AR-IN-A-BOX

CYBER AWARENESS GAME

Online Retail Hack

BE THE STRONGEST LINK
BREAK THE KILLCHAIN

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

DISCLAIMER

Game Rules

- Create teams of **5**
- Choose a Team Leader
- Choose a Team Name
- Split the Task Per Color
- Answer the Questions
- One correct answer: **+10 Points**
- One wrong answer: **-5 points**
- Use a Hint: **-5 points**
- You have: **45’**

Team leader tasks

- Understand the challenges
- Split the team & assign tasks
- Team awareness and exchange of info
- Ask for help
- **Submit solution (answer sheet + hint folder)**

THE GAME STARTS HERE

SCENARIO – MEGACORP HACKED

MegaCorp, a leader in online retail has been hacked based on information leaked on the public internet.

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

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

You have 45' minutes left before all our data are wiped out.

GOOD LUCK!

THE NEWS

The Daily

Saturday, September 10, 2022

MEGACORP HACKED

MEGACORP 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.

ANSWER SHEET

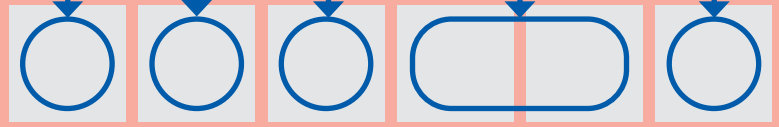
What is the name of the first known victim of the PHISING ATTACK?

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

Which Badge ID was used to performed UNAUTHORIZED ACCESS?

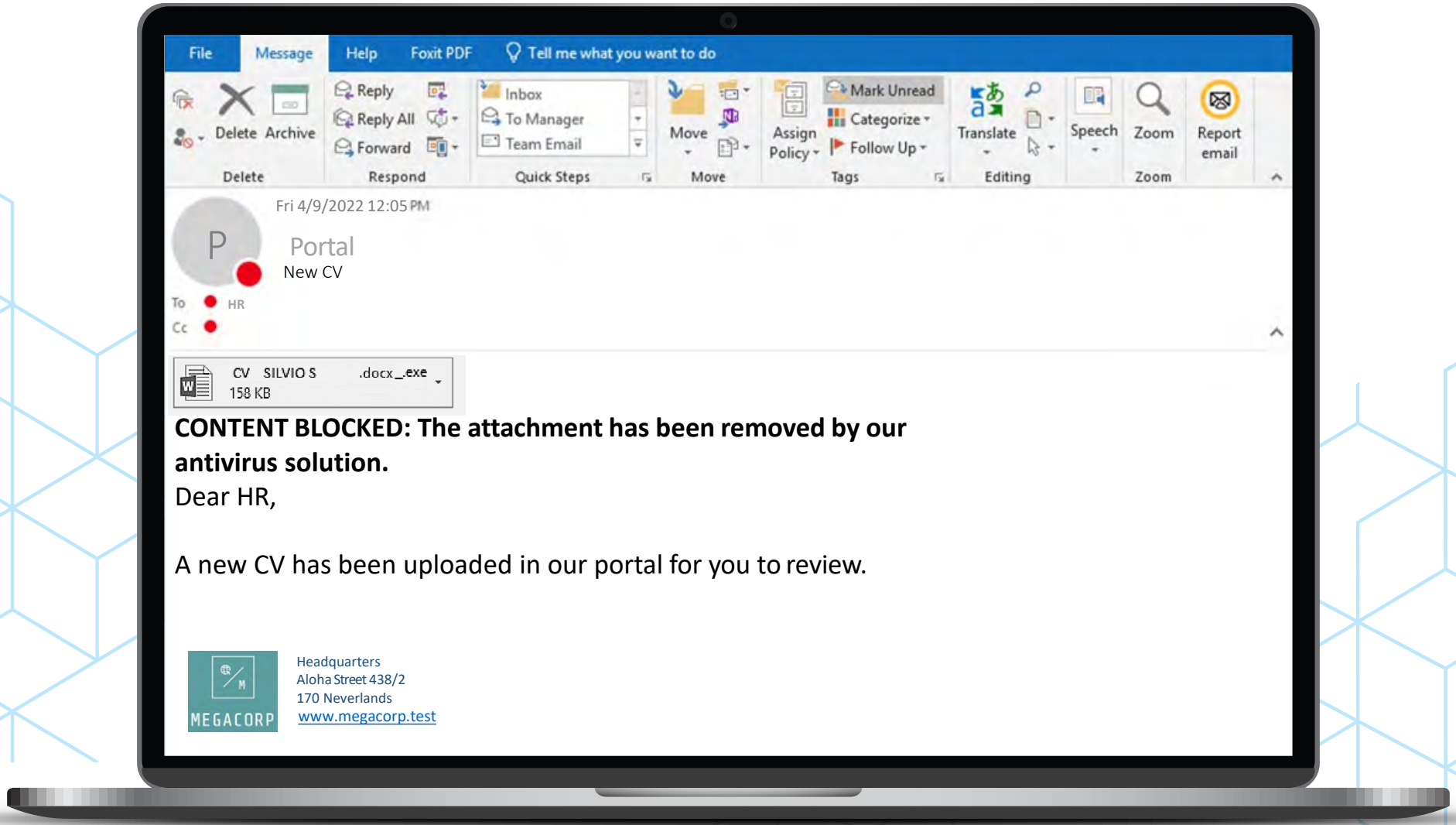
What time was the first FAKE NEWS item posted?

ENCRYPTION KEY



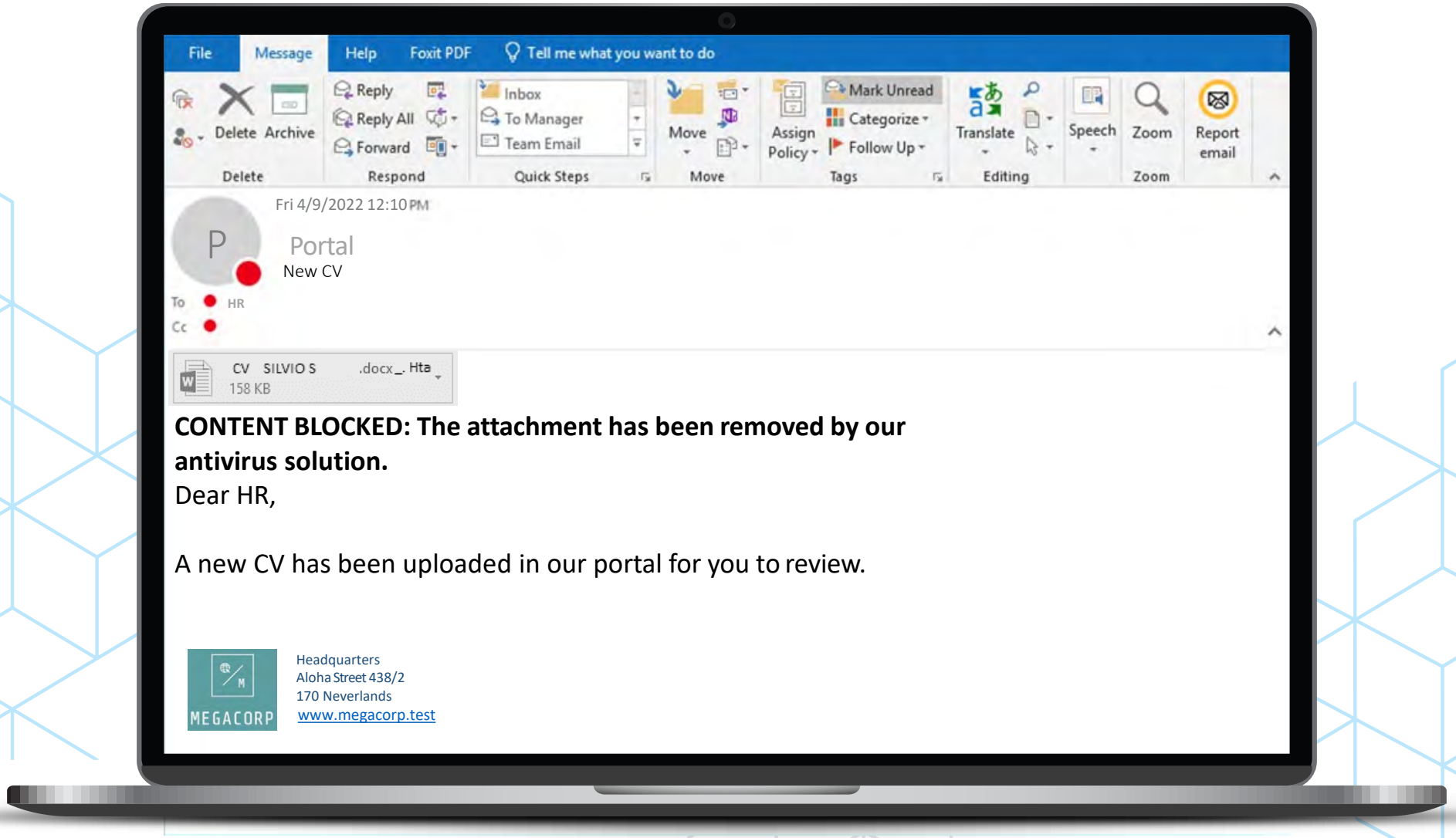
What is the filename of the decrypted file?

SUSPICIOUS MAIL



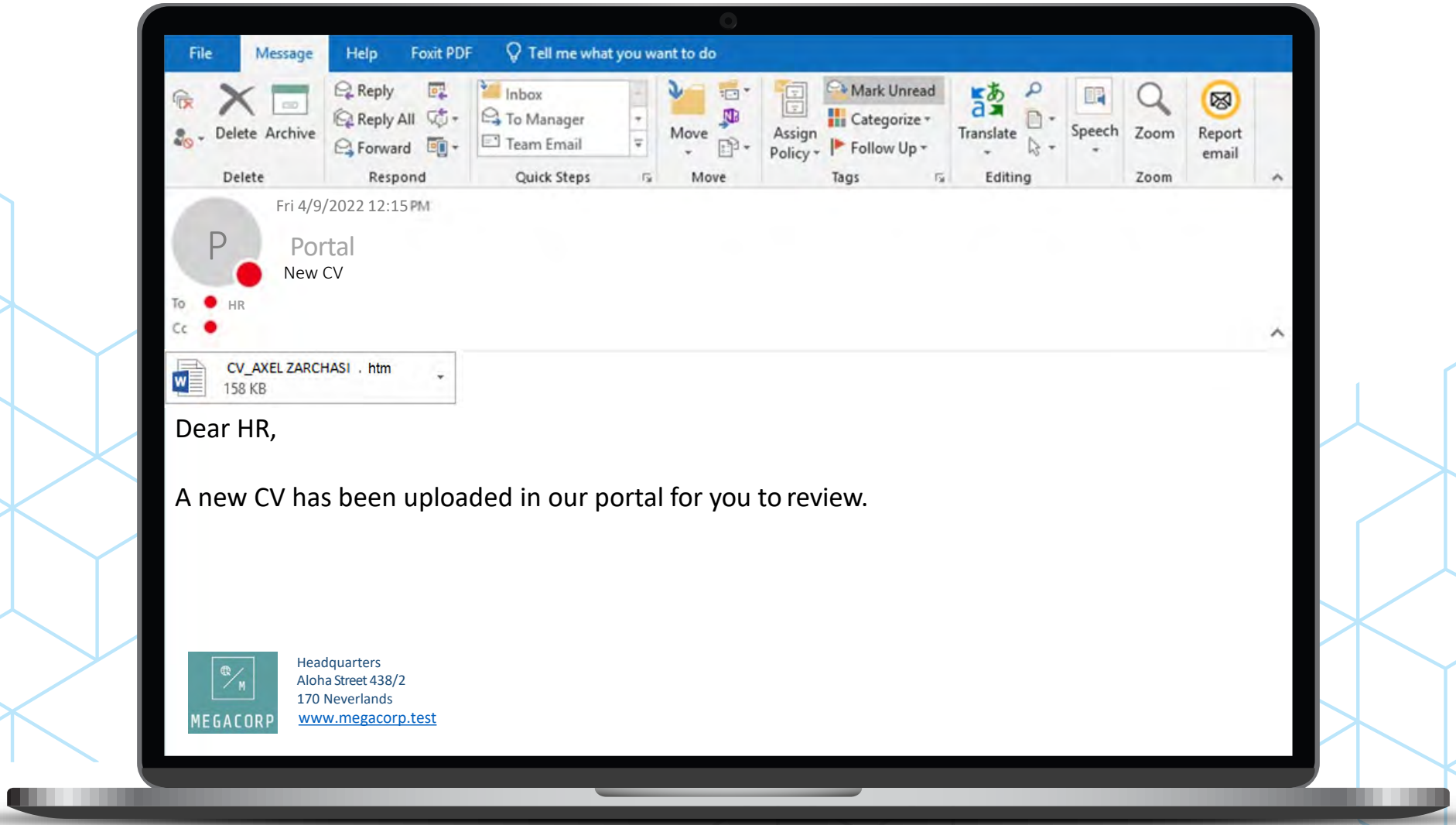
PHISHING ATTACK

SUSPICIOUS MAIL



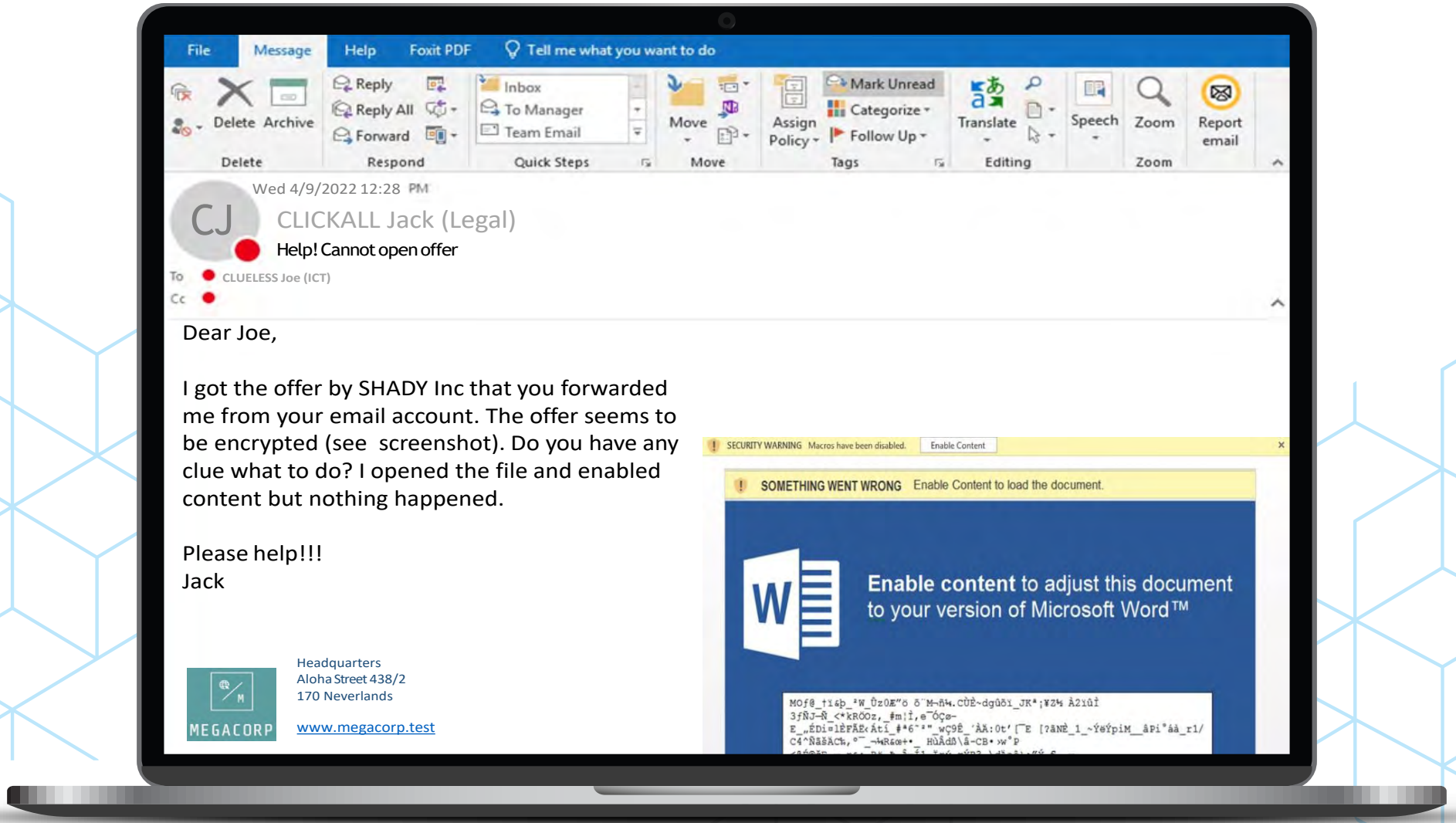
