Topic 3

# Password Security and Authentication

Slides developed by

# What you will learn in these slides…

## Best practices for creating strong passwords

- NIST password guidelines

## Multi/Two-factor Authentication

- Three principles of ‘something you ___’

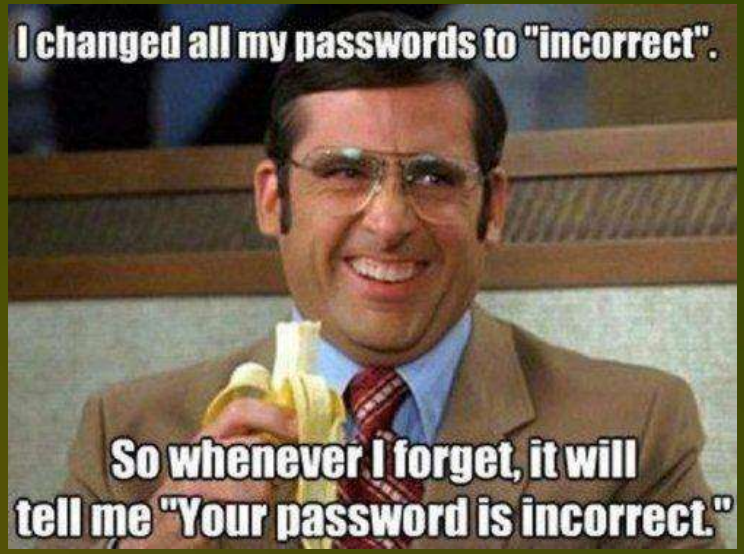
# What makes a good password?

Is it something like:

- 123456
- abcdef
- password

Or something like:

- potatoCh1p8390#
- WerkHard23@school
- yriefncmstefksckmo



# Why do we need to create strong passwords?

- Protect your accounts from unauthorized access
  - Use a different password for each of your accounts
- Safeguard your sensitive information
  - Ensures that your online activities are confidential
- Reduce the risk of identity theft
  - Attackers who steal your identity may pose as you to trick others
  - If you suspect an unusual sign-in to your account which wasn't done by you, change your password immediately!

# Characteristics of a strong password

- Sufficient password Length
- May include both upper/lowercase, digits and symbols
- Avoid sequential characters (e.g., abcd) or repeated ones (e.g., 1111)
- Do not use easily guessable information
  - Name, Birthday, Address etc.
- Good to use passphrases as they include more characters
  - The password ‘mynameisspongebob’ is much stronger than ‘spongebob’

# NIST

- NIST (National Institute of Standards and Technology) is a US federal agency that issues guidelines for managing digital identities
- Password guidelines are stated in NIST Special Publication (SP) 800-63B (800-63-4, 2024)
  - Some good practices will be discussed in the next slide!
  - Do note: At the time that these slides were created, NIST SP 800-63-4 had just been released. For the 2017 version, refer to NIST SP 800-63B (800-63-3, 2017)
- NIST will also be referenced in Topic 8 so stay tuned!

# NIST good password practices mentioned

- Password length
  - Minimum 8-12 characters for user-generated passwords (highly recommended to be at least 15 characters)
  - Maximum of 64 characters (spaces included)
- Focus on length of password rather than various character types
  - Special characters (@, #, $ etc.) are still allowed but no longer required
  - Longer passwords are harder to crack and easier to remember for users as compared to random combinations
- Change password only when you think/feel it's compromised
  - Need not be changed 'every 60-90 days' which was the old practice

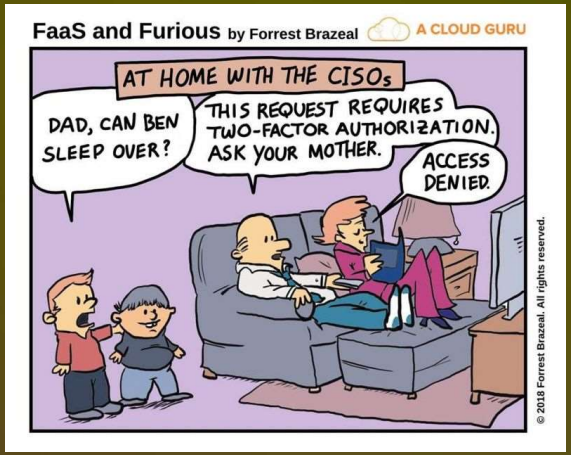
Reference: https://scytale.ai/resources/2024-nist-password-guidelines-enhancing-security-practices/

