MEL CYBER TASK FORCE UPDATE

Social Engineering Preparedness

The town of Erie, CO received a request from their contractor to transfer funds to a certain account to pay for a local bridge project. Total payments were in excess of $1,000,000. All was legitimate except for the transfer account. A cybercriminal, posing as the town's contractor, sent the request to change transfer accounts, and left with all of the money. It was found the request to change accounts was never verified with the vendor. The FBI is currently investigating the matter.

What

This duping or impersonation is commonly known as **Social Engineering** or **Business/Vendor Email Compromise**. Erie's incident is one of thousands of similar incidents reported each year. In 2018 and 2019, we saw numerous reports of increases in this activity amongst cybercriminals, and many occurring in New Jersey.

How

We most typically see the following types of Social Engineering incidents:

- Request seeming to be from an employee to change their direct deposit information
- Request seeming to be from a vendor to change their payment information
- Request seeming to be from an employee for a project
- Request seeming to be from an employee for their W2

Similar to targeted phishing attacks, cybercriminals will spoof email addresses of your contacts, use domains that mimic a trusted domain or actually compromise a legitimate account. The criminals will also shape email to seem legitimate.

Prevention

The NJCCIC provides the following recommendations to prevent Social Engineering.

- ✓ **Email Filters**: Identify and block emails using known phishing tactics and those from suspicious IPs
- ✓ **Email Gateway Rules**: Flag communications in which the "reply" email is different from the "from" email
- ✓ **Email Identification Warning**: Mark emails coming from outside your organization with a visible warning label to users stating "External Email" or similar
- ✓ **Reporting**: Identify a procedure for identifying and reporting social engineering emails
- ✓ **Multiple Approvals**: Establish (and train) procedures requiring requests for highly sensitive information or large financial transactions to be authorized by multiple individuals via non-email communication
- ✓ **Domain-Based Message**: Implement domain-based message authentication, reporting and conformance (DMARC) to reduce the risk of spoofing
- ✓ Review the MEL's Email Dos and Don'ts Infographic, and distribute to all employees (link below and attached)
- ✓ Verify source and instructions of any monetary transaction or other unusual requests via phone call or in-person
- ✓ If you are compromised, report to your supervisor and bank, immediately

Check-out the MEL's Email Dos and Don'ts Infographic here:
https://njmel.org/wp-content/uploads/2017/12/MEL-Email-Infographic-FINAL.jpg

Check-out the full article from NJCCIC here:
https://www.cyber.nj.gov/be-sure-to-secure/dont-be-fooled-bec?rq=direct%20deposit

For details, contact the MEL Underwriting Manager or your local JIF Executive Director

EMAIL DOs & DON'Ts

EMAIL ADDRESSES

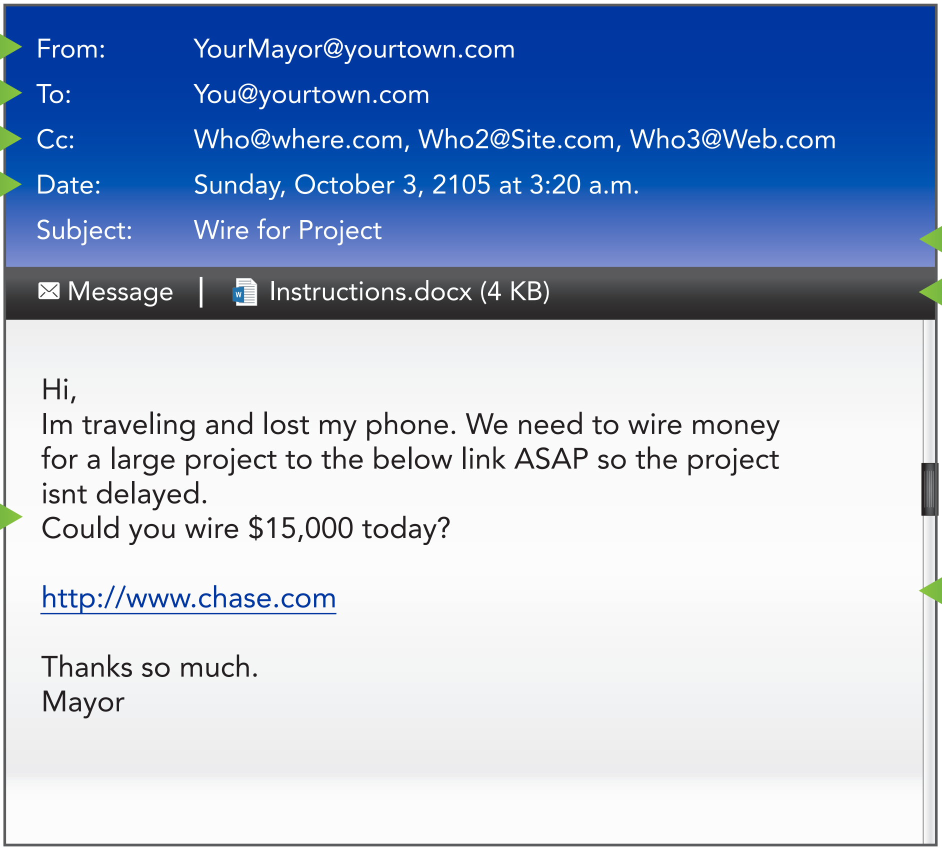
- Do you recognize the sender and the CCs?
- Is the sender's email spelled correctly? (i.e. "YourMayor" vs. "YourMay0r")

DATE & TIME

- Was the email sent on a typical day and at a typical time?

EMAIL CONTENT

- Are the format and grammar in the email typical for the sender?
- Does the content seem atypical?
- Did the sender seem overly urgent?
- Does the email ask for person info/login info?



From: YourMayor@yourtown.com
To: You@yourtown.com
Cc: Who@where.com, Who2@Site.com, Who3@Web.com
Date: Sunday, October 3, 2105 at 3:20 a.m.
Subject: Wire for Project

✉ Message | Instructions.docx (4 KB)

Hi,
Im traveling and lost my phone. We need to wire money for a large project to the below link ASAP so the project isnt delayed.
Could you wire $15,000 today?

http://www.chase.com

Thanks so much.
Mayor

SUBJECT

- Is the subject a typical style for the sender?
- Does the subject match the email content?

ATTACHMENT

- Is an attachment needed for the email content?
- Were you expecting the attachment?
- Is it a ".txt" file?

LINKS

- Does the link look appropriate?
- Does the web address match the hyperlink shown (scroll over the hyperlink)?

DON'T GET PHISHED!

. . . but if you do, remember to

1 Report to Claim Administrator

2 Call XL Catlin 24/7 Breach Hotline at **(855) 566-4724** and they will triage your incident.

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND • MEL •