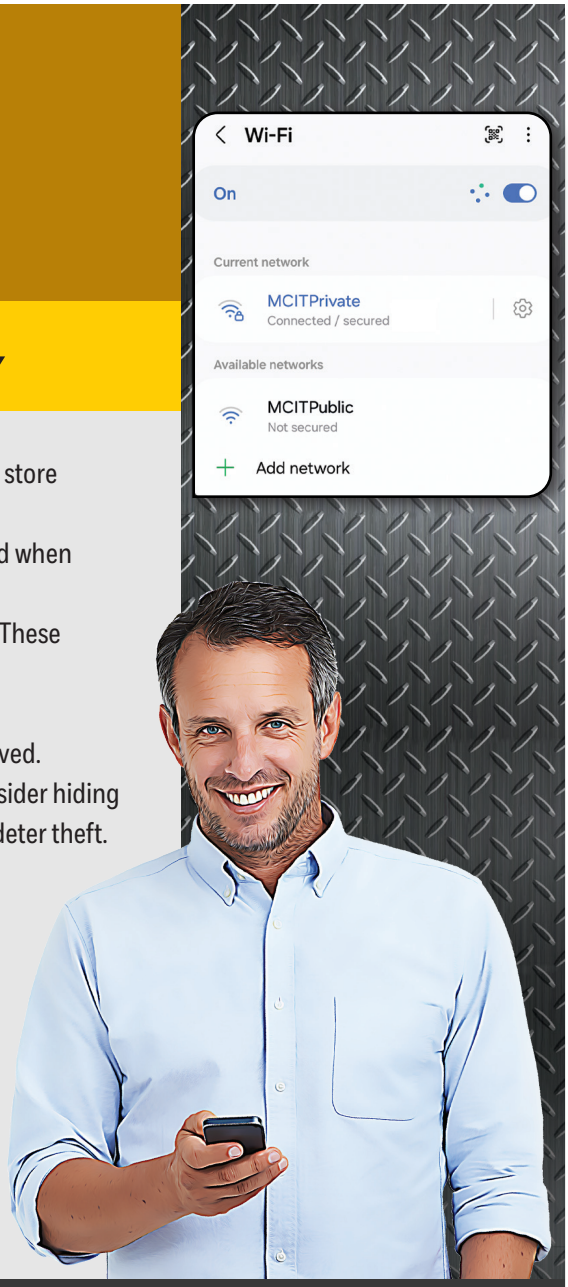
Loss Prevention
QUICK REVIEW
DATA SECURITY

MOBILE DEVICE SECURITY

- Limit the amount of data stored on the device. Whenever possible, do not store sensitive data on mobile devices.
- Mobile equipment should be protected with a secure password and locked when inactive.
- When transmitting private or sensitive data always use a secure network. These networks typically require a password to access *(see image)*.
- Any private or nonpublic data should be encrypted.
- Mobile devices should be updated regularly as systems or apps are improved.
- Keep devices with you or locked in secure locations away from others. Consider hiding these items from view when storing them in vehicles or other locations to deter theft.
- Avoid using the device in an area where others can view the screen.
- Use and regularly update trusted antimalware or security tools for your mobile devices.
- Securely wipe all private data from devices before they are removed from service, transferred to a new user or sold. Consider using services that allow IT professionals to remotely lock or wipe data devices lost to theft or negligence.
- Remember that simply using a mobile device does not guarantee immunity from viruses or hacking. If you would not do something with your work computer, do not do it with your mobile device.



IF A DEVICE IS MISSING OR YOU SUSPECT A DATA BREACH

- Do not panic and make the situation worse by complying with instructions from malicious programs or hackers.
- Report the situation to a supervisor or IT.
- Follow IT and supervisor directions and the policies of our organization.

NOTES:

Click Wisely

© 2024 MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST
This document is intended for general purposes only and should not be construed as legal or coverage advice on any specific matter.