



# Multi-Factor / Two Step Verification -- Why, What, and Where

Presented by Joe Chappell - Connected  
HHI

# Presentation Flow



Terminology



Background



Current State



What's Next

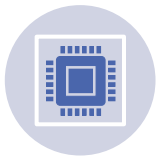


Q&A



\*Full presentation available for download

# Terminology



Two Step (Google)



Two-Factor  
Authentication  
(2FA)



Multi-Factor  
Authentication  
(MFA)



One Time  
Passcodes (OTP)



Security Key



Authenticator  
Apps

We will use Multi-Factor Authentication for this presentation

# The evolution of passwords

---



## The Roman “watchword”

Back in the day, the Roman army used “watchwords”—passphrases that proved you were a member of the unit. This early authentication system was a fast way to tell if someone was a friend or an enemy.



## The Prohibition password

In the 1920s, Prohibition led to the rise of “speakeasy” bars where alcohol was sold illegally and on the down-low. Presenting a card, code phrase, or saying a password was your ticket to getting inside.



## The 1st digital password

In 1961, MIT computer science professor Fernando Corbato created the first digital password as a project problem-solver. When he built a giant time-sharing computer, several users needed their own private access to the terminals. His solution? Give each user their own password.

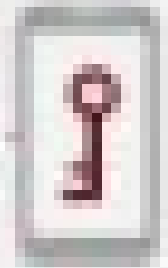


## Web 2.0 password overload

Today, there are passwords for almost everything. Each person has about 100 of them, and they’re often shared between family, friends, and coworkers. (Netflix, anyone?) Trying to remember all these details on a daily basis has led to major password fatigue.




# What's Multifactor Authentication




# Authentication Methods

Knowledge - Something You Know - passwords, PIN, username



Possession - Something You Have - fobs, security keys, one-time-passcodes



Inherence - Something You Are - Biometrics




Location



Time

A glowing green padlock is positioned on the left side of the slide, set against a dark background of a circuit board with glowing lines and nodes. The padlock itself is translucent and filled with a bright green light, giving it a digital or cybernetic appearance.

# Drivers for Multi-Factor Authentication

- ▶ Password Re-Use
  - ▶ Password Theft
  - ▶ Password Hacking
- 
- The right side of the slide features an abstract background composed of several overlapping, semi-transparent blue triangles and polygons of varying shades, creating a modern, geometric design.

Government



```
graph TD; Government[Government] --> Industry[Industry]; Industry --> Consumer[Consumer];
```

Industry

Consumer

MFA Adoption





## Consumer Drivers of MFA

- ▶ Financial Services
- ▶ Healthcare
- ▶ Online Shopping
- ▶ Google
- ▶ Microsoft
- ▶ Apple



# Evolution of MFA Methods

- ▶ Secret Phase - “Boston”
- ▶ Generic Security Question - “Mother’s Maiden Name”
- ▶ Customized Security Question - “Who makes the best electric bass?”
- ▶ Security Devices - cards and fobs
- ▶ One-Time-Passcode Generators - cards, keys, fobs
- ▶ Biometrics - Retina, fingerprint, facial, and voice scans
- ▶ Authenticator Apps

# One Time Passcodes

- ▶ Can be generated by a service and sent via email or text with a limited lifetime (5 minutes, 10 minutes, ...)
- ▶ Often generated in an authenticator application based on a shared secret and the time. (Time-based One-time-passcodes) that changes every frequently (Often every 30 seconds).
- ▶ Passcodes are often six numeric digits but can be longer and can include alpha characters
- ▶ Can be generated by dedicated OTP devices - RSA and Bank of America are examples

# Amazon Authentication Request



## Two-Step Verification

For added security, please enter the One Time Password (OTP) that has been sent to a phone number ending in 297

Enter OTP:

