CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

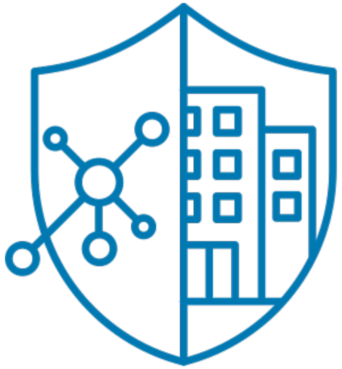
PASSWORD AND MULTI-FACTOR AUTHENTICATION (MFA) WEBINAR SERIES #1

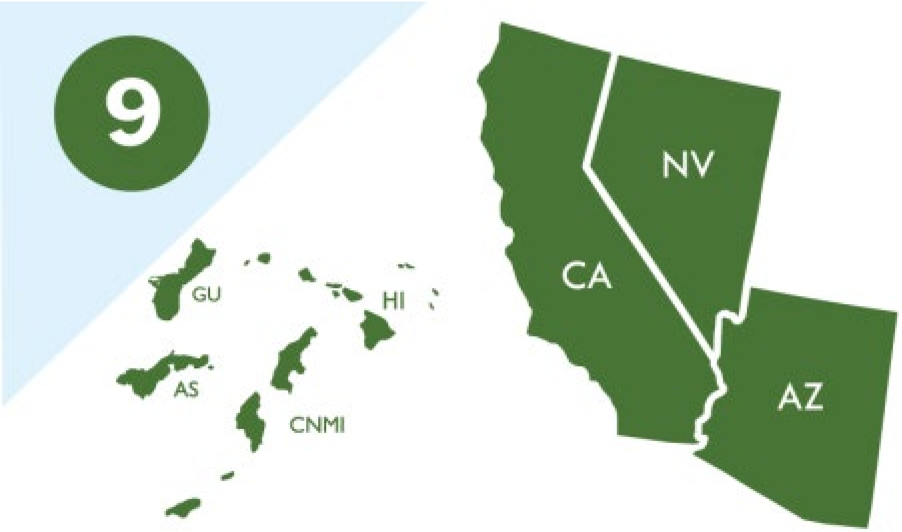
Jennilyn LaBrunda
February 5, 2024

CISA Mission and Vision

