Cybersecurity made simple with Pause Verify Report

Employee Cybersecurity Awareness Micro Training

Achieve better cybersecurity results with simple concepts and action steps

OFFICE OF THE COMPTROLLER
COMMONWEALTH OF MASSACHUSETTS

What is Cybersecurity?

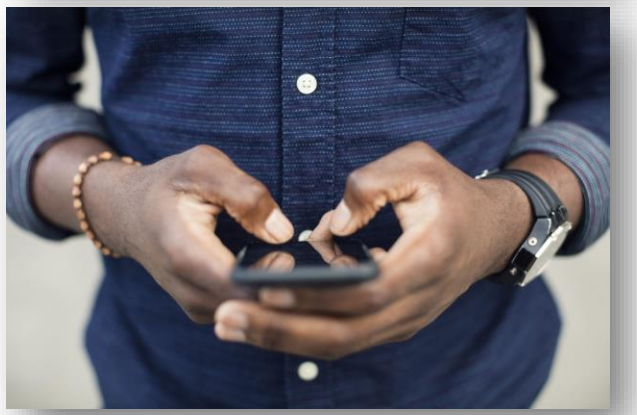
Protection of Data and Systems With Internal Controls

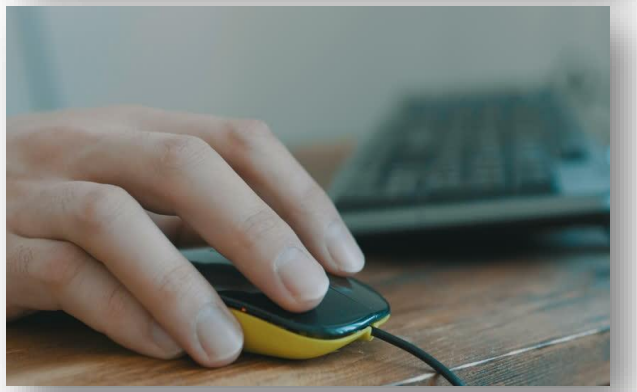
Cybersecurity Internal Controls protect from:

- **Data theft**
  Personally Identifiable Information, Social Security Numbers
- **Stolen funds**
  Misdirected payroll or vendor paychecks
- **Unauthorized systems access**
  Hacking
- **Network disruptions or damage**
  Ransomware and malware
- **Repair costs from an incident**
  Reimaging networks and devices
- **Damages for data breaches**

Why Does this Matter to Me?

- ★ **Government data and systems are high value assets and prime targets**
- ★ **Cyber criminals are highly organized (conglomerates) and seek to shut down systems, steal data and funds**
- ★ **Artificial intelligence is being used in cyber crimes**
- ★ **Criminals target you to trick you into helping them steal data and money, or lock down your networks**





If you touch it…

You're touching data and systems.

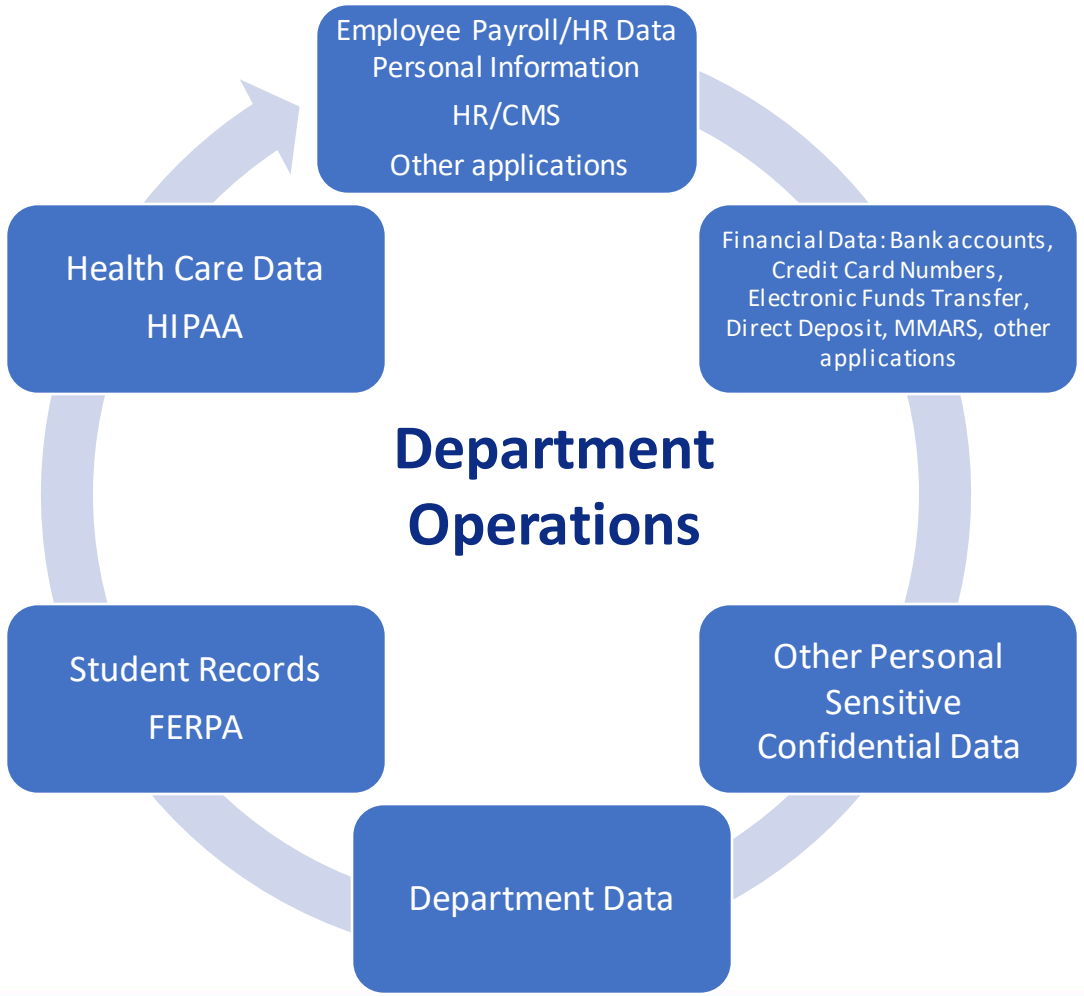
Don't be a Cyber Victim.

Don't let the bad guys in.

Data you may touch triggers protections

Any data you touch has legal and compliance rules.

If it is personally identifiable information or confidential you MUST PROTECT the data and systems from cyber fraud.



You must protect confidential data

- ★**You are responsible for protection of all data you touch**
- ★**Follow IT policy for handling confidential data**
  - Do NOT send confidential data through email
  - Remove (not just hide) confidential data prior to sharing/posting
  - Password protect/encrypt confidential information in all locations
    - (Shared network drives, cloud drives, Teams)
  - Don’t give access to confidential data unless person is authorized
- ★**If you are unsure, ask your manager or IT**

Two Major Cybersecurity Risks for You at Work

1. **Tricked into opening (malicious links, texts, documents, audio files)**
   Ransomware can lock up network files and systems

2. **Tricked into processing a transaction request from an imposter posing as employee or vendor.**
   Loss of funds for Department and payees

How Do I Protect Myself, Data and Systems?

PAUSE before opening

★ **Am I expecting this email, call, text, file, invite?**

★ **Do I recognize the sender?**

- Is the email listed in mass.gov, Outlook or Teams address book?
- Is name, email or phone different than what you have on file?

★ **Is there a sense of urgent demanding an immediate response?**

★ **Is there a threat or warning such as:**

- "account access is locked" "password has expired"
- "account will be closed" "unauthorized login attempt"
- "update your laptop now" "confirmation needed"

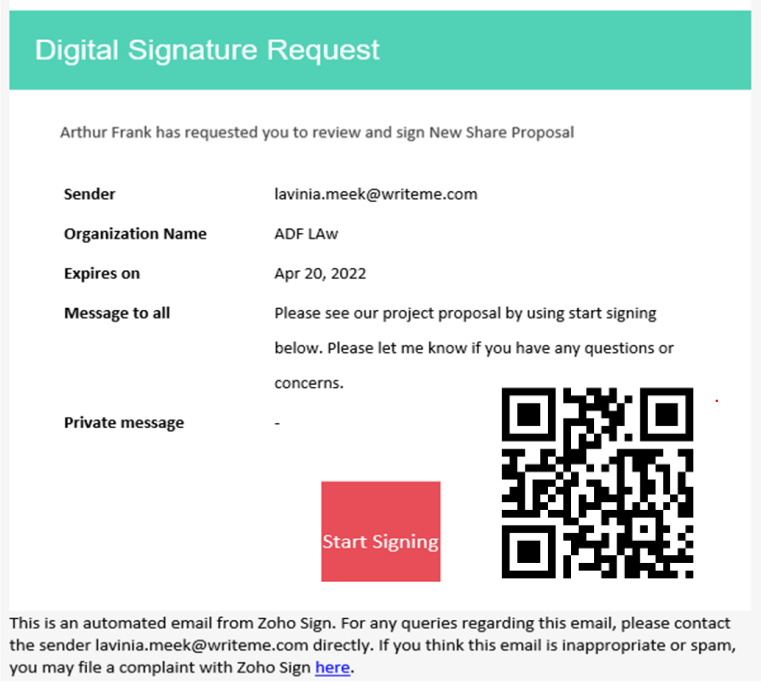
★ **Is the greeting generic?**

★ **Did it come at a strange time?**

