AR-IN-A-BOX

CYBER AWARENESS GAME

EnergyCorp hacked

BE THE STRONGEST LINK
BREAK THE KILLCHAIN

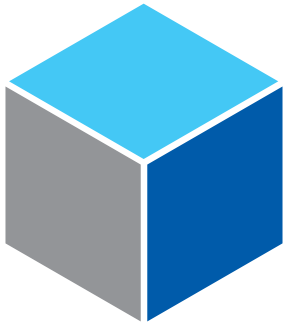
DISCLAIMER

Game Rules

- Create teams or Play Individually
  - Choose a Team Leader
  - Choose a Team Name
- Answer the Questions
- Discuss your Solution

THE GAME STARTS HERE

PHASE 1



SCENARIO – ENERGYCORP HACKED

EnergyCorp, the Energy Service Provider Giant has been hacked based on information leaked on the public internet. The hack appeared to take place early September but it went unnoticed till the 10th of September 2022, when attackers published stolen data online.

Attackers appeared to have gained initial access via a successful **PHISHING ATTACK**.

To make matters worse **UNAUTHORISED ACCESS** has been detected in EnergyCorp headquarters and a **RANSOMWARE** hit the company the same day. Days after the initial event **FAKENEWS** appeared online causing major damage to ENERGYCORP's reputation.

You are the lead Cyber Security Investigator recruited to provide answers on who is behind the hack and try to stop him/her before its too late.

We gathered as much evidence as possible. Analyze them quickly.

The attackers claim that they will wipe all data if we don't pay.

GOOD LUCK!

FULL EMPLOYEES LIST

Badge ID	Name	Department
AA11AA1	Whale John	Chief Executive Officer
FA23RN1	Mill Anna	Chief Financial Officer
IT23RL2	Clueless Joe	ICT
AL3XZA4	Clickall Jack	Legal
IT21NO6	Darc Marc	ICT
IT11NI9	Marly Maria	ICT
AN21AB1	Elton Jack	HR
FQ23MN1	Morgan Monica	HR
II12RO2	Lee Kim	COMS
AL3SZW9	Cross Michael	COMS
IT22NO7	Dollar Sam	Sales
IT22MIA	Prince Stan	Sales
AI2XZQ9	Maze Luke	Secretary
IT22MI9	Jasper Joanne	Software Developer
DS21NM9	Frank Alex	Security Officer

UNAUTHORISED ACCESS

THE NEWS

The Daily W

Tuesday, September 13, 2022

ENERGYCORP HACKED!

Energy giant Energy Corp said it has been a victim of a cyberattack linked to targeted Phishing campaign. The breach has exposed personal data, and data of its subsidiaries. It has notified some of its stakeholders.

"The on going investigation has shown that an unauthorized party gained access to various files during a limited window of time," Energy Corp said in a statement.

TASK UPDATE #1

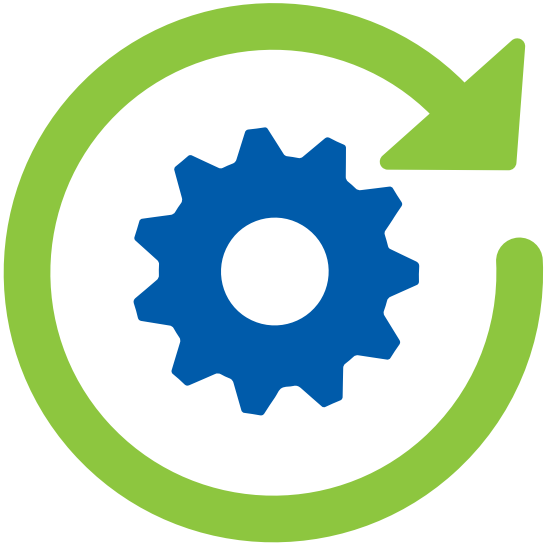
A number of suspicious emails have been recovered while investigating the hack.

Your task is to go through the communications of various individuals and identify the perpetrator and possible victims.

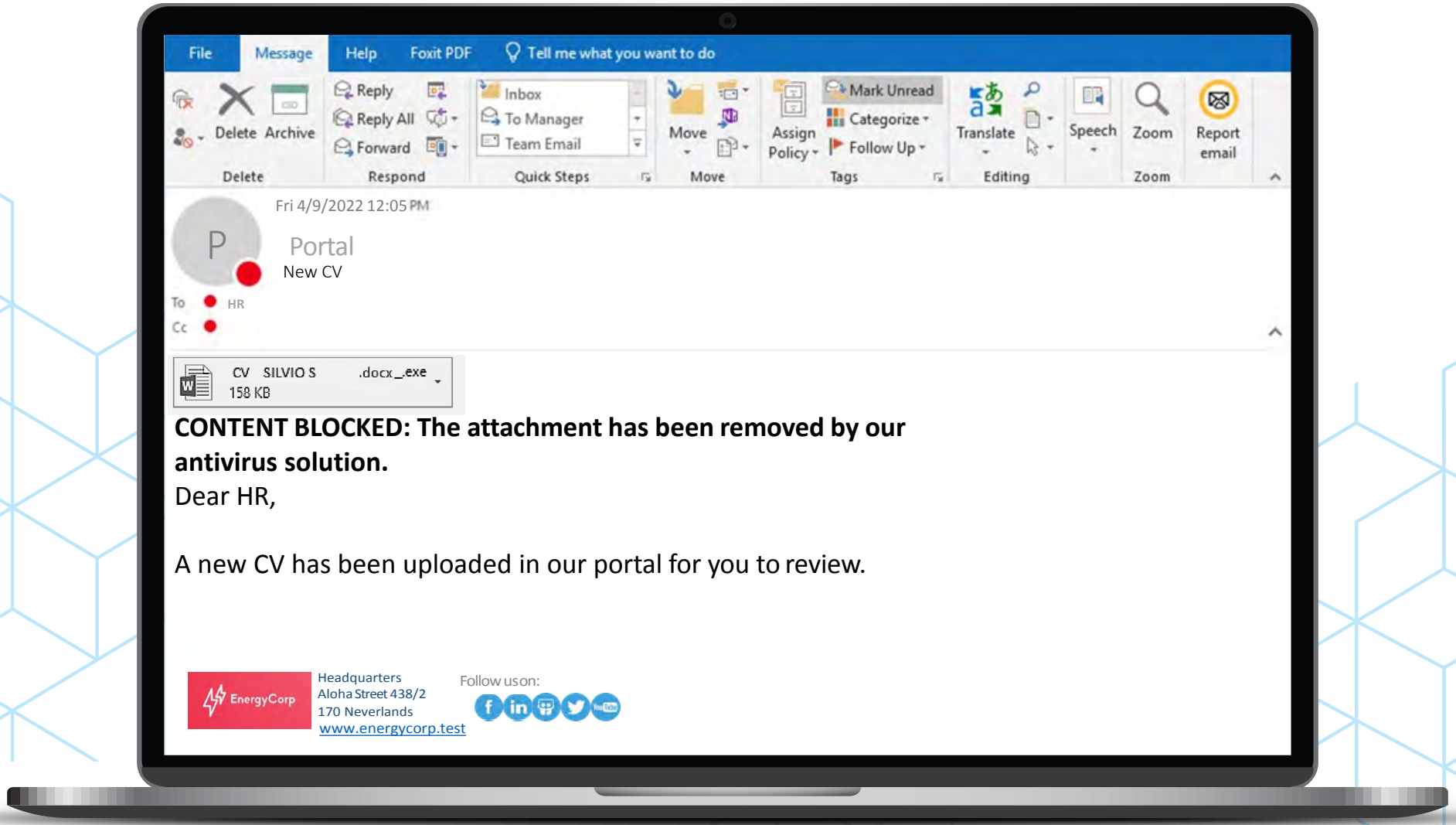
It is believed, based on our analysis, that the attacks started from a single email. That's how the hackers got access to the ENERGYCORP file servers.

We count on you to perform the analysis as fast as possible.

