



AR-IN-A-BOX

CYBER AWARENESS GAME

EnergyCorp hacked

BE THE STRONGEST LINK
BREAK THE KILLCHAIN





DISCLAIMER

Copyright © European Union Agency for Cybersecurity (ENISA), 2022

This document and information contained in this document may be excerpted, copied, printed, republished, made available to the public by wire or wireless means and/or otherwise provided to third parties only under the condition that the source and copyright owner is clearly stated as follows:

“Source: ENISA Cyber Awareness Training Material, Copyright © European Union Agency for Cybersecurity (ENISA), 2022”. If you do republish we would be grateful if you link back to the ENISA website **www.enisa.europa.eu**. No part of this document, including any part of the information contained therein, in whichever format, whether digital or otherwise, may be altered, edited or changed without prior express and written permission of the European Union Agency for Cybersecurity (ENISA), to be requested via email to “**access-documents@enisa.europa.eu**”, clearly stating the element (document and/or information) and term of use requested.

The present document is being distributed without warranty of any kind, either express or implied in relation to its content and/or use and the views expressed herein do not necessarily represent the opinions or the stated policy of ENISA. To the extent permitted by the applicable law, ENISA shall not be liable for any damages arising from the content and use of the present document.

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 – 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.

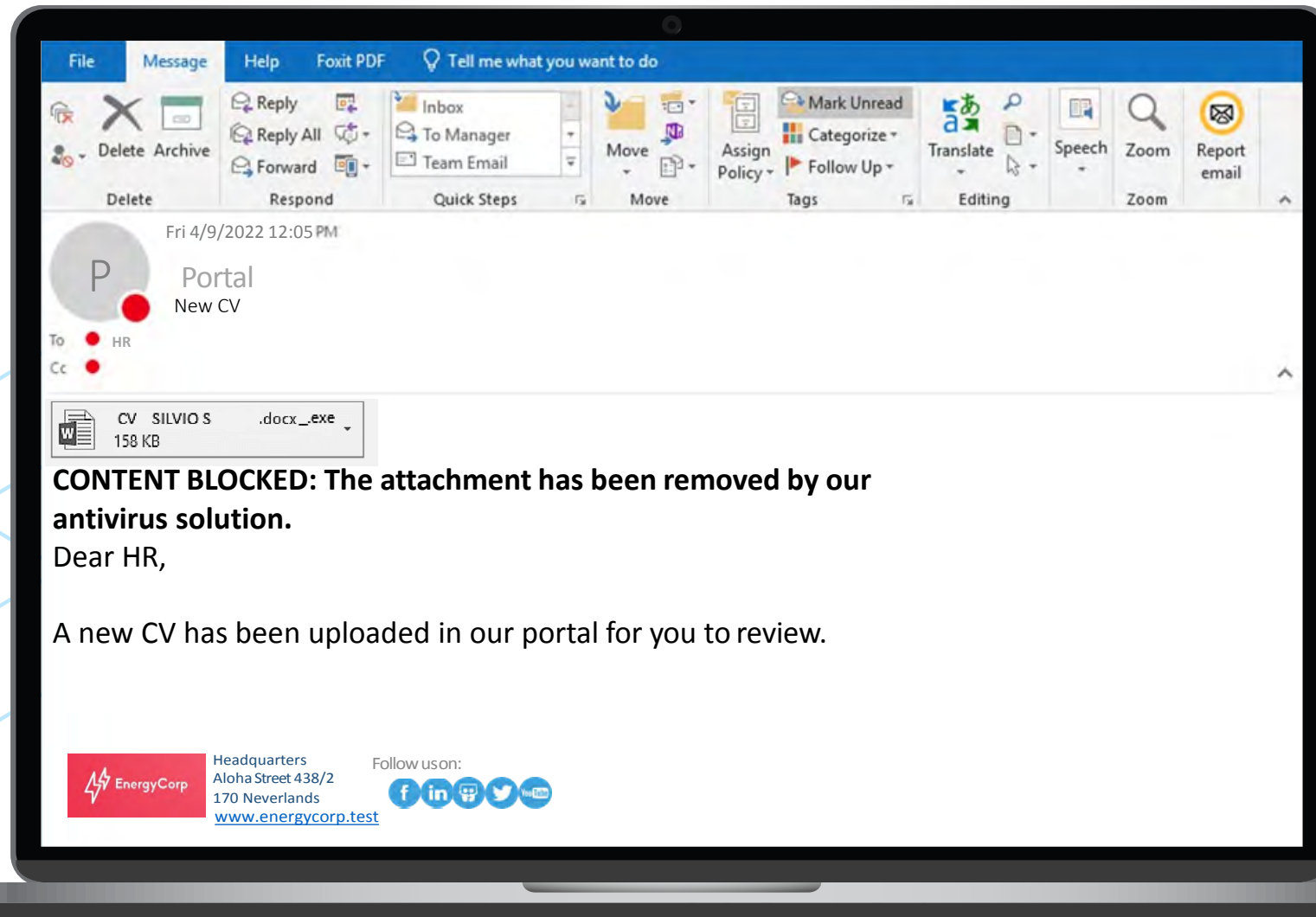
You have **45' minutes** left before all our data are wiped out.

GOOD LUCK!

