CRA
COLORADO
ROOFING ASSOCIATION

Virtual Member Lunch

Oct 5, 2022

Thank you for joining us!

CYBERSECURITY

Considerations for the construction industry.

A conversation with Thomas Ritter of Maynard Cooper Gale

To earn your CIU's you must s sign in and/or stay on the webinar the full time. Thank you!

Thank you to our Sponsors:

Industry Leader

Silver Sponsors

Webinar Courtesies:

- Thank you to our virtual attendees for being on-time.
- Participant videos are turned off in this hybrid Zoom webinar format.
- All attendees are muted.
- Please participate through poll questions & be sure to use the Q&A and Chat functions for your questions.
- Final note, in order to earn CIU credit, you will be required to answer a final poll question at the end of today's presentation.

Agenda

- Noon | Start Program and Webinar Housekeeping Items

  Debbie Hathorne, CRA Executive Director

- 12:02 | CRA Announcements & Speaker Intro

  Debbie Hathorne, CRA Executive Director

  12:05| Cybersecurity Presentation

  Thomas Ritter*, Maynard, Cooper, Gale*

- 12:55 | Q & A

MAYNARD COOPER GALE

CYBERSECURITY & PRIVACY PRACTICE GROUP

Cybersecurity Considerations for the Construction Industry

OCTOBER 5, 2022

CRA
COLORADO ROOFING ASSOCIATION

First Poll Question

- In the past 24 months, my company or a company I know has suffered a security incident?

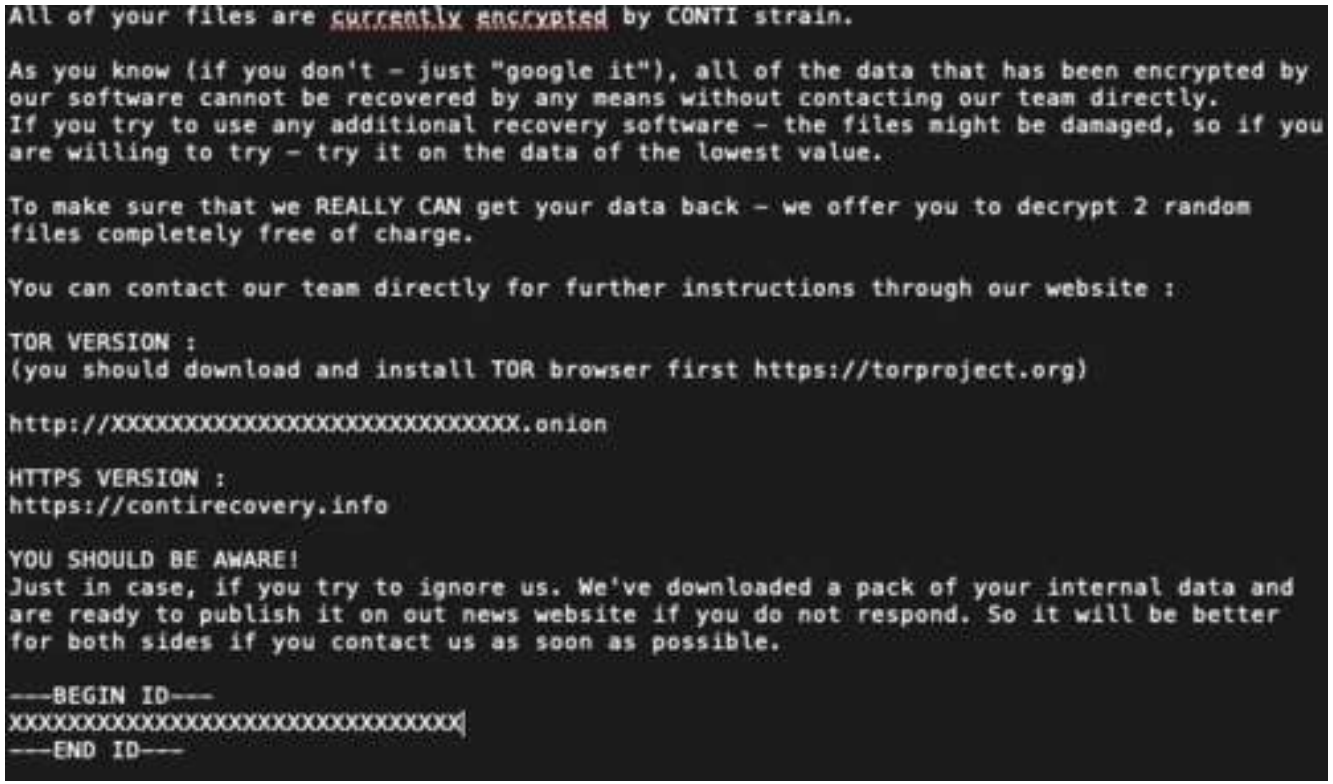
A. YES

B. NO

Common Attacks

Ransomware

Business Email Compromise



```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by
our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you
are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random
files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.onion

HTTPS VERSION :
https://contirecovery.info

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and
are ready to publish it on out news website if you do not respond. So it will be better
for both sides if you contact us as soon as possible.

---BEGIN ID---
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
---END ID---
```

Ransomware

- A threat actor's deployment of malware inside an organization's network that results in the encryption of systems, file and data
- In 2022, construction was the number 2 industry hit by ransomware.[1]
- "But I'm not big enough to be a target."

- [1]Nordlocker, https://nordlocker.com/ransomware-attack-statistics/

Ransomware Continued

- In 2022, there have been 410 reported cases of ransomware by construction companies.

- Evolution of ransomware into lock and leak

- Impact from supplier/manufacturing side
  - Knauf ransomware attack in July.

Ransomware Continued

- Options:
  - Negotiate/pay
  - Restore from backups/rebuild

- Back up and running, but wait
  - Was sensitive data accessed or acquired?
  - Legal notice (customers, employees)

Business Email Compromise

- A real life example . . .

BEC

- "Man-in-the-Middle" attack
  - Compromise business email account to conduct fraudulent wire transfer (usually by way of intercepting legitimate wiring instructions and altering them)
  - $43 billion problem, according to the FBI

- Social engineering to exploit the human psyche
  - Even when account is not legitimately compromised, threat actors can create legitimate looking email address to impersonate company executives or other trusted individuals
    - Similar domains (e.g., "I" instead of "l")
    - Spoofed email tricks user into providing account credentials or other information

-

Question Every BEC Client Wants to Know

- Any guesses?

Are the lost funds recoverable?

Another Poll Question

- If a wire is not recalled within ___ day(s), the likelihood of recovery is extremely unlikely.

A. 1 day
B. 3 days
C. 7 days

Lost Funds

- "Within 72 hours, if the wire hasn't been recalled, you have less than a 9% chance of recovering funds."

- U.S. Secret Service Electronic Crimes Task Force Bulletin – Business Email Compromise - (June 2018)

Lost Funds

- Priority is ensuring wire retraction/recall request has been made to the financial institution.
  - Sending financial institution's "Fraud Investigation and Security" Department

- Financial Fraud Kill Chain (FFKC)
  - Financial Crimes Enforcement Network (FinCEN)
    - Eggmont Group (166 financial intelligence units worldwide)
    - USSS
    - FBI
    - Local law enforcement
- 3 conditions must be present for FFKC