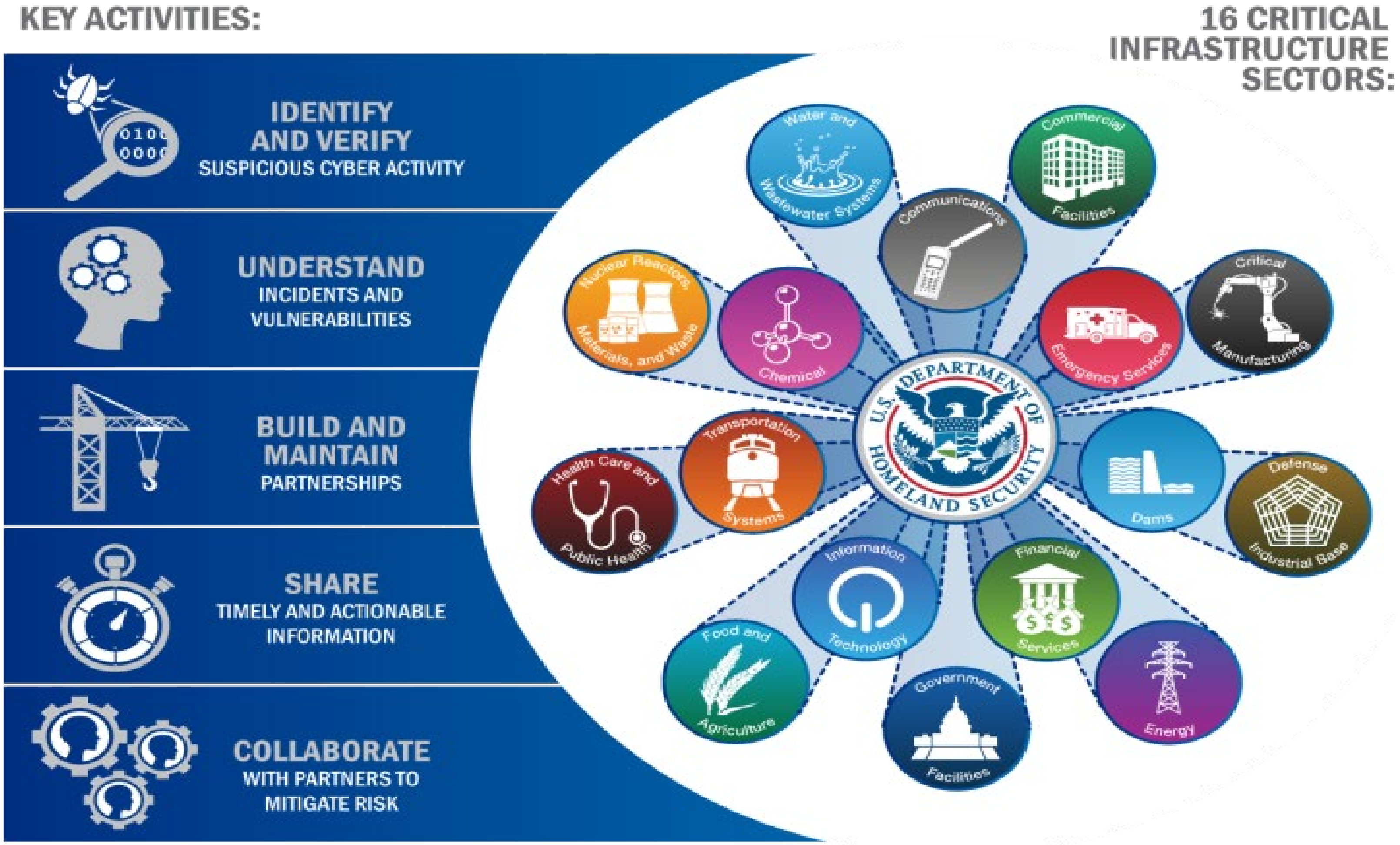
Our **mission** is to lead the national effort to understand, manage, and reduce risk to our nation’s cyber and physical infrastructure.

Our **vision** is a secure and resilient critical infrastructure for the American people.





Serving 16 Critical Infrastructure



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

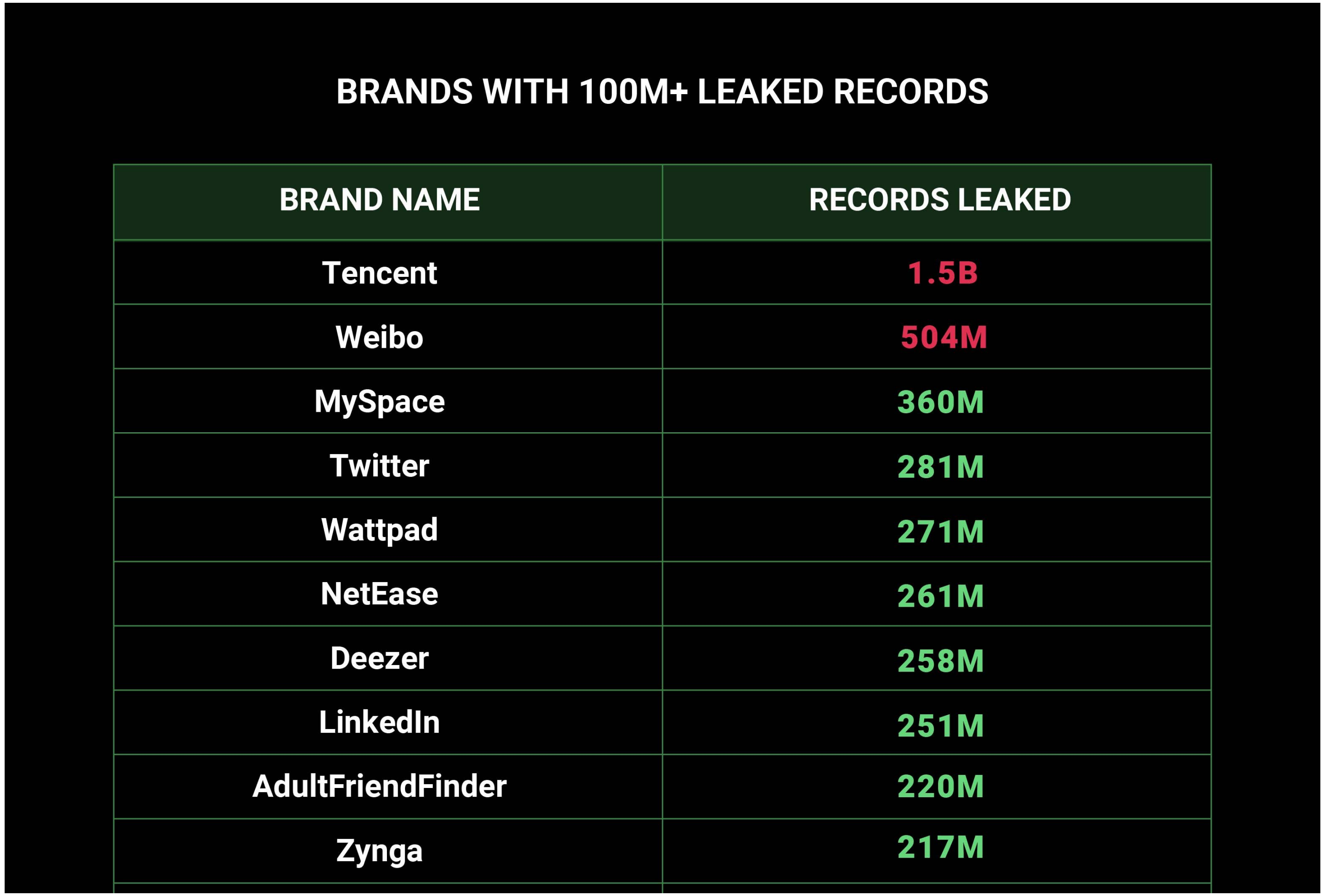
16 CRITICAL INFRASTRUCTURE SECTORS:

- Water and Wastewater Systems
- Commercial Facilities
- Communications
- Nuclear Reactors, Materials, and Waste
- Chemical
- Emergency Services
- Critical Manufacturing
- Transportation Systems
- Health Care and Public Health
- Dams
- Defense Industrial Base
- Information Technology
- Financial Services
- Food and Agriculture
- Government Facilities
- Energy

PASSWORD MANAGEMENT

Mother of all breaches

- MOAB reveals over 26 billion records leaked
- Includes sensitive data and usernames/passwords



BRANDS WITH 100M+ LEAKED RECORDS

BRAND NAME	RECORDS LEAKED
Tencent	1.5B
Weibo	504M
MySpace	360M
Twitter	281M
Wattpad	271M
NetEase	261M
Deezer	258M
LinkedIn	251M
AdultFriendFinder	220M
Zynga	217M

Let’s start with Why

- Password-based cyber attacks
  - **Brute force attacks**
    - Dictionary attacks
    - Password spraying
    - Mabna Institute cyber theft
  - **Phishing and Social engineering**
    - MGM breach
  - **Default passwords**
    - Exploitation of Unitronics Vision Series programmable logic controllers (PLCs)

Sources:
https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic
https://www.nbcnews.com/tech/security/mgm-las-vegas-hackers-scattered-spider-rcna105238
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Top 20 Passwords

