PART 2 - ACCOUNT PROTECTION
Small Systems Aren't Small Potatoes, Why Rural Water Utilities Need Cybersecurity and What To Do About It

NRWA

WATER ISAC

PART 2 - ACCOUNT PROTECTION WEBINAR TAKEAWAYS

PASSWORD PROTECTION AND ACCOUNT MANAGEMENT

- Never reuse the same password on a different account
  - Do not use simple variations either *(rX5gJoe1, rX5gJoe2, rX5gJoe3, etc.)*
  - If you have reused passwords in the past, go back and change them over time
- Password length of at least 18 characters for important accounts
- Use a password manager *(1password, lastpass, dashlane, etc.)*
- Close accounts when people leave
- Only use Admin passwords when required

MULTIFACTOR AUTHENTICATION

- Reduces the risk from successful phishing attacks due to credential harvesting or stolen credentials
- Reduces the risk posed from poor password practices
- Two or more factors are better than one

REMOTE ACCESS

- Only provide remote access to systems if there is a real business need that cannot be met another way.
- When providing remote access minimize your exposure:
  - Reduce the number of users who have access
  - Limit what users can access, and for what purpose
  - Control the time that remote access is provided
  - Control where users can access from
- When providing remote access use a secure solution:
  - A virtual private network (VPN) with end to end encryption and device authentication
  - Segregate your network so there is no direct access to your systems remotely
  - Use multi-factor authentication (MFA) on all account logins