Good Luck,
The Management

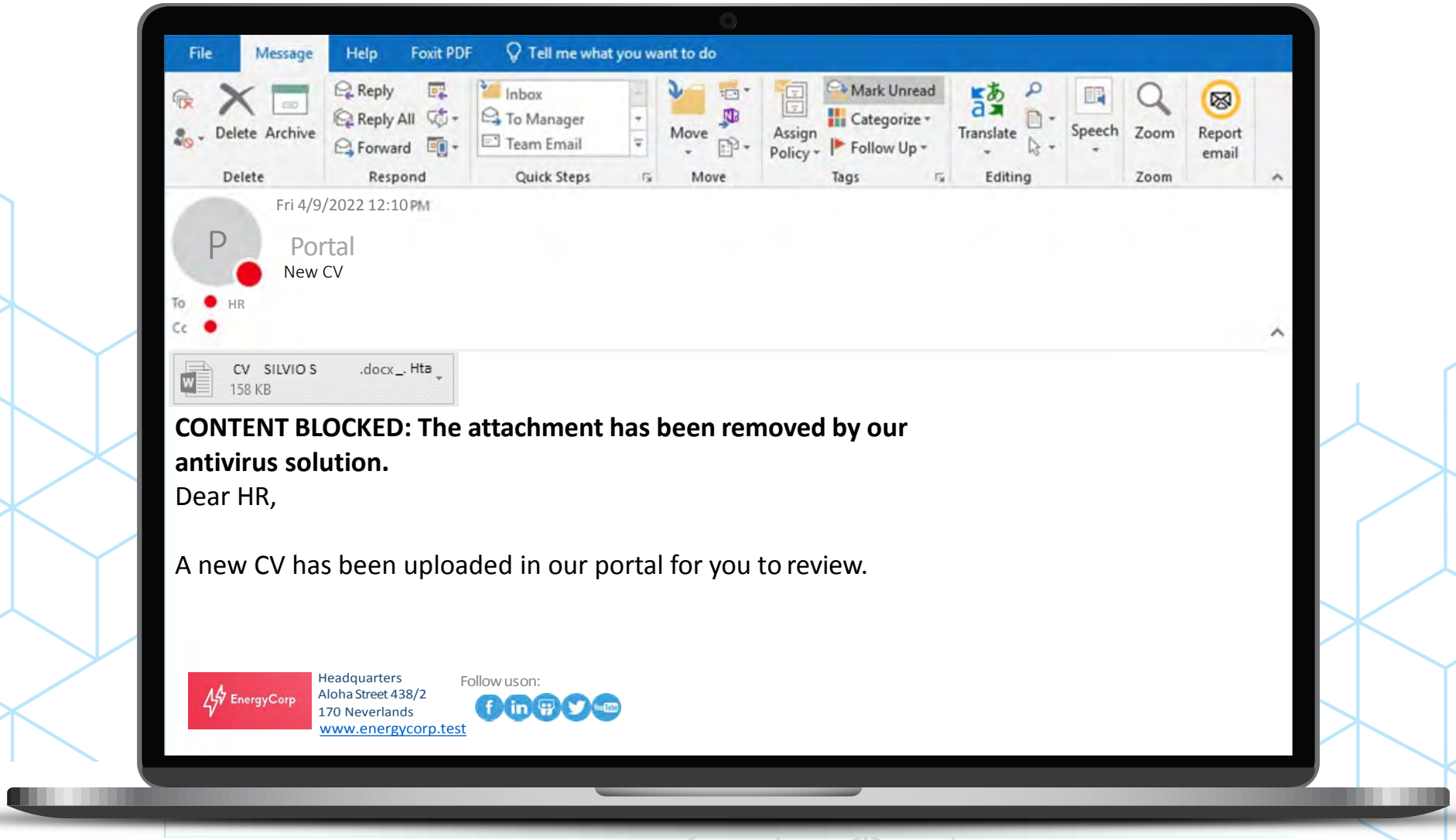


SUSPICIOUS MAIL



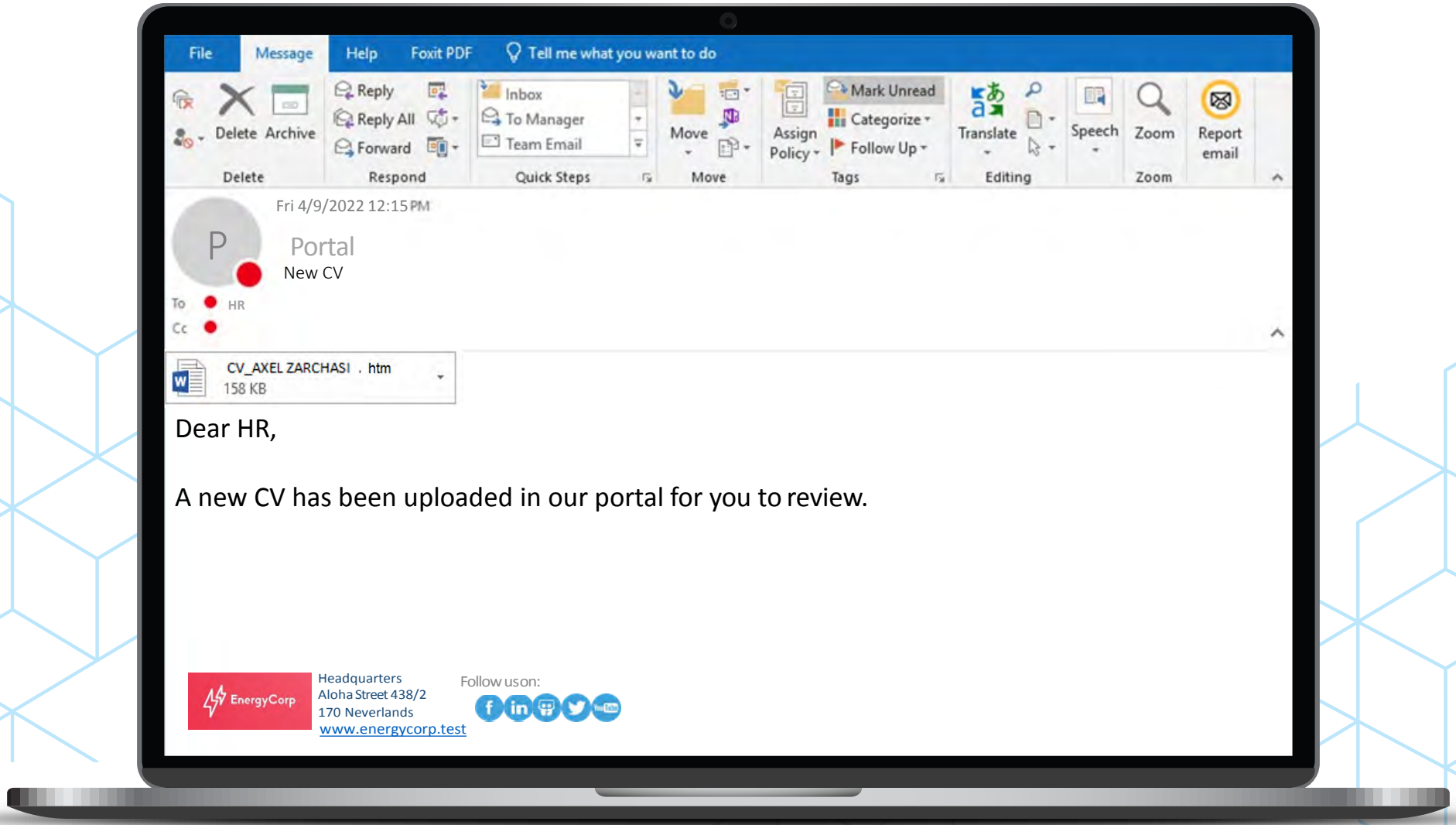
PHISHING ATTACK

SUSPICIOUS MAIL



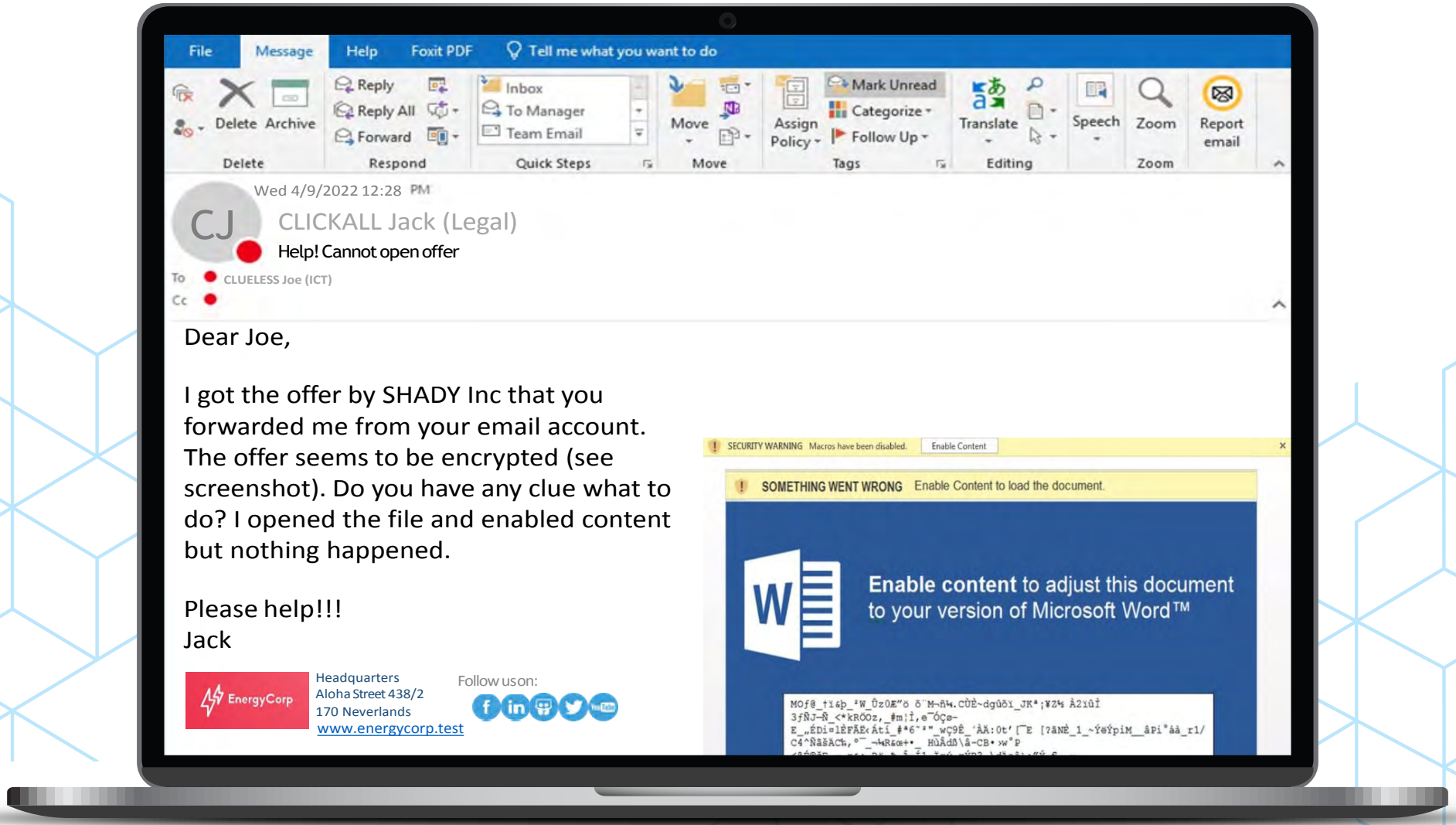
PHISHING ATTACK

SUSPICIOUS MAIL



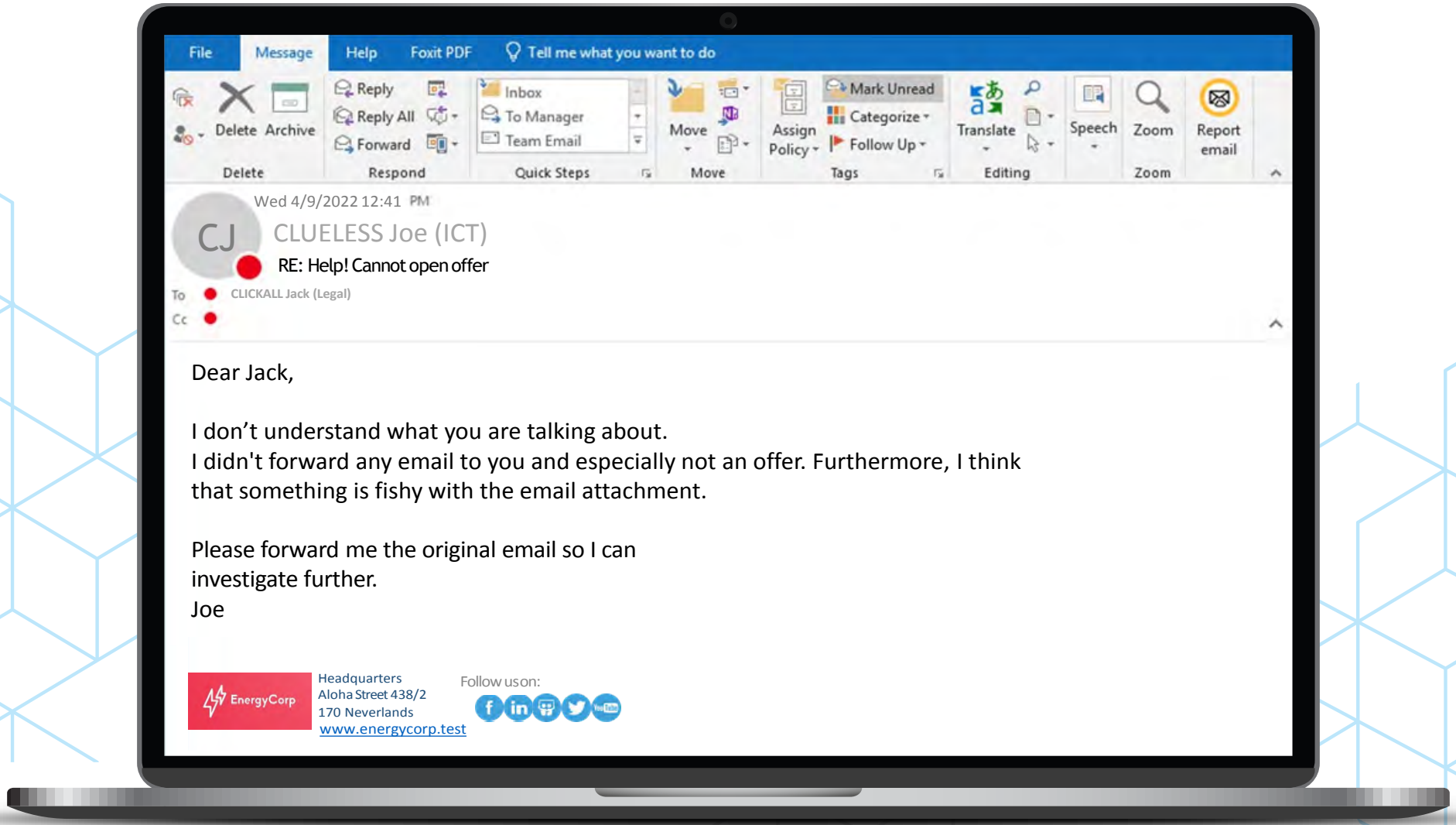
PHISHING ATTACK

SUSPICIOUS MAIL



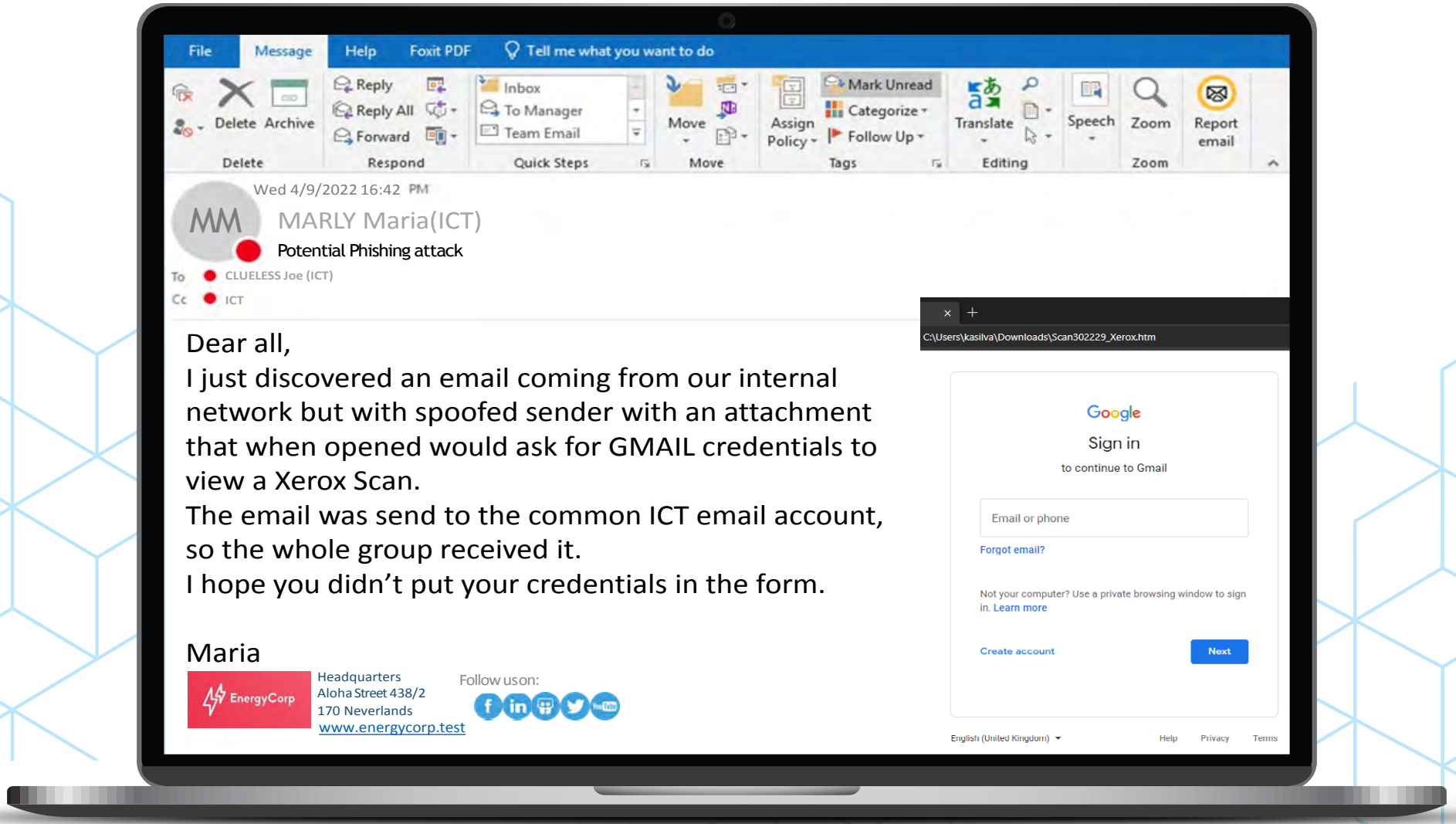
PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

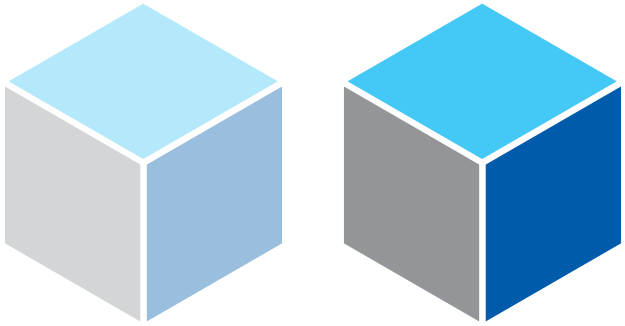
Action Time

Based on you experience can you please draft some answers on the following questions:

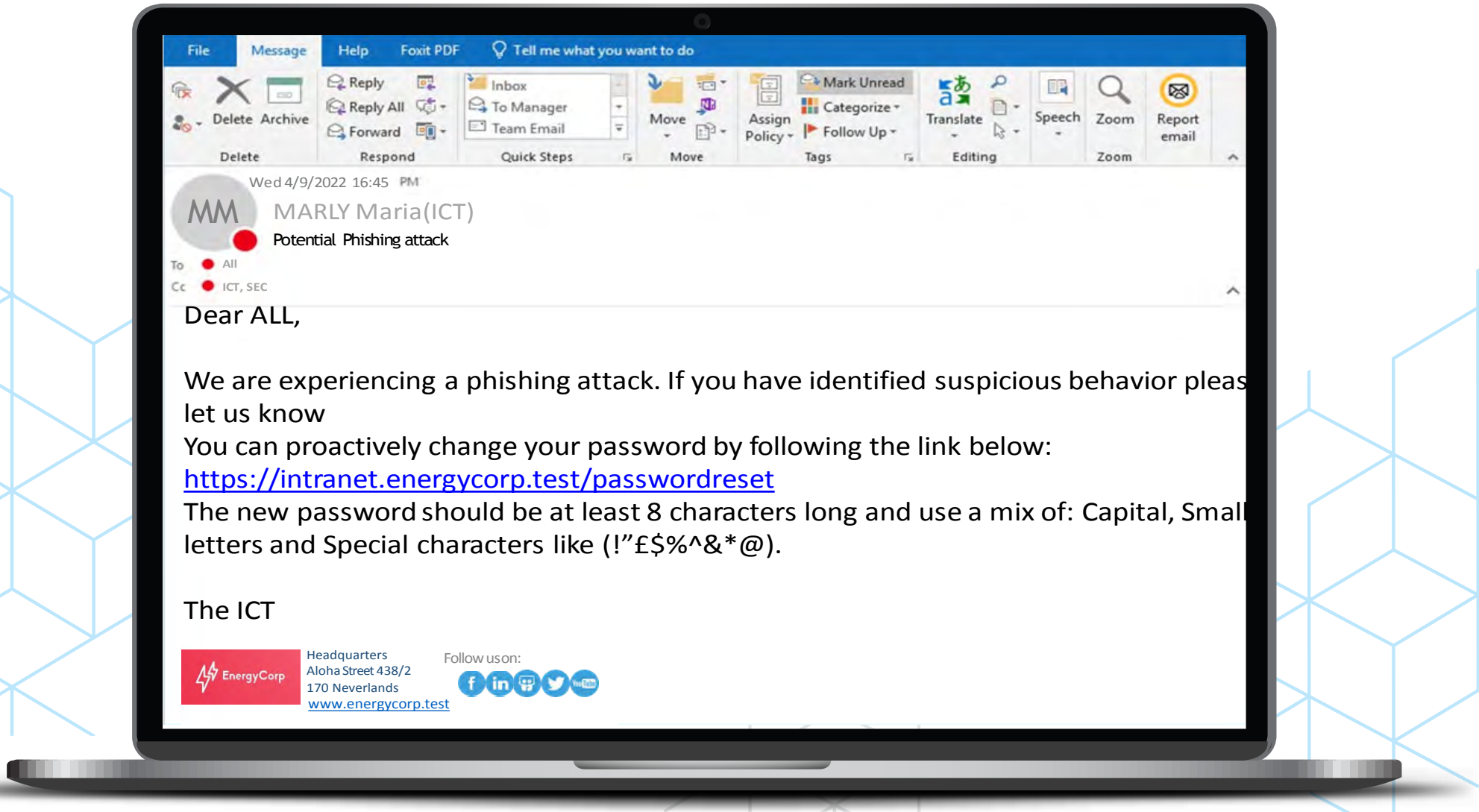
- **Q1.** Which type of attack most likely took place?
- **Q2**. Can you explain the attackers steps so far?
- **Q3.** Was the email Antivirus configured correctly?