THE NEWS

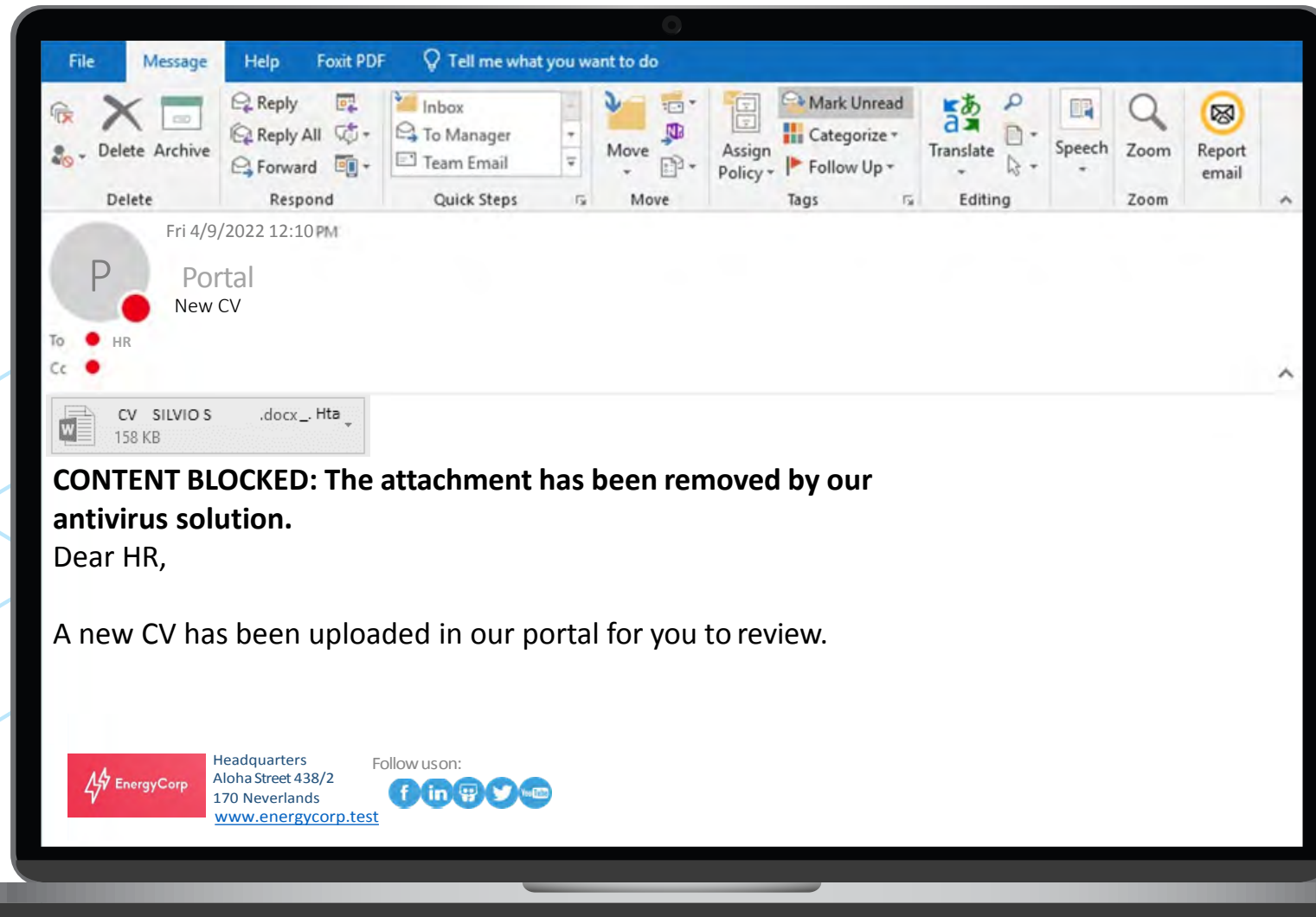


SUSPICIOUS MAIL



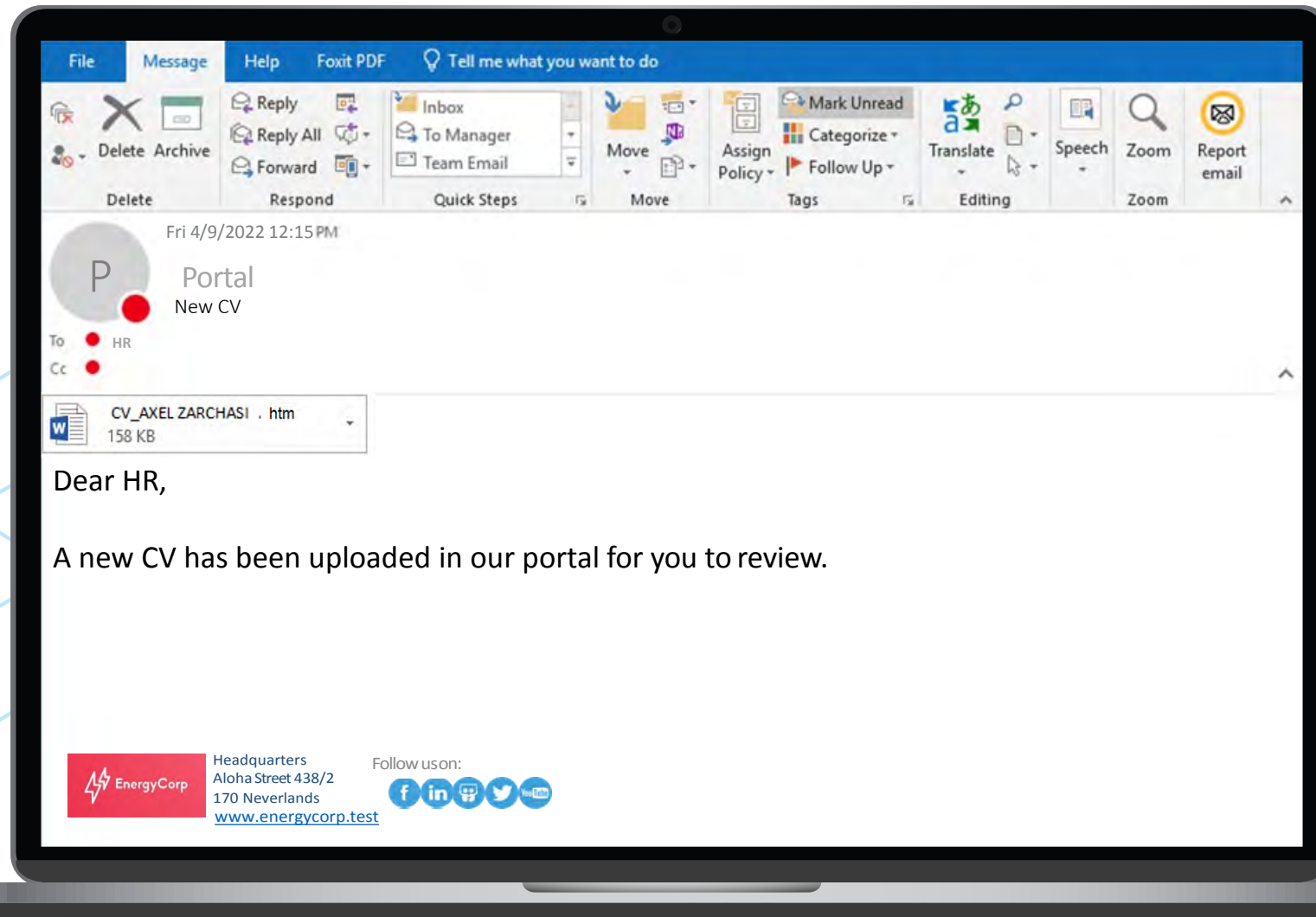
PHISHING ATTACK

SUSPICIOUS MAIL



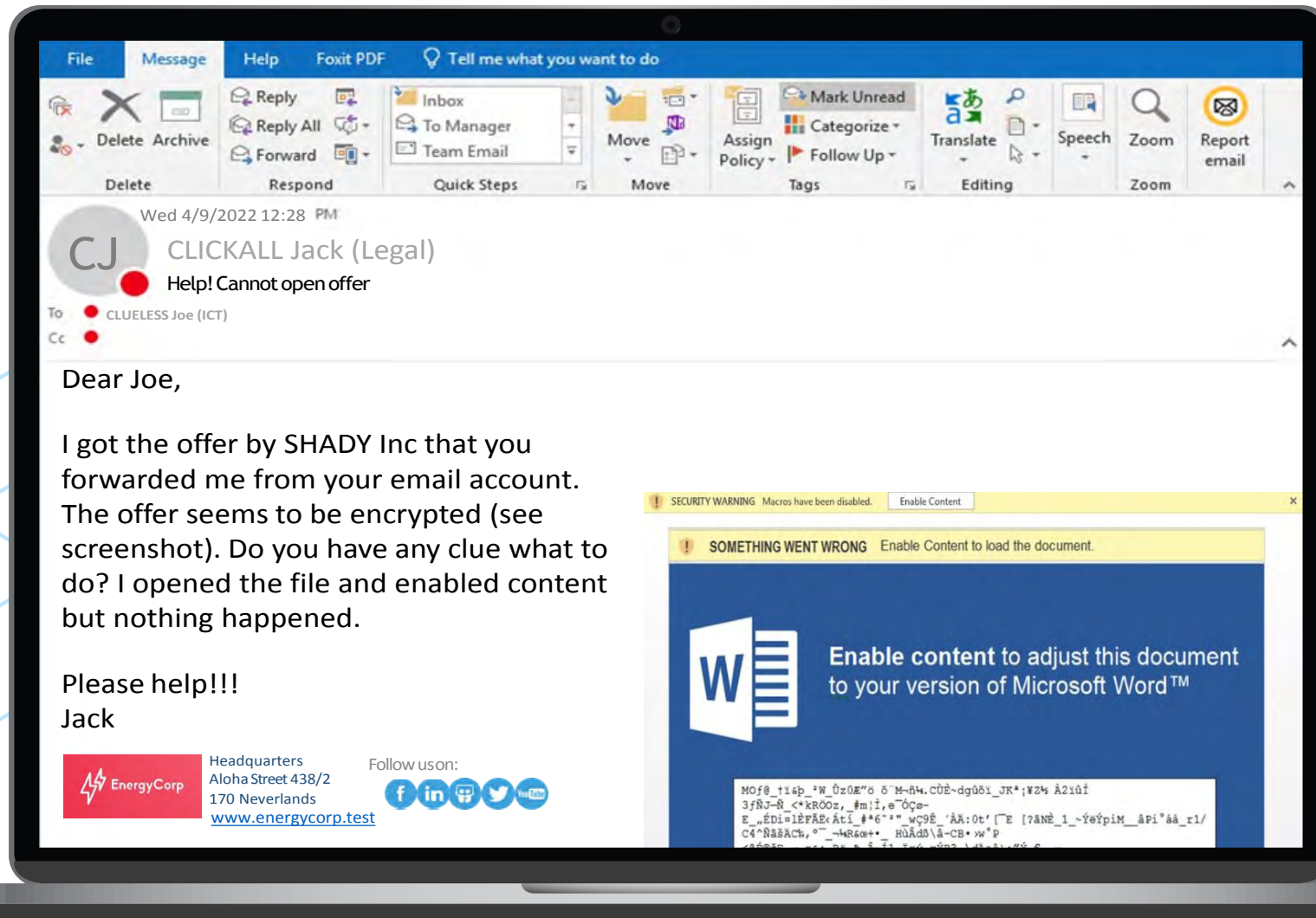
PHISHING ATTACK

SUSPICIOUS MAIL



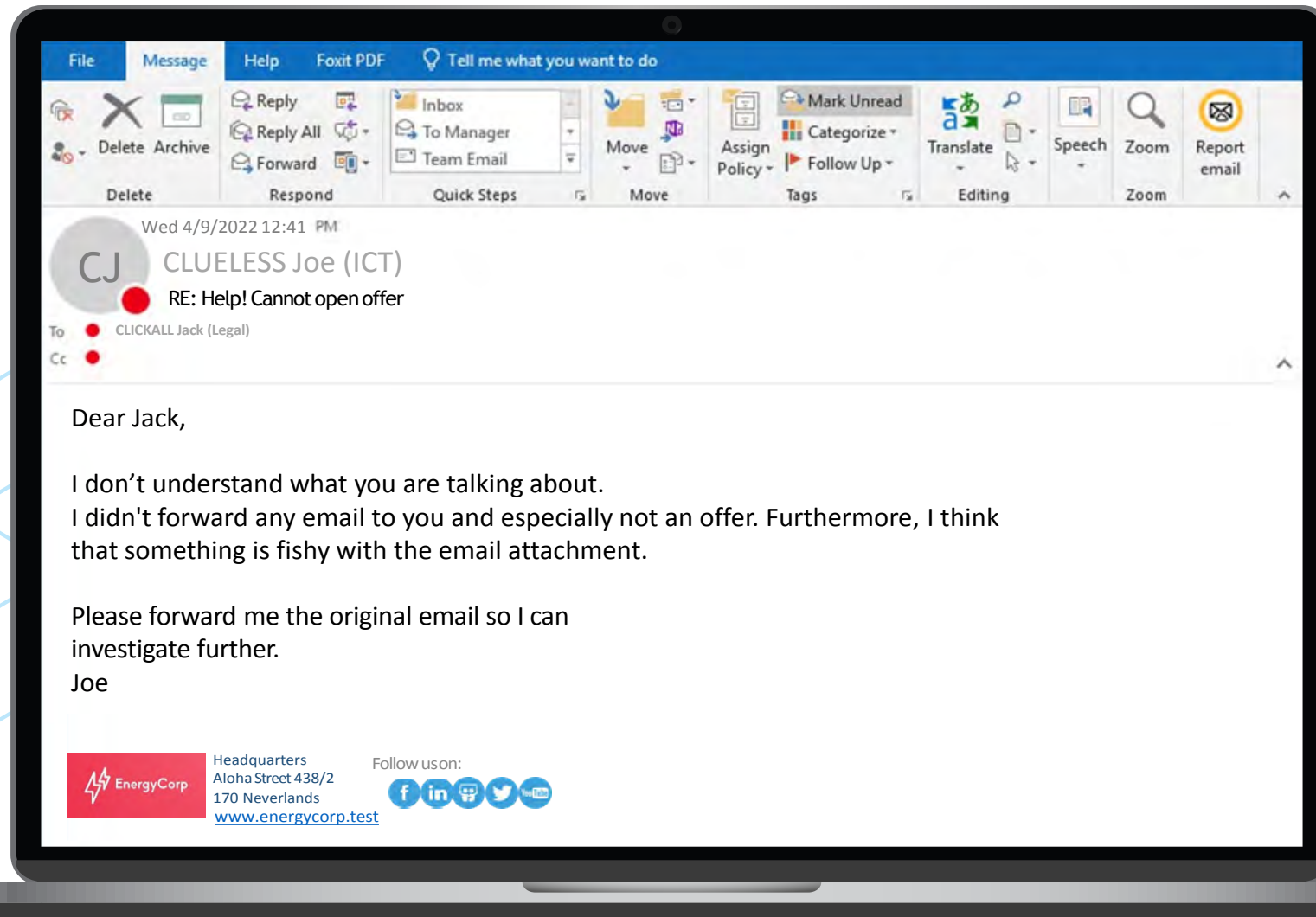
PHISHING ATTACK

SUSPICIOUS MAIL



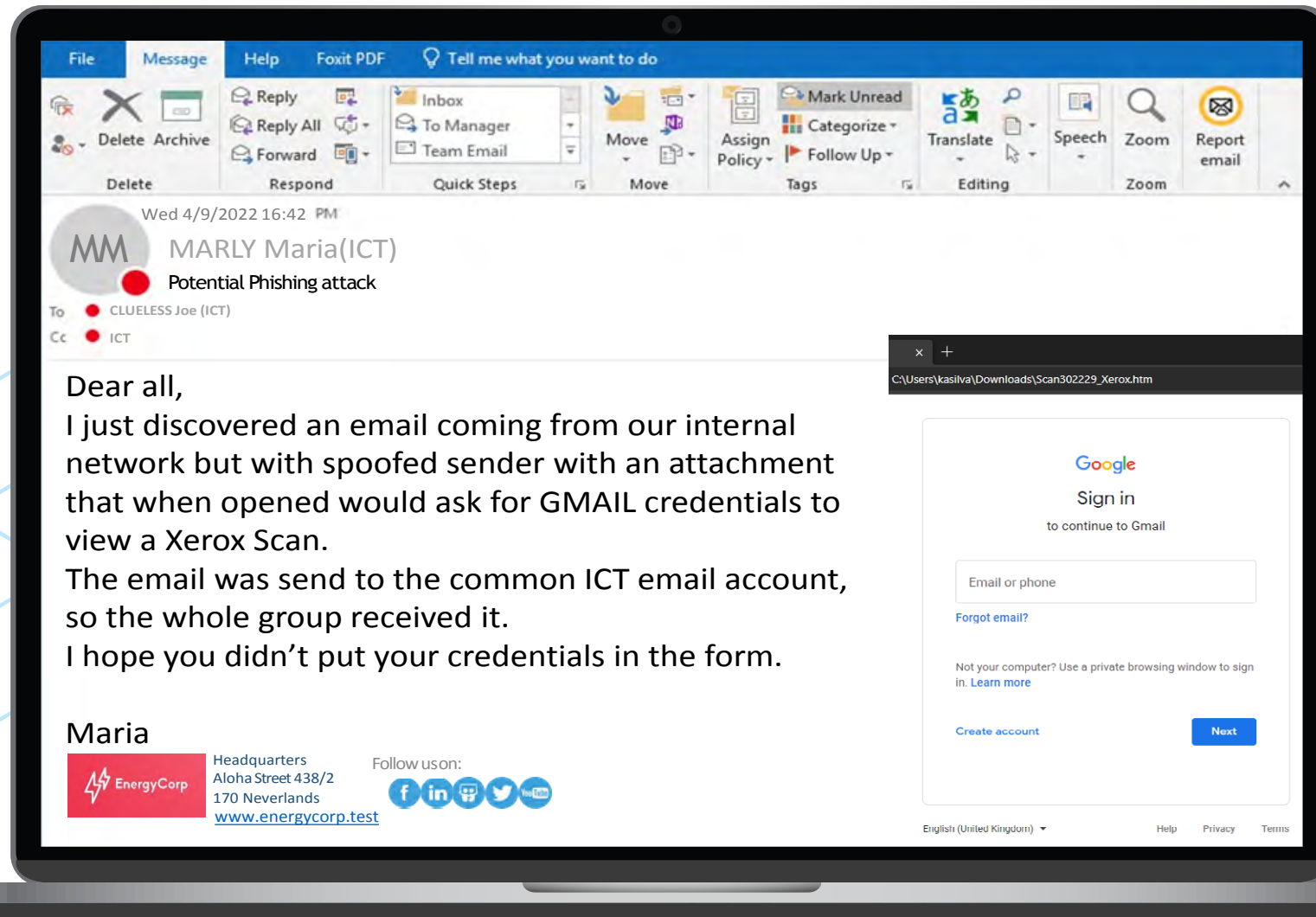
PHISHING ATTACK

SUSPICIOUS MAIL



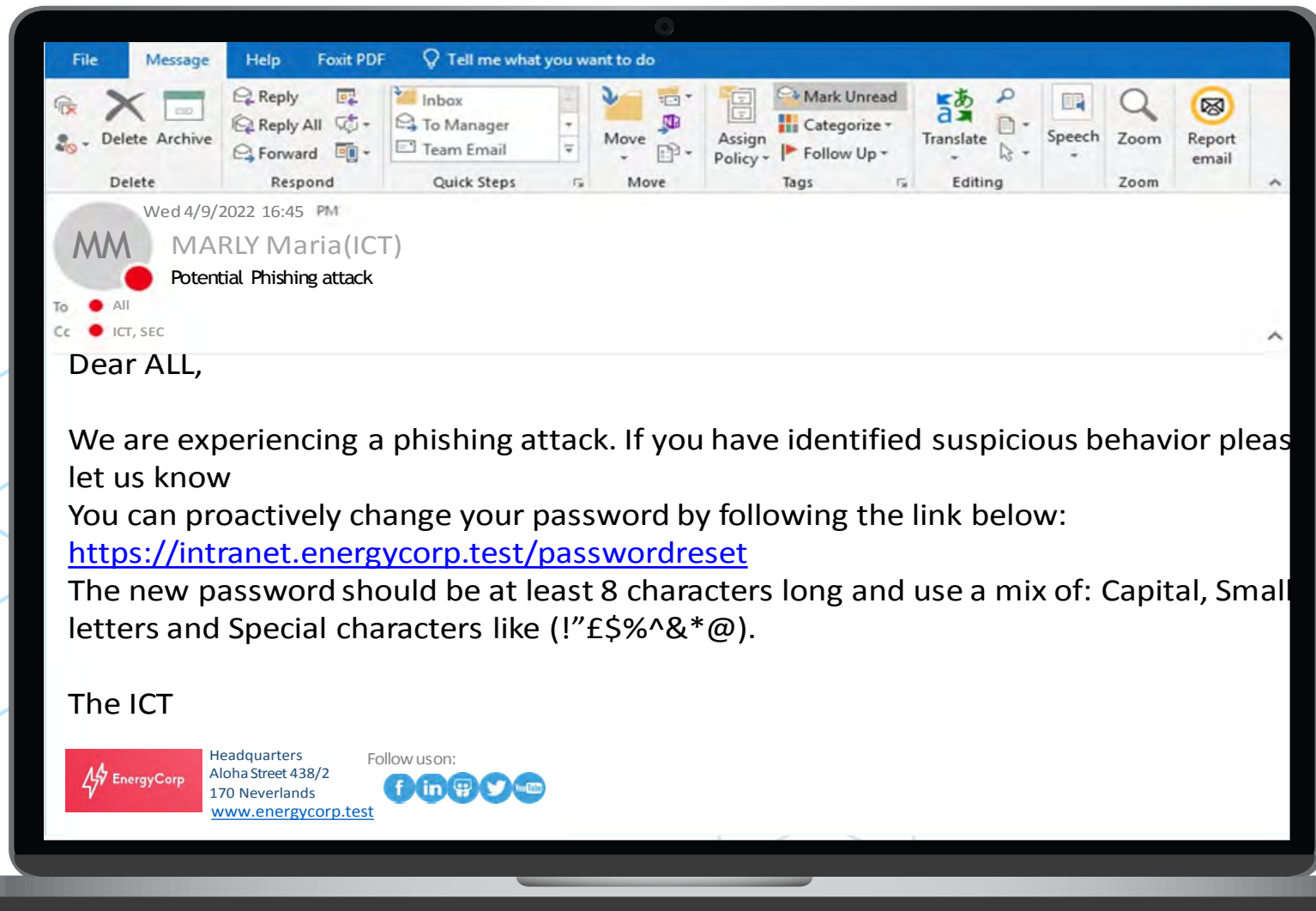
PHISHING ATTACK

SUSPICIOUS MAIL



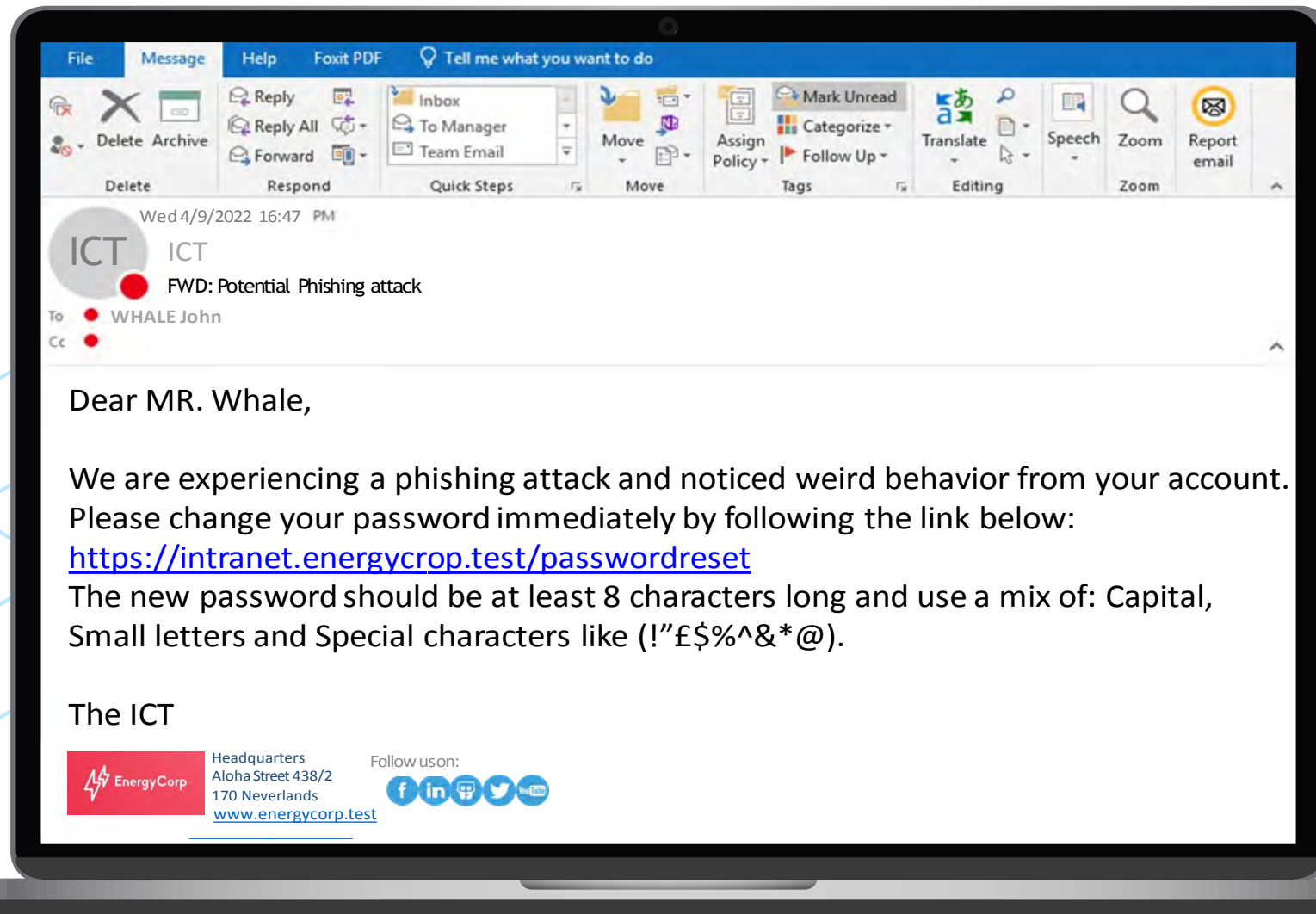
PHISHING ATTACK

SUSPICIOUS MAIL



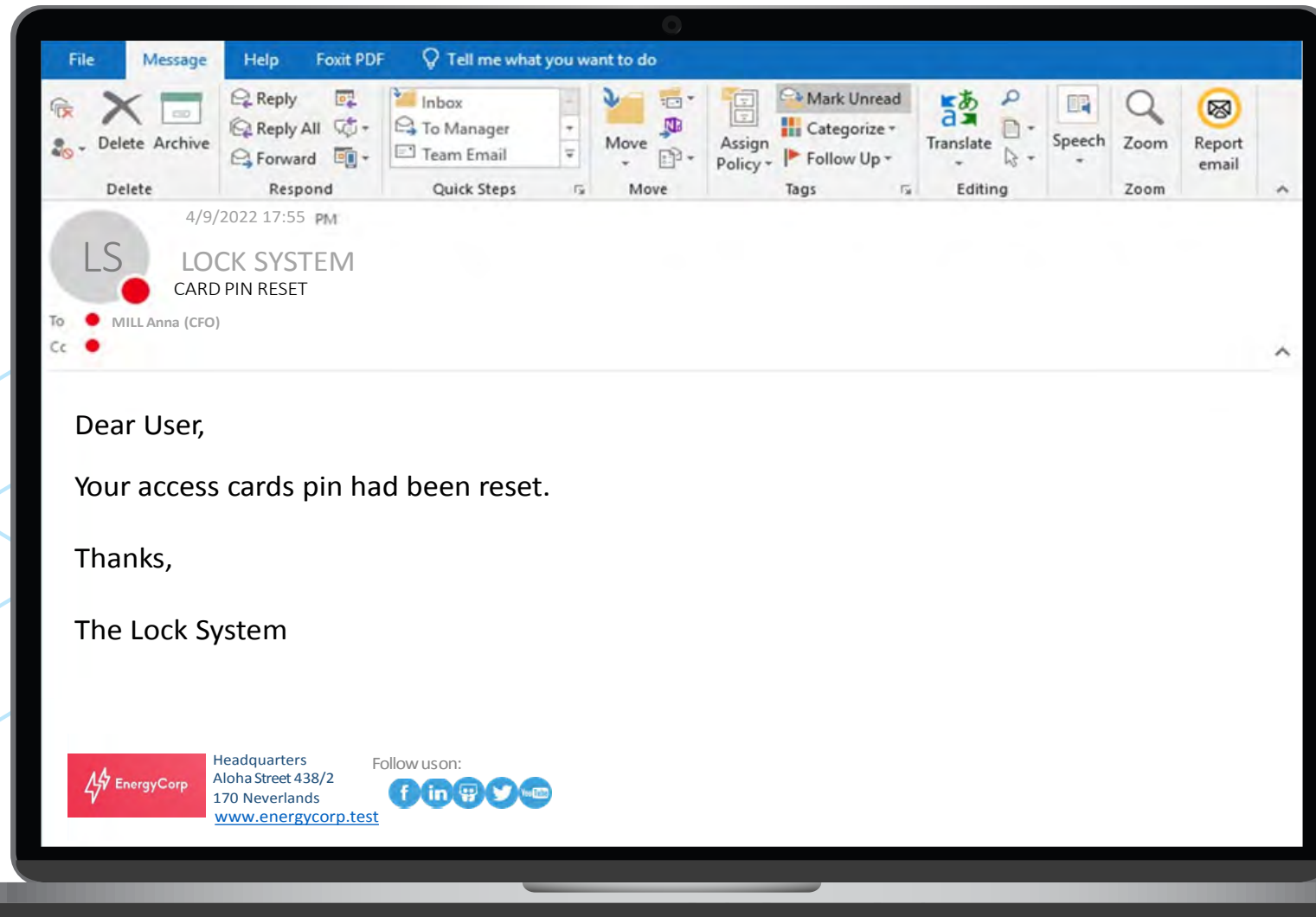
PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



PHISHING ATTACK

MORE SOCIAL MEDIA POSTS

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_ENERGYCORPSE

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



FAKE NEWS

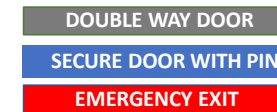
ACCESS LOGS – ENERGYCORP



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



UNAUTHORISED ACCESS

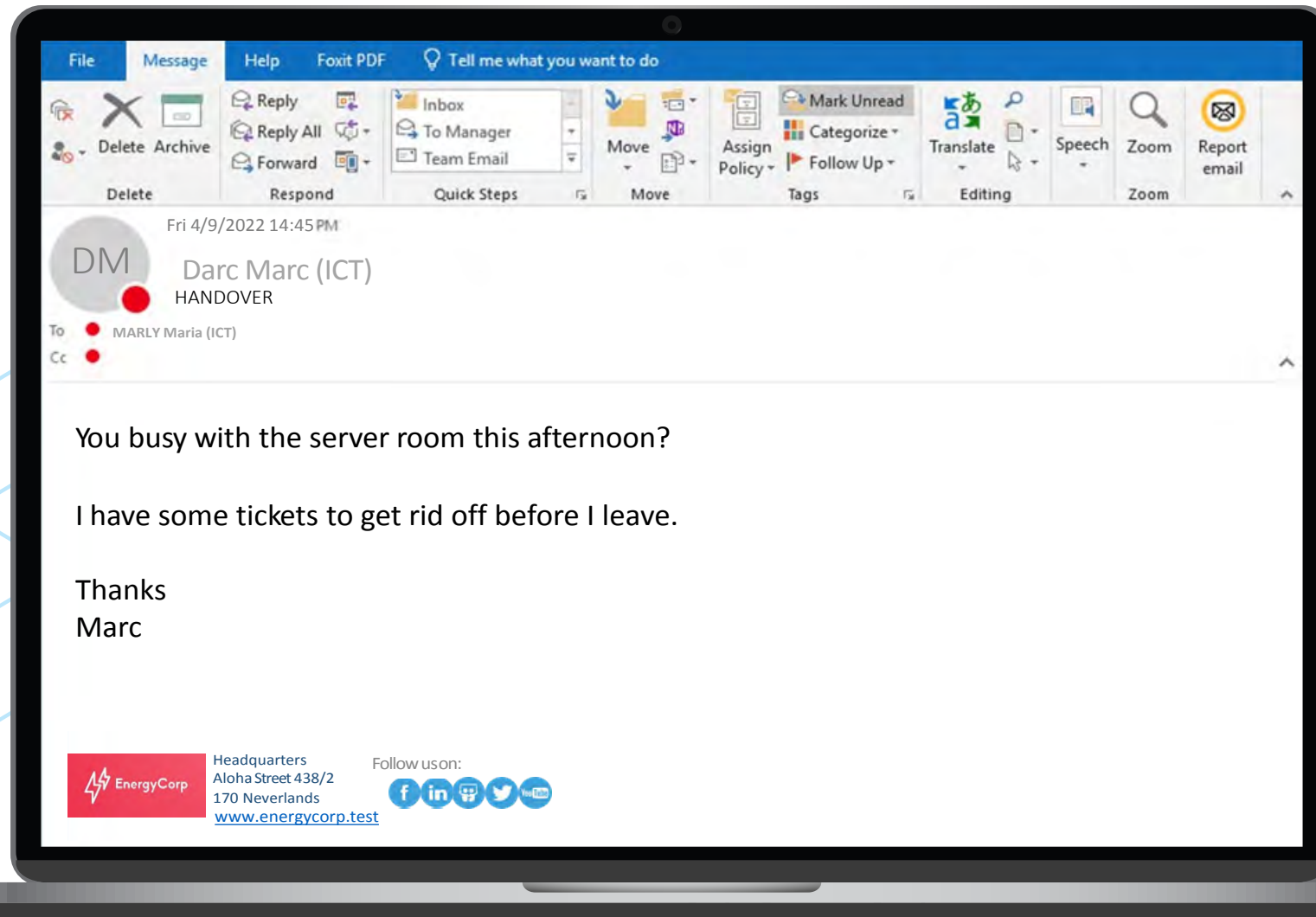


FULL EMPLOYEES LIST

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

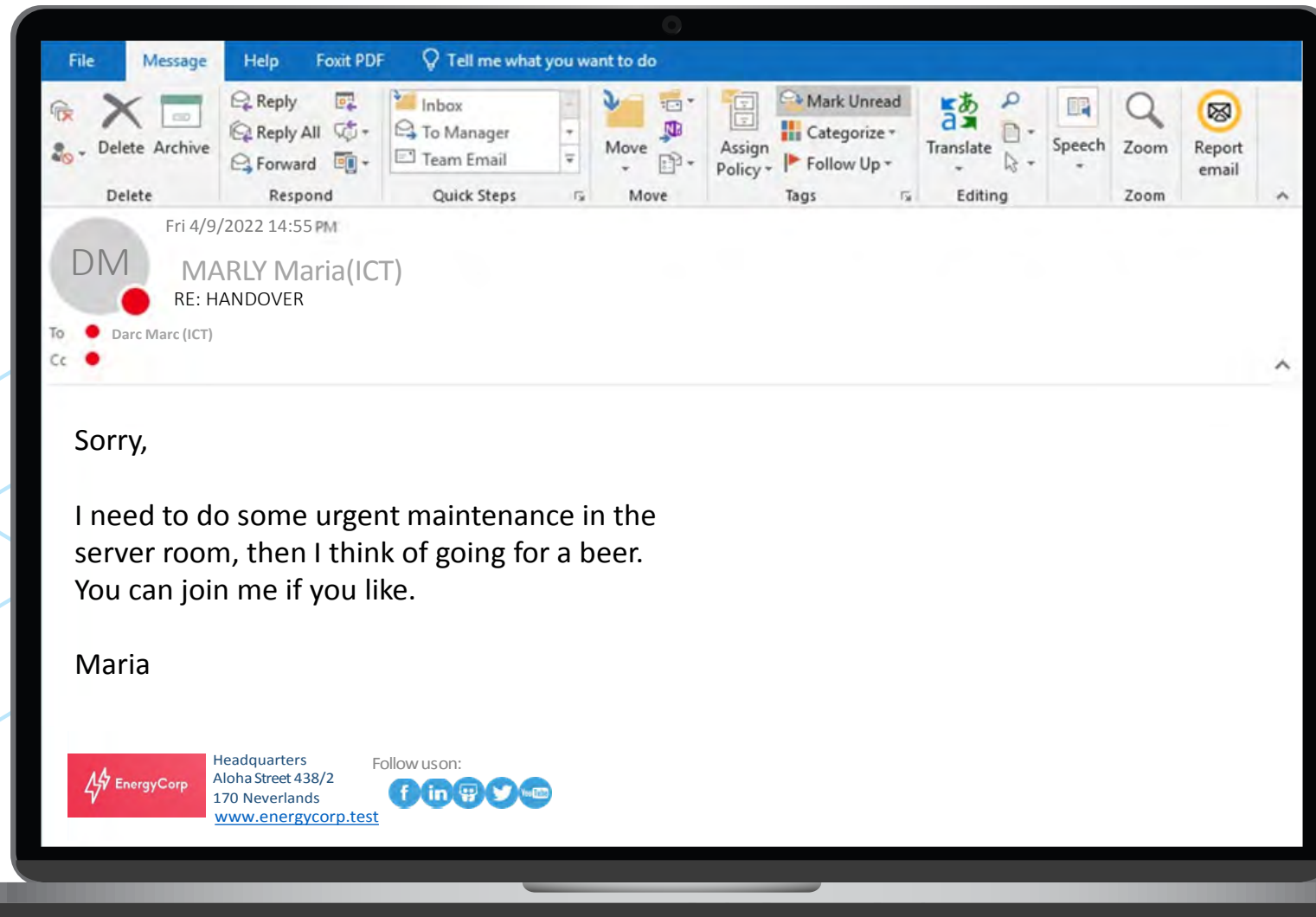


SUSPICIOUS MAIL



PHISHING ATTACK

SUSPICIOUS MAIL



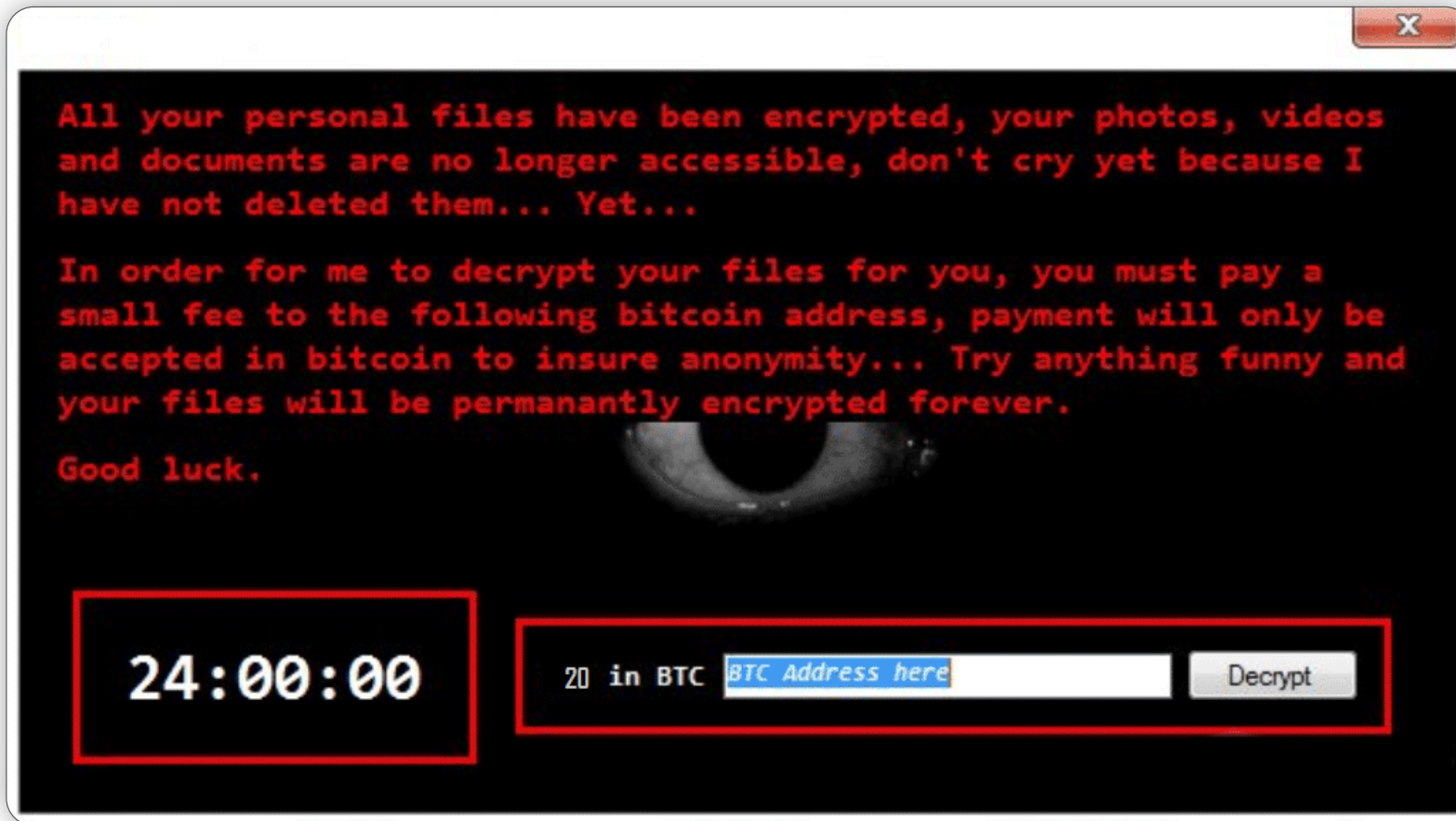
PHISHING ATTACK

MORE (SOCIAL) MEDIA POSTS





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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



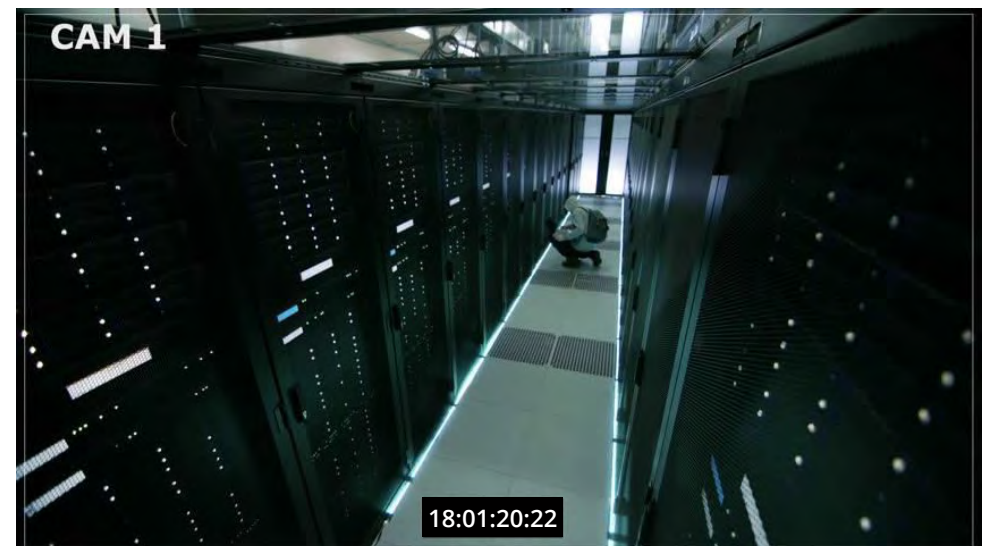
RANSOMWARE

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?

[illegible]

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