Don't require OTP on this browser

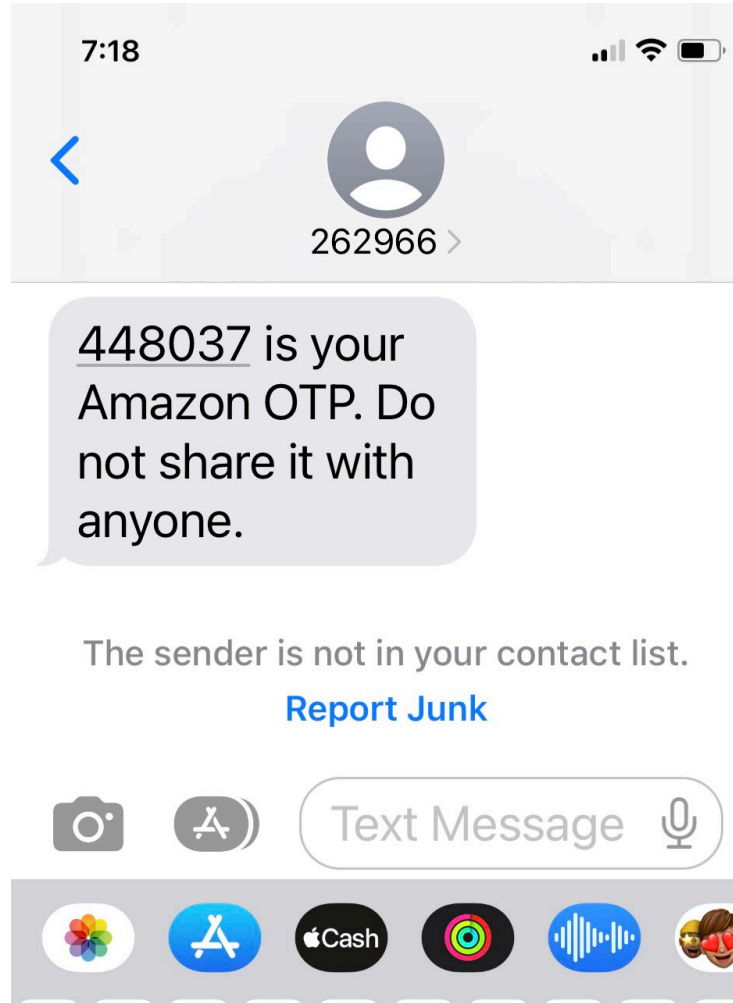
Sign in

• [Didn't receive the OTP?](#)

[Conditions of Use](#) [Privacy Notice](#) [Help](#)

© 1996-2023, Amazon.com, Inc. or its affiliates

# Amazon OTP Text



# Bank of America - Idem Key Example



# Authentication Applications


- ▶ Microsoft Authenticator, Google Authenticator, and Authy are 3 of the most common authentication apps.
- ▶ Some services require a specific authenticator application, but many leave the choice to the user
- ▶ Authenticator applications can be used for a multitude of services
- ▶ The process of adding a service involves registering your authentication application with the service and establishing a shared secret that is used to validate the OTP
- ▶ Authentication Apps often require user authentication before providing the OTP (password, facial scan, ...)
- ▶ Microsoft is adding a number and optionally application and location information to authentication requests





jchappell@connectedhhi.com

## Approve sign in request

 Open your Authenticator app, and enter the number shown to sign in.

22

No numbers in your app? Make sure to upgrade to the latest version.

[I can't use my Microsoft Authenticator app right now](#)

[More information](#)



## Simple to Complex - Less Secure to More Secure

- ▶ Text or Email OTPs
- ▶ Application based authentication applications
- ▶ Biometric protected authentication applications
- ▶ Biometric protected security keys



# Microsoft “Passwordless” with Authenticator



# Take Aways

- ▶ Password hygiene is still important - unique and relatively complex
- ▶ MFA should be used whenever you have something that you value and would like to protect
- ▶ When it is your choice, select the level of MFA that is appropriate for what you are safeguarding
- ▶ Don't even think about using MFA if your phone, tablet, and computer are not password or biometrically secured!!



**Connected HHI**

## Q&A

- ▶ Joe Chappell
- ▶ Connected HHI
- ▶ [jchappell@connectedhhi.com](mailto:jchappell@connectedhhi.com)
- ▶ [www.connectedhhi.com](http://www.connectedhhi.com)
- ▶ 843-715-9894