THE GAME STARTS HERE

PHASE 2

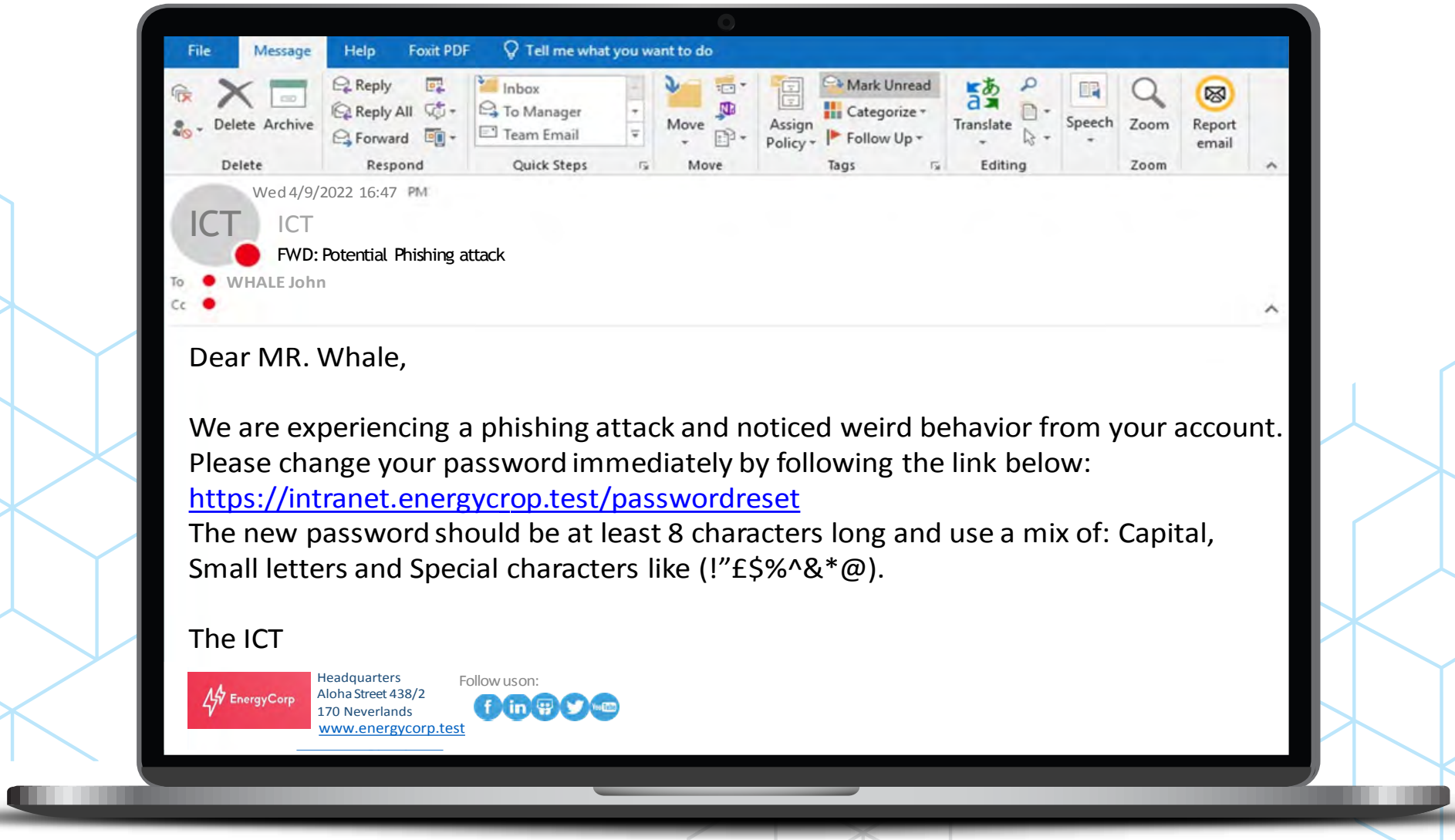


SUSPICIOUS MAIL



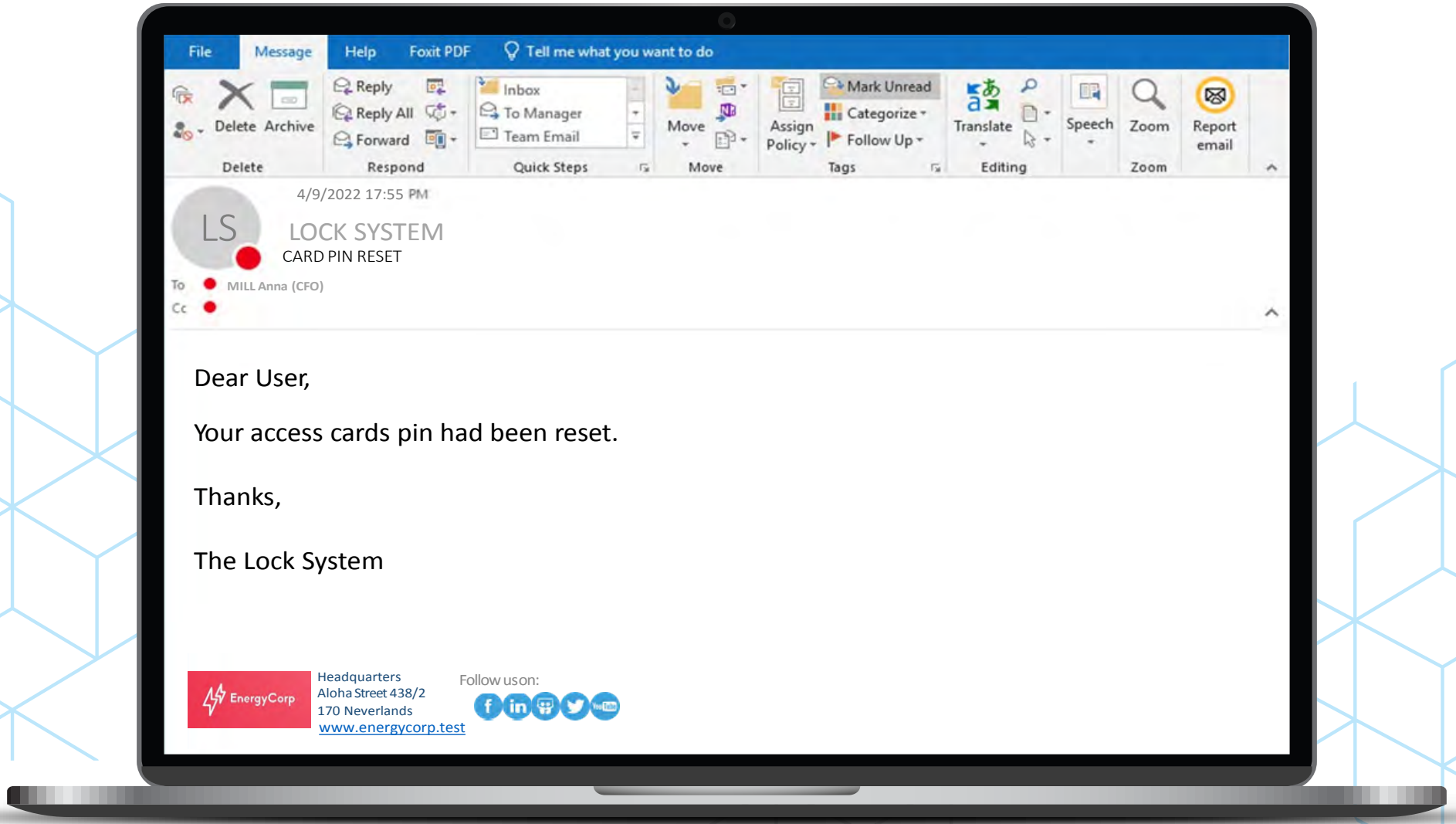
PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

MORE SOCIAL MEDIA POSTS

TITLE: Energy Giant Hacked
Published: 10 September

EnergyCorp, the energy giant has been hacked based on information leaked on the public internet. The attack has not yet been confirmed by the company itself but sources close to the company claim that the information leaked is legitimate. The leak consists of usernames and encrypted passwords of employees.
Furthermore sensitive files have been leaked along with personal information of contractors and suppliers.
SOURCE: PASTEBINPOST1

TITLE: ENERGY MEGA HACK
Published: 12 September

Featured Article: ENERGY MEGA HACK
Project MEDUSA,

After the public exposure of various projects of ENERGYCORP leaked online thanks to ZAaap, one stands out the most!
As part of a joint effort between EnergyCOPR and several high profile politicians, the CEO of EnergyCorp ordered the R&D department halt all efforts for green energy since 2014.

The alerting information proves how corrupted the politicians are and how companies like ENERGYCORP are bribing their way out of costs, sacrificing the health of citizens worldwide.

ANONNEWS
@OPERATION_ENERGYCOPRSE

ENERGYCORP exposed. MEDUSA secret files leaked. Bribing your way out of clean energy will not work this time! #energycorpse

3:24 PM · Sep 14, 2022 · Twitter Web App

7.6K Retweets **417** Quote Tweets **1.0K** Likes

SCAN ME

Scan me

FAKE NEWS

Action Time

Based on you experience can you please draft some answers on the following questions:

- **Q4.** Can you spot a bad practice in password management?
- **Q5.** Is there anything else suspicious in the emails? More attacks maybe?

THE GAME STARTS HERE

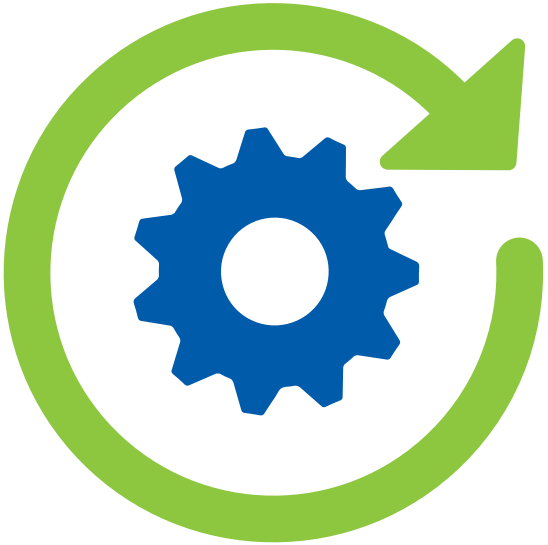
PHASE 3

TASK UPDATE #1

Suspicious activity has been detected in ENERGYCORP HQ.
We believe the recent hacks might be the work of an INSIDER.
The access logs from the supposed date of the hack have been recovered along with relevant HR information's. Dig into the logs to identify the SECURITY breach that lead to stolen the info and the ransomware infection. We count on you to perform the analysis as fast as possible.

Good Luck!

Good Luck,
The Management

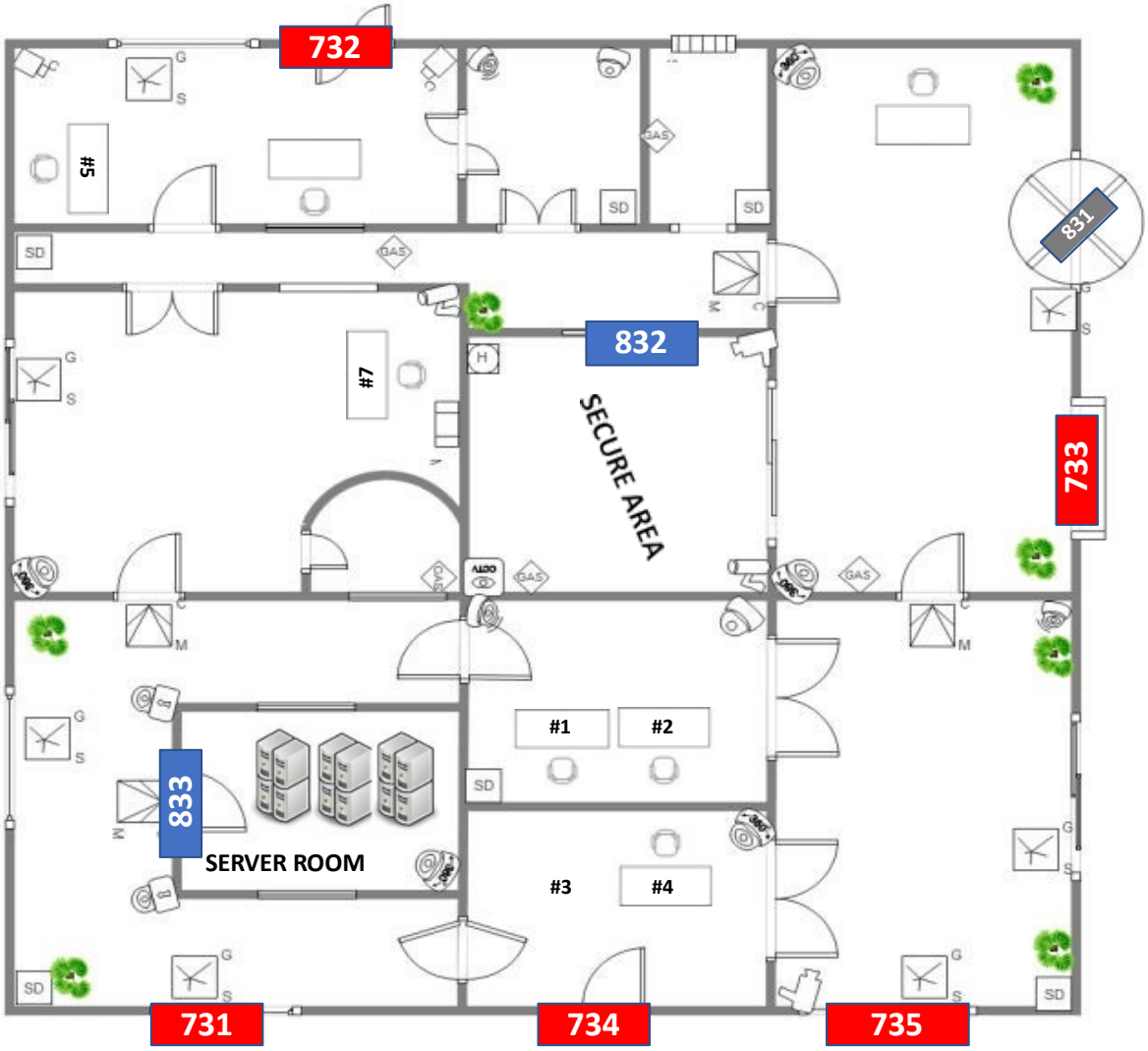


ACCESS LOGS – ENERGYCORP

BADGE ID	Name	READER ID	Date	TIME
FA23RN1	Mill Anna	831	04/09/2022	8:30
IT23RL2	Clueless Joe	831	04/09/2022	8:38
AL3XZA4	Clickall Jack	831	04/09/2022	9:00
IT21NO6	Darc Marc	831	04/09/2022	9:05
IT21NO6	Darc Marc	732	04/09/2022	12:20
IT23RL2	Clueless Joe	832	04/09/2022	13:48
IT11NI9	Marly Maria	831	04/09/2022	14:00
FA23RN1	Mill Anna	832	04/09/2022	16:45
IT11NI9	Marly Maria	833	04/09/2022	17:03
IT11NI9	Marly Maria	832	04/09/2022	17:08
IT21NO6	Darc Marc	832	04/09/2022	17:58
IT11NI9	Marly Maria	831	04/09/2022	17:59
FA23RM1	Mill Anna	833	04/09/2022	18:01
FA23RN1	Mill Anna	831	04/09/2022	18:04
AL3XZA4	Clickall Jack	831	04/09/2022	18:20
IT23RL2	Clueless Joe	831	04/09/2022	18:30

UNAUTHORISED ACCESS

ENERGYCORP FLOOR PLAN & ACCESS BADGES



DOUBLE WAY DOOR

SECURE DOOR WITH PIN

EMERGENCY EXIT

CLUELESS Joe
ICT
ID: IT23RL2

CLICKALL Jack
LEGAL
ID: AL3XZA4

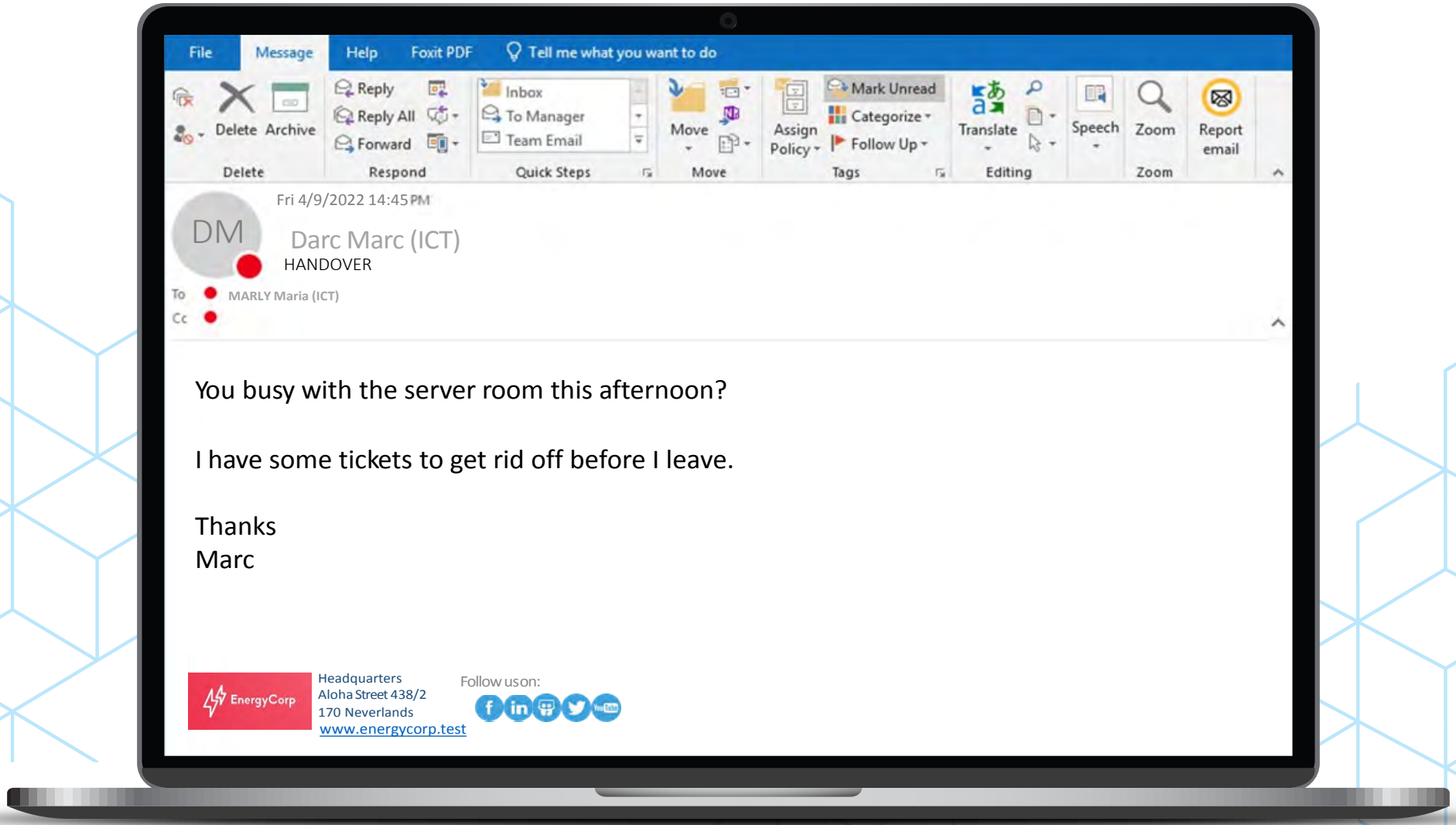
MILL Anna
CFO
ID: FA23RN1

DARC Marc
ICT – Contractor
ID: IT21NO6

MARLY Maria
ICT
ID: IT11NI9

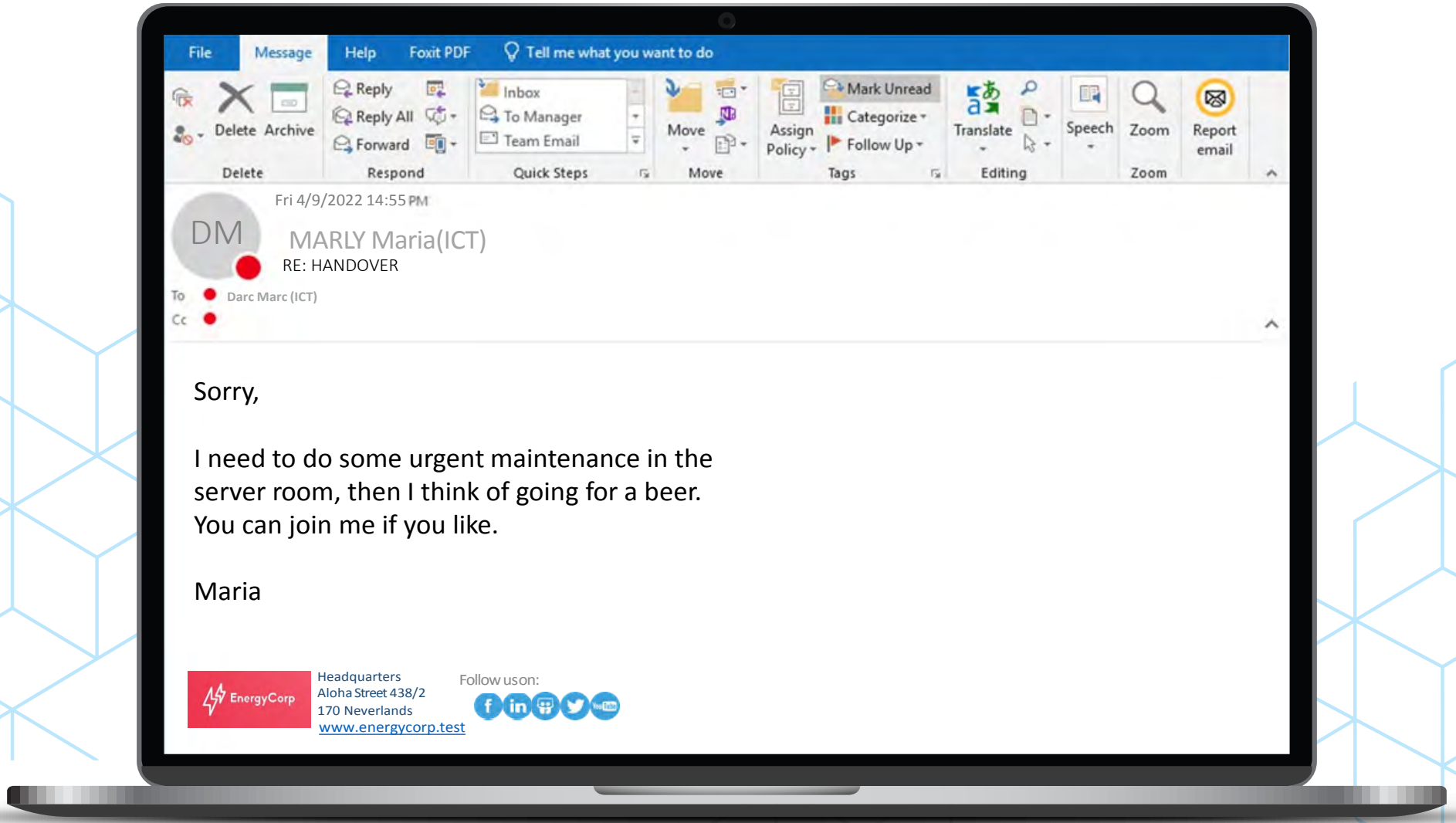
UNAUTHORISED ACCESS

SUSPICIOUS MAIL



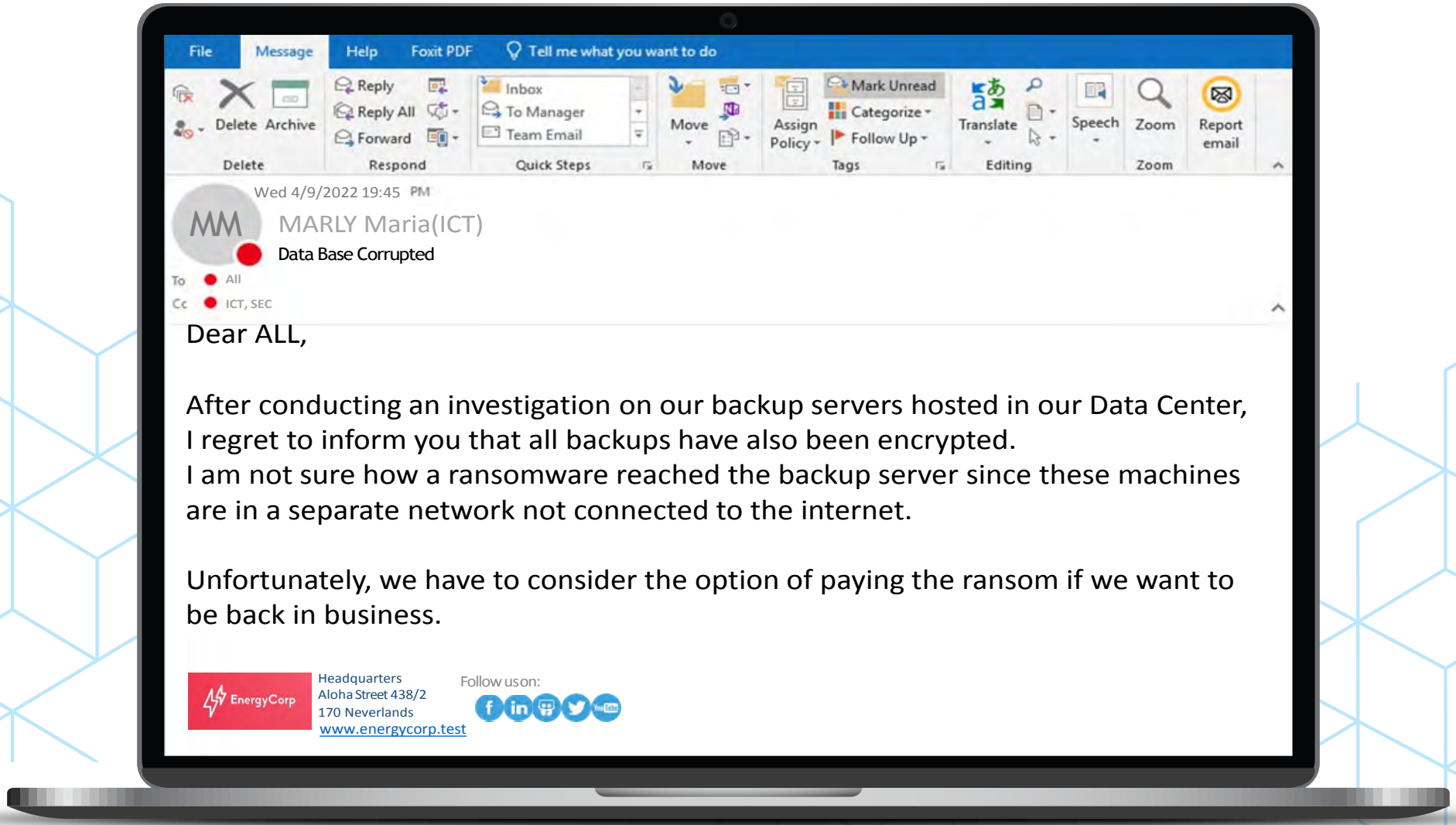
PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

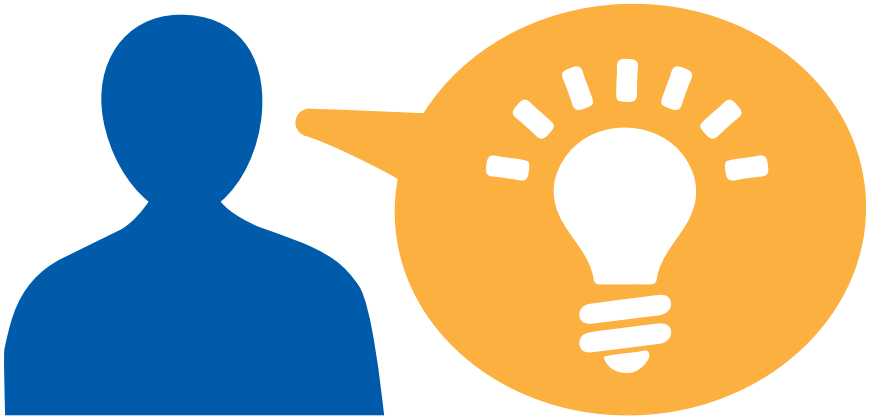
MORE (SOCIAL) MEDIA POSTS

FAKE NEWS

Action Time

Based on you experience can you please draft some answers on the following questions:

- **Q6.** What could have been a measure taken that could have saved your data for the scenario presented, making paying the ransom obsolete?
- **Q7.** What would be the correct steps to follow in case of public leakages of your clients DB after a hack?
- **Q8.** What would be the steps to follow in case of defamation (fake news) against your company after a hack?

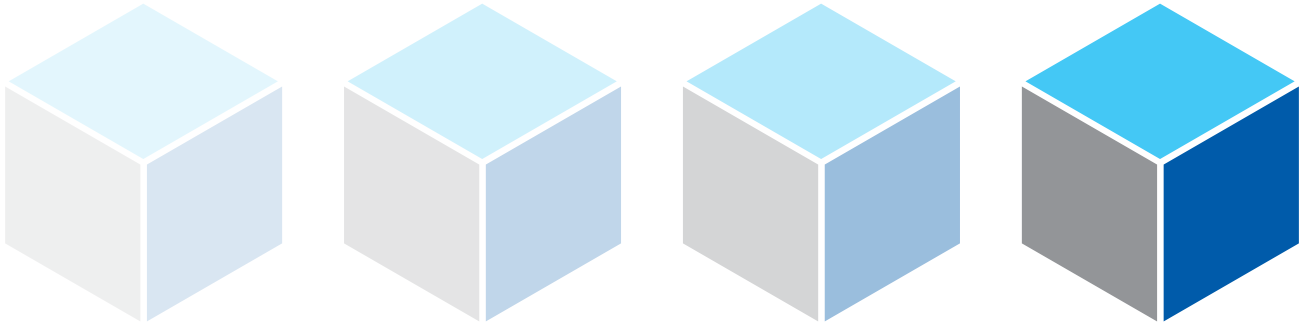


DRAFT YOUR SOCIAL MEDIA RESPONSE

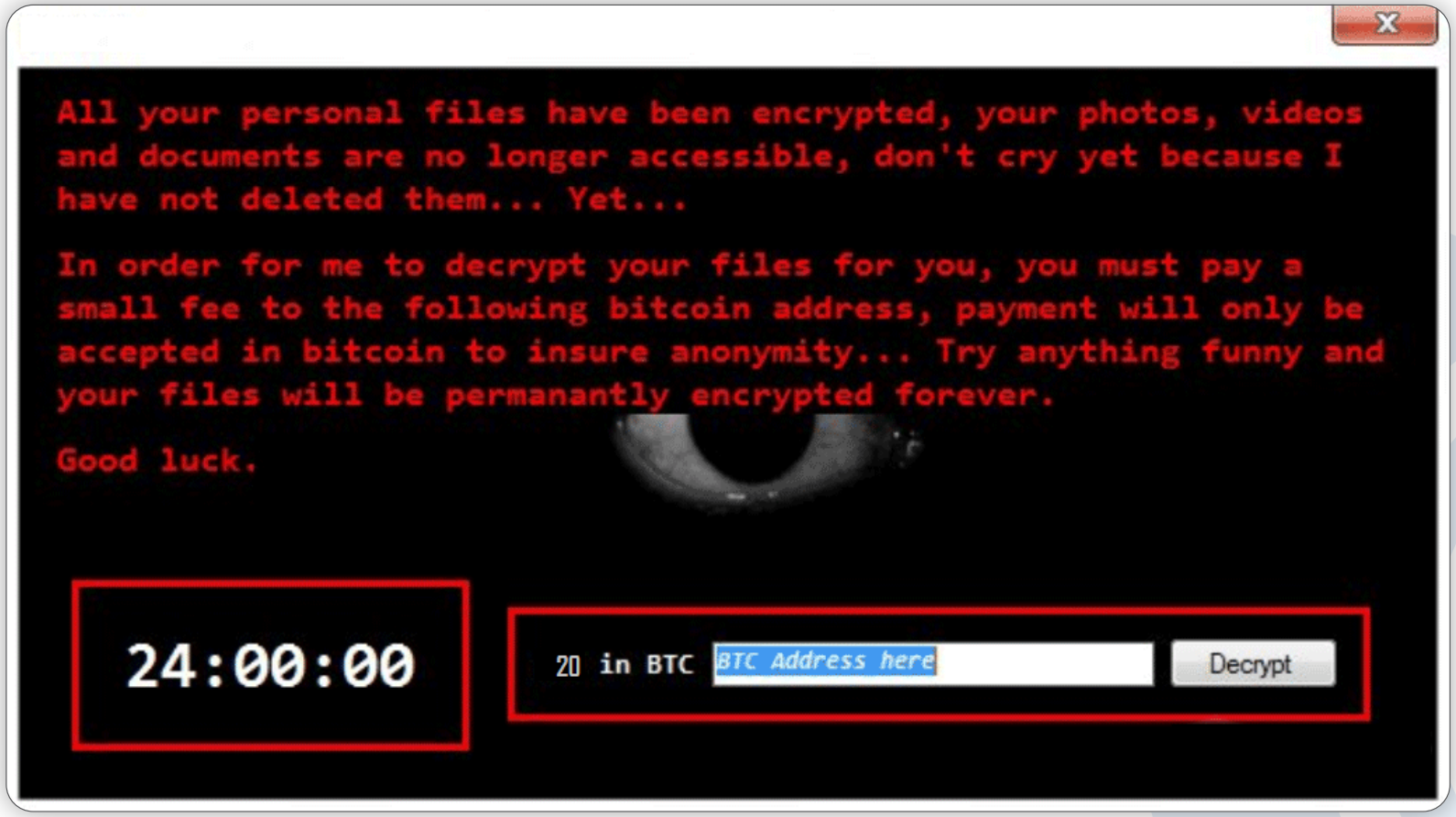
FAKE NEWS

THE GAME STARTS HERE

PHASE 4



THE RANSOMWARE NOTE



File to unlock:

UVOAQGY DEIA.db

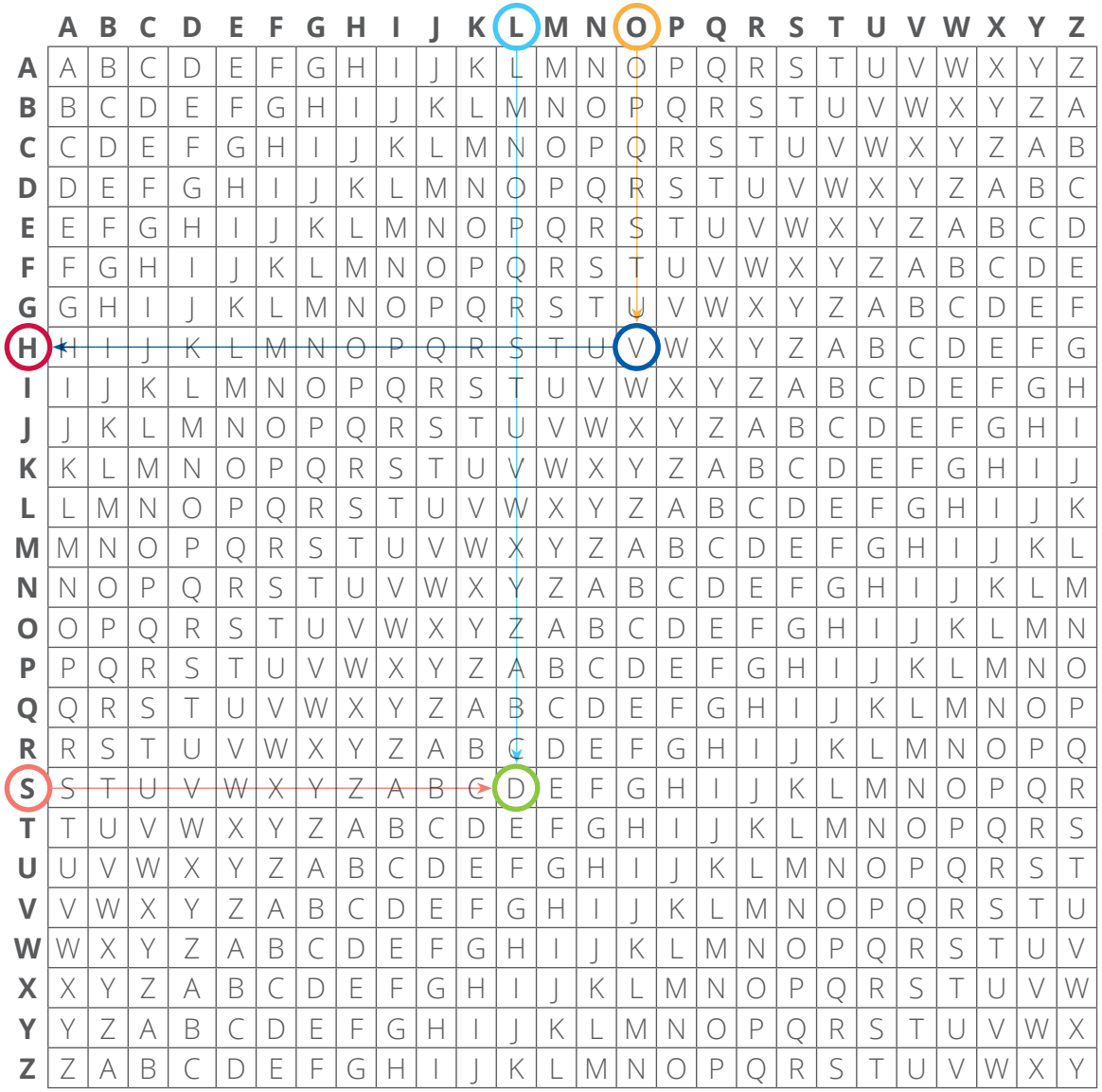
Decrypt the FILENAME using the correct key

RANSOMWARE

HOW DOES VIGENERE WORK – EXAMPLE

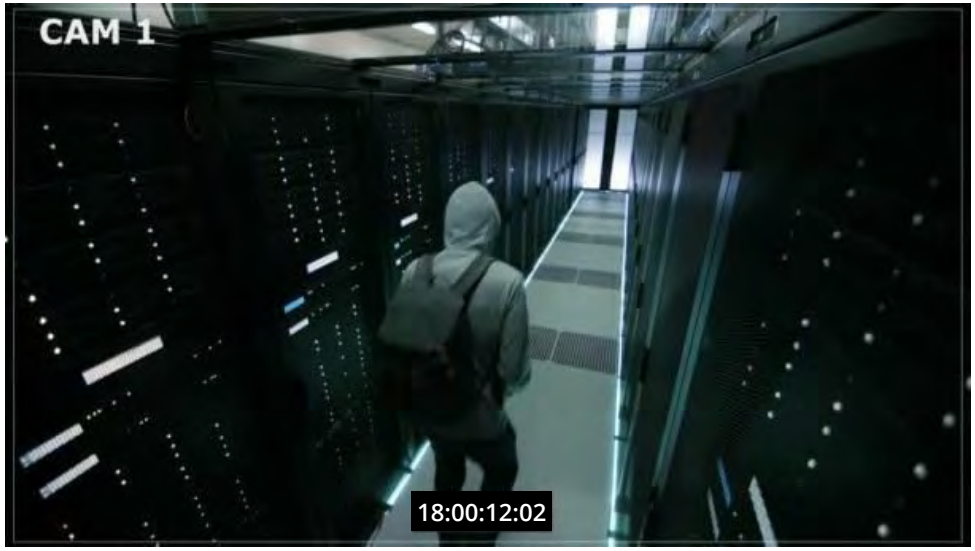
To encrypt:
SECRET PHRASE
Key:
LOCKME
ENCRYPTION MECHANISM:
S E C R E T P H R A S E
L O C K M E L O C K M E
D S E B Q X A V T K E I

To decrypt:
DSEBQXAVTKEI
Key:
LOCKME
DECRYPTION MECHANISM:
L O C K M E L O C K M E
D S E B Q X A V T K E I
S E C R E T P H R A S E



RANSOMWARE

Server Room: Camera Footage



Beware:
Badges can be cloned!
Anyone can be the attacker.

UNAUTHORISED ACCESS

ANSWER SHEET

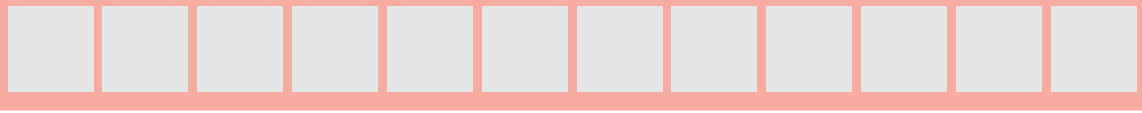
What is the name of the first known victim of the PHISING ATTACK?

[Surname Name as seen in the Badge with space*]

Which Badge ID was used to performed UNAUTHORIZED ACCESS?

ENCRYPTION KEY

What is the filename of the decrypted file?



Which article is the source of fake news? [Article Name*]

SOLUTION

What is the name of the first known victim of the PHISING ATTACK?

[Surname Name as seen in the Badge with space*]

C	L	U	E	L	E	S	S		J	O	E		

Which Badge ID was used to performed UNAUTHORIZED ACCESS?

F	A	2	3	R	M	1

ENCRYPTION KEY

F	E	A	R	M	E

What is the filename of the decrypted file?

P	R	O	J	E	C	T		Z	E	R	O

Which article is the source of fake news? [Article Name*]

E	N	E	R	G	Y		M	E	G	A		H	A	C	K