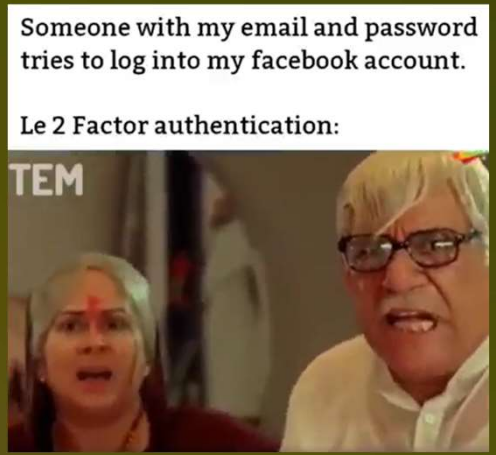
# Recap from Topic 1

- AAA Model
  - Authentication
  - Authorization
  - Accounting

# Multi/Two-Factor Authentication (MFA/2FA)

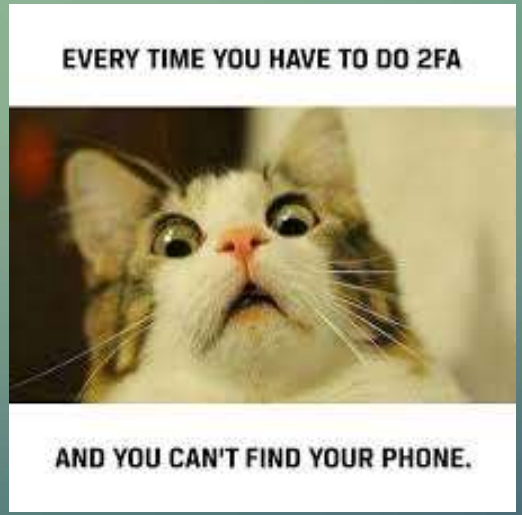
- Simply knowing a password is not secure enough (others may know your password too!)
- MFA/2FA ensures that other forms of verification are used to ensure that it is really you who is accessing a resource
- Two forms of authentication are often used, hence the term 2FA



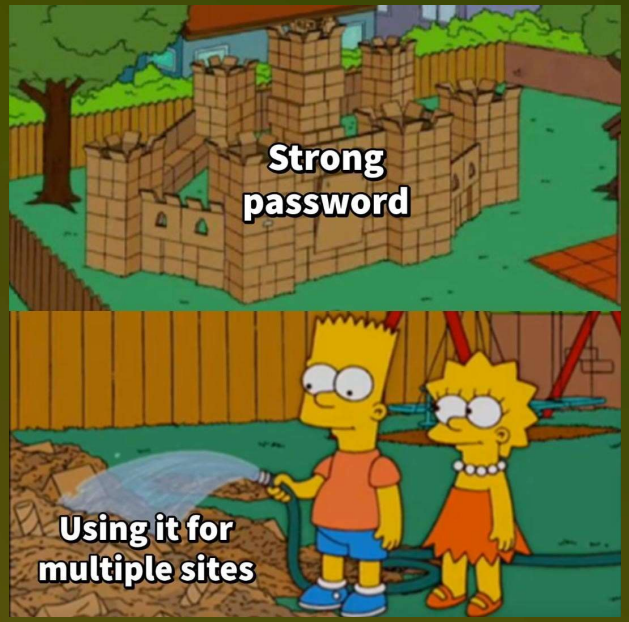
# MFA/2FA principles

- Something you **know**
  - Password, PIN, Credit Card number
- Something you **have**
  - OTP, Keycard, Most tangible forms of verification
- Something you **are**
  - Fingerprint, Facial recognition, Other biometric forms



# Topic 3 Summary

- Best practices for creating strong passwords
- NIST password requirements
- Multi/Two-factor Authentication




## In the next topic...

**Malware Detection and Prevention**

- Common types of malware
- Various ways to detect malware
- Good ways to prevent malware