April 2025 Cyber Security Tip: Safety in the Workplace

State team members play a crucial role in maintaining a strong security posture for the State of Missouri. Here are some tips to help protect you, your computer, and the State's data.

- Do not allow unauthorized access to secure parts of the building. Require anyone following you to swipe their badge before entering to ensure they have authorization to the secure area.
- Be aware of any sensitive printed information on your desk that can be viewed by unauthorized individuals. Keep this information secure and dispose of any sensitive printed material by finding a locked shred box or run documents through an approved shredder.
- Make sure to log out or lock your screen if you leave your desk to prevent unauthorized access to sensitive digital content.
- Do not plug unauthorized devices into your workstation. These devices can contain malicious programs or allow a malicious actor to bypass security when plugged in.
- Keep passwords in a password management tool such as "Pleasant Password." **Do not write passwords down**.
- See something, say something. If you become aware of a potential security risk, or if State data may have been compromised, email the Office of Cyber Security (OCS) immediately at **cyber.security@oa.mo.gov**.
- For additional workplace safety tips, visit the OCS website at **cybersecurity.mo.gov/state-employee-security-tips**.

Key takeaway: Assume responsibility for cyber safety best practices in the workplace. As a State team member, each of us have a responsibility to protect Missouri's data.

OFFICE OF CYBER SECURITY
MISSOURI OFFICE *of* ADMINISTRATION