JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Securing Authentication and Authorization

Security Architecture & Tool Sets

Securing Authentication

- Technical and administrative controls can help secure the authentication process
- Uses strong passwords/passphrases
- Password management is a concern
  - Consider Single-Sign-On
  - Token-based for multifactor
  - Password safes (LastPass, Dashlane, etc)
- Encrypt communications between clients and authenticators using TLS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Securing Authorization (Users)

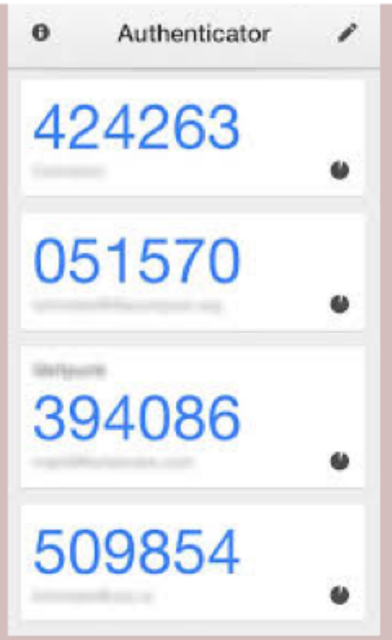
- Access control ensures users are matched with rights/privileges
- Polices to control what rights are given
- Implement management systems for approving rights
- Monitor/report on which accounts have which rights assigned

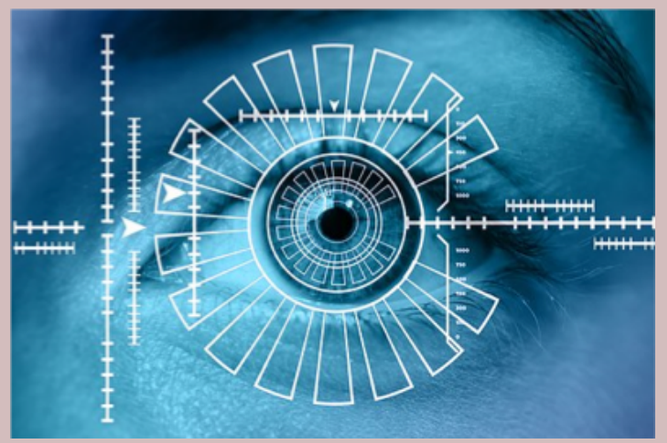
Securing Authorization (Admin)

- Privileged User Management concerns giving admin rights to users
- Use additional monitoring and logging
- Implement separation of duties
- Use appropriate training
- Prevent admin accounts from being used as daily accounts

Multifactor Authentication

- Use two or more factors for authentications
  - Knowledge factors
  - Possession factors
  - Biometric factors
  - Location factors



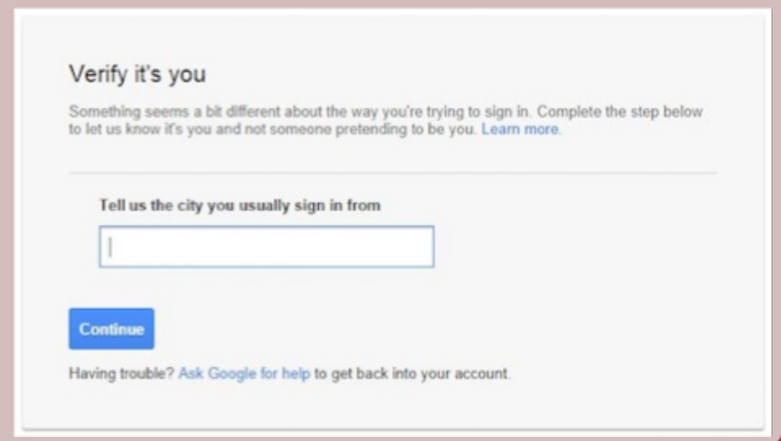


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Context-Based Authentication

- Authentication decision is based on information about the user, system, etc.

- User's role or group membership
- Time of day in relation to user's hours
- IP address and reputation
- Frequency of access
- Location (IP or GPS)
- Type of device



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE