MEL CYBER TASK FORCE UPDATE

Case Study #1: Sharing is (NOT) Caring

Background

The municipality has a common shared drive-type of network setup, where documents can be shared by various employees and saved in a centralized manner. Remember this setup as it is important for the success of the attack.

Attack

Attackers utilized a typical phishing vector including a fake link, which when clicked would deploy malware. An employee was duped and clicked on this fake link, downloading two strains of malware to the system. While downloaded software (including malware) would normally just affect the device it is downloaded to, one of the strains of malware was designed to find shared drives and spread across the network.

Circling back to the network design mentioned earlier, the shared drive was open to all employees with no segregation or encryption/password protection. This means, Department of Public Works could access financial records and Police could access Human Resource records. As a result, the malware was able to access all of these confidential and sensitive records. The event cost over $100,000 in legal and forensics costs.

Prevention *Included in MEL Cyber Risk Management Program: MEL Cyber RMP*

1. **Unsolicited Emails**: Avoid clicking on links and opening attachments from unsolicited emails. Learn to identify phishing emails, and similar duping types of attacks on the web.
2. **Shared Drive**: While having a shared drive is not an issue itself, not having segregation, password protection, user privileges and/or encryption is an issue.
3. **Protect Information**: Should the above two techniques not have been deployed, the municipality would have still been protected should they have deployed document protection for the sensitive documents, such as (complex) password protection or encryption.

Closing Thoughts

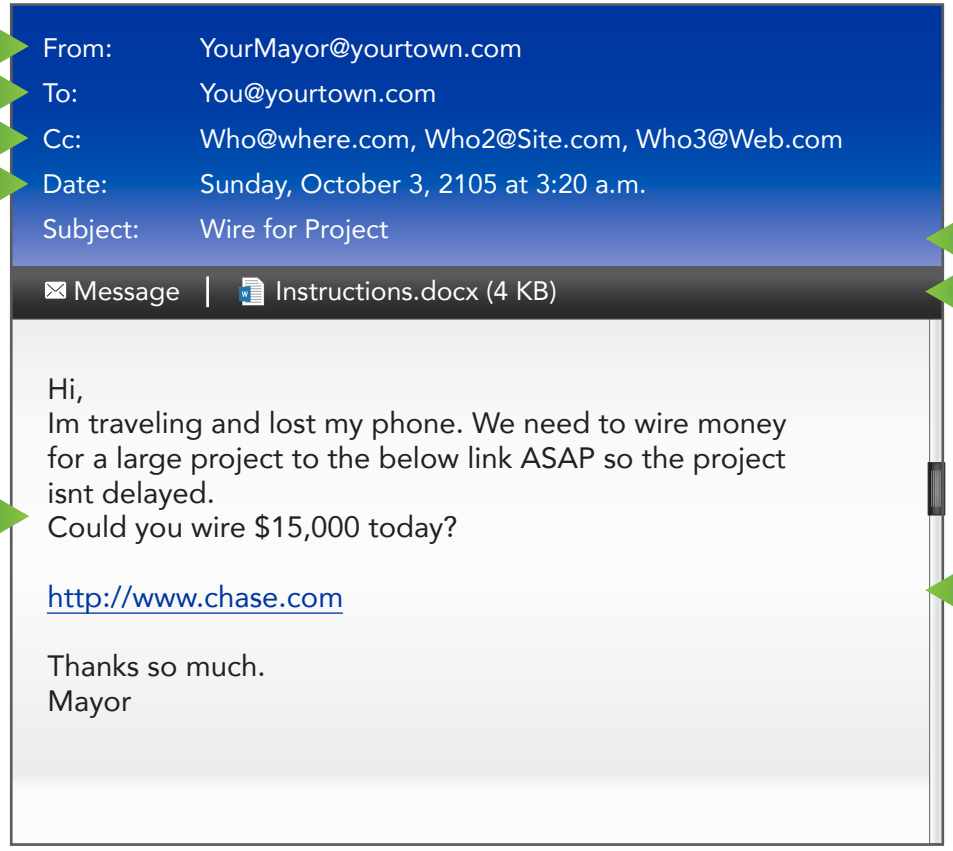
While this event was resolved before the attackers could successfully exfiltrate the sensitive information, imagine if just a little more time went by. Maybe the attacker decides to expose the municipality's errors and publish the confidential data of all of its citizens? Or what if the attacker took the banking information of the municipality and siphoned funds from their account? The possibilities are abundant. ***Bonus Points: Remember the "human error" in this attack.***

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?



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 ·