MassDEP
Drinking Water Program

CYBERSECURITY AWARENESS MONTH 2022

# Cybersecurity

## Tips For Public Water Systems

For Cybersecurity Awareness Month, we are highlighting actions/steps you can take to secure your sensitive data and stay safe online.

**Review** First, review your current security level. Identify system components and network connections to assess risk (i.e., know what you're protecting).

**Strong Password:** Passwords are your first line of defense against cyber-attacks. Use a strong password. Make sure it's: long – at least 15 characters, and avoid using common or easily guessable passwords, such as simple keyboard patterns, when creating your passwords. Don't share your password with anyone or use the same or similar password for multiple accounts. For more tips view/download the MassDEP poster on password hygiene **here**.

**Multi-factor Authentication:** Use two-factor authentication. You need more than a password to protect your remote system access and important online accounts. Enabling MFA makes you significantly less likely to get hacked.

**Software Update:** Keep computers, devices, and applications, including Supervisory Control and Data Acquisition (SCADA) /industrial control systems (ICS) software, patched and up to date. Keep automatic software updates enabled whenever possible. This will ensure that software updates are installed as quickly as possible. Install the latest version of anti-malware protection. Routinely run a complete scan of your system to check for any malware infections. Access/download the MassDEP poster with more tips on software updates **here**.

**Train Staff:** Train staff to identify, respond and report cyberattacks. Implement an employee cybersecurity training program.

**Think Before You Click:** More than 90% of successful cyber-attacks start with a phishing email. Train staff to identify, respond and report cyberattacks that begin with a phishing email, or similar ploys using text messaging or voice mail. Make them very suspicious of emails that ask for their password or for them to call a phone number to resolve an account-related problem. Review/ download MassDEP poster with more tips on recognizing and responding to phishing attacks **here**.

**Secure Remote Access Methods**: All remote access should be subject to monitoring, audit, and prompt patching.

**Emergency Response Plan (ERP):** Keep your ERP up-to-date and include actions to take in case of a cyber breach. See MassDEP Guidelines and Policies for Public Water Systems Appendix O- Handbook for Water Supply Emergencies for more information.