Amplifying Our Voice: Leading Boldly for Our Students, Our Professions, and Our Union

Trust is Not an Internal Control

Susan Hardey, NEA Manager of Information Systems
Paul McCorkle, CFO/CIO
COMPETENCY: STRATEGY & FISCAL HEALTH

• NEA Leadership Competency progression level:
  • Level 2: Mobilizing & Power Building

• NEA Leadership Competency theme:
  • Promotes stewardship and financial integrity of the organization
NEA Strategic Goal 6: Enhance Organizational Capacity

• NEA Strategic Goal
  • Building the capacity of the local, state and national union to ensure the success of public education

• NEA Organizational Priorities
  • Supporting Professional Excellence
Trust is not an internal control

• You trust your colleagues, co-workers, employees to do the right thing...
• You trust your boss, employer, supervisor, to provide you appropriate directives...
• You trust when you receive a notification about an outstanding invoice, or a wire transfer, or a payroll change...

• Or should you?
CEO/CFO Fraud

• CEO/CFO Fraud is a scam in which cybercriminals spoof company email accounts, impersonating executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential information.

• This is accomplished through phishing scams, impersonation, social engineering, and other methods – causing the unsuspecting employee to react quickly and against standard internal controls and protocols.

• And it doesn’t just happen to others...
This was sent to a local treasurer...

From: Adean111@comcast.net
Reply-to: john.blades2@aol.com
To: [Redacted]
Subj: Wire Transfer

Shirley,

Are you at your desk? I'll need you to process a Wire Transfer/Check to a vendor. Let me know if you are available so I can send you the instruction.

Regards,
Alfreda
From: Mike <presidentofboard1@aol.com>
Date: December 14, 2017 at 11:33:16 AM EST
To: [Redacted]
Subject: EXPENSE REIMBURSEMENT

Morning [Redacted]

I will need you to take care of a payment to a vendor for me. How much is our current Account Balance? I will provide you with the Vendor's information you need in making the payment. I will appreciate swift response.

Thanks
Mike.
This was sent to a staff union treasurer...

From: Susan [mailto:chief.officer18@aol.com]
Sent: Monday, December 10, 2018 11:08 AM
To: Timothy [redacted]
Subject: Expense Reimbursement

Timothy,

Need you to complete some task for the association immediately. Am currently unavailable?

Susan [redacted]
What were they going for?

• The end goal for each email attempt was
Phishing and other scams

• Phishing – throwing a net
  • Scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly

• Spear-phishing – aiming at someone specific
  • Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information
Phishing and other scams (cont’d)

• Whaling – targeting officers, governance, treasurers, ...
  • Specific type of phishing attack that targets high-profile employees

• Ransomware – Targets the computers, not the individuals
  • Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
It can happen to anyone
Phishing...

From: [redacted] <manager@promedicalplan.com>

Sent: Wednesday, January 30, 2019 10:01 PM

Subject: The approval.

see attached

Expires Feb 25, 2019

Documents.pdf 145.5 MB
I know emilyou1 one of your passwords. Let's get straight to purpose. Neither anyone has compensated me to check about you. You don't know me and you are probably thinking why you are getting this e-mail?

Let me tell you, I placed a software on the adult videos (pornographic material) web site and do you know what, you visited this site to have fun (you know what i mean). When you were watching video clips, your internet browser started out working as a Remote control Desktop that has a key logger which provided me with accessibility to your display as well as web camera. Just after that, my software program obtained your complete contacts from your Messenger, Facebook, as well as emailaccount. Next i made a double-screen video. 1st part displays the video you were viewing (you have a good taste :) ), and 2nd part displays the recording of your cam, yea it is u.

There are just two choices. We should study these options in details:

Very first choice is to just ignore this message. In this scenario, i most certainly will send your tape to every one of your personal contacts and think about the disgrace you can get. and as a consequence should you be in a romantic relationship, exactly how is it going to affect?