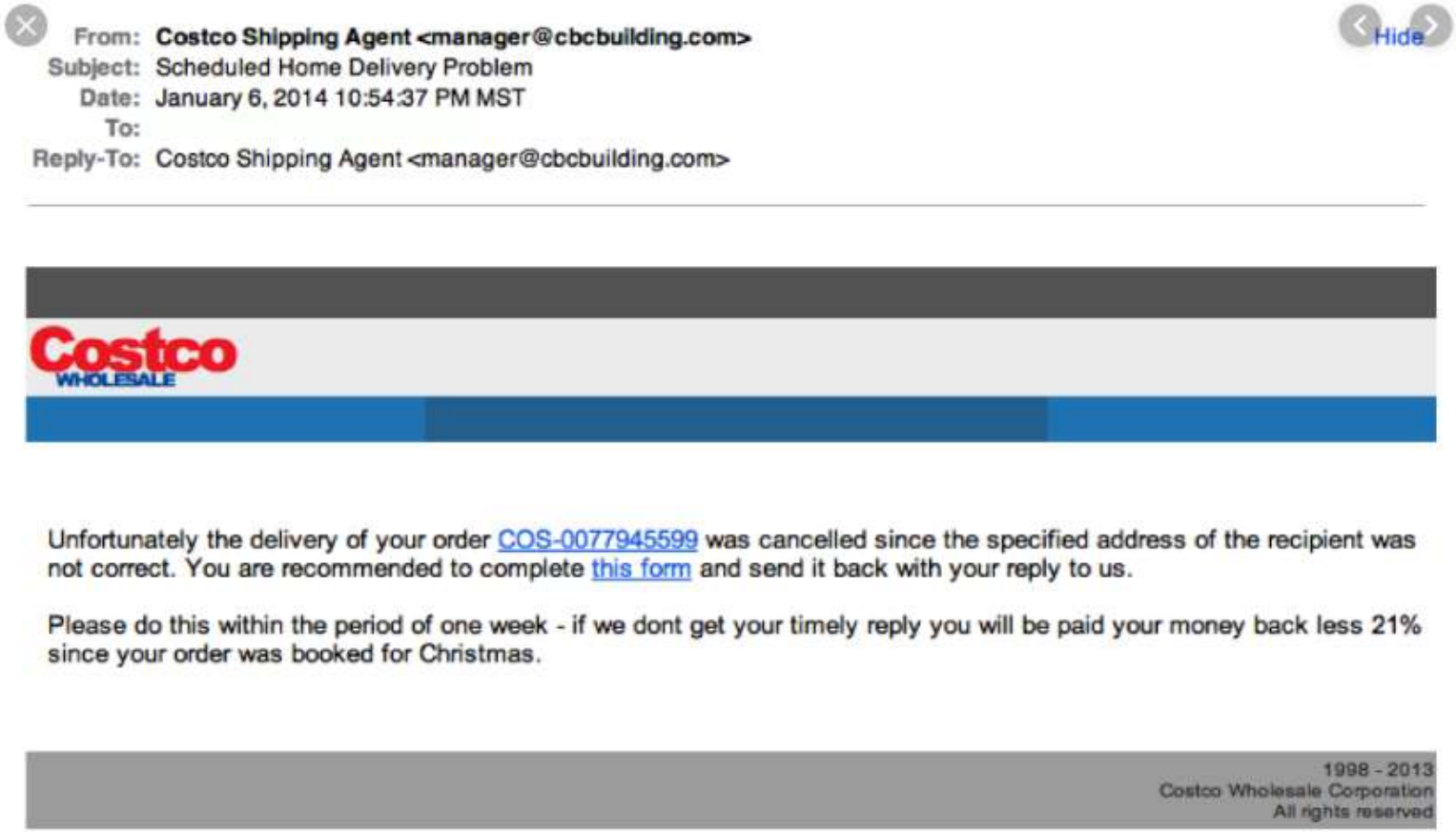
Where to Start

- Security through lens of two extreme perspectives
- A house starts with a solid foundation
- Hundreds of clients, almost all of which were lacking in many of the same security controls

Email - Beware

DON'T click on links or attachments in suspicious emails.

What makes an email suspicious?



From: **Costco Shipping Agent <manager@cbcbuilding.com>**
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Hide

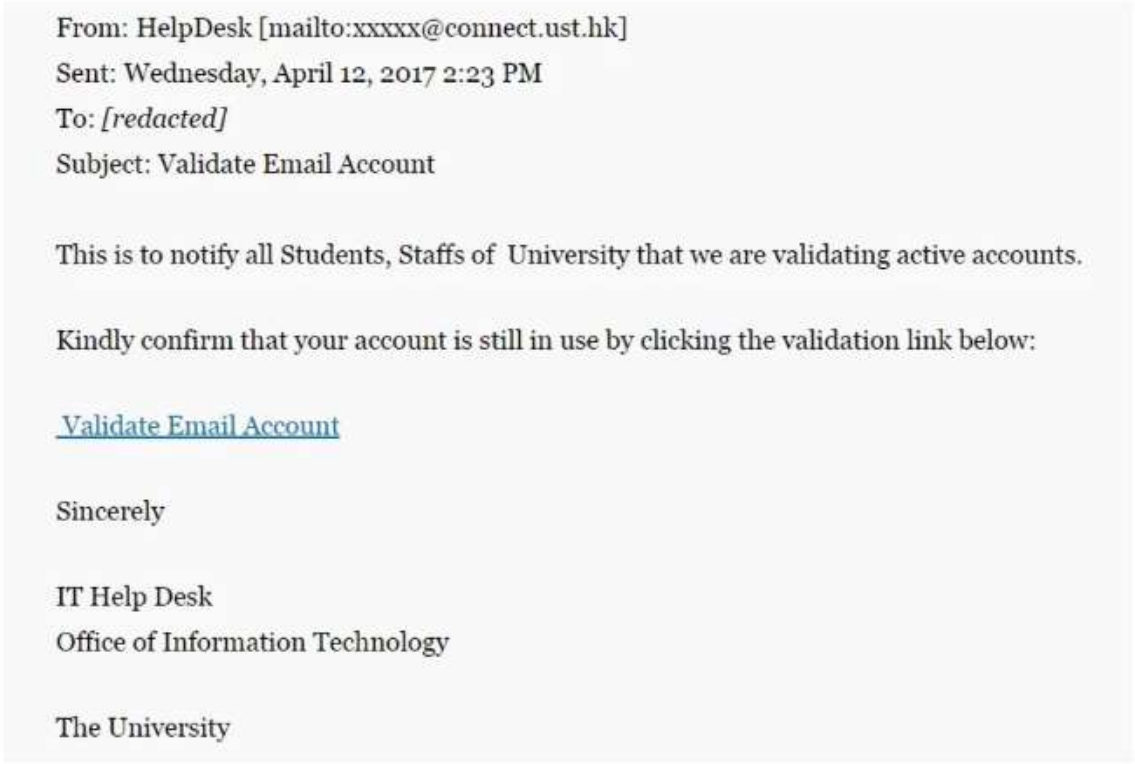
Costco WHOLESALE

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

Email Beware

- NEVER enter your email account credentials in response to an email.



From: HelpDesk [mailto:xxxxx@connect.ust.hk]
Sent: Wednesday, April 12, 2017 2:23 PM
To: *[redacted]*
Subject: Validate Email Account

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely

IT Help Desk
Office of Information Technology

The University

Requests for Information

- Ask the sender in person.
- Call the sender or other contact using a previously established, trusted phone number.
- Use dual controls for funds transfers.
- Beware of any change in wiring instructions, bank name, or payment method.
- Employees in HR, Payroll, Procurement, and Finance should receive special training.

VALIDATE all requests to send sensitive information or to transfer funds.

Multi-factor Authentication

- Multi-Factor Authentication (MFA) is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting two (2) or more pieces of evidence (or factors) to an authentication mechanism:
  - Knowledge (something they and only they know)
  - Possession (something they and only they have)
  - Inherence (something they and only they are)
- Types
  - Code
  - Push notification

Multi-factor Authentication Continued

- Why doesn't everyone have it?
  - Sometimes (still) perceived by clients as:
    - Inconvenient
    - Time consuming
    - Unaware
- Legacy protocols as method of circumvention
- COVID and work from home + general human error
  - Confusion/frustration
  - Accidentally authorize push notification

Username and Password Managers

- Use complex passwords.
- Don't use common names.
- Change passwords regularly.
- Don't use your social media passwords for work.
- Don't make your passwords easily accessible.

- Services available
  - Dashlane, LastPass, LogMeOnce

Preservation Efforts

- Call forensics

- Licensing and log retention
  - E5 licensing
    - Must be enabled pre-unauthorized access event
  - 90 days or longer
  - Unified audit logs enabled
- Litigation hold
  - Preservation of mailbox content

Secure your Files

Lock your file drawers.

Lock your car.

Clean your desk.

Safeguard badges and keys.

Encrypt, when possible.

- *If you SEE something, SAY something.*

- *TRAIN, TRAIN, TRAIN*

Last Poll Question

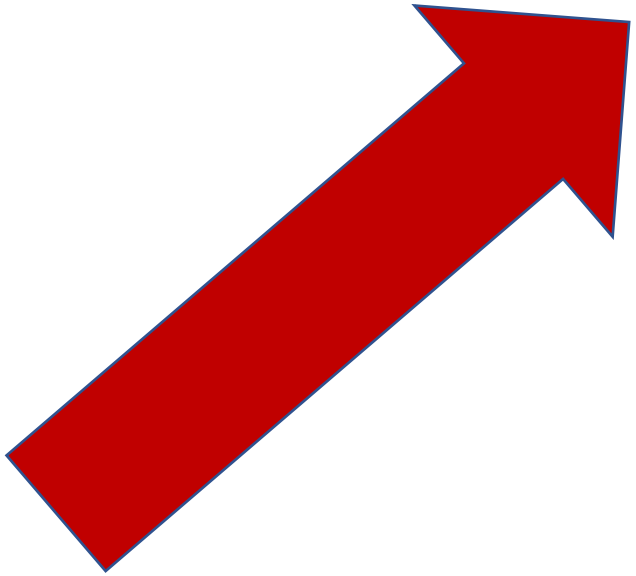
- My business has some sort of cyber insurance coverage

A. TRUE
B. FALSE
C. I don't know.

Cyber Insurance

- Evolution of cyber insurance

- Recent rise in premiums



Obtaining Cyber Insurance

- Be prepared for security questions
  - MFA?
  - Security Incidents in past
  - How much PII do you have

Questions

Thomas Ritter

Direct: (615) 795-2035

Email: tritter@maynardcooper.com

MAYNARD

COOPER GALE

CYBERSECURITY & PRIVACY PRACTICE GROUP

maynardcooper.com

Final comments:

- Thank you Thomas!
- A survey will be sent after the seminar, please take the time to respond. Your feedback helps us plan future webinars and seminars.
- Thank you for staying on the webinar the full time.
- Please answer this final poll question to earn your CIUs. Then, you are free to hop off and end your session.
- A copy of the presentation will be available at:
  https://www.coloradoroofing.org/member/education

Thank You for attending!