Do Not Open

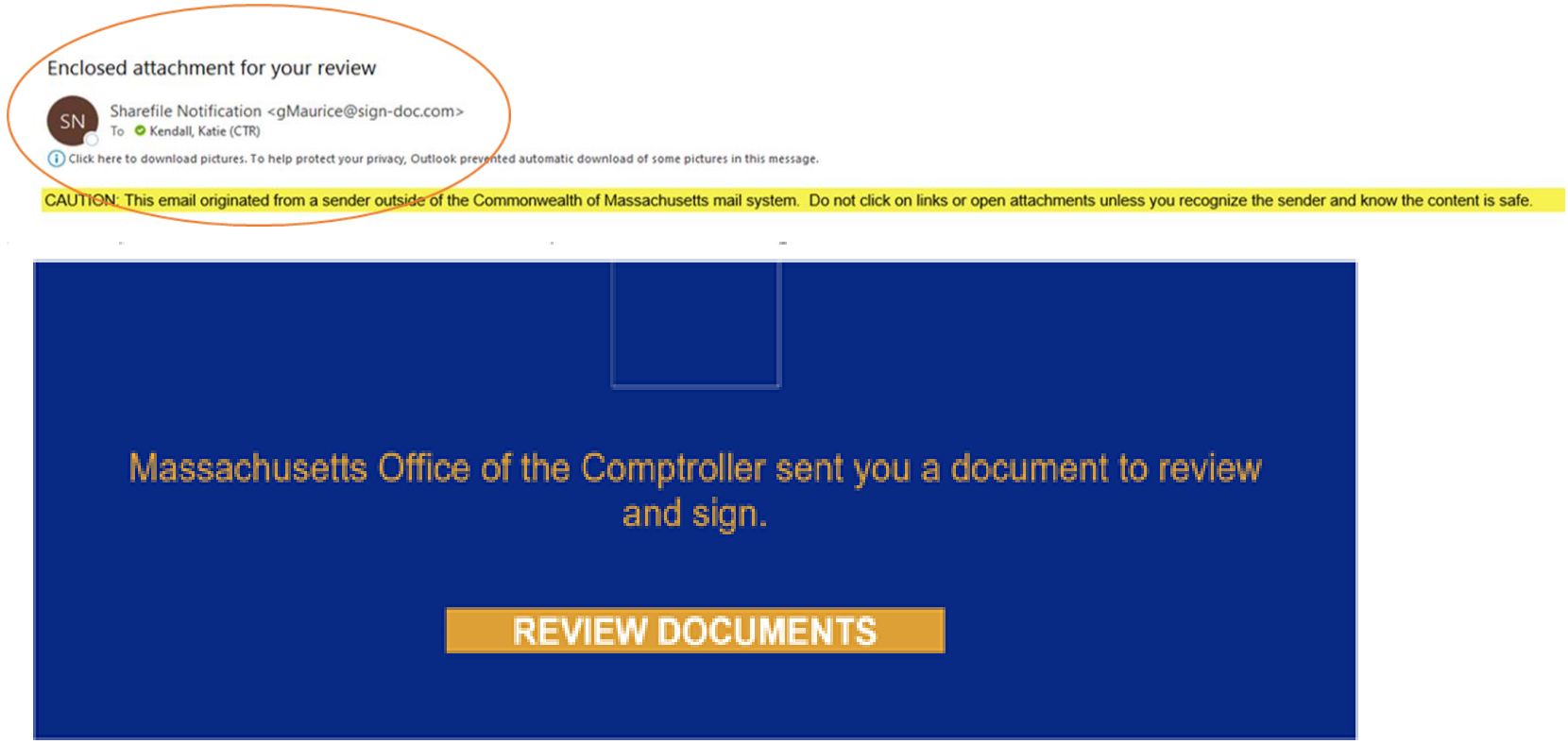
PAUSE

- ★ Criminals use colors and graphics to encourage opening
- ★ Links, Logos, QR Codes, audio files can be infected



Electronic signatures

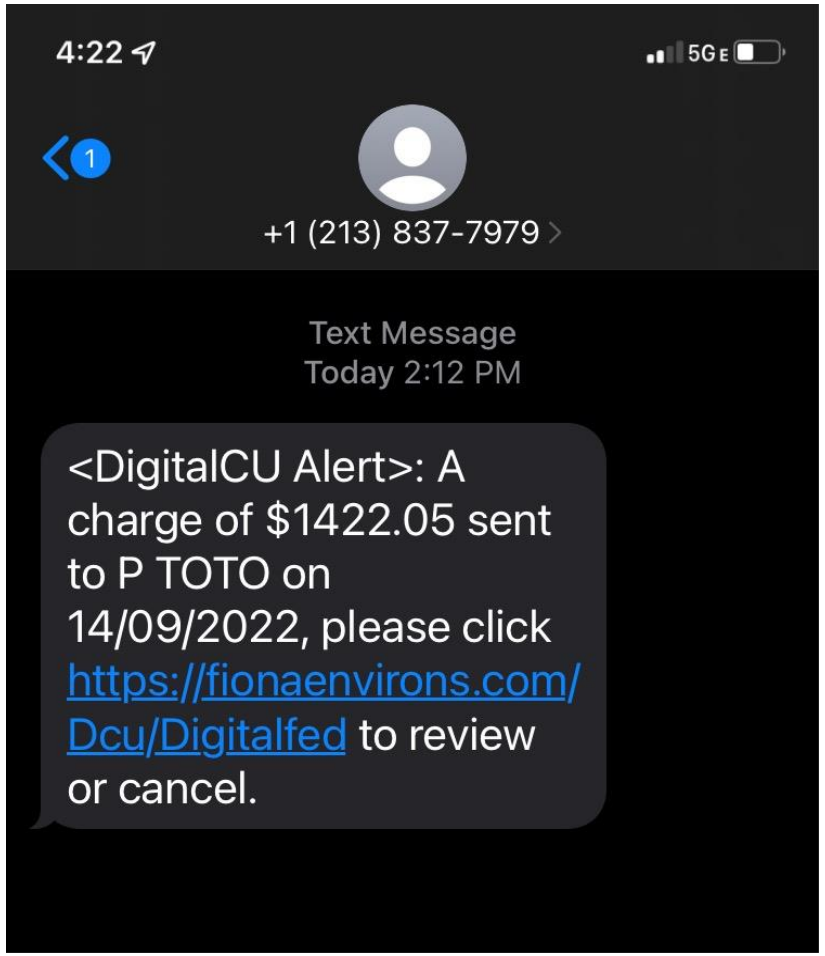
DocuSign, Adobe Acrobat Sign



These may look official but always PAUSE and VERIFY with the sender that these emails are legitimate.

