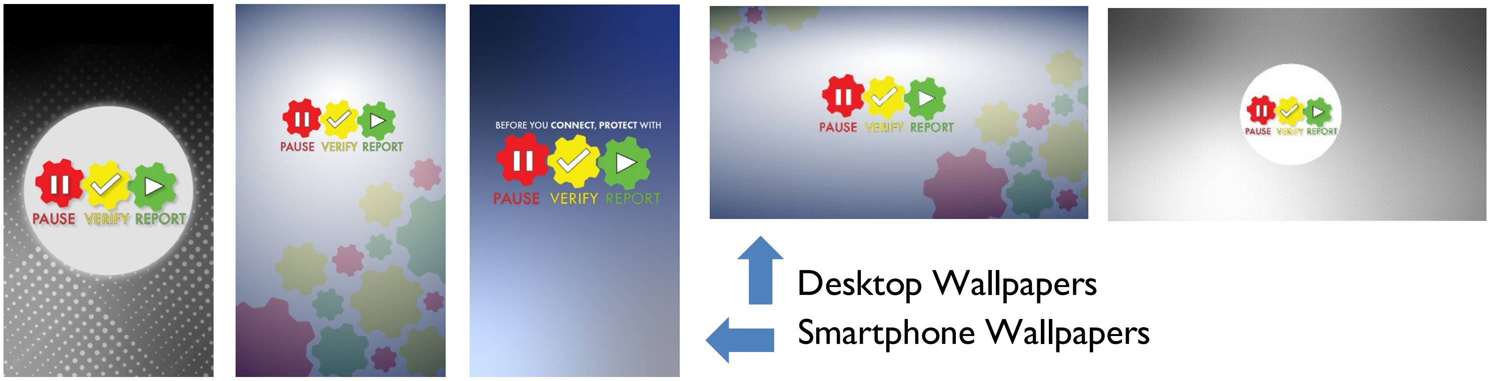
CTR CYBER - CYBERSECURITY AWARENESS MONTH TRAINING PACKAGE

To assist departments with Cybersecurity Awareness Month the Office of the Comptroller (CTR) has compiled a list of resources posted on CTR Cyber that you can use as free resources to share with your staff. CTR Cyber is updated weekly, so book mark this page and check back for weekly tips!

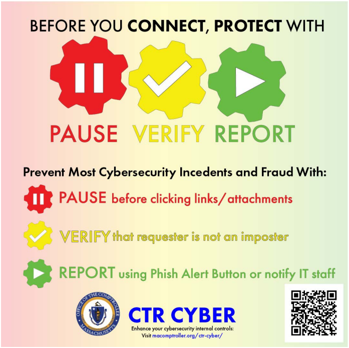
Our slogan for October2024 Cybersecurity Awareness Month is:

Feel free to share this logo with your staff, as well as our desktop and smartphone wallpapers, and digital business card.



Desktop Wallpapers
Smartphone Wallpapers

Pause, Verify, and Report are 3 simple cybersecurity internal controls that your staff can use to prevent most incidents and fraud attempts, which can protect your department and prevent and costly time and resources for containment and remediation. Including Pause Verify and Report reminders for your staff throughout the fiscal year are recommended internal controls to prevent fraud, waste and abuse of Commonwealth resources, and can be included as part of your Internal Control Plan and system of internal controls.



BEFORE YOU **CONNECT**, **PROTECT** WITH

PAUSE VERIFY REPORT

Prevent Most Cybersecurity Incedents and Fraud With:

PAUSE before clicking links/attachments

VERIFY that requester is not an imposter

REPORT using Phish Alert Button or notify IT staff

CTR CYBER

Enhance your cybersecurity internal controls:
Visit macomptroller.org/ctr-cyber/

This digital business card can be saved and shared among staff, it redirects to more information on our website.

CTR CYBER - CYBERSECURITY AWARENESS MONTH TRAINING PACKAGE

CTR Cybersecurity Awareness Training Page Your one stop shop for up to the minute Cybersecurity Awareness Tips.

Pause Verify Report Training (great for all staff)(10 min) Employee Cyber Awareness Micro Training, we simplify Cybersecurity with three simple steps: Pause, Verify, Report. Cybersecurity simply is the protection of data and systems with internal controls.

All Hands on Deck (52 mins). In November 2023, Comptroller William McNamara and Secretary Jason Snyder and other cybersecurity leaders from throughout the Commonwealth of Massachusetts joined the Office of the Comptroller for a live webinar, talking about how everyone throughout an organization must play a critical role in protecting the Commonwealth's data, systems, and resources.

Pause, Verify and Report Content: Use this content to share with staff, talk about in staff meetings and for internal Cybersecurity Awareness Trainings.

View Cybersecurity Tips for Work

View Cybersecurity Tips Working on the Go

View Cybersecurity Tips For Leadership/IT

View Cybersecurity Tips For You at Home

CTR CYBER - CYBERSECURITY AWARENESS MONTH TRAINING PACKAGE

CTR CYBER 5 – A collection of short videos from local and global cybersecurity experts that you can use to discuss important cybersecurity issues with staff and get great tips for protecting your department.

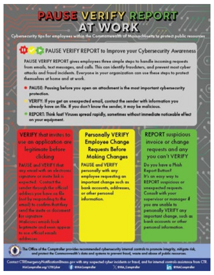
Infographics: Leadership at state agencies can support Cybersecurity Awareness Month by sharing this infographic with their employees and/or posting it in state offices. The tools and procedures in this document are critical to protecting state resources, and can be useful reminders in addition to departments' mandatory cybersecurity training.

What is Pause Verify Report? Every state employee is on the front lines keeping the Commonwealth of Massachusetts safe from cyber attacks. Share this infographic and send it to staff to help spread the word about PAUSE VERIFY REPORT.

WHAT IS PAUSE VERIFY REPORT?

Click the image to access a PDF of this one-sheet infographic. Full page copies can be found in the Appendix at the end of this document.

Pause Verify Report at Work State employees are the Commonwealth's best defense to protect data privacy. Statutory privacy and data protection laws require internal controls to protect data and to ensure that operations and systems are not disrupted due to a cyber incident.


PAUSE VERIFY REPORT AT WORK

Pause Verify Report on the Go Protecting Commonwealth of Massachusetts property from cyber-attacks has to happen not only in the office or at home, but when state employees traveling for work or are otherwise on the go.

PAUSE VERIFY REPORT ON THE GO AND TRAVEL

Pause Verify Report at Work - while Teleworking Reminders to always be vigilant against cybersecurity attacks against state networks and fraud attempts targeting public funds, especially while working away from the office.

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

Pause Verify ReportFor Leadership and IT Leadership and IT units at departments throughout the Commonwealth of Massachusetts can post this infographic at state offces. Send it to managers as a reminder to build a strong culture of cybersecurity internal controls.

PAUSE VERIFY REPORT
FOR LEADERSHIP/IT

PAUSE VERIFY REPORT to Improve your Cybersecurity Awareness

Leadership and IT staff are critical partners supporting a strong culture of cybersecurity internal controls. Even inadvertent mistakes can disrupt a network and downtime impedes your mission and costs valuable resources.

- PAUSE: Pausing before you open an attachment 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.

Leadership "Tone from the Top" Must Prioritize Cybersecurity

Leadership and managers are responsible for establishing a strong internal controls "Tone from the Top" that identifies that cybersecurity internal controls are part of the foundation of all operations and are a top organizational priority.

Leadership Must Assign Key Staff to Ensure Cybersecurity Compliance

Ensure that Leadership has specifically assigned staff at all levels of the organization (IT, HR, Legal, Policy, Fiscal, Budget, Payroll, Program and Operations staff) to meet the required cybersecurity and data protection internal controls.

EOTSS Information Security Standards are the Commonwealth's Minimum Internal Controls

The Commonwealth's default data and security standards and internal controls must be included in a Department's Internal Control Plan, implemented, tested, and included in staff training.

Risk Assessments are Part of Your Internal Control Plan

In addition to ongoing cybersecurity compliance, ensure that the annual Internal Control Plan review process includes a risk assessment of cybersecurity risks and controls.

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

WHAT IS

PAUSE VERIFY REPORT?

3 simple internal controls that everyone in your organization can use to protect your networks at work and at home:

- PAUSE: Pausing before you open an attachment 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.

How do you PAUSE?

Whenever you receive an email, call or text, PAUSE before clicking on a link or attachment, or responding, which gives you time to protect your organization from an incident or fraud.

VERIFY Who You are Interacting with before you Act

Part of our public work is to use official information on file to VERIFY that requests are legitimate, and that we are not unknowingly dealing with an imposter, or opening a malicious attachment or link.

REPORT suspicious emails or requests and any you can’t VERIFY

REPORT any emails that you believe are suspicious to your IT team. Consult with your supervisor or manager with any “odd” requests or if you are unable to personally VERIFY any important change, such as bank accounts or other personal information.

Do you have a Phish Report Button?

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 f @MAComptroller X @MA_Comptroller in @MAComptroller

PAUSE VERIFY REPORT AT WORK

Cybersecurity tips for employees within the Commonwealth of Massachusetts to protect public resources

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. Everyone in your organization can use these steps to protect themselves at home and at work.

- PAUSE: Pausing before you open an attachment 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.

VERIFY that invites to use an application are legitimate before clicking

PAUSE and VERIFY that any email with an electronic signature or invite link is expected. Contact the sender through the official address you have on file (not by responding to the email) to confirm that they send the invite or document for signature.

Malicious emails look legitimate and even appear to use official emails addresses.

Personally VERIFY Employee Change Requests Before Making Changes

PAUSE and VERIFY personally with any employee requesting an important change such as bank accounts, addresses, or other personal information.

REPORT suspicious invoice or change requests and any you can't VERIFY

Do you have a Phish Report Button?

It's an easy way to REPORT suspicious or unexpected requests.

Consult with your supervisor or manager if you are unable to personally VERIFY any important change, such as bank accounts or other personal information.

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

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

PAUSE VERIFY REPORT FOR LEADERSHIP/IT

PAUSE VERIFY REPORT to Improve your Cybersecurity Awareness

Leadership and IT staff are critical partners supporting a strong culture of cybersecurity internal controls. Even inadvertent mistakes can disrupt a network and downtime impedes your mission and costs valuable resources.

- PAUSE: Pausing before you open an attachment 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.

Leadership "Tone from the Top" Must Prioritize Cybersecurity

Leadership and managers are responsible for establishing a strong internal controls "Tone from the Top" that identifies that cybersecurity internal controls are part of the foundation of all operations and are a top organizational priority.

Leadership Must Assign Key Staff to Ensure Cybersecurity Compliance

Ensure that Leadership has specifically assigned staff at all levels of the organization (IT, HR, Legal, Policy, Fiscal, Budget, Payroll, Program and Operations staff) to meet the required cybersecurity and data protection internal controls.

EOTSS Information Security Standards are the Commonwealth's Minimum Internal Controls

The Commonwealth's default data and security standards and internal controls must be included in a Department's Internal Control Plan, implemented, tested, and included in staff training.

Risk Assessments are Part of Your Internal Control Plan

In addition to ongoing cybersecurity compliance, ensure that the annual Internal Control Plan review process includes a risk assessment of cybersecurity risks and controls.

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

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　@MAComptroller　@MA_Comptroller　@MAComptroller