BE CAUTIOUS WHEN TELEWORKING!

- **When teleworking, be cautious about unintentionally triggering a cyber incident that can crash your equipment, networks, applications or Enterprise Systems. Please take your time and verify before you click!!**
  - Do NOT click on links or attachments unless you know these are safe. Hover over links and virus check attachments first to be safe.
  - Do NOT "enable macros" in documents (often malicious).
- **Practice "Professional Skepticism" and be suspicious of all incoming emails and phone calls**
- **Cybercriminals are becoming increasingly sophisticated at targeting employees with schemes**
  - Do NOT open emails or click on links for "eye-catching" subjects like "you have won a prize", "look at what your co-worker did!", "Coronavirus death in your neighborhood!" Biggest scams going around now involve emails involving "coronavirus" or "COVID-19" so be careful!!
  - Do NOT reply to or click on links in any email from providers asking you to "validate" your account, "there was an unauthorized login attempt" or "your account will be closed". Providers will not ask you to validate through email, but will require you to log in to your account.

PROFESSIONAL SKEPTICISM

- **Do NOT rely solely on electronic paperwork or phone calls when making employee/vendor bank account or address changes.**
- **Always validate major changes separately with on-file contact information and independently contacting the requester to make sure they are legitimate.**
  - Cybercriminals are counting on you to respond quickly without validating or double checking identity.
  - You must delay completing a request until you can separately validate and identify the legitimacy of a request and requester with information you have on file. Most fraud happens when "changes" to addresses and bank accounts are made from email requests or phone calls.
- **Fraudsters OFTEN pose as colleagues, contractors, bank officials or others that you already know, so be especially vigilant when a caller is friendly and acts as if they know you. Unless you are certain of their identity, validate first or check with your supervisor.**

NEVER USE FREE WI-FI, EVER

- Do NOT perform work business, banking or bill paying using your laptop, cell or mobile device on 'free' Wi-Fi (ex. Airport Wi-Fi, coffee house, trains while commuting)
  - Employees performing business functions, especially transactions and banking should be using VPN on a secured network
- Do NOT "plug in" your work devices or BYOD used for work to "free" USB charging portals or using free charging cables, which can be loaded with malware.
- Never provide PII, business credentials, login or account information to gain access to 'free' Wi-Fi or ANY application
- Use unique "strong" passwords and don't use same password on multiple applications
- Make sure operating systems, virus and malware protections are up-to-date according to your Department security requirements

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

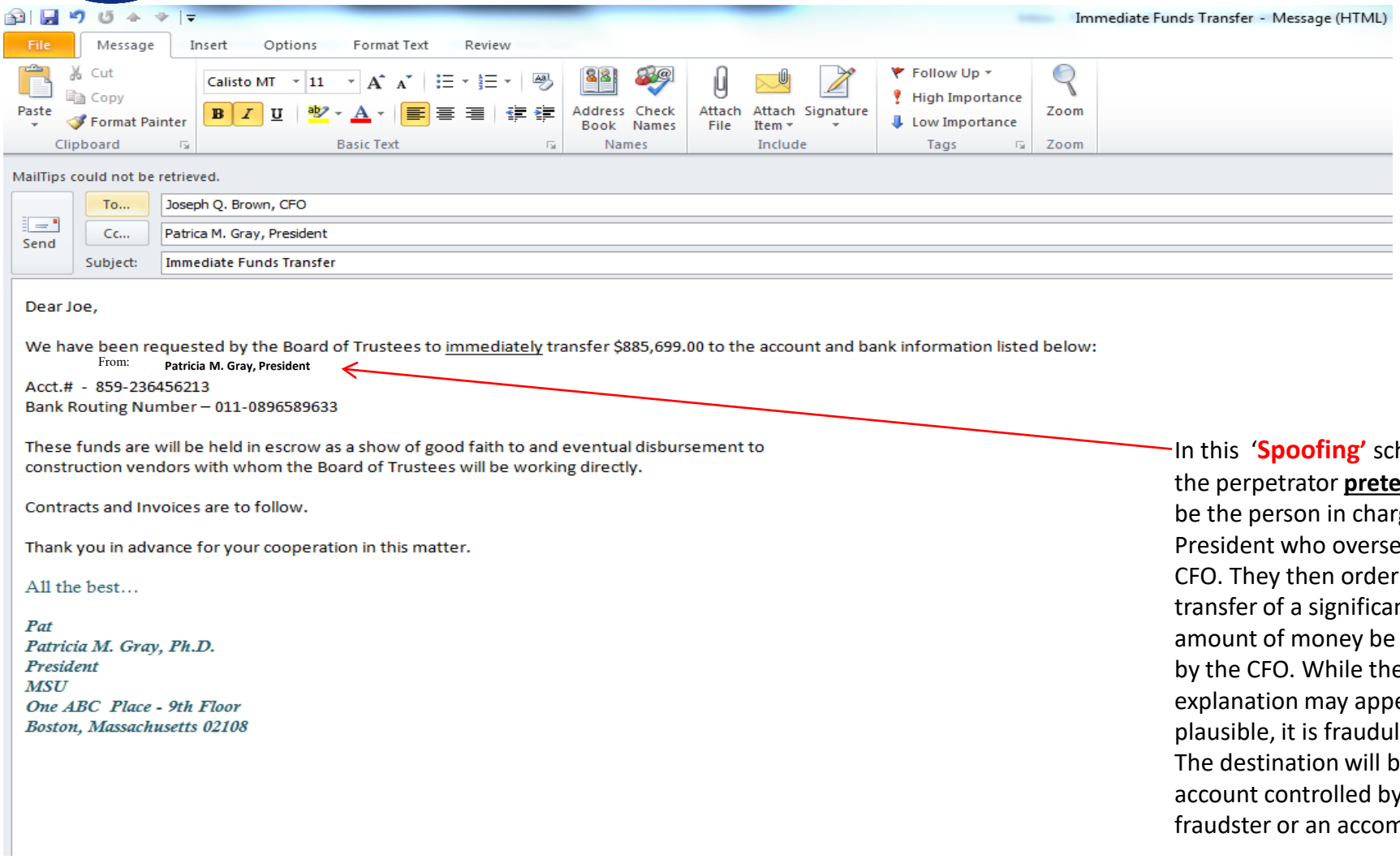
ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

EXAMPLE OF SPOOFING EMAIL



Immediate Funds Transfer - Message (HTML)

File | Message | Insert | Options | Format Text | Review

Paste | Cut | Copy | Format Painter | Clipboard | Calisto MT | 11 | Basic Text | Address Book | Check Names | Names | Attach File | Attach Item | Signature | Include | Follow Up | High Importance | Low Importance | Tags | Zoom | Zoom

MailTips could not be retrieved.

Send

To... Joseph Q. Brown, CFO

Cc... Patrica M. Gray, President

Subject: Immediate Funds Transfer

Dear Joe,

We have been requested by the Board of Trustees to immediately transfer $885,699.00 to the account and bank information listed below:

From: **Patricia M. Gray, President**

Acct.# - 859-236456213
Bank Routing Number – 011-0896589633

These funds are will be held in escrow as a show of good faith to and eventual disbursement to construction vendors with whom the Board of Trustees will be working directly.

Contracts and Invoices are to follow.

Thank you in advance for your cooperation in this matter.

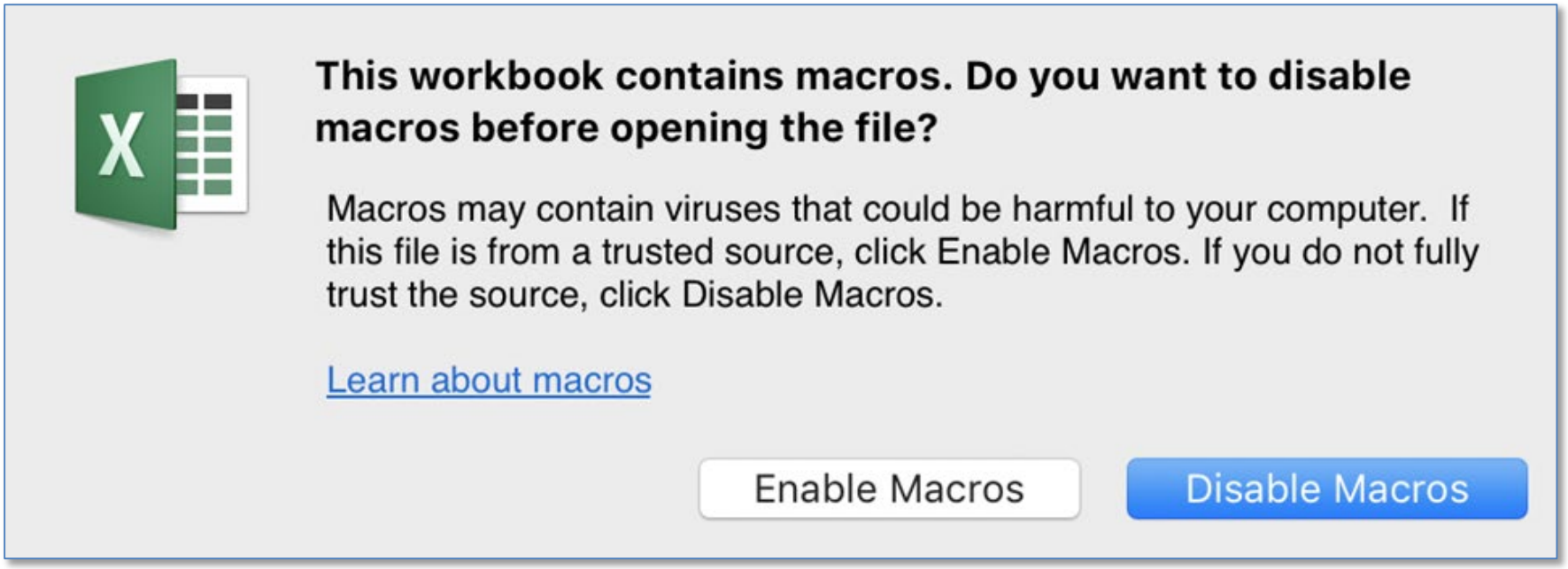
All the best…

Pat
Patricia M. Gray, Ph.D.
President
MSU
One ABC Place - 9th Floor
Boston, Massachusetts 02108

In this **'Spoofing'** scheme the perpetrator **pretends** to be the person in charge, the President who oversees the CFO. They then order a transfer of a significant amount of money be made by the CFO. While the explanation may appear, plausible, it is fraudulent. The destination will be an account controlled by the fraudster or an accomplice.

DO NOT OPEN ATTACHMENTS FROM STRANGERS – DO NOT ENABLE MACROS – PRESUME MALICIOUS

- If you get a pop up like this – assume malicious. Check with IT staff before opening.



- DO NOT CLICK!!!

From: Amazon <management@mazoncanada.ca> on behalf of

not an Amazon email address
(note the missing A in Amazon)

To: @sheridanc.on.ca

Cc:

Subject: Suspension

amazon.com

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

CONTACT YOUR SUPERVISOR OR IT STAFF WITH QUESTIONS OR CONCERNS

- If you suspect an email or call may be suspicious, contact your supervisor
- If you suspect an email or attachment may be malicious, or just "does not look right", or there is any unusual activity with your machine, connection etc. after opening an email or attachment, contact your IT staff immediately.
- Check the Cyber Center Cybersecurity Alerts for additional guidance: https://www.macomptroller.org/cyber-center