PHISHING ATTACK

SUSPICIOUS MAIL



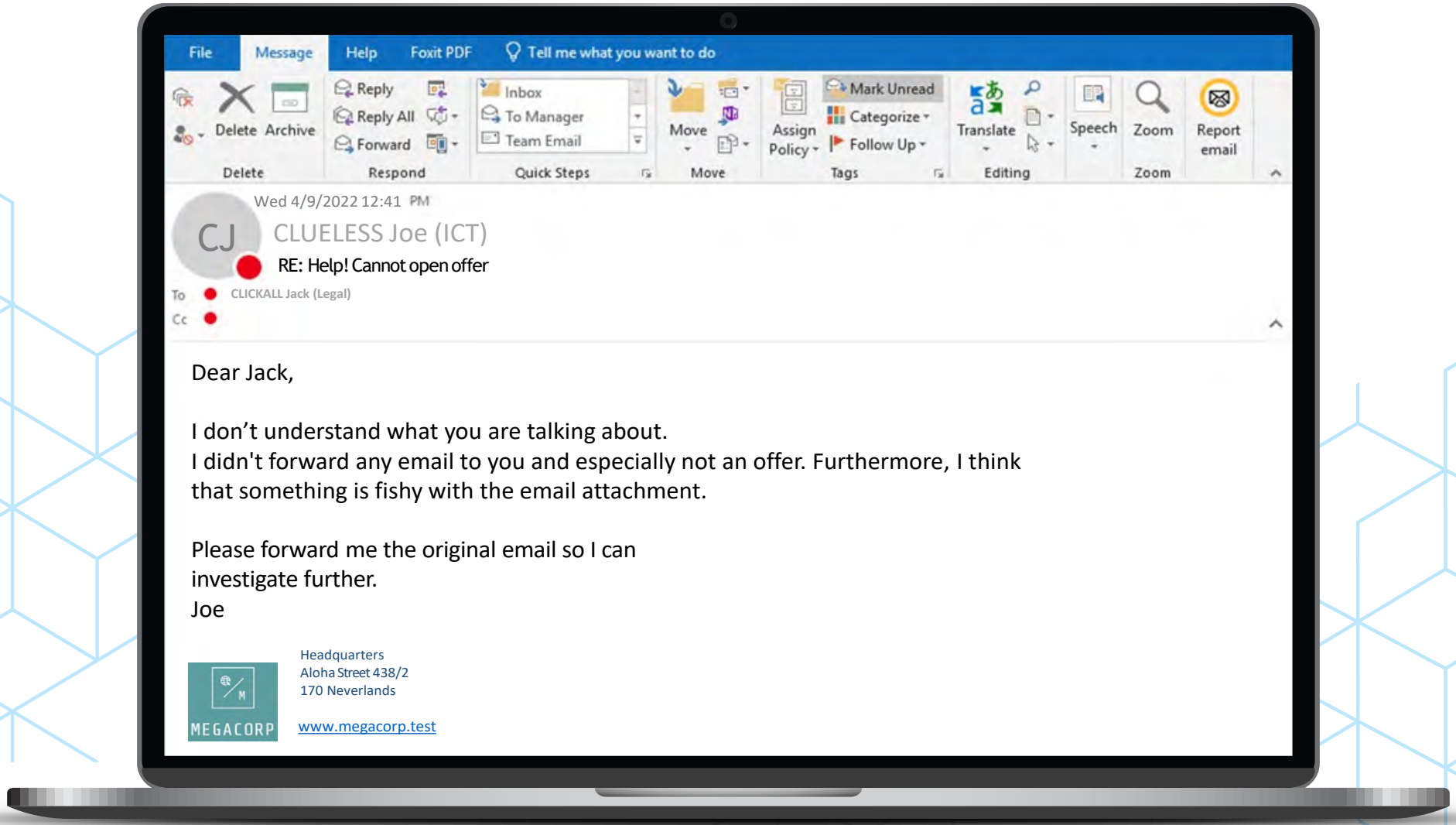
PHISHING ATTACK

SUSPICIOUS MAIL



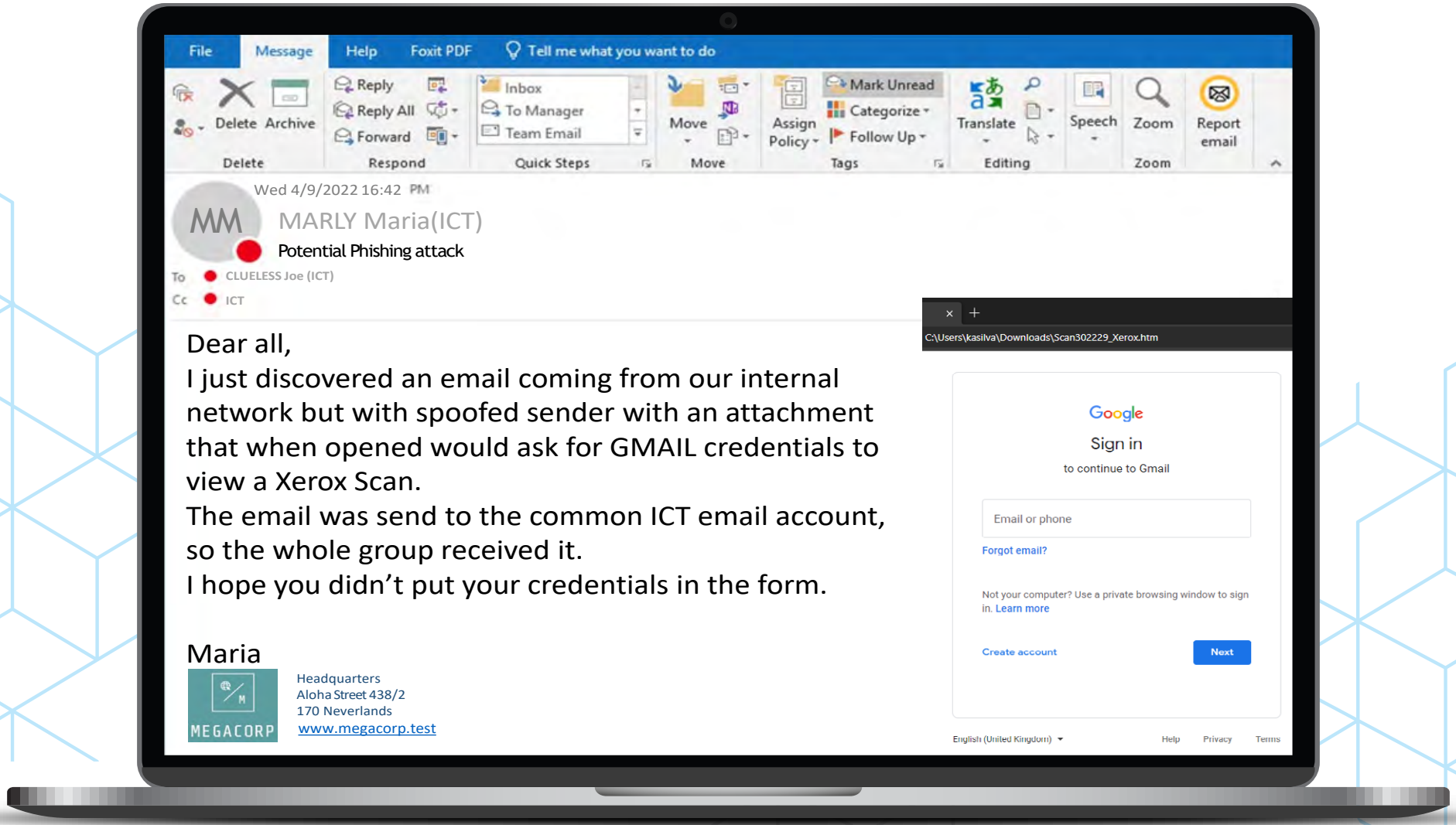
PHISHING ATTACK

SUSPICIOUS MAIL



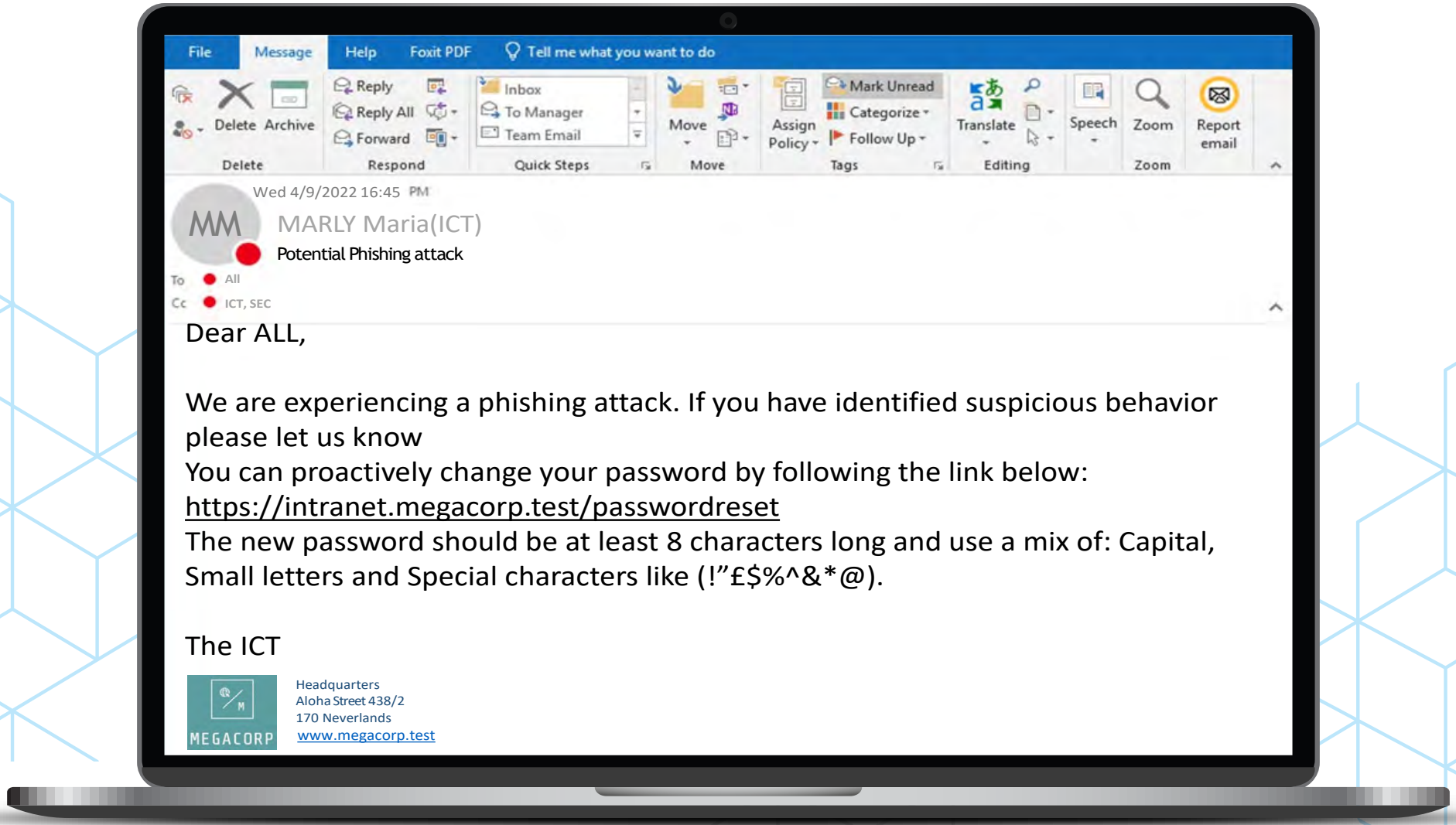
PHISHING ATTACK

SUSPICIOUS MAIL



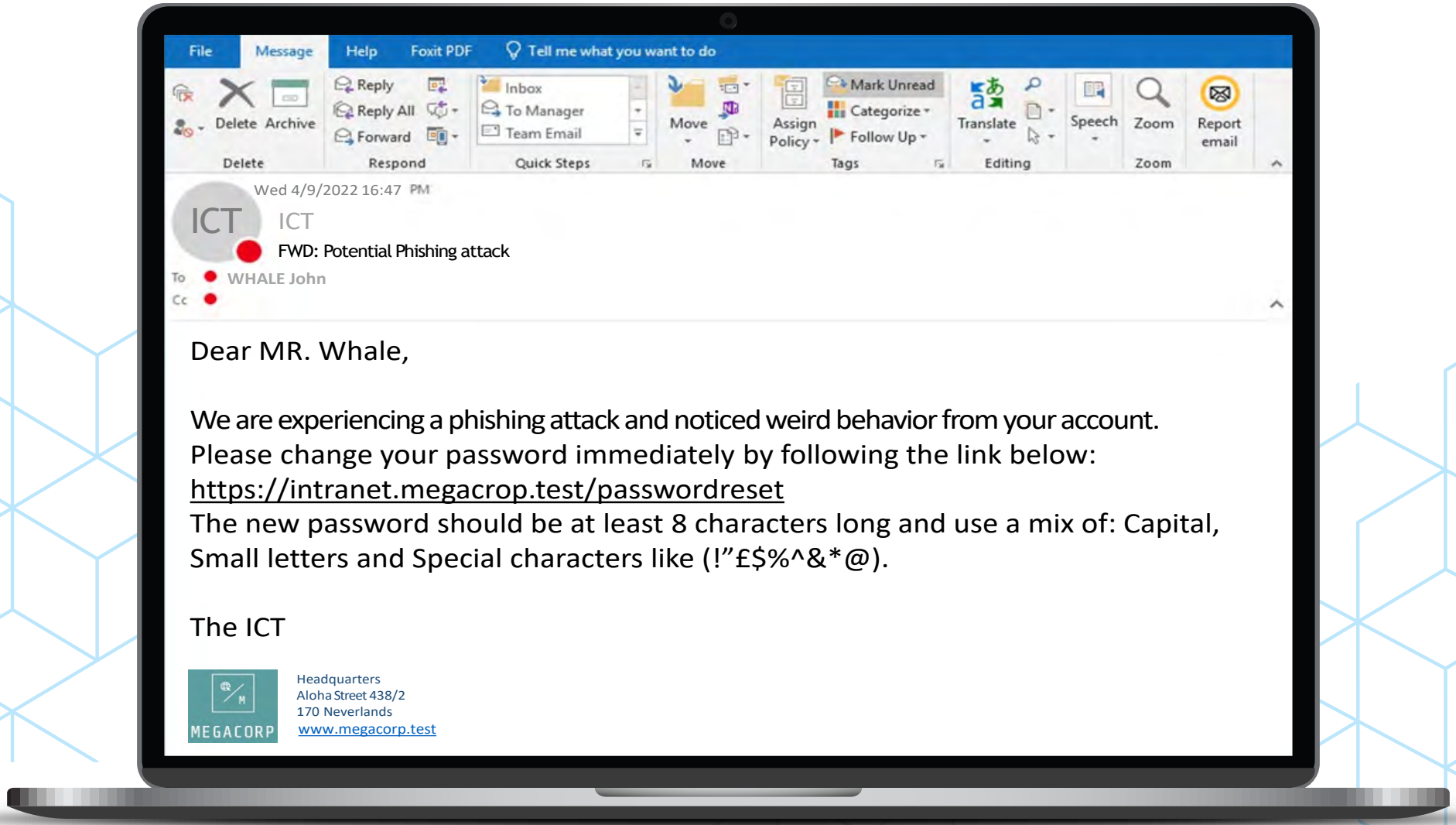
