AR-IN-A-BOX

MINI GAME

EnergyCorp hacked

BE THE STRONGEST LINK
BREAK THE KILLCHAIN

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DISCLAIMER

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.

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.

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.

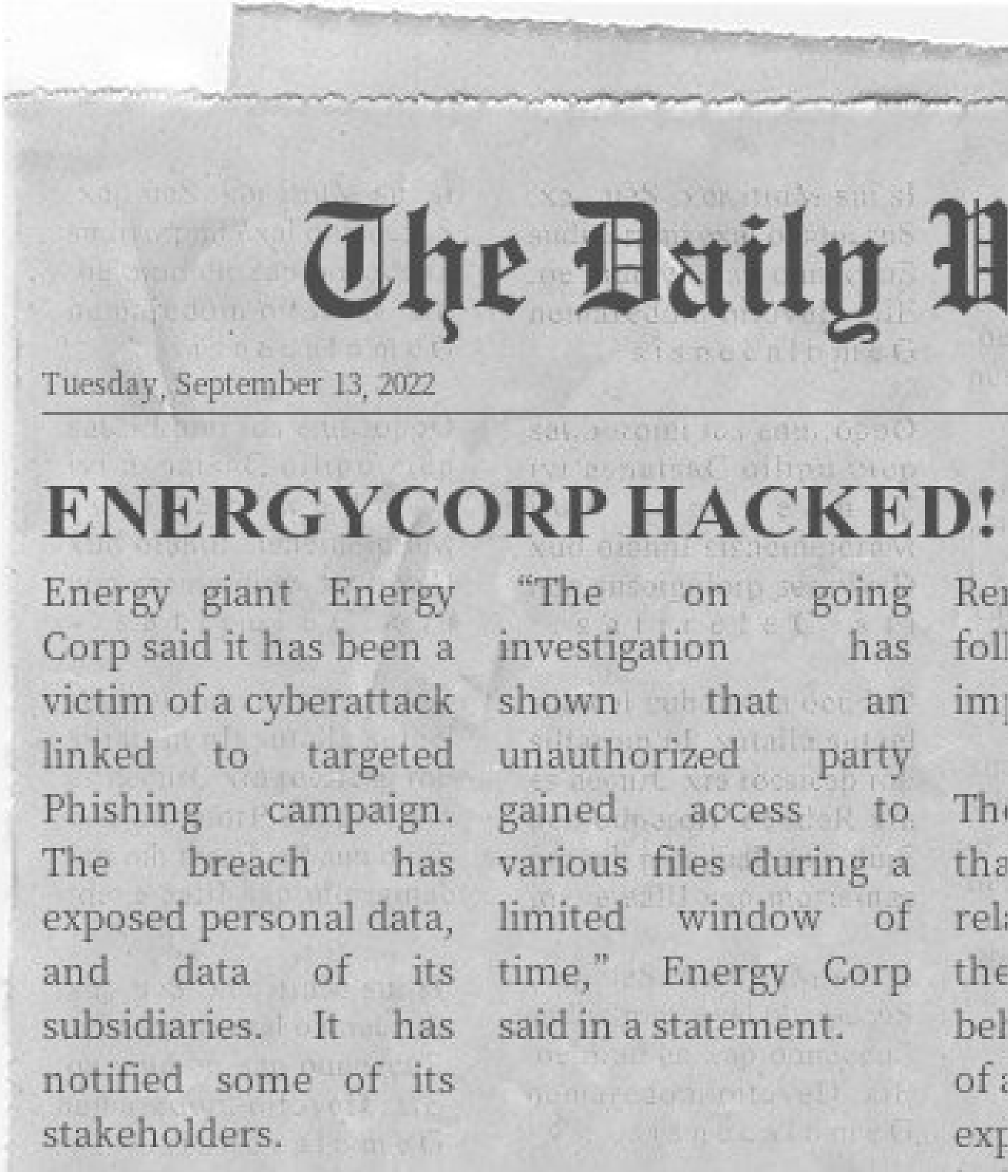
The attackers claim that they will wipe all data if we don’t pay.

You have **20’ minutes** left before all our data are wiped out.

GOOD LUCK!

THE NEWS

LIVE
BREAKING NEWS
ENERGY GIANT HACKED
14:23
ENERGYCORP HAS BEEN ALLEGEDLY HACKED BY ZAAAP HACKING TEAM. DATA LEAKED



The Daily

Tuesday, September 13, 2022

ENERGYCORP HACKED!

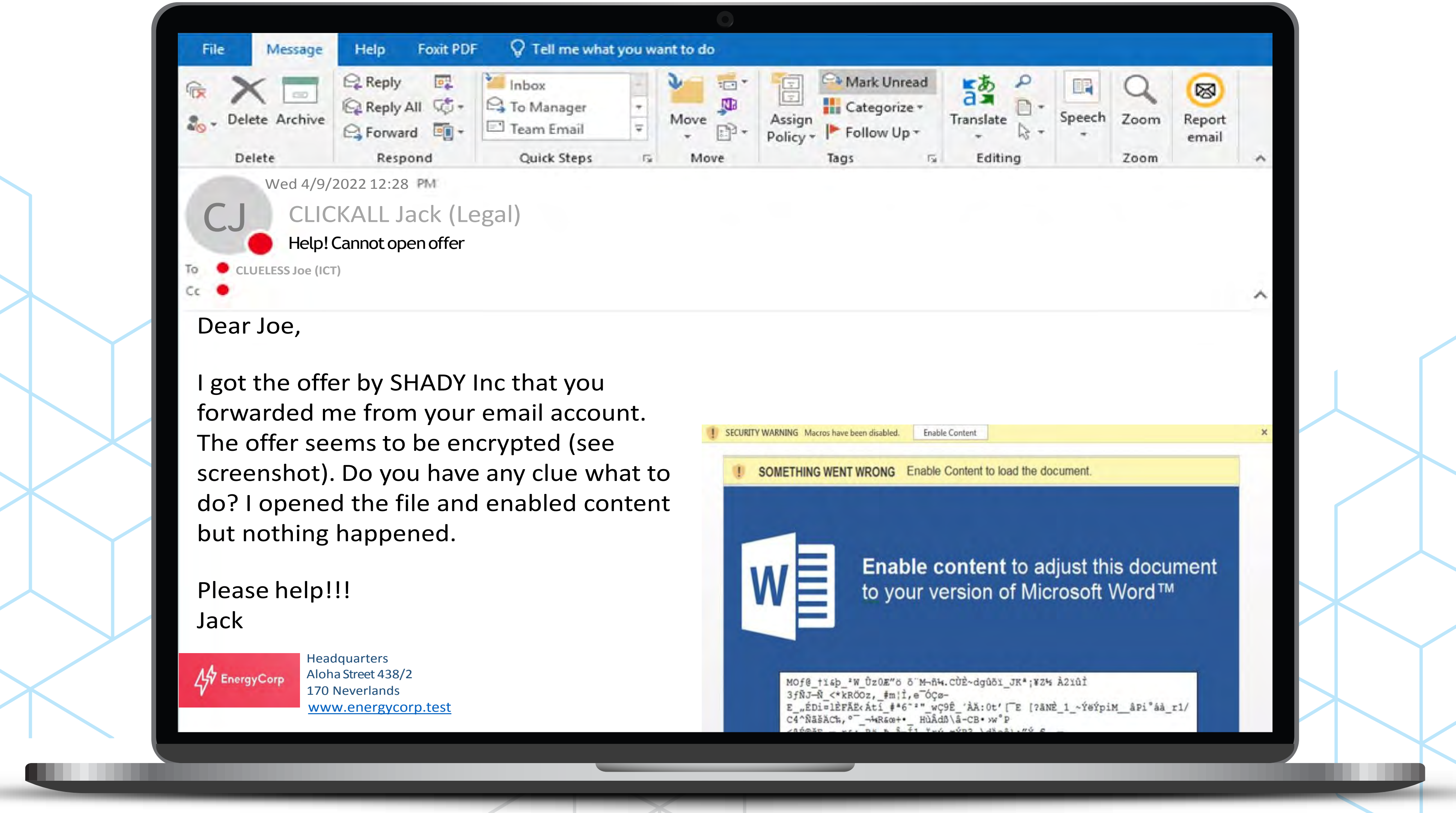
Energy giant Energy Corp said it has been a victim of a cyberattack linked to targeted Phishing campaign. The breach has exposed personal data, and data of its subsidiaries. It has notified some of its stakeholders.

“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.

Re
fol
im

Th
tha
rel
the
bel
of a
exp

SUSPICIOUS MAIL



Wed 4/9/2022 12:28 PM

CLICKALL Jack (Legal)

Help! Cannot open offer

To CLUELESS Joe (ICT)

Cc

Dear Joe,

I got the offer by SHADY Inc that you forwarded me from your email account. The offer seems to be encrypted (see screenshot). Do you have any clue what to do? I opened the file and enabled content but nothing happened.

Please help!!!
Jack

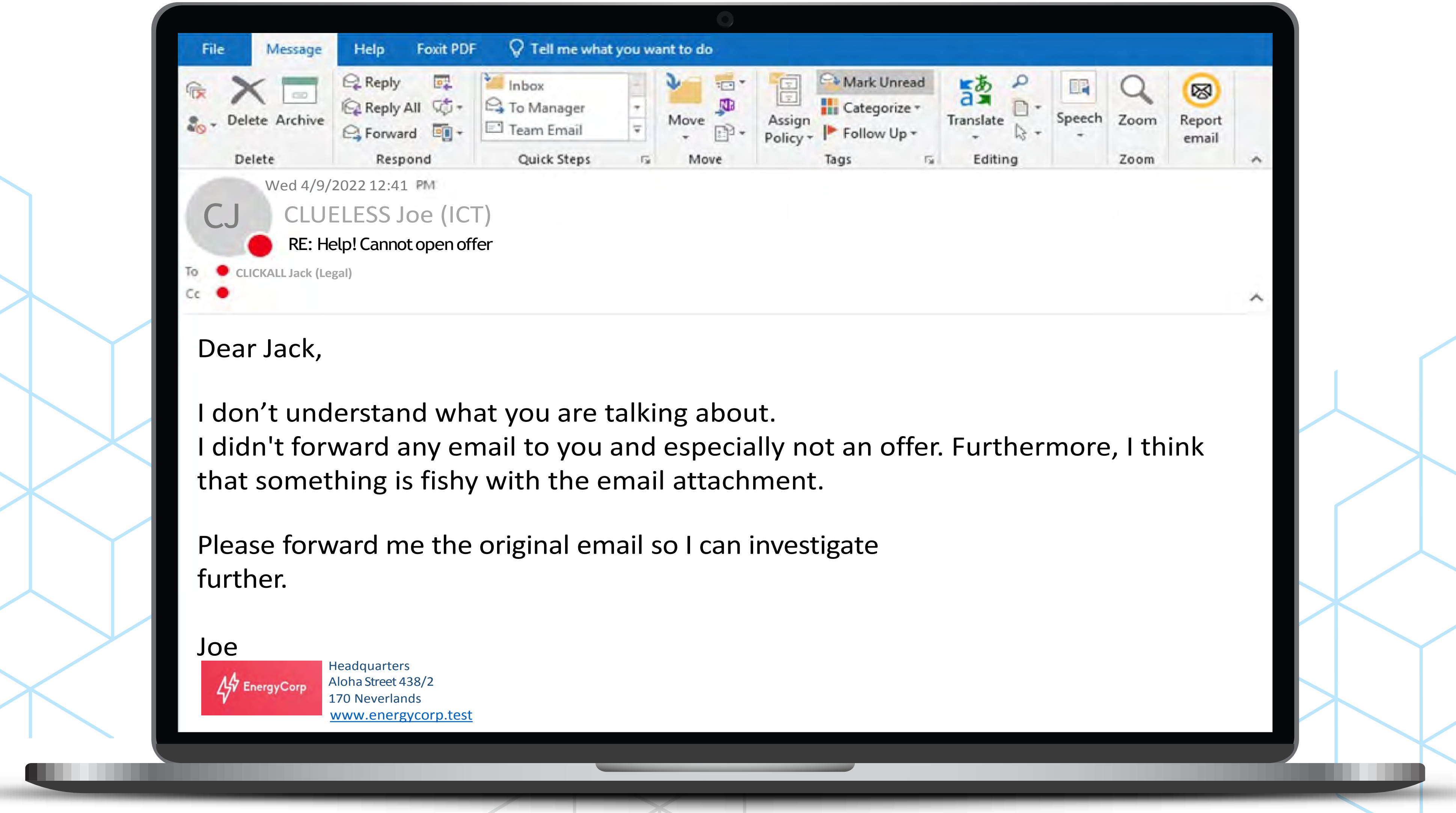
EnergyCorp
Headquarters
Aloha Street 438/2
170 Neverlands
www.energycorp.test

SECURITY WARNING Macros have been disabled. Enable Content

SOMETHING WENT WRONG Enable Content to load the document.

Enable content to adjust this document to your version of Microsoft Word™

SUSPICIOUS MAIL



Wed 4/9/2022 12:41 PM

CLUELESS Joe (ICT)

RE: Help! Cannot open offer

To CLICKALL Jack (Legal)

Cc

Dear Jack,

I don’t understand what you are talking about.
I didn't forward any email to you and especially not an offer. Furthermore, I think that something is fishy with the email attachment.

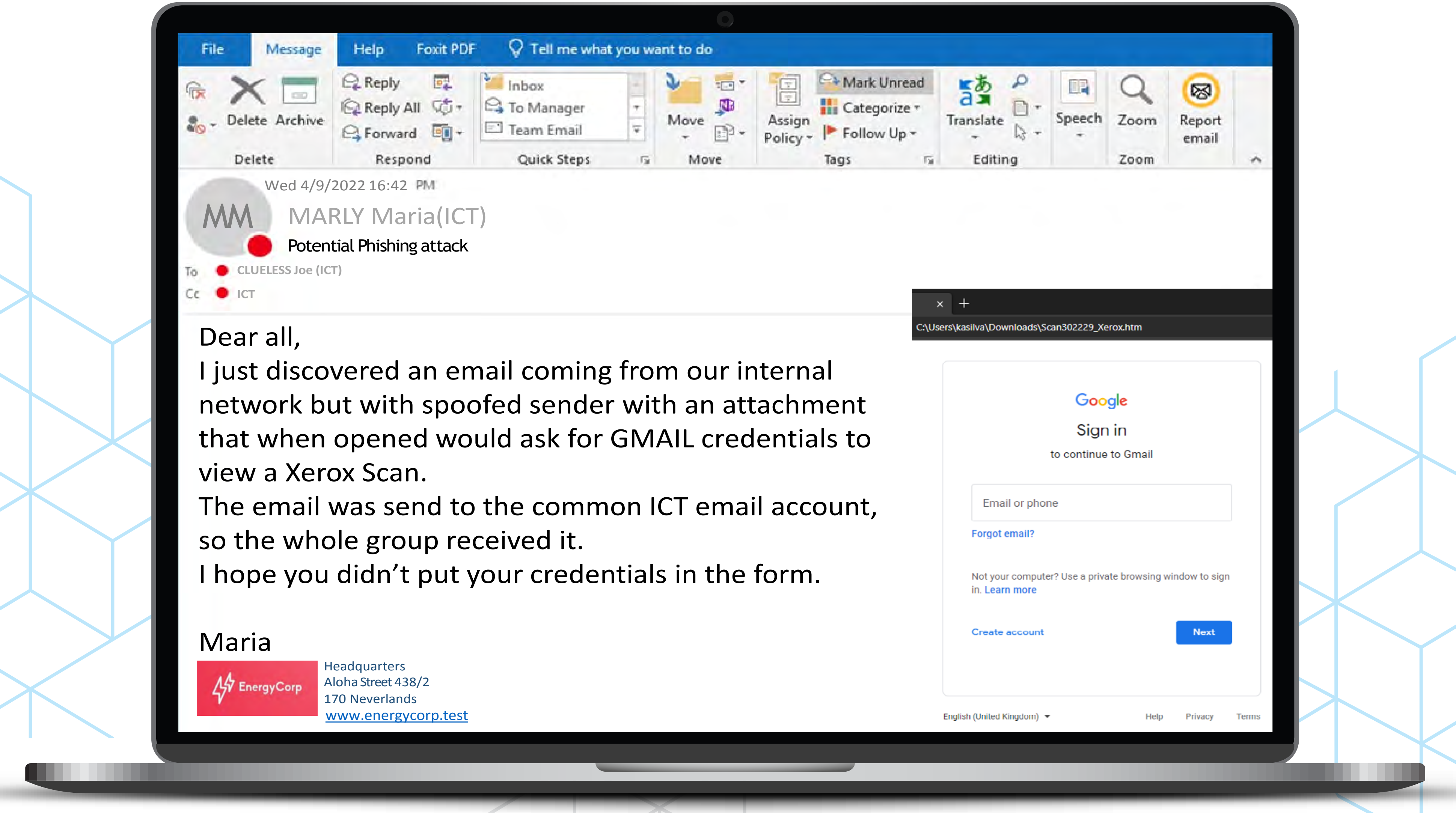
Please forward me the original email so I can investigate further.

Joe

EnergyCorp

Headquarters
Aloha Street 438/2
170 Neverlands
www.energycorp.test

SUSPICIOUS MAIL



Wed 4/9/2022 16:42 PM

MARLY Maria(ICT)

Potential Phishing attack

To ● CLUELESS Joe (ICT)

Cc ● ICT

Dear all,

I just discovered an email coming from our internal network but with spoofed sender with an attachment that when opened would ask for GMAIL credentials to view a Xerox Scan.

The email was send to the common ICT email account, so the whole group received it.

I hope you didn't put your credentials in the form.

Maria

EnergyCorp

Headquarters
Aloha Street 438/2
170 Neverlands
www.energycorp.test

C:\Users\kasilva\Downloads\Scan302229_Xerox.htm

Google

Sign in

to continue to Gmail

Email or phone

Forgot email?

Not your computer? Use a private browsing window to sign in. Learn more

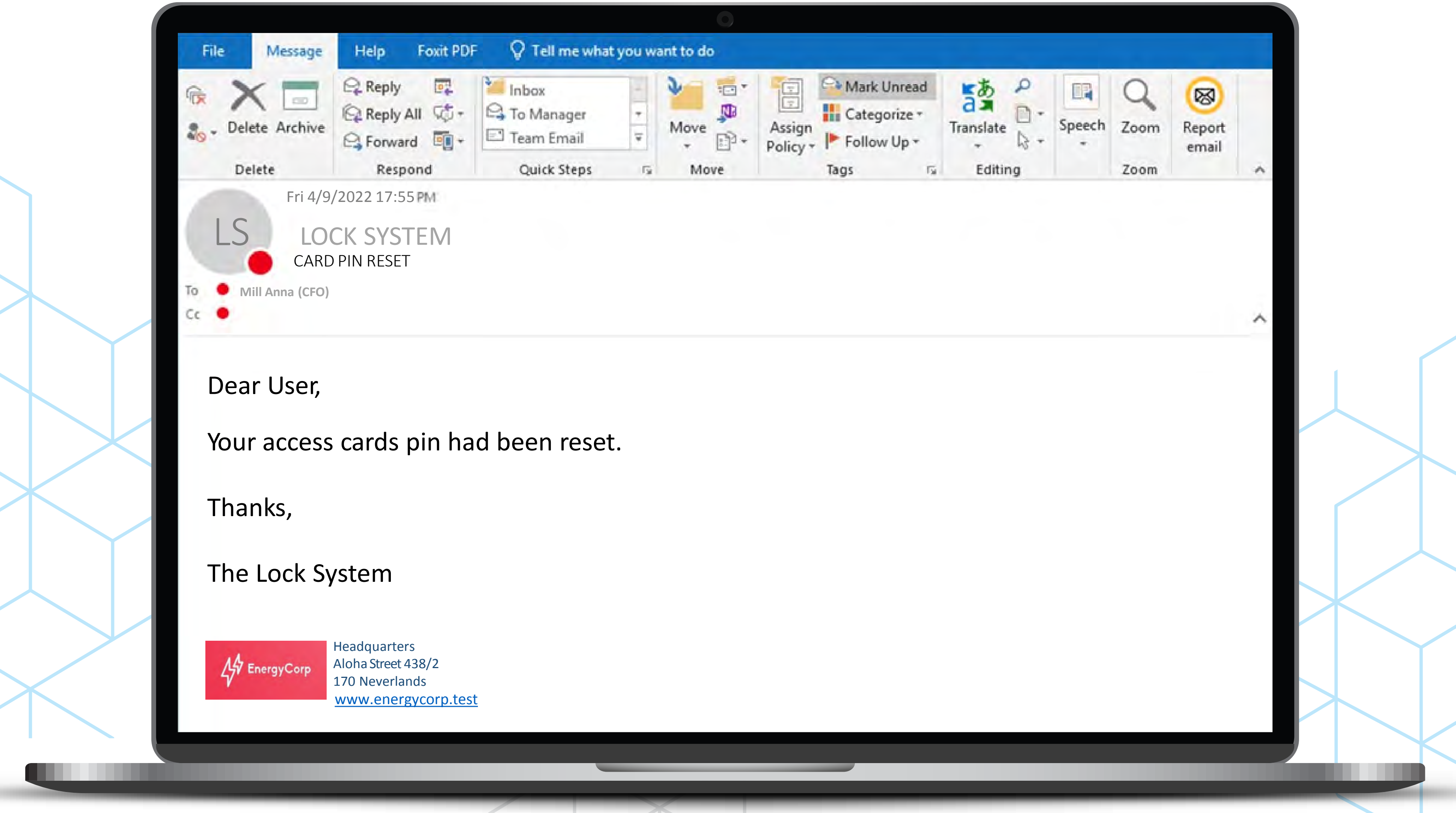
Create account

Next

English (United Kingdom)

Help Privacy Terms

SUSPICIOUS MAIL



Fri 4/9/2022 17:55 PM

LOCK SYSTEM

CARD PIN RESET

To ● Mill Anna (CFO)

Cc ●

Dear User,

Your access cards pin had been reset.

Thanks,

The Lock System

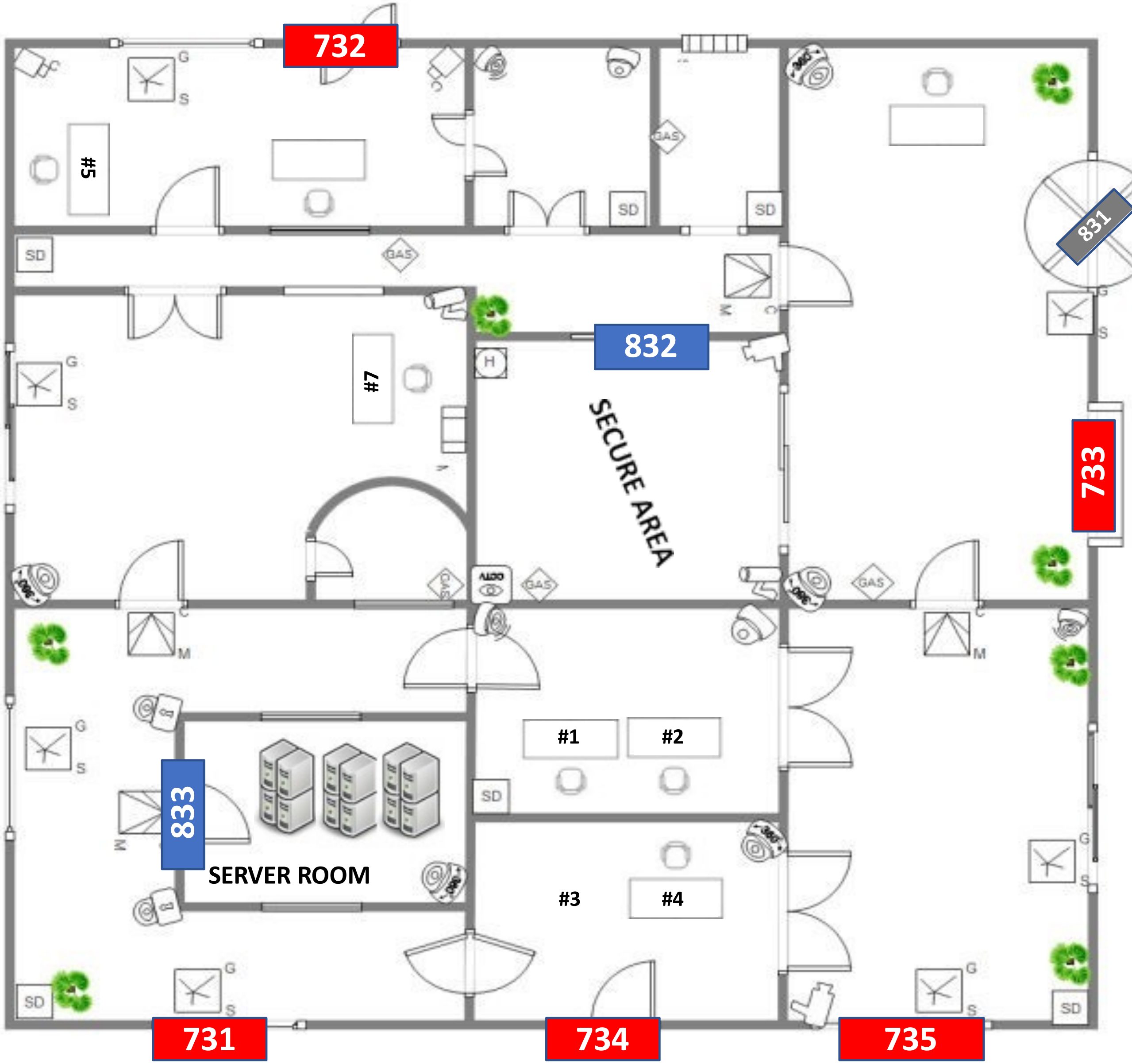
EnergyCorp

Headquarters
Aloha Street 438/2
170 Neverlands
www.energycorp.test

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

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

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

HOW DOES VIGENERE WORK – EXAMPLE

To encrypt:

SECRET PHRASE

Key:

LOCKME

ENCRYPTION MECHANISM:

SECRETPHRASE

LOCKMELOCKME

DSEBQXAVTKEI

To decrypt:

DSEBQXAVTKEI

Key:

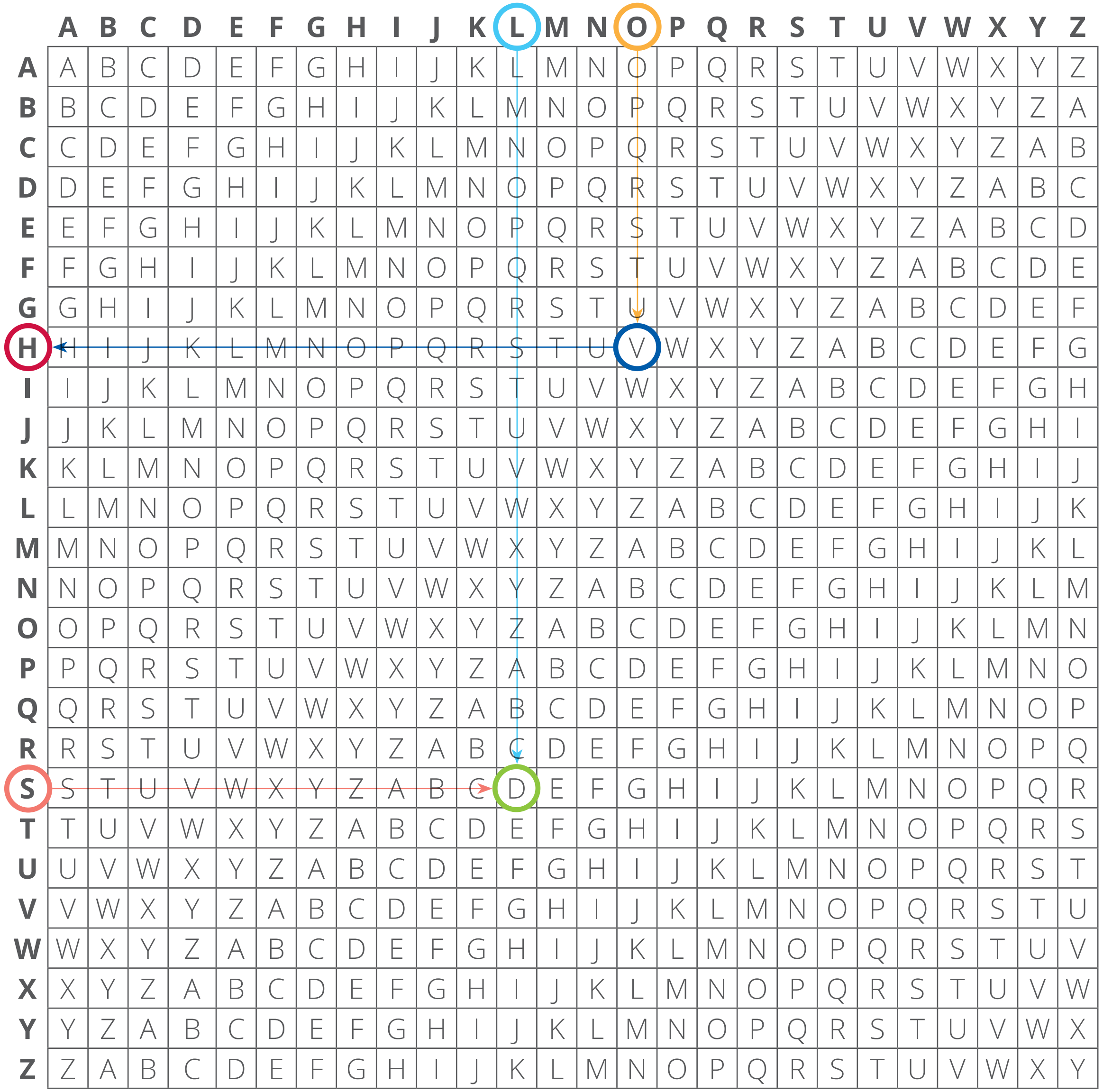
LOCKME

DECRYPTION MECHANISM:

LOCKMELOCKME

DSEBQXAVTKEI

SECRETPHRASE

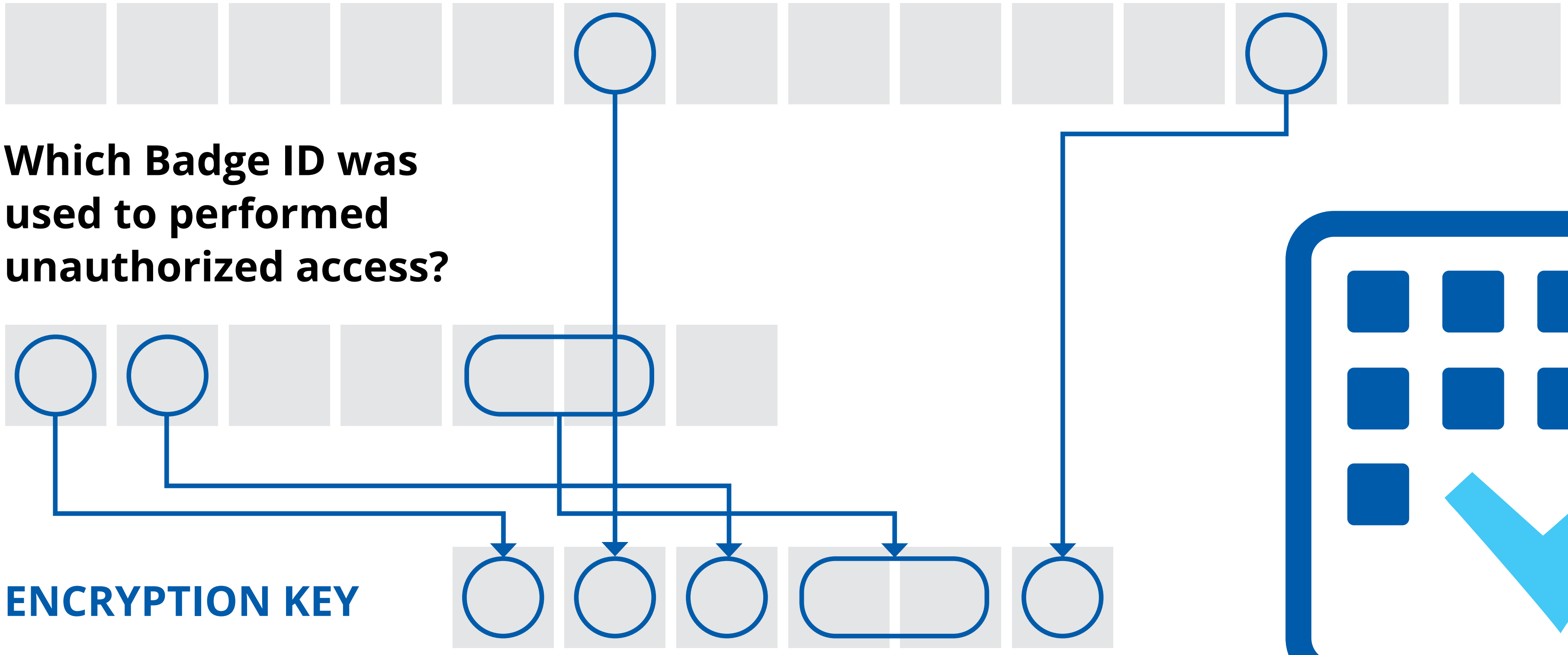


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

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?

ANSWER SHEET

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