AR-IN-A-BOX

MINI GAME

Online Retail Hack

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 – 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.

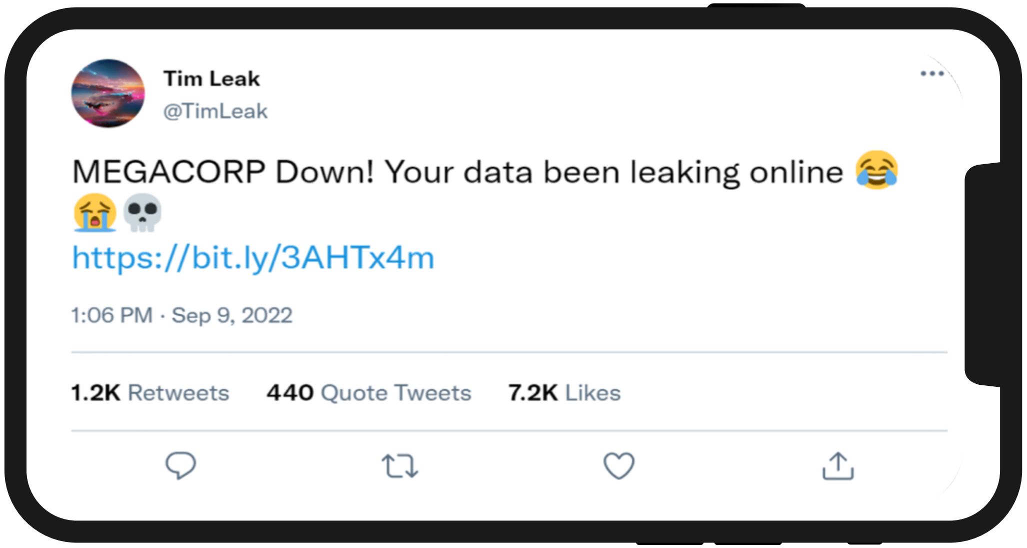
You are the lead Cyber Security Investigator recruited to provide answers on who is behind the hack and try to stop him/her before its too late.

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

You have 30’ minutes left before all our data are wiped out.

GOOD LUCK!

THE NEWS

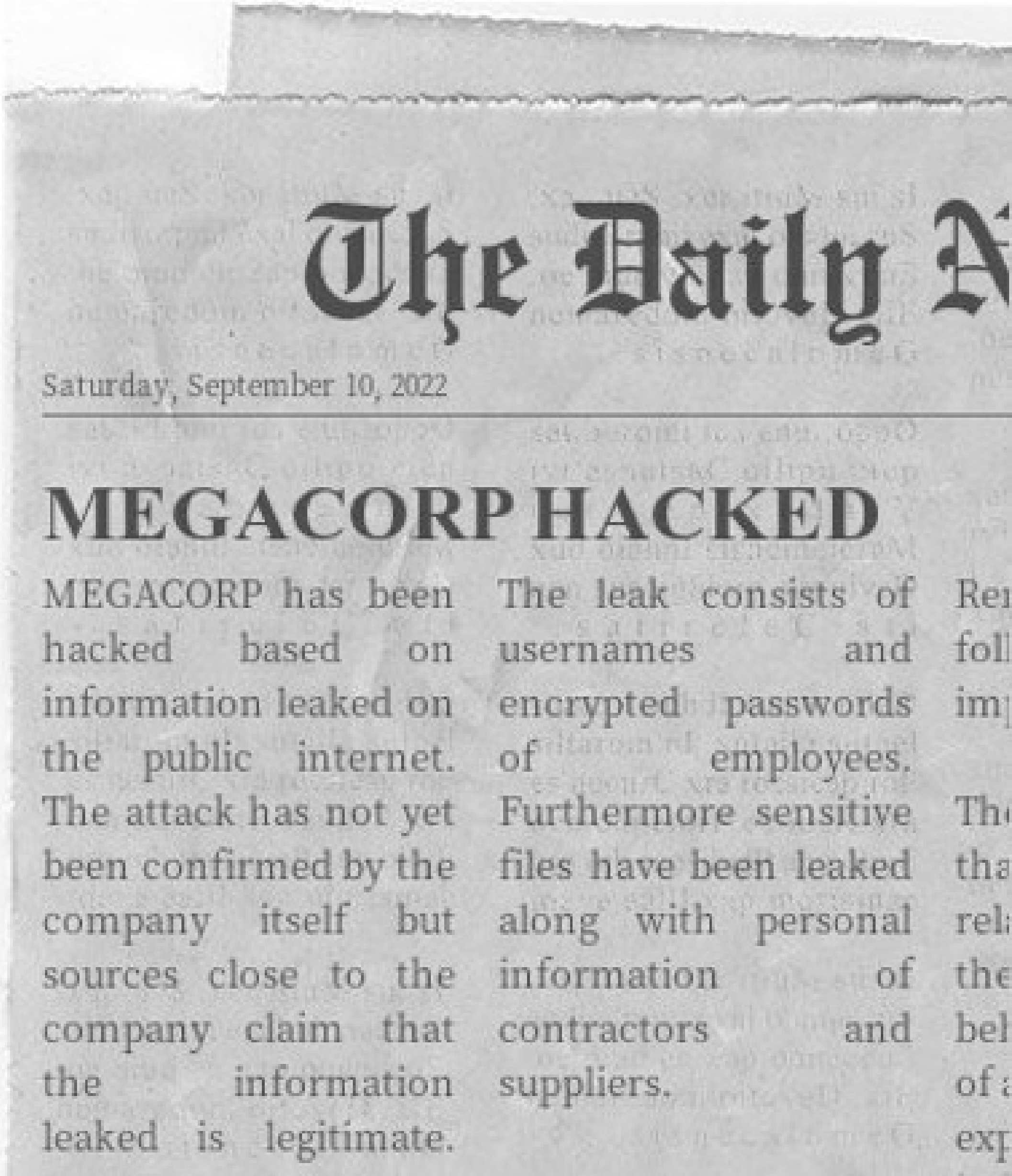


Tim Leak
@TimLeak

MEGACORP Down! Your data been leaking online 😂😭💀
https://bit.ly/3AHTx4m

1:06 PM · Sep 9, 2022

1.2K Retweets **440** Quote Tweets **7.2K** Likes



The Daily

Saturday, September 10, 2022

MEGACORP HACKED

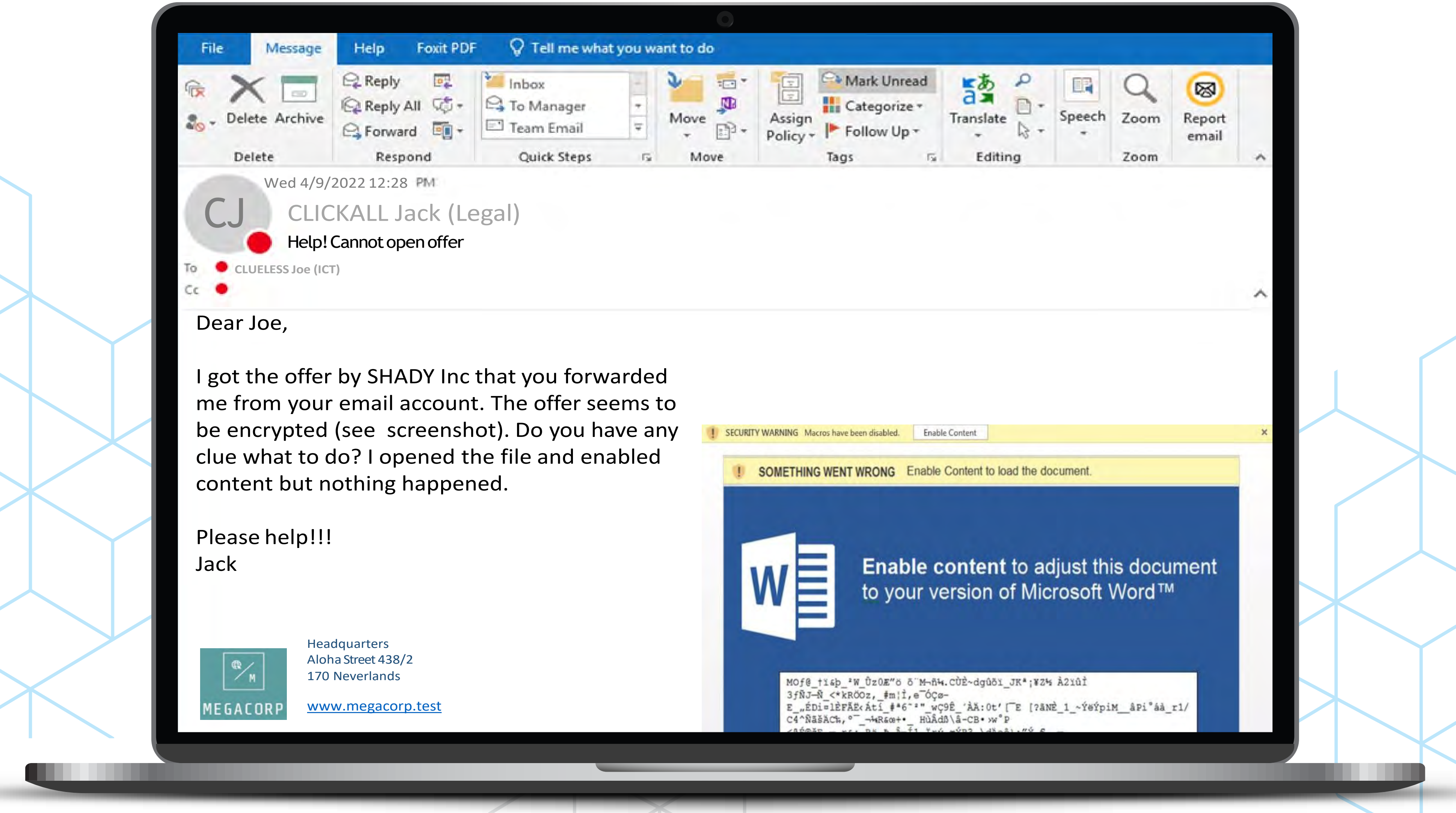
MEGACORP has been hacked based on information leaked on the public internet. The attack has not yet been confirmed by the company itself but sources close to the company claim that the information leaked is legitimate.

The leak consists of usernames and encrypted passwords of employees. Furthermore sensitive files have been leaked along with personal information of contractors and suppliers.

Re
foll
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

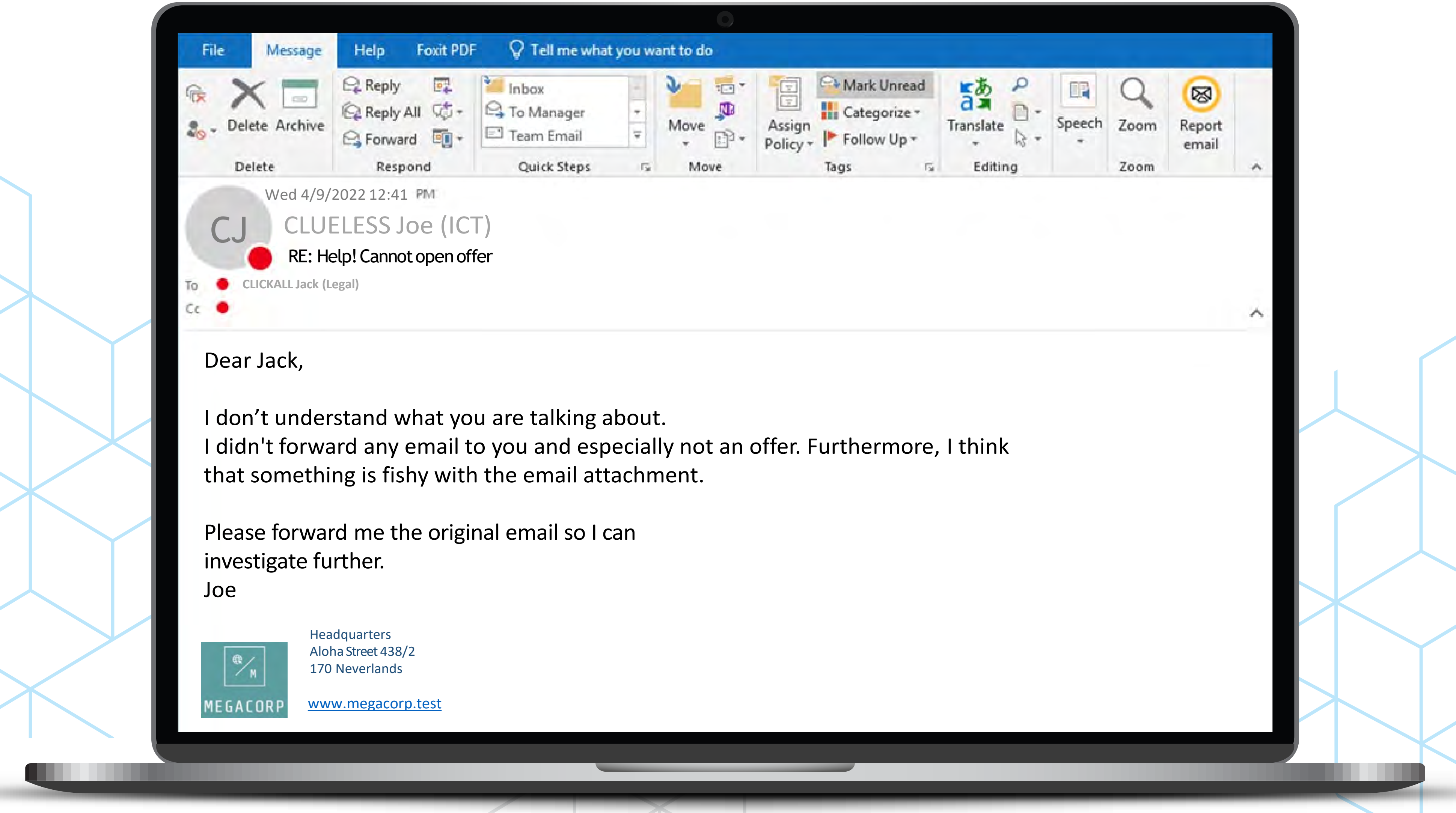
Headquarters
Aloha Street 438/2
170 Neverlands
www.megacorp.test

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

CJ

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.

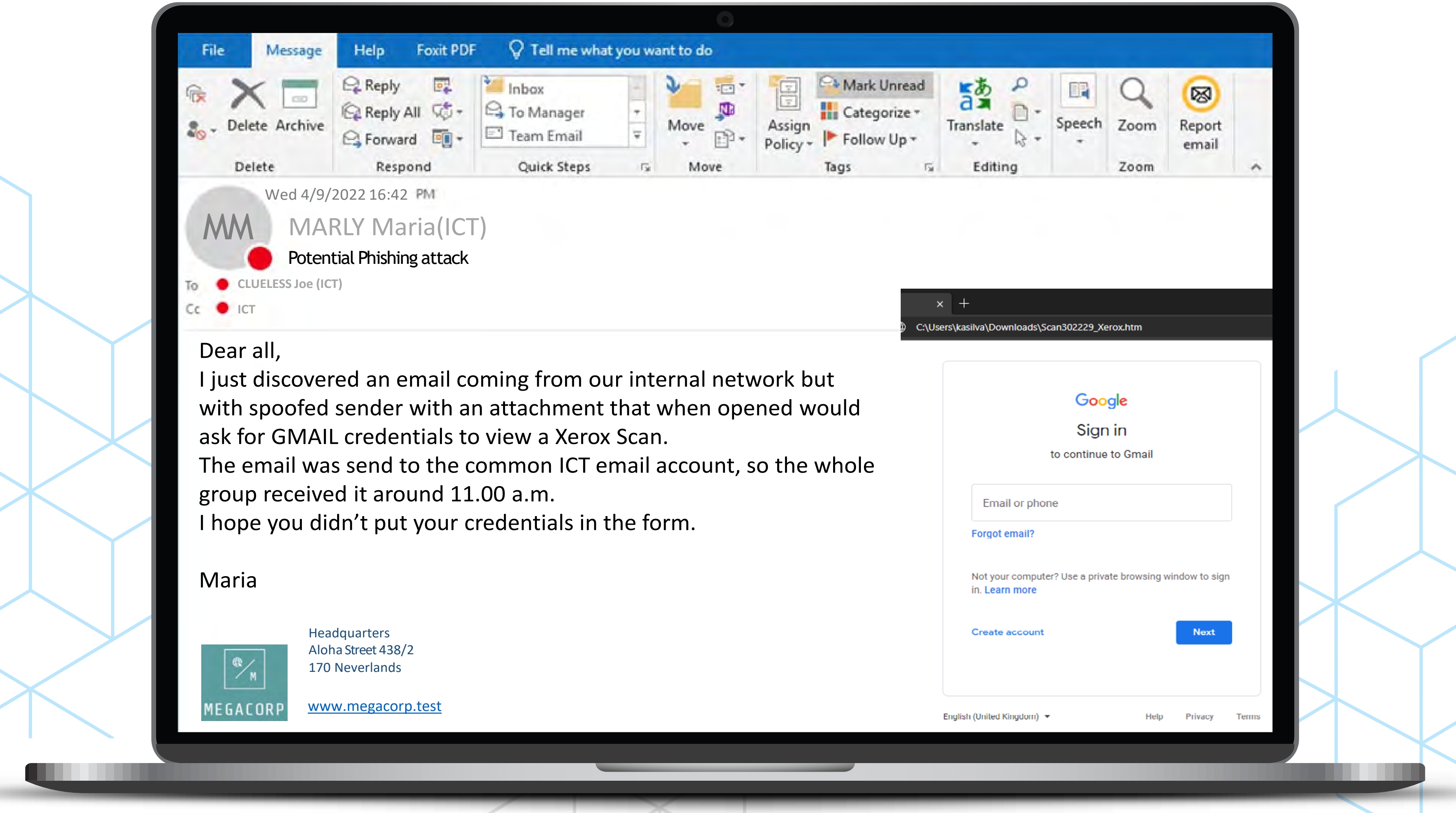
Please forward me the original email so I can investigate further.
Joe

MEGACORP

Headquarters
Aloha Street 438/2
170 Neverlands

www.megacorp.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 around 11.00 a.m.
I hope you didn't put your credentials in the form.

Maria

MEGACORP

Headquarters
Aloha Street 438/2
170 Neverlands

www.megacorp.test

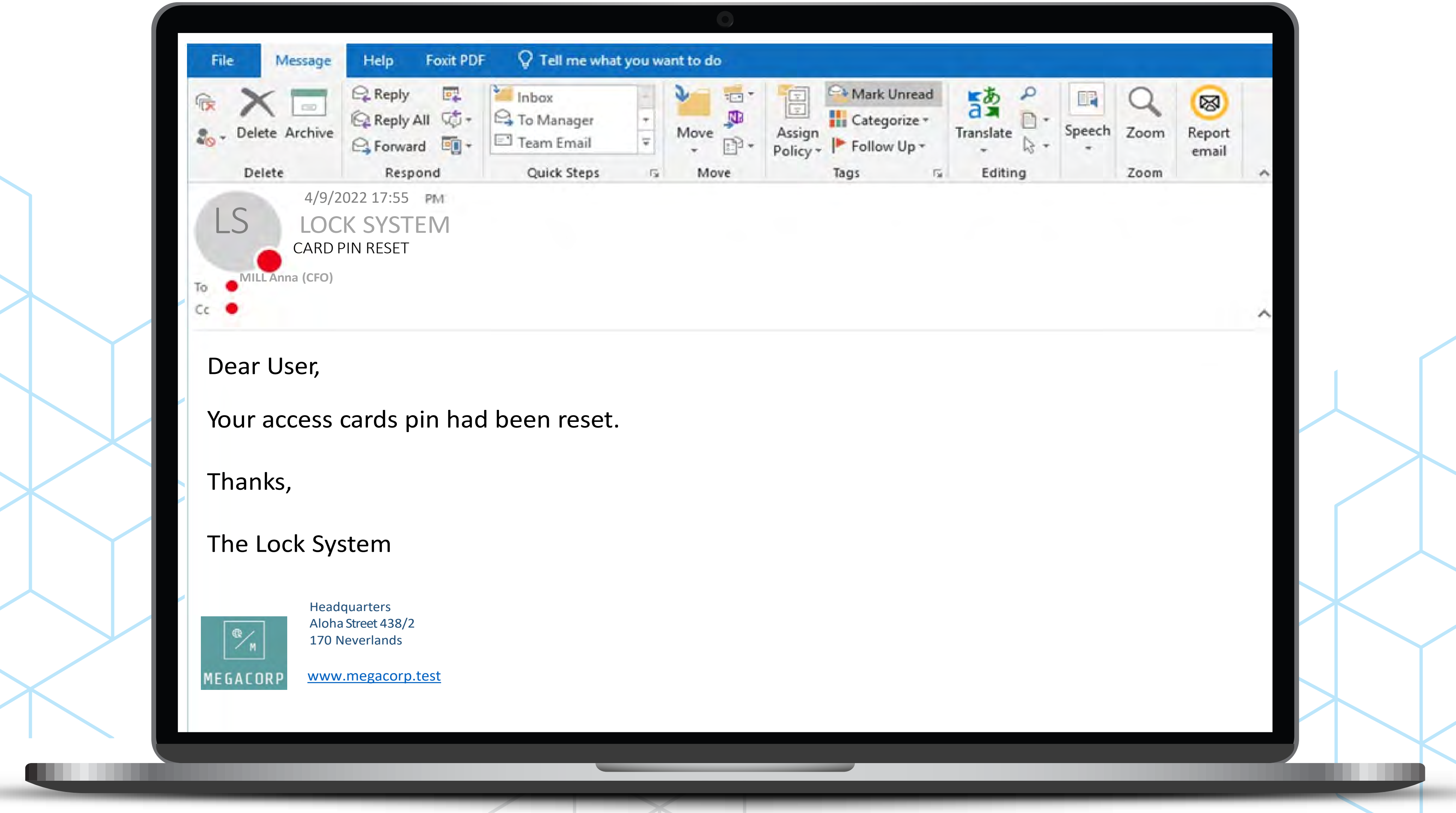
C:\Users\kasilva\Downloads\Scan302229_Xerox.htm

Sign in

to continue to Gmail

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

SUSPICIOUS MAIL



4/9/2022 17:55 PM

LOCK SYSTEM

CARD PIN RESET

MILL Anna (CFO)

Dear User,

Your access cards pin had been reset.

Thanks,

The Lock System

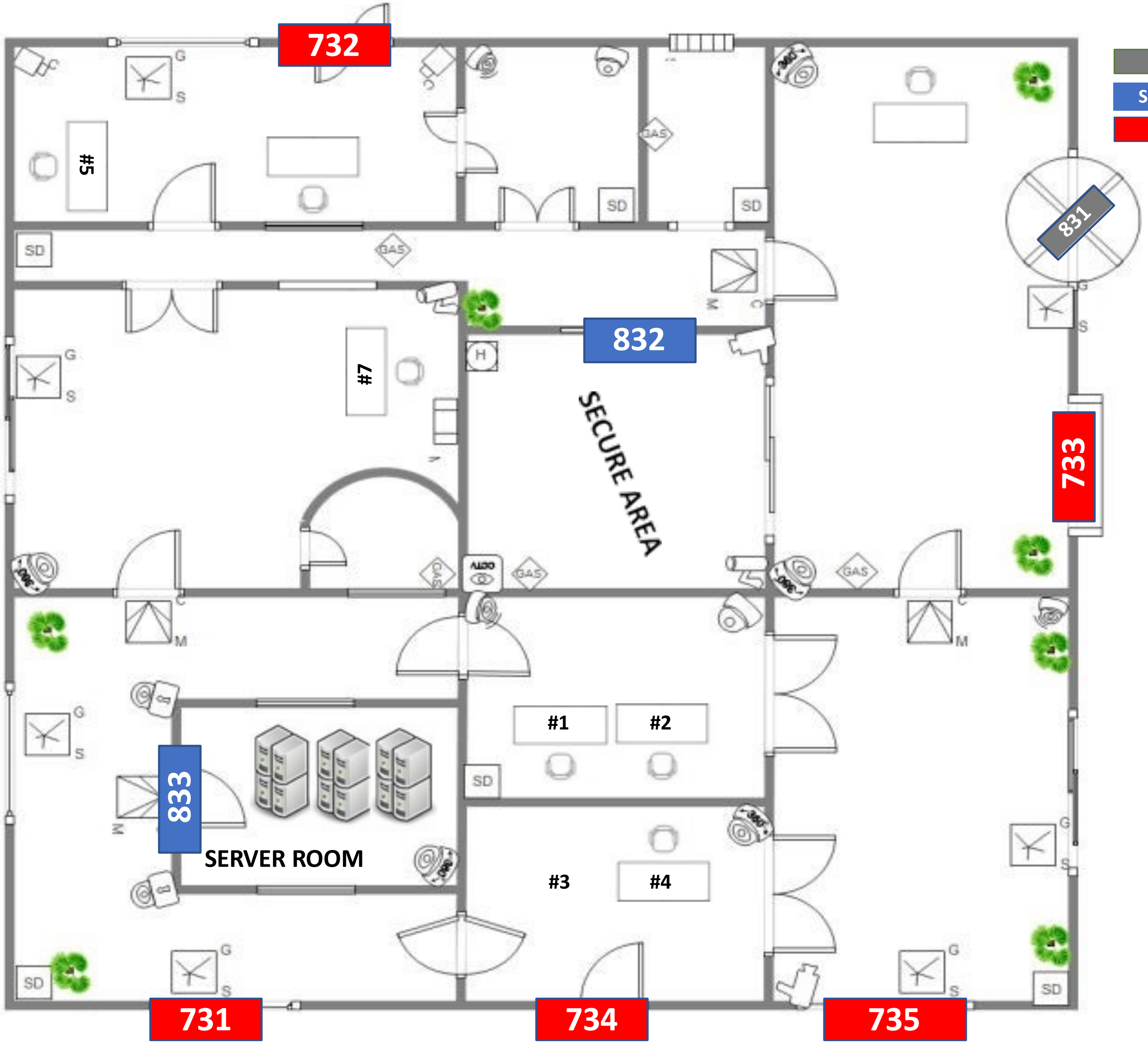
Headquarters
Aloha Street 438/2
170 Neverlands

www.megacorp.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

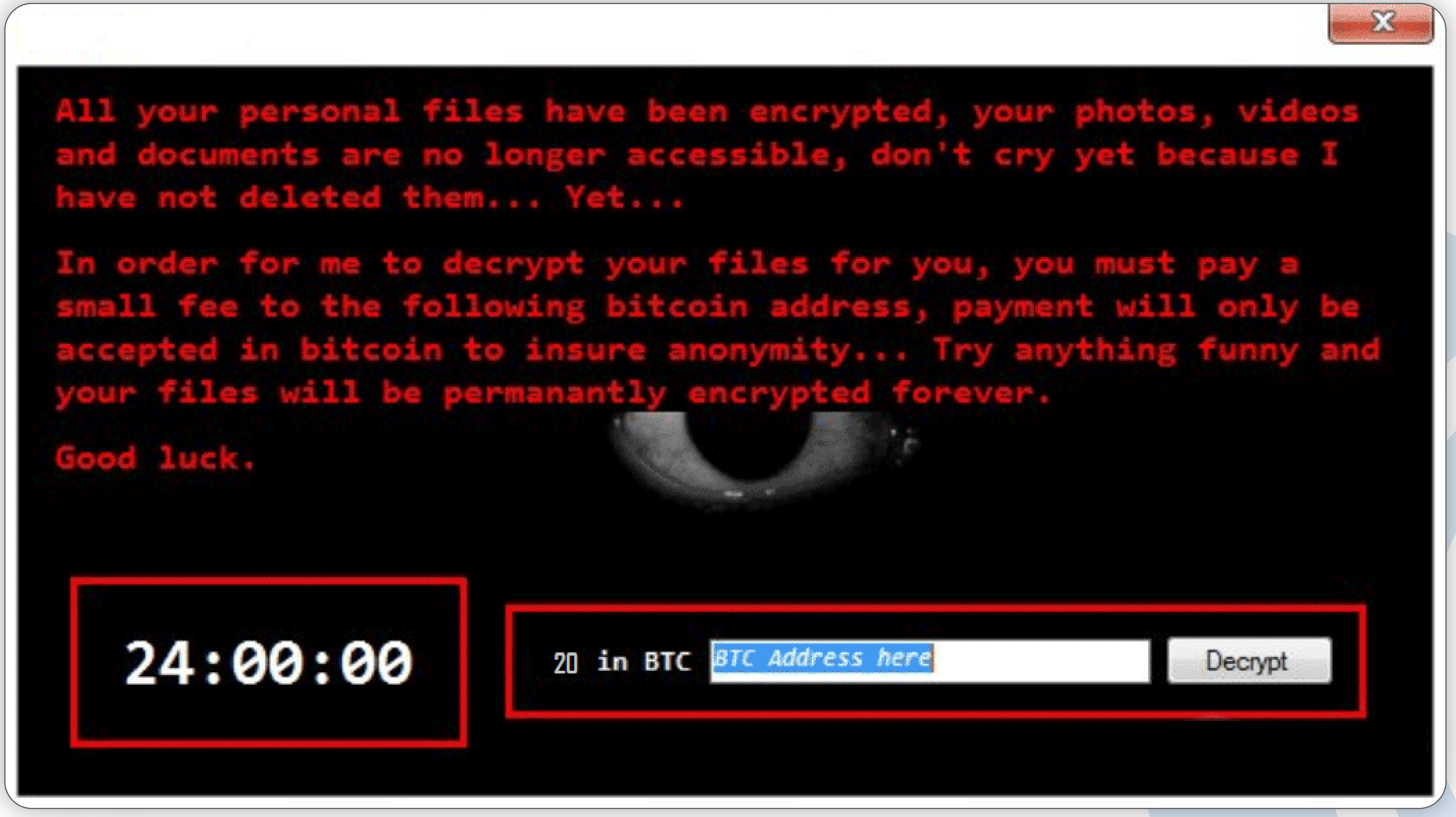
CLICKALL Jack
LEGAL
ID: AL3XZA4

MILL Anna
CFO
ID: FA23RN1

DARC Marc
ICT – Contractor
ID: IT21NO6

MARLY Maria
ICT
ID: IT11NI9

THE RANSOMWARE NOTE



All your personal files have been encrypted, your photos, videos and documents are no longer accessible, don't cry yet because I have not deleted them... Yet...

In order for me to decrypt your files for you, you must pay a small fee to the following bitcoin address, payment will only be accepted in bitcoin to insure anonymity... Try anything funny and your files will be permanantly encrypted forever.

Good luck.

File to unlock:

UVOAQGY DEIA.db

Decrypt the FILENAME using the correct key

HOW DOES VIGENERE WORK – EXAMPLE

To encrypt:

SECRET PHRASE

Key:

LOCKME

ENCRYPTION MECHANISM:

SECRETPHRASE
LOCKMELOCKME
DSEBQXAVTKEI

To decrypt:

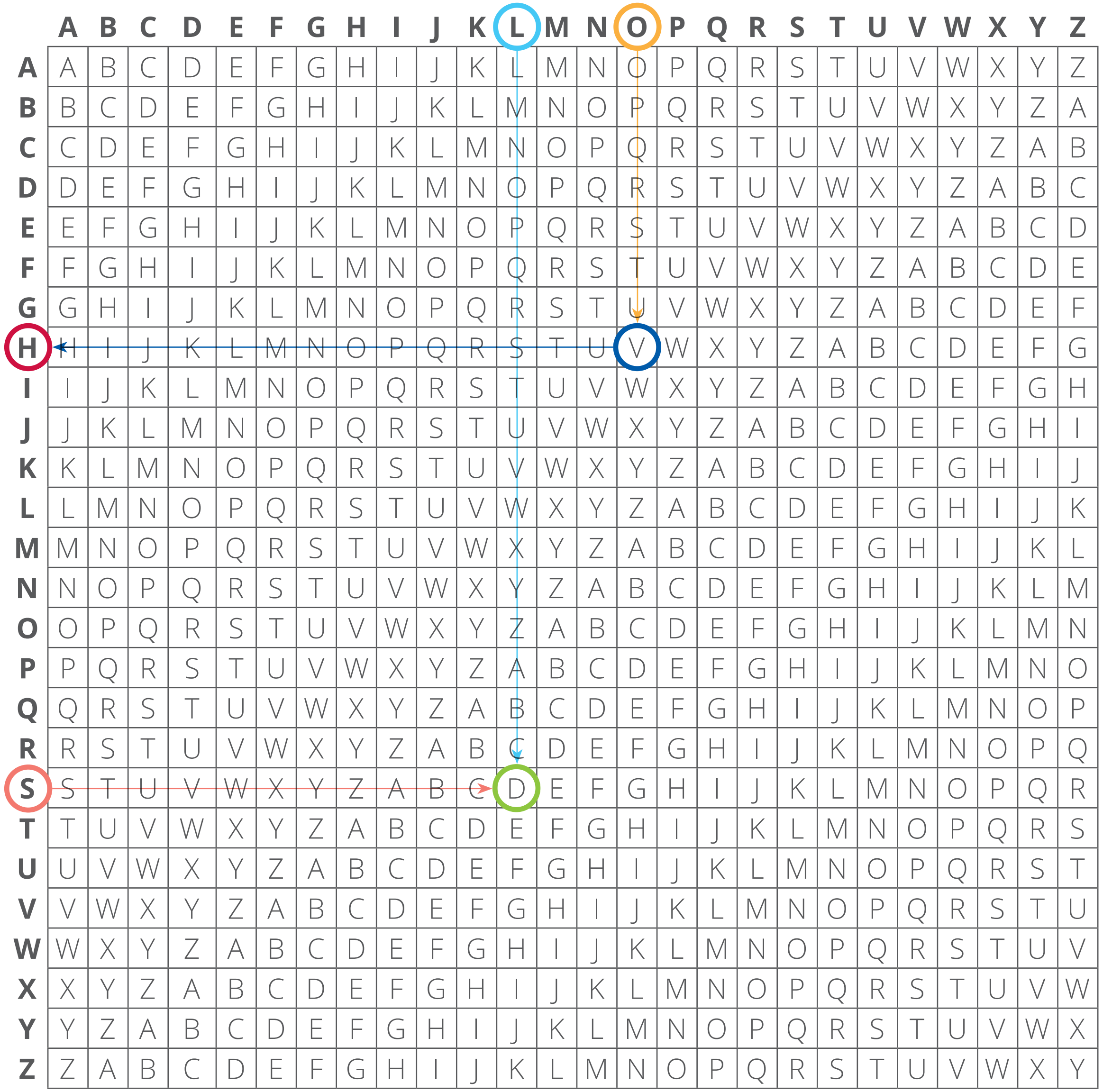
DSEBQXAVTKEI

Key:

LOCKME

DECRYPTION MECHANISM:

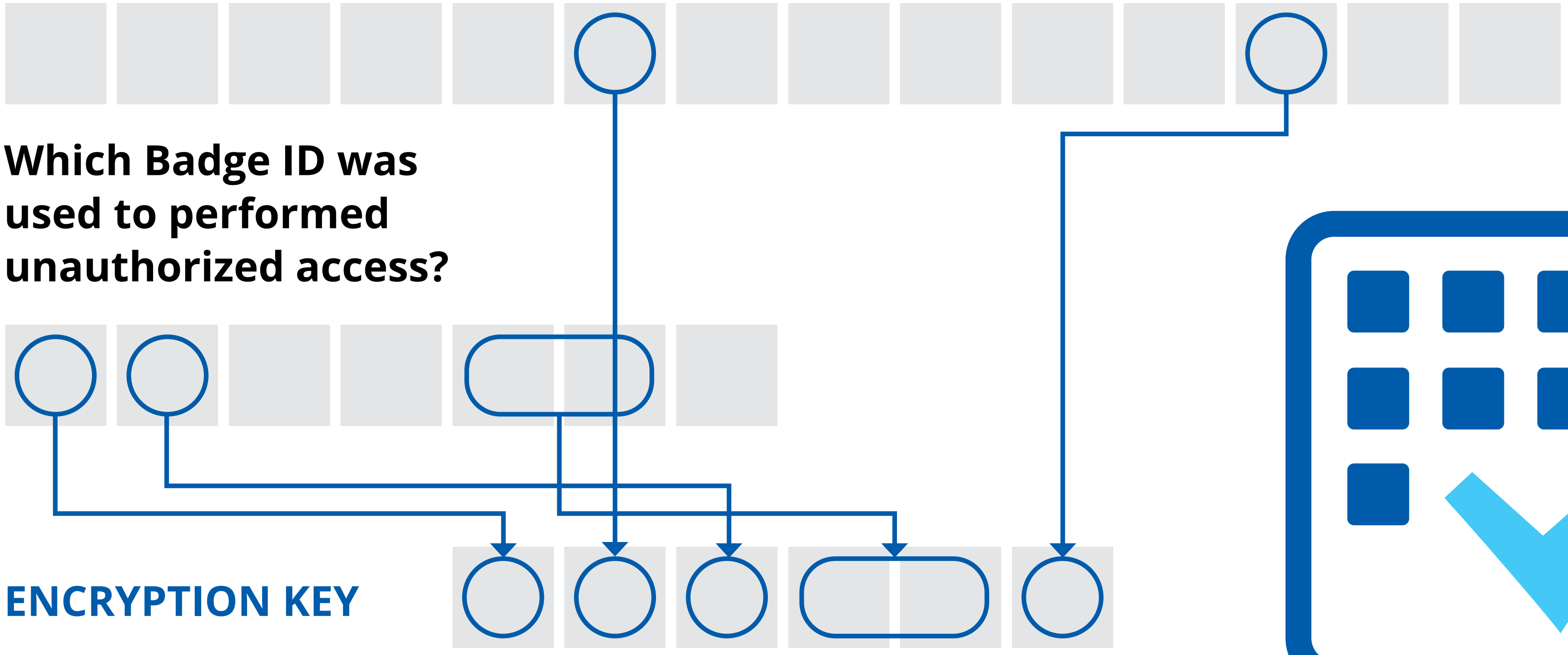
LOCKMELOCKME
DSEBQXAVTKEI
SECRETPHRASE



	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?

AR-IN-A-BOX

BE THE STRONGEST LINK

BREAK THE KILLCHAIN

MINI GAME

SCAN ME

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

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