Watch out for phishing texts

PAUSE



- ★ **Never open links in texts**
  - Log in to your official account to verify activity
  - Change your password if you are concerned
    - (16+ non-repeating characters)
    - Multi-Factor Authentication
- ★ **Do not call the number provided**
  - Use official help desk number

Verify, verify, verify

- ★Do not open until you verify – it may be an imposter
- ★Do NOT rely solely on electronic paperwork, calls or texts
- ★Always VERIFY major changes personally with the requester
  - Payroll or Banking account (Direct Deposit employees/vendors)
  - Personal information changes (address, phone, email)
  - Contract document or amendment changes
  - Office 365 shared files or requests to collaborate

Assume every email or text message may be malicious

How do I personally Verify?

- You might be dealing with an imposter.
- Contact the sender using an **alternate** channel. **Do not reply to email or text.** Contact the sender's official email or phone on file.
- Use in person or video (Zoom, FaceTime or Teams). Phone calls can be AI-generated voice clones.
- Ask employee/vendor to show an official ID (on screen or screenshot).
- Set up a validation PIN or keyword for vendor authorized signatories.

Report concerns immediately

- ★If you cannot verify request/requester is legitimate
- ★Trust your gut. If the request seems odd, REPORT it.
- ★Report to your supervisor/assigned contact in IT.
- ★Use the “Phish Alert Report” Button if set up.
- ★Follow your assigned internal protocols.

Speedy reporting can help stop an attack.

Keep Your Workstations Secure

★ Use office-approved equipment and VPN

- Avoid using personal devices for work
- Do not use personal email for work
- Do not send work to personal email

★ Never use public Wi-Fi for work (even with password)

- Use cellular, cellular hotspot and always use VPN

★ Be careful researching internet

- Links, pictures, sites may be infected

Keep Your Workstations Secure

- **Pause –** Do not plug your devices into any public or free USB port, charging cables, or flash drives.
- **Verify –** Ensure that you are using work-provided cables and plugs. Consider bringing your own cables, plugs, or a rechargeable power bank.
- **Report –** Request that any USB flash drive you receive be scanned by IT on a separate secured computer so it does not infect your work network.

Keep Your Workstations Secure

- ★ **Use long and strong passwords**
  - Choose passwords that are 16+ non-repeating characters
  - Don’t use similar passwords as social media accounts
- ★ **Always use Multi-Factor Authentication**
- ★ **Always use VPN (even if you can access work files without it)**
- ★ **Follow department instructions for updates and patches**

Keep Your Virtual Workstations Secure

★ **Change your home Wi-Fi Name and Password**

- Follow provider instructions or customer service can assist
- Use a password that's 16+ non-repeating characters
- This requires updating all smart devices, apps, games – Better to be safe

★ **Never** allow others (kids, family, friends) to use office-assigned devices

Keep Your Virtual Workstations Secure

- **You can set up multiple Wi-Fi router networks with different names and passwords, for example**
  - Work only (use different name such as “Hybrid” or “AA7756Wk”)
  - Family and smart devices
  - Guest network
- **Try not to use smart devices on same network used for work** (ex. Alexa, Google Assist, Nest, Wink, Ring, etc.)

Hackers are looking for weak devices

Pause, Verify, Report at Home

Keep your family data and equipment safe

Remind kids, elders, and friends to pause before clicking

Always make sure the email, text, or call requester is valid, as well as what they're asking for

Send spam to service providers and delete suspicious emails or texts

Cybersecurity is simple when you Pause, Verify, Report

macomptroller.org/ctr-cyber

Cybersecurity tips at work and home

Contact your supervisor or manager for IT support