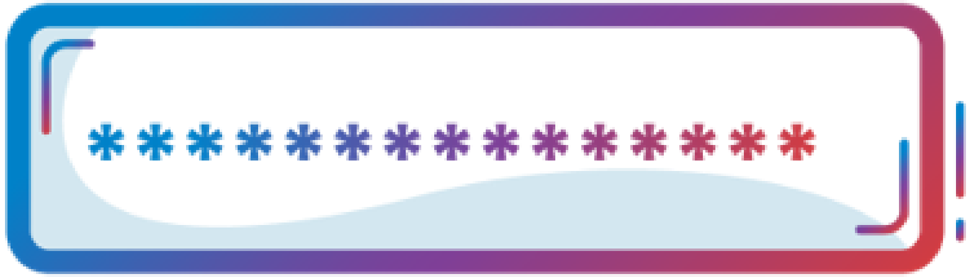
- Most common passwords used in the United States
- Obtained from over 43TB database extracted from various public sources including the dark web
- Cracked within 1 second

123456	UNKNOWN
password or Password	password1 or Password1
admin	Abc123
1234	1q2w3e4r
12345	123123
1234567	reset
12345678	qwerty or qwerty123
123456789	sh[redacted]bird
1234567890	111111
12345678910	info

Source: https://NordPass.com/most-common-passwords-list

Use Strong Passwords

CREATE STRONG PASSWORDS:



Example: Life-is-2_$hort_2-W@ste!
24 characters

- **Long**
  - At least 16 characters
- **Unique**
  - NEVER reuse passwords
- **Complex**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces

Use a Password Manager

WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.

Password Manager Features

Features to consider:

- End-to-end encryption
- Ease of use; password fill-in
- Cross platforms and browser extensions
- Ability to do encrypted export
- Additional features like travel mode, authenticator app, breach monitoring
- Cost

MULTIFACTOR AUTHENTICATION (MFA)

Multifactor Authentication (MFA)

WHAT IS IT?

- Increases the difficulty for threat actors to gain access to your information
- 2 or more verification factors:
  - Something you know, something you have, something you are
- Adds additional layer of security for authentication

