Cybersecurity is Not Just for the Office

Dan Laprade (MWWA Training Coordinator)
dlaprade@masswaterworks.org (413-883-7030)

When water operators hear the term 'cybersecurity' they often relegate that issue to people working with SCADA or staff using computers in the office. While using laptops and tablets in the field presents a risk so does using smartphones. Virtually any wireless communication (Wi-fi and cellular signals) is vulnerable to being compromised and the consequences can be significant. Stolen or hacked devices allow malicious actors to access sensitive data or disrupt an operator's ability to monitor/correct important system operations.

Field staff should keep the following tips in mind:

- Lock Devices: Always secure phones, tablets, and laptops with a strong PIN, password, or biometric lock when not in use.
- Report Losses Immediately: If a device goes missing, report it right away so corrective actions can be taken quickly.
- Update Regularly: Allow devices to install updates, which often include crucial security fixes.
- Think Before Connecting: Be cautious when using public Wi-Fi and stick to secure utility networks. Turn off Bluetooth when not actively using it.
- Strong Passwords: Use strong, unique passwords for all work accounts and never share them.
- Secure the Screen: Get in the habit of locking the device screen whenever stepping away.
- Handle Data Carefully: Only access the data needed and avoid storing sensitive information on personal devices.
- Be Wary of the Unexpected: Be cautious of suspicious emails, texts, or calls asking for prompting to click a link. Verify any request that seems unusual.
- Trust Your Gut, Ask Questions: If something feels off or unusual, ask a supervisor or the IT department for guidance.
- Follow Policies: Adhere to the water utility's cybersecurity guidelines.

1. What is the most significant risk associated with an operator's mobile device being stolen?
    a) Increased battery drain
    b) Unauthorized access to sensitive information or control systems
    c) Slower network connectivity
    d) Damage to the device's screen

2. The best way to connect to a secure mobile network when working in the field is to.....
    a) Use a Public Wi-Fi Connection(PWFC)
    b) Use a Virtual Private Network (VPN).
    c) Use a 'Hotspot'
    d) All of the above
    e) None of the above

3. What should an operator do if their work-issued mobile device is lost or stolen?
    a) Try to locate it using an Airtag™ or other similar tracking device.
    b) Report it immediately to their supervisor or IT department.

c) Wait until the end of their shift to report it.
d) Call 911.

4. Which of the following is NOT a good practice for passwords?
a) Including a mix of uppercase and lowercase letters.
b) Something that is easy to remember and used on other devices.
c) Incorporating numbers and symbols.
d) Ensuring they are unique for different accounts.

5. What should an operator do if, upon logging in, an unusual link pops up that must be clicked on in order to proceed.
a) Click on the link and follow the instructions carefully.
c) Contact a supervisor or IT department to determine its authenticity
c) Ask a colleague if they are encountering the same thing.
d) All of the above
e) None of the above

MassDEP provides many cybersecurity resources available to public water systems including a free training video approved for 1 TCH: Cybersecurity Resource Hub

[AI generated image]