Session 206: Password Techniques and Strategies to Promote a Higher Level of IT Security

Frank Ruelas,
Facility Compliance Professional
St. Joseph’s Hospital and Medical Center/Dignity Health
(francisco.ruelas@dignityhealth.org)

Lunch follows this session!
Objectives...
Let’s break them down.

• Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.
• Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.

• **Common myths and mistakes that may compromise the strength of passwords.**

• Review and consideration of effective administrative, physical, and technical safeguards to apply to your organization’s password management policy.
• Learn key criteria applicable to passwords that have the potential to contribute to a higher level of security with respect to the organization’s information system.
• Common myths and mistakes that may compromise the strength of passwords.
• Review and consideration of effective administrative, physical, and technical safeguards to apply to your organization’s password management policy.
Role Check!

Which is your area of focus?
A. Privacy
B. Security
C. Compliance
D. Information Technology (IT)
E. Depends on the day

5WH1
Who

• Workforce members
• Contractors
• High level users
• IT management
• IT administrators

What

• Strength
• Syntax
• Sharing
• Security
Where
- Devices
- Location of User
- Asset location
- Remote access

When
- On duty
- Off duty
- Establishing access
- Terminating access
- Modifying access

Passwords
- Devices
- Location of User
- Asset location
- Remote access

Passwords
- On duty
- Off duty
- Establishing access
- Terminating access
- Modifying access
Passwords

- User verification
- Applicability
- Familiarity
- Contributes to security
- Required

Why

Passwords

- User awareness
- Policy and procedure
- Auditing access
- Auditing syntax

How
Passwords

Who
• Workforce members
• Contractors
• High level users
• IT management
• IT administrators

Why
• User verification
• Applicability
• Familiarity
• Contributes to security
• Required

What
• Strength
• Syntax
• Sharing
• Security

When
• On duty
• Off duty
• Establishing access
• Terminating access
• Modifying access

Where
• Devices
• Location of User
• Asset location
• Remote access

How
• User awareness
• Policy and procedure
• Auditing access
• Auditing syntax

Safeguards

User awareness
Policy and procedure
Auditing access
Auditing syntax

Strength
Syntax
Sharing
Security

On duty
Off duty
Establishing access
Terminating access
Modifying access

Devices
Location of User
Asset location
Remote access

User verification
Applicability
Familiarity
Contributes to security
Required

Familiarity
Contributes to security
Required

Safeguards
Administrative Safeguards:
Focus on behavior
Administrative Safeguards: Focus on behavior

- Don’t share

Administrative Safeguards: Focus on behavior

- Don’t share
- Don’t write down
Administrative Safeguards: Focus on behavior

- Don’t share
- Don’t write down
- Don’t post

Physical Safeguards: Focus on tangible barriers
Physical Safeguards: Focus on tangible barriers

• Function activated

Physical Safeguards: Focus on tangible barriers

• Function activated
• Interface enabled
Administrative Safeguards

Physical Safeguards

Technical Safeguards

Technical Safeguards: Focus on use of technology

Expiration date
Administrative Safeguards

Physical Safeguards

Technical Safeguards

Technical Safeguards: Focus on use of technology
- Expiration date
- Syntax

Physical Safeguards

Technical Safeguards
Changing Passwords

Frequency

- 3 months: 65%
- 6 months: 30%
- Annually: 5%
Syntax

Strength

Mitigate the risk of someone guessing a password
Have you ever wondered?

• How many password combinations?
  • Consider the following
    • Letters – Capitalized – 26...25 for ease
    • Letters – Lowercase – 26...25 for ease
    • Numbers – All digits - 10
    • Special characters - 20

Have you ever wondered?

• 80 possible choices for each position
  • 4 characters – 40 million possible
  • 8 characters– 1.6 quadrillion

...I think you get the idea.
When you consider what a password can do...

Passwords for voicemail

- 1234
- 0000
- 2580
- 1111
- 5555
Next steps...

• Continued training
• Exercises
• Other threats: Social Engineering

Want to know...

• ...how to check if an email’s password was potentially compromised?
• ...if a password was hacked?
• ...how to decipher a password?