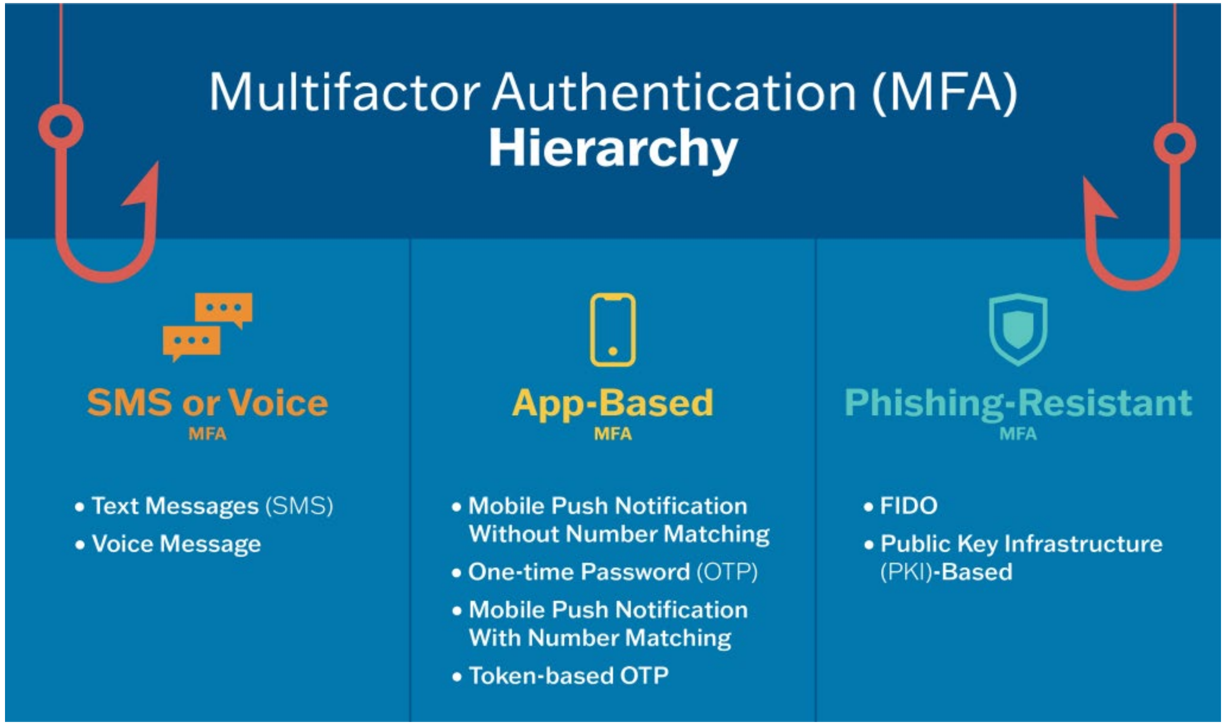
Turn on Multifactor Authentication

WHERE SHOULD YOU USE MFA?

- **Email**
- **Accounts with financial information**
  Ex: Online store, bank accounts
- **Accounts with personal information**
  Ex: Social media

Types of MFA

- Some MFAs are better than others
- **SMS or Voice MFA**
- **App-based MFA**
- **Phishing resistant MFA**
  - **P**ublic **K**ey **I**nfrastructure (PKI)-based
  - **F**ast **ID**entity **O**nline (FIDO)



Multifactor Authentication (MFA)
Hierarchy

SMS or Voice
MFA

- Text Messages (SMS)
- Voice Message

App-Based
MFA

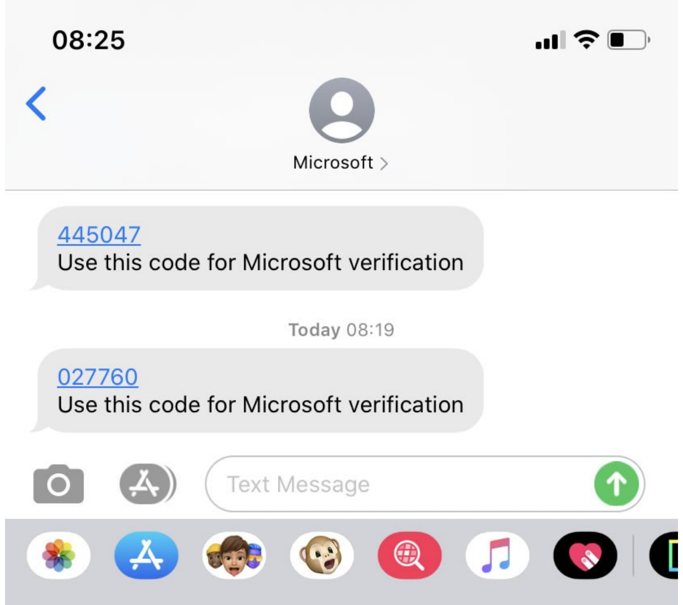
- Mobile Push Notification Without Number Matching
- One-time Password (OTP)
- Mobile Push Notification With Number Matching
- Token-based OTP

Phishing-Resistant
MFA

- FIDO
- Public Key Infrastructure (PKI)-Based

SMS or Voice MFA

- Pros:
  - Any MFA is better than no MFA
- Cons:
  - SMS and voice calls are not encrypted and can be intercepted
  - Vulnerable to phishing, sim cloning, and sim swapping
  - Must update when changing phone numbers
- SIM swap attack on SECs X (Twitter) account