Second alternative will be to pay me $900. Lets name it as a donation. Then, i most certainly will right away delete your videotape. You could keep on daily live like this never took place and you will not ever hear back again from me.

You will make the payment through Bitcoin (if you don't know this, search 'how to buy bitcoin' in Google search engine).

BTC address: 18TuYkz6WSkGcyr9j3i1kxFU1a1nQ2uir
[CaSe-SeNSITIve copy & paste it]

if you may be planning on going to the cop, okay, this email message can not be traced back to me. I have dealt with my steps. i am not trying to charge a fee very much, i just want to be paid. I've a unique pixel in this e-mail, and right now i know that you have read through this email message. You now have one day in order to make the payment. if i don't get the BitCoins, i will send out your video to all of your contacts including relatives, colleagues, etc. Nonetheless, if i do get paid, i will erase the recording immediately. If you need proof, reply Yes then i definitely will send your video to your 5 contacts. It is a non-negotiable offer and thus please do not waste my time & yours by responding to this email.
How to protect against these threats

• Passphrases, not passwords

• Avoid using Public WIFI

• Never send sensitive information via email

• Recognize the Red Flags of suspicious emails

• Establish internal controls to validate requests, keep systems updated
Passphrases – No Longer Passwords

• Think of a phrase, no longer just a word

• Don’t be afraid of complexity – it doesn’t have to be difficult

• Use an inspirational life goal as your passphrase!
  • I will lose 25 pounds by Arbor Day!
  • Today I will mostly be positive!
  • I’m not going back 2 prison over this.
Passphrases – No Longer Passwords (cont’d)

• Use a different passphrase for each different system

• Use a password locker if it gets too tough to remember them all

• Whenever possible, use Two-Factor Authentication (2FA/MFA)
Public WIFI

• Use only if you have to!
• Use your phone’s hot spot first!
• Verify the network name, twice
• Turn off any sort of sharing, turn firewalls on
• Never install software while on Public WIFI
• When you’re done, FORGET the network
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 microsoft-support.com)?
- I don’t know the sender personally and they weren't vouch 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.

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.?

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.

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?

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’s a misspelling of a known web site. For instance, www.bankofamerica.com — the “m” is really two characters — “r” and “n.”
Establish Internal Controls

• For financial requests – establish procedures, and stick with them
  • Identify and only use authorized accounts for email communications
  • Ensure ways of validating “unusual” or emergency requests
Trust is not an internal control (cont’d)

Paul McCorkle
CFO/CIO
South Dakota Education Association
Security

• Security – Not just computer systems
• Board Policy
  • Directs the organization, but not the detail
• Protocol
  • Actions/steps taken
• Procedure
  • The actual step by step process
Policies

• Statement adopted by board enabling an action to occur
• Not just tech related
  • Financial matters
  • Membership - e.g. cost of dues allowing members to drop membership
  • Tech use
Protocols

• Protocols – triggers a process or procedure to be followed

• Cancelling membership
  • Under what circumstances – e.g. financial hardship, moving
  • Who approves – e.g. president, leadership

• Examples of protocols
  • Media
  • Grants
  • Cancelling membership
  • Breach of data systems
Procedures

• Procedures – Actual process
• Importance of a process manual
  • Why
• How to enter a membership
• How to cancel a membership
Procedures (cont’d)

• How to pull a report
• How to reset the internet
• How to change passwords
• What necessary procedure, step-by-step process used when there is a breach
Session Outcomes

The content from this session can be used in the following ways in your current position/role:

• Establish internal controls that include security procedures and protection
• Know how to avoid the pitfalls of popular cyber attacks – Phishing and CEO Fraud are on the rise!
• Understand your responsibility in protecting the Association and its members
Questions?

• Any questions?

• Please complete the evaluation for this breakout session by using the NEA Summit Mobile App!

• Please visit the Leadership Development Resources website at www.nea.org/leadershipdevelopment