




PAUSE VERIFY REPORT ON THE GO AND TRAVEL

Visit <https://www.macomptroller.org/cybersecurity-awareness-training-on-the-go/> with tips and internal controls to protect your workstations and networks on the go.

PAUSE VERIFY REPORT to Improve your Cybersecurity Awareness

PAUSE VERIFY REPORT gives employees three simple steps to handle incoming requests from emails, text messages, and calls. This can identify fraudsters, and prevent most cyber attacks and fraud incidents.

-  **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.

Follow your Office Off-Site and Travel Policies

PAUSE and make sure you are following your department's telework policy when you are away from your office approved workstations, and any travel policy before attempting to access work networks, sites, emails, and files.

VERIFY with your manager and IT staff how to access work networks properly when you are commuting or traveling, including setting up a cellular hotspot and VPN.

No Public Wi-Fi

Even password public Wi-Fi is not secure! Do not access work networks unless you are using an approved hotspot and VPN if you are away from your secured workstations.

Bluetooth - Don't Pair in Public

If you are on the go and working away from your secure workstations, **PAUSE** and turn off Bluetooth if you are working in crowded areas. Using wired connections for your mouse, keyboard, headphones, and hotspots is always the safest option when working on the go.

Don't Plug into Public or Free USB cables, ports, or flash drives.

PAUSE and do not plug your devices into any Public or free USB charging cables, ports or flash drives.

VERIFY that you are using your own or work provided cables and bring your own power bank.

REPORT to your IT staff with any USB flash drive so it can be scanned on segregated machines.



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](https://www.macomptroller.org/CTRCyber)

 @MAComptroller

 @MA_Comptroller

 @MAComptroller