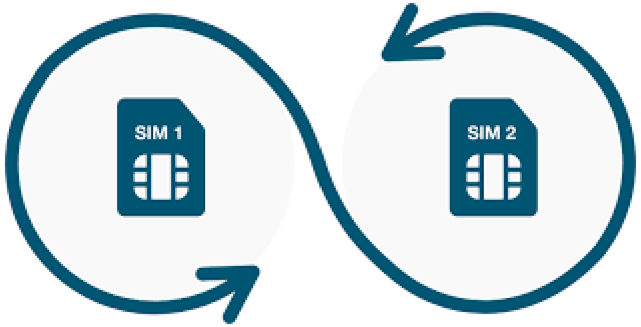
08:25

Microsoft

445047
Use this code for Microsoft verification

Today 08:19

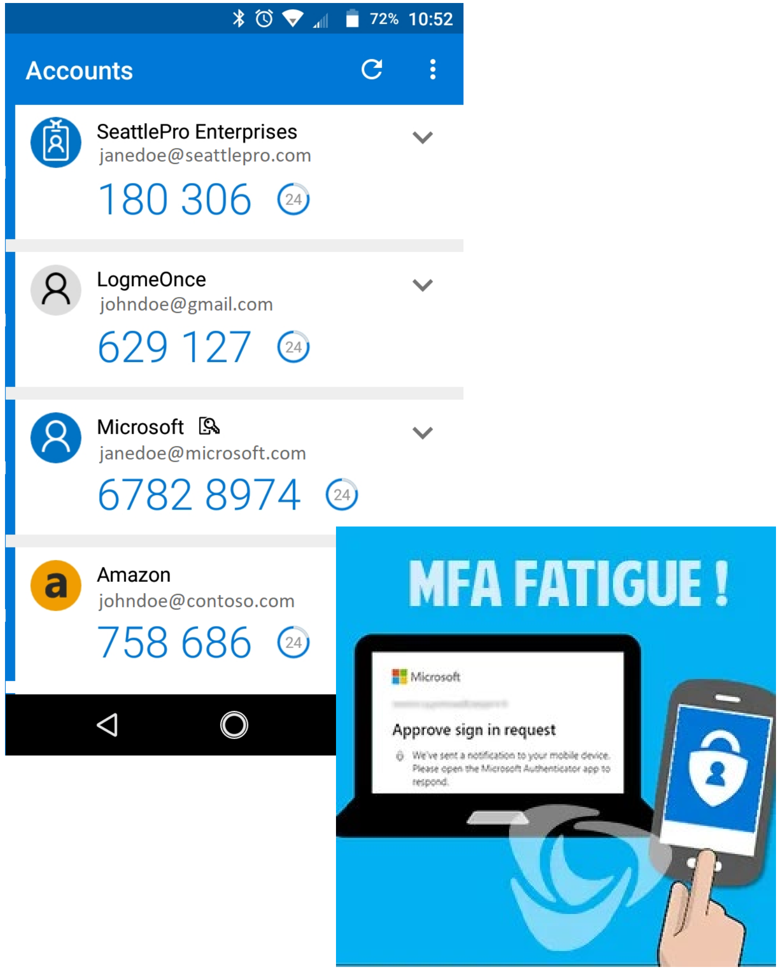
027760
Use this code for Microsoft verification



Source: https://www.msn.com/en-us/news/other/sec-report-reveals-sim-swap-attack-behind-hacked-x-account/ar-BB1h748B

App-based MFA

- Pros:
  - Easy to implement
  - Free or inexpensive
- Cons:
  - Must have a mobile phone and app installed
  - Time limit on One-Time Password (OTP)
  - Weak or no reception to receive push notifications
- MFA fatigue attack on Uber



