Setting Expectations

Lights!
- Camera & Audio

Action!
- Participatory Activities

Camera!
- Recorded Session

Cut!
- Q & A
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
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
**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.
Making Cybersecurity Personal

Shane Middleton
UC Merced IT Security Analyst
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.
• 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 Hash: a one-way transformation on a password, turning the password into a string.

<table>
<thead>
<tr>
<th>Password</th>
<th>Hash Function</th>
<th>Database (Hex MD5 Hash)</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>Hash = H(password)</td>
<td>8531ab28b1ffcc32016b5f38e7f650f7b</td>
</tr>
<tr>
<td>123456789</td>
<td>Hash = H(password)</td>
<td>4b9ff53081ae2b193e85a007c5bdf34</td>
</tr>
<tr>
<td>qwerty</td>
<td>Hash = H(password)</td>
<td>c45a108d730a41f40ff525b5a3b039bb</td>
</tr>
<tr>
<td>password</td>
<td>Hash = H(password)</td>
<td>0c6975129201c9956a91428a952923c4</td>
</tr>
</tbody>
</table>

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

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

Data sourced from HowSecureismyPassword.net
• **Chegg Data Breach**
  • **Affected 40 million users**
  • Hackers didn't access financial or SSN data
  • Password hashes were obtained
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
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.
OIT Services
Phil Herechski
UC Merced IT Security Analyst
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
ENCRIPTION – WINDOWS, OS X, LINUX, & (MOST) MOBILE DEVICES

• 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
ANTI-VIRUS PROTECTION

• 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
DEVICE BACKUP AND RECOVERY

• 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

• 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

Available for: FACULTY, STAFF, STUDENTS
2021 NL WEST CHAMPS

Best Team in the NFL

GIANTS

2021 NL WEST CHAMPS

SF
VIRTUAL PRIVATE NETWORK (VPN)

• 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

Available for: FACULTY STAFF STUDENTS

UNIVERSITY OF CALIFORNIA MERCEDE OFFICE OF INFORMATION TECHNOLOGY
Simple Best Practices

James McKinzie
IT Security Analyst
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
Passwords:

- samuel123
- m0nk3y99
- 49lakestreet
- Y#Cb3$D6dZyF

Pass-phrases:

- I love ice-cream!
- Jerry lives in Bugtussle KY
- I can see tham, y'all.
- 2 be or not 2 be, that is the?
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?
1. Enable Auto Updates
   • This installs critical updates as soon as they are released
2. Make sure your operating system is up to date
   • 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
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
Quinnce Reider, Student Technology Consultant
Christy Snyder, Communications & Promotions Support
That’s all, folks!