PHISHING ATTACK

SUSPICIOUS MAIL



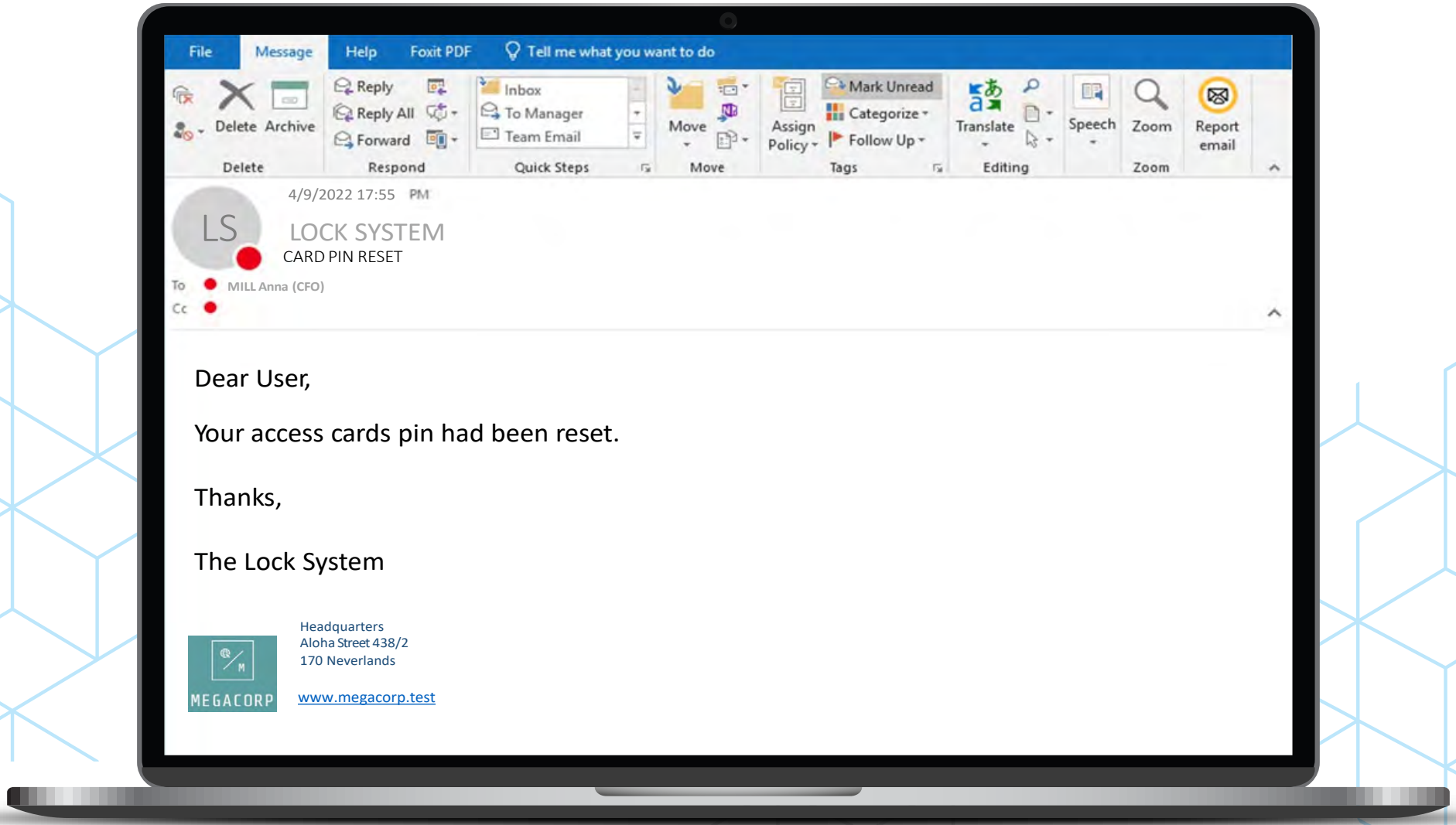
PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

MORE SOCIAL MEDIA POSTS

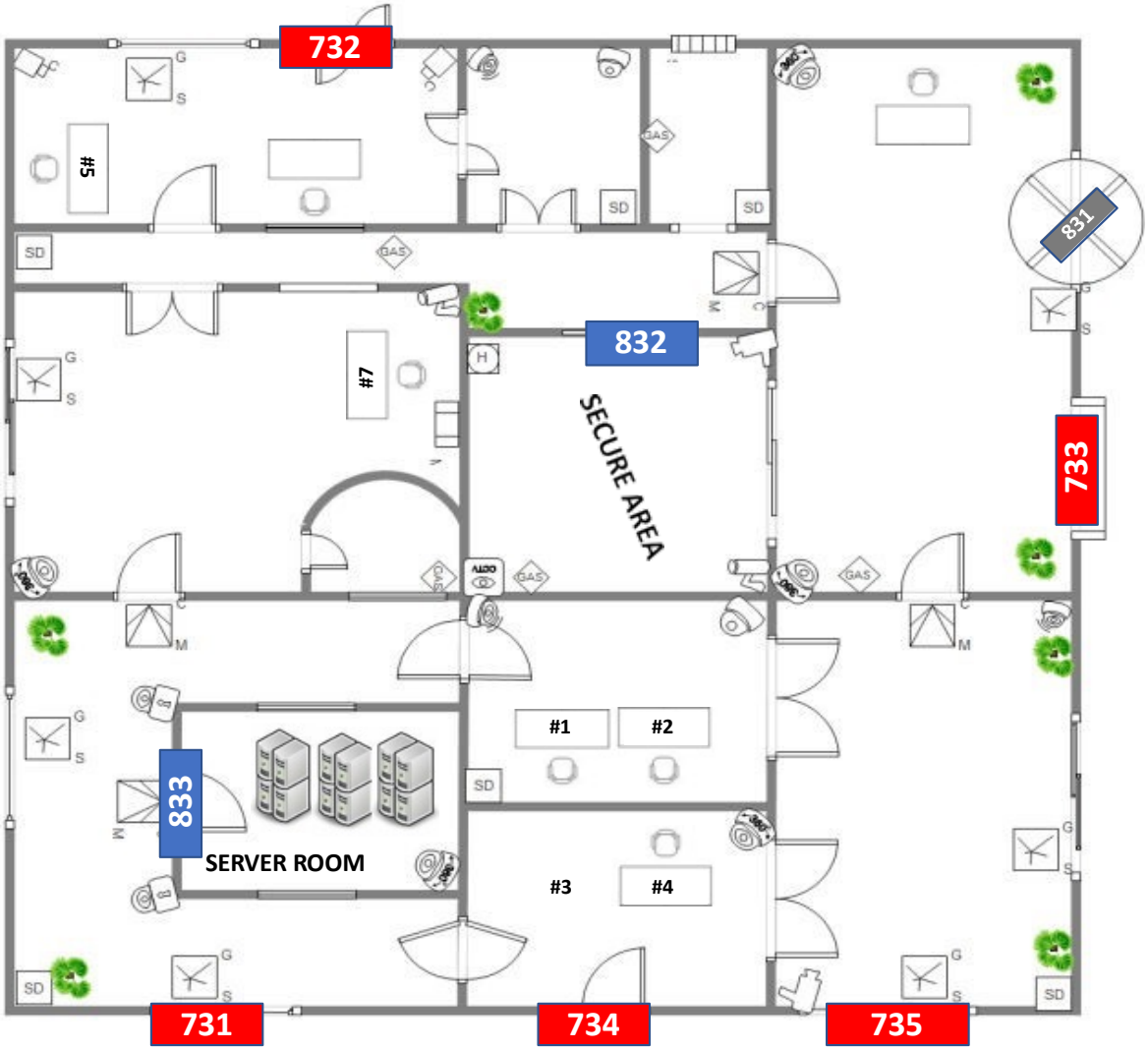
FAKE NEWS

ACCESS LOGS – MEGACORP

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

MEGACORP 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

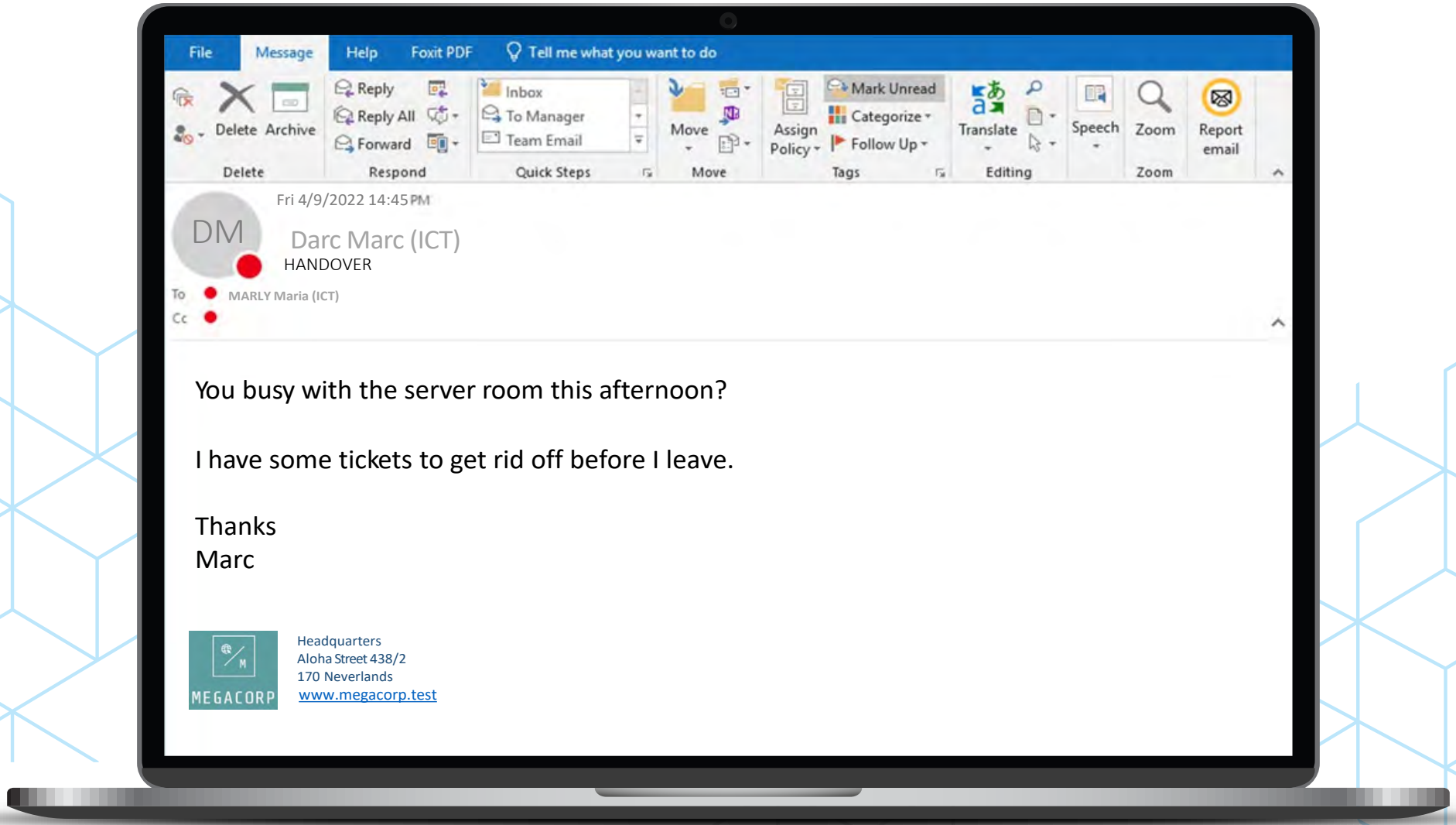
UNAUTHORISED ACCESS

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

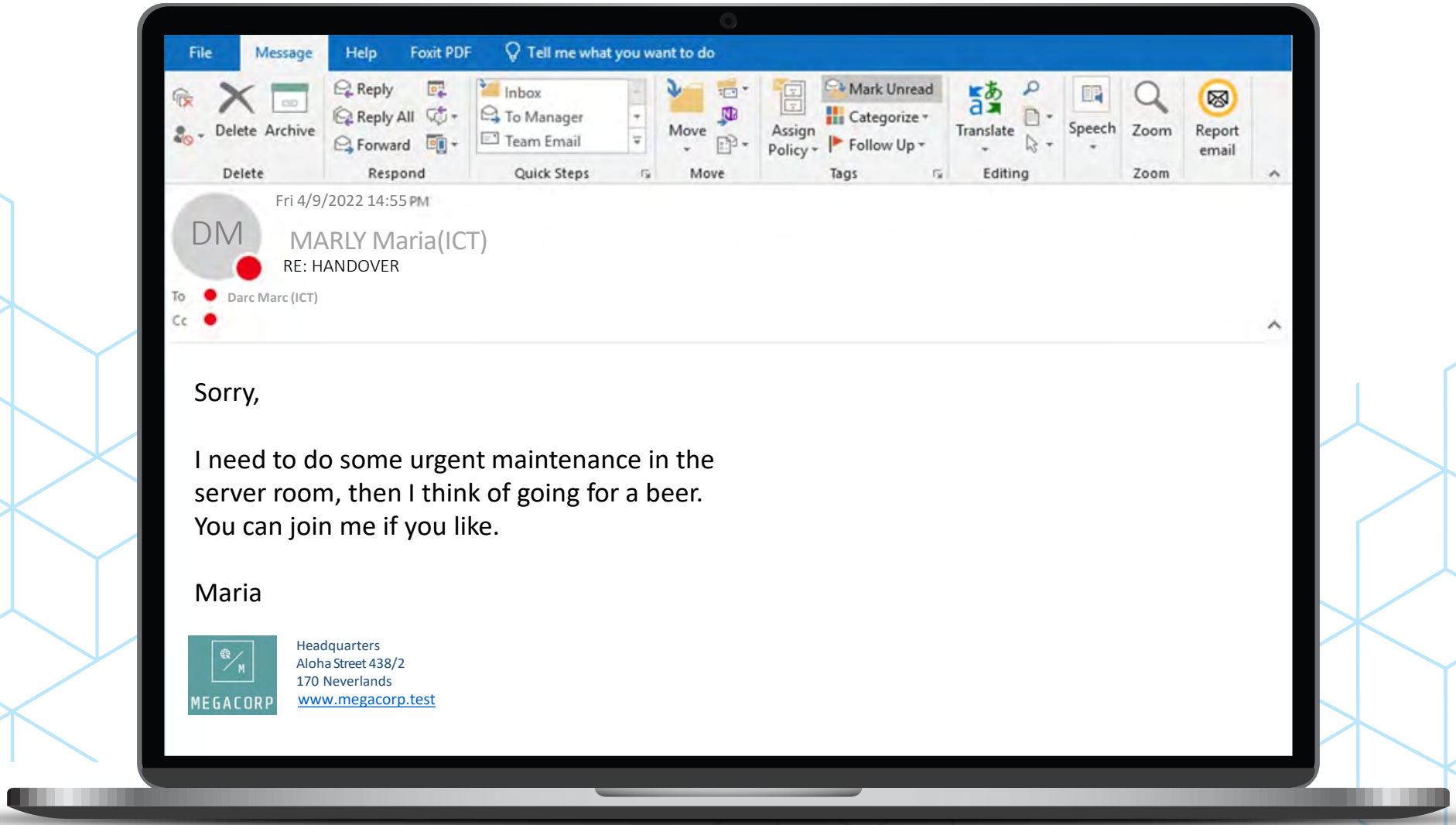
UNAUTHORISED ACCESS

SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

MORE (SOCIAL) MEDIA POSTS

CompromiseDB
@cyber_analyst

MEGACORP's data leak analyzed. Two documents leaked containing: usernames, encrypted passwds of employees, limited personal info of contractor and supplier. We are monitoring the leak flow closely. Stay tuned!

3:26 PM · Sep 9, 2022

1 Retweet **22** Quote Tweets **18** Likes

AverageJoe
@Joe_Average

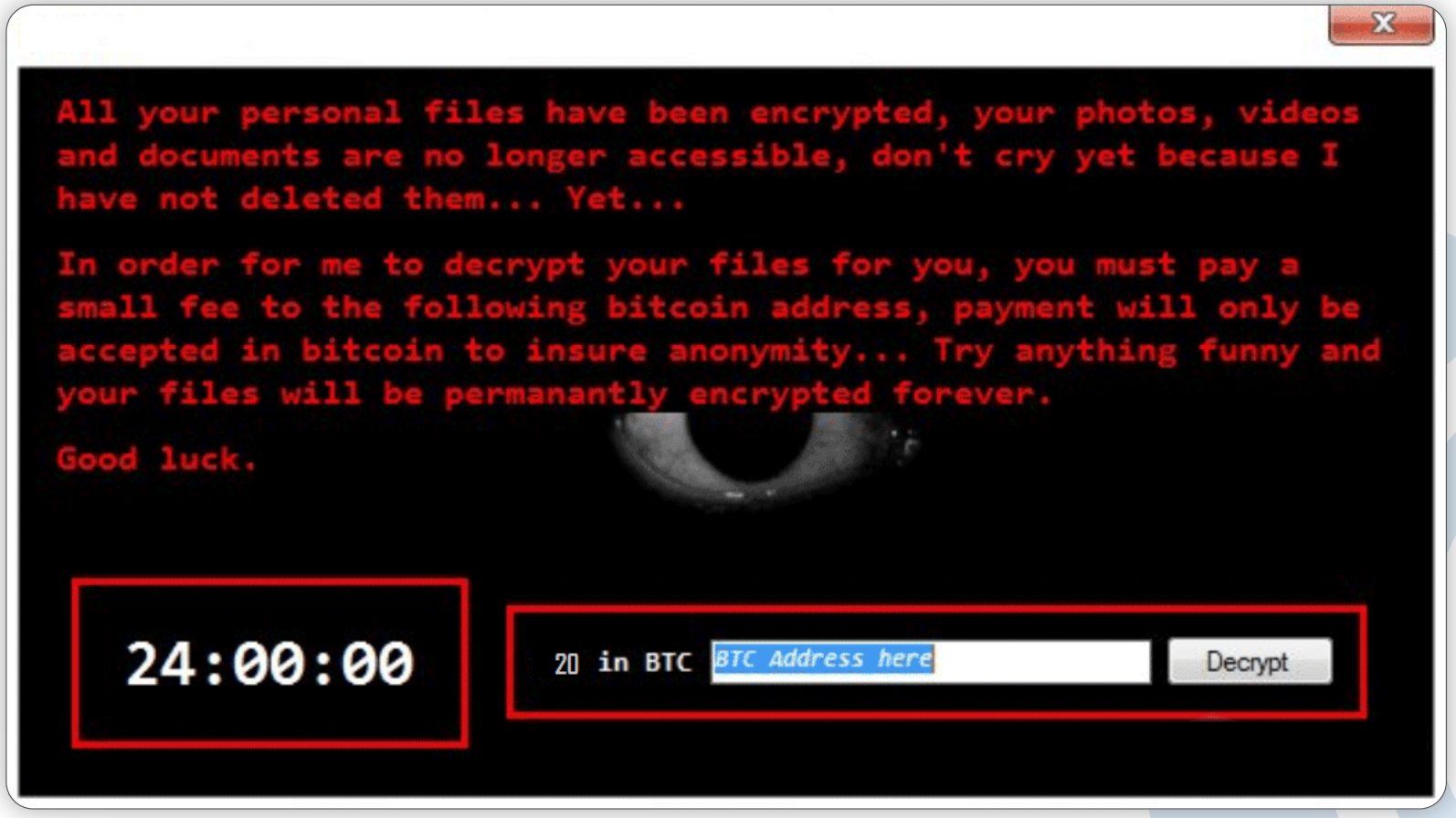
@MEGACORP are you kidding us? Leave our data alone!!! Props to @Timleak #MEGABOYCOTT,#MEGACORPSE 💀💀💀

4:26 PM · Sep 9, 2022

2.5K Retweets **660** Quote Tweets **20.4K** Likes

FAKE NEWS

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:

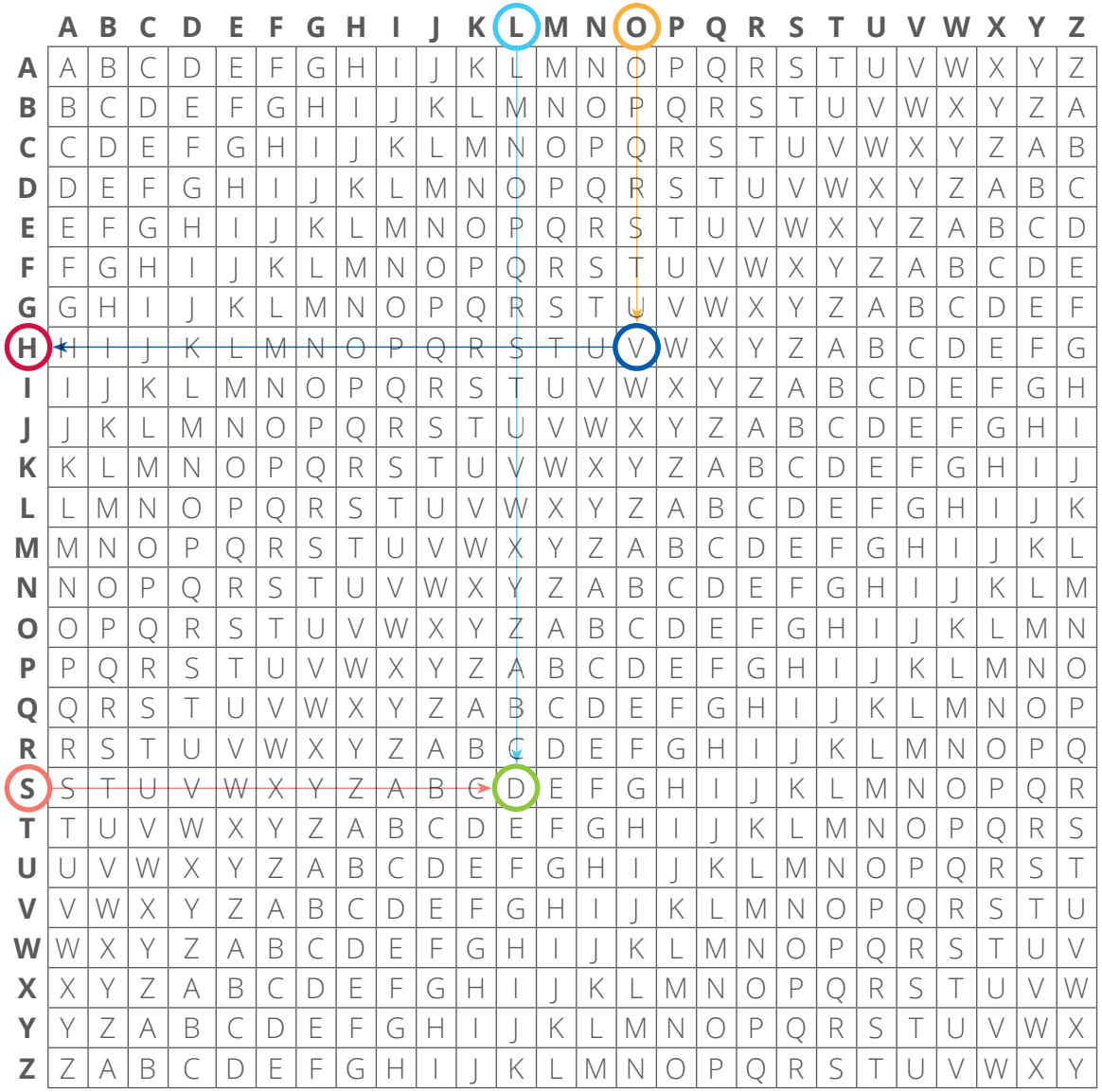
LOCKME

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

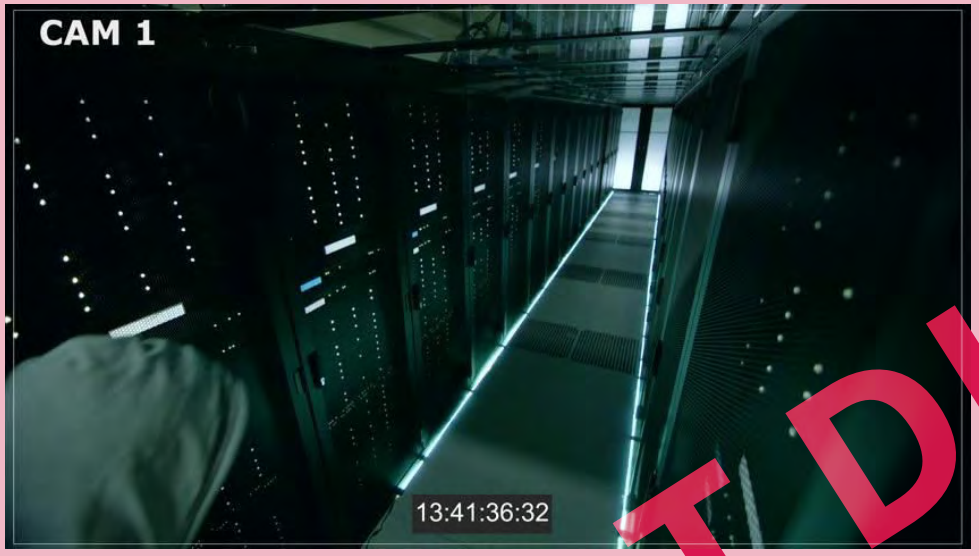
S E C R E T P H R A S E



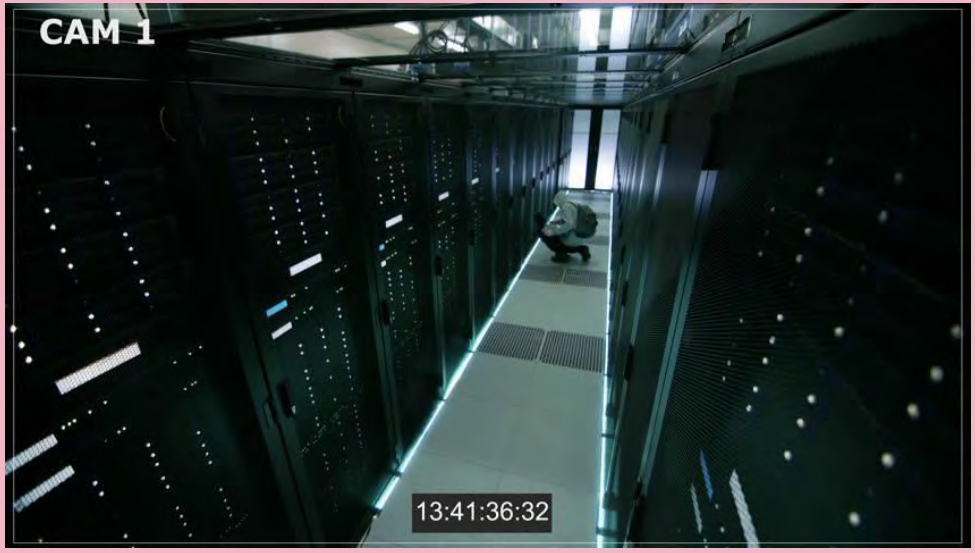
RANSOMWARE

HINT

Server Room: Camera Footage



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



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

What time was the first FAKE NEWS item posted?

1 6 : 0 5

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