72% 10:52

Accounts

SeattlePro Enterprises
janedoe@seattlepro.com
180 306 24

LogmeOnce
johndoe@gmail.com
629 127 24

Microsoft
janedoe@microsoft.com
6782 8974 24

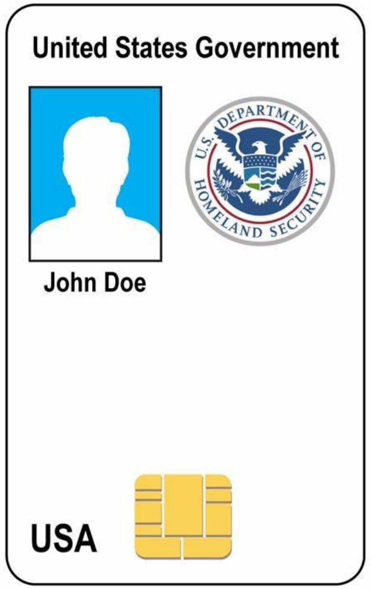
Amazon
johndoe@contoso.com
758 686 24

MFA FATIGUE !
Microsoft
Approve sign in request
We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Source:
https://www.securityweek.com/high-profile-hacks-show-effectiveness-mfa-fatigue-attacks/

Phishing resistant MFA

- **PKI** (Public Key Infrastructure)-based
- **FIDO** (**F**ast **ID**entity **O**nline)
- Features to consider:
  - Durability
  - Ease of use
  - Widely supported form factor (USB-C, USB 2.0, key cards); mobile phones
  - Supports Single sign-on
  - Broad range of authentication options (e.g. MFA, tokens, One Time Password, passwordless)



fido ALLIANCE

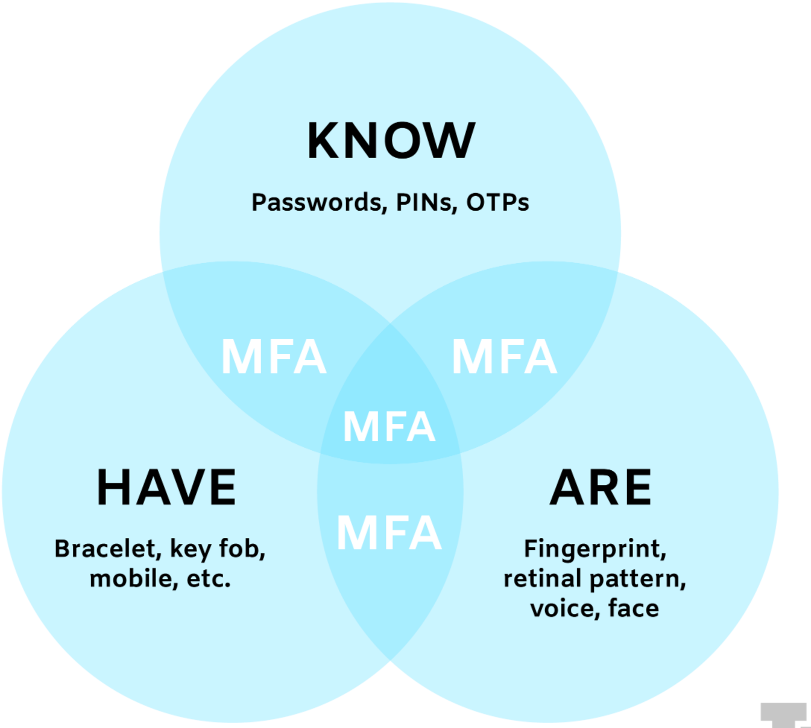
fido ALLIANCE

fido

fido

Implementing MFA

- What resources do I want to protect from compromise?
- Which users are high-value targets?
- Implementation challenges:
  - Some systems may not support phishing-resistant MFA
  - Difficult to deploy phishing-resistant MFA to all staff members at once
  - Concerns that users will resist migration to phishing-resistant MFA


KNOW

Passwords, PINs, OTPs

HAVE

Bracelet, key fob, mobile, etc.

ARE

Fingerprint, retinal pattern, voice, face

For more information:
www.cisa.gov

Jennilyn LaBrunda
Cybersecurity Advisor (Region 9)
Guam, CNMI, & American Samoa
Jennilyn.Labrunda@cisa.dhs.gov
808-260-3143

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA