PAUSE VERIFY REPORT
WHILE TELEWORKING

Tips for Commonwealth of Massachusetts state government employees to protect public resources while teleworking

- PAUSE: Pause before opening an attachment. This is the most important cybersecurity protection.
- VERIFY: If you get an unexpected email, contact the sender with information you already have on file. If you don't know the sender, it may be malicious.
- REPORT: Think fast! Viruses spread rapidly, sometimes without immediate noticeable effect on your equipment.

Give your Wi-Fi a New Name

Secure your virtual workstation router and Wi-Fi with a new name and long and strong password.

VPN all day, every day

Secure your virtual workstation by always signing into your work assigned VPN (virtual private network) while working.

Watch out for Imposters

Fraudsters open pose as employees and vendors to trick you into responding.
When teleworking keep your workstation secure and PAUSE VERIFY REPORT when reviewing emails, texts, calls, and other requests.
This will protect your department's data and systems.

Don't Make it Personal - Use only Office Assigned or Approved Devices

Follow your department's telework policy before accessing work networks, sites, email, and files while teleworking.

Don't Play with Risky AI Chatbot Tools

Everything you type into an AI chatbot search bar can be seen publicly, giving hackers information to attack your office network. Check with IT before using AI tools.

The Office of the Comptroller provides recommended cybersecurity internal controls to promote integrity, mitigate risk, and protect the Commonwealth's data and systems to prevent fraud, waste and abuse of public resources.

Contact CTREmergencyNotification@mass.gov with any suspected cyber incidents or fraud, and for internal controls assistance from CTR.

MAComptroller.org/CTRCyber   @MAComptroller   @MA_Comptroller   @MAComptroller