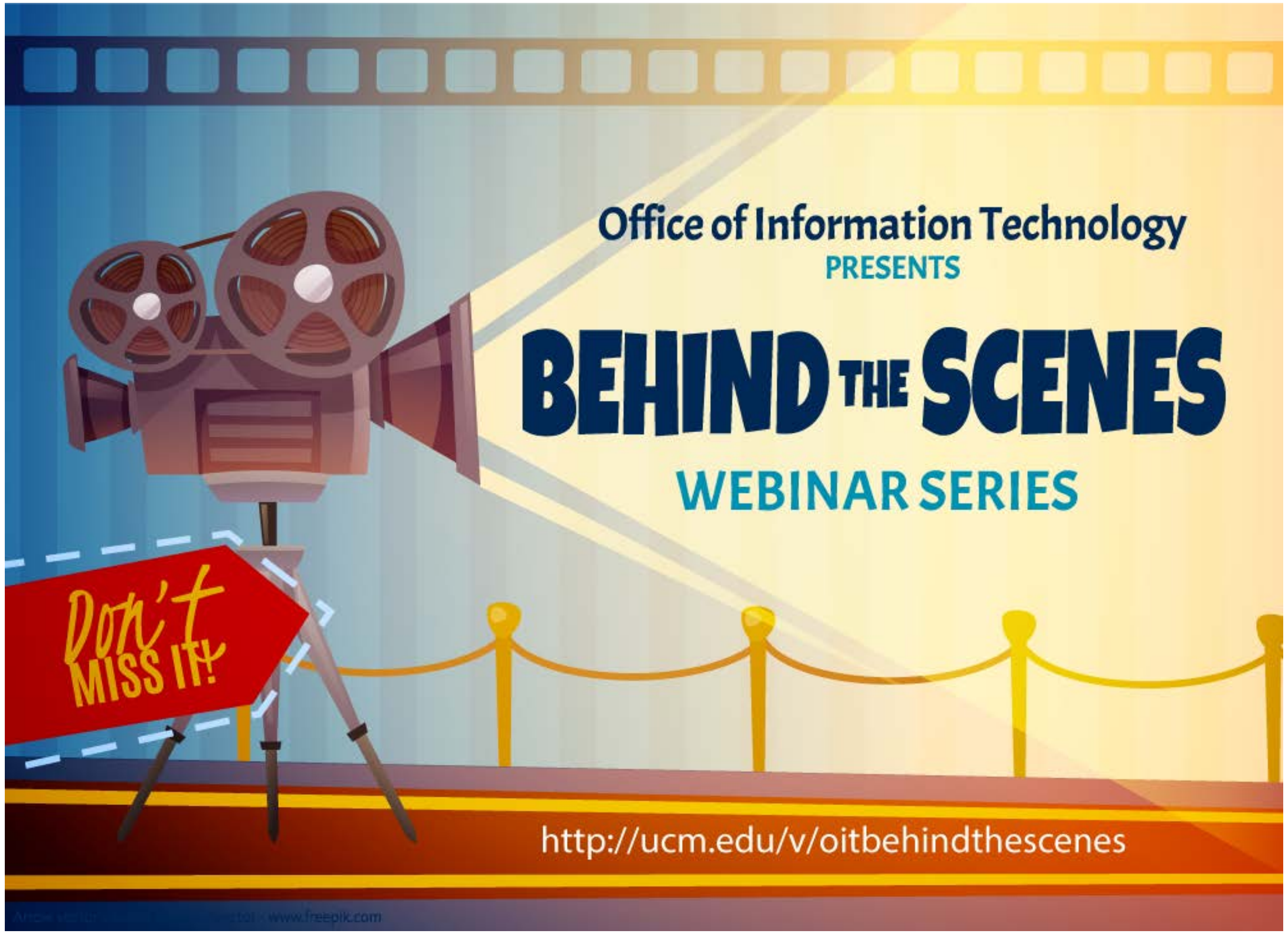
Q&A

COMING SOON: MORE BEHIND THE SCENES!

Oct 27 – How We Handle Cybersecurity Threats

Nov – OIT Incident Management

Jan – Classroom Support



http://ucm.edu/v/oitbehindthescenes

OIT Behind the Scenes: Protecting Your Data & Online Identity 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
Tolgay Kizilelma, Subject Matter Expert
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 & Promotions Support

That’s all, folks!