AR-IN-A-BOX

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

CYBER AWARENESS GAME

MiniBiz Hacked

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:

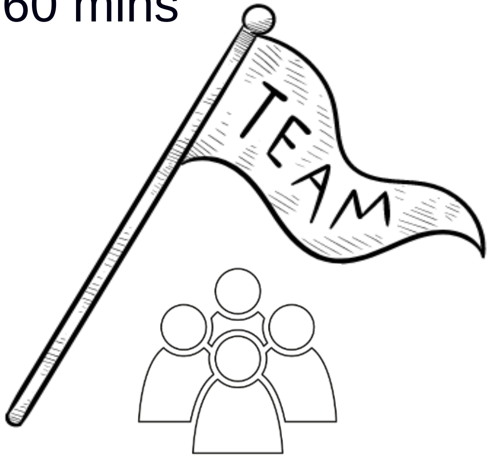
“Source: ENISA Cyber Awareness Training Material, Copyright © European Union Agency for Cybersecurity (ENISA), 2024”. If you do republish we would be grateful if you link back to the ENISA website www.enisa.europa.eu. No part of this document, including any part of the information contained therein, 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

- Introduce game and instructions
- Create teams or Play Individually
  - Choose a Team Leader
  - Choose a Team Name
- Distribute clues to each team
- Discuss your Solution
- Game total duration: 60 mins

Option - Quiz



1 - 4 people per team

Unlimited number of teams

ENISA EUROPEAN UNION AGENCY FOR CYBERSECURITY

SCENARIO – MINIBIZ HACKED

MINIBIZ

MiniBiz has suffered a CEO fraud and ransomware attack. The initial hack appeared to take place early September, but it went unnoticed till the 10th of September 2024, when the bank accounts of the MiniBiz were emptied and its systems blocked.

Attackers appeared to have gained initial access via a successful **VISHING and/or SMISHING and/or PHISHING ATTACK.**

To make matters worse **FRAUDULENT PAYMENT** was made in MiniBiz 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 further damage occur.

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!

SCENARIO – MINIBIZ PROFILE

- MiniBiz is a technology company that specialises in website development. It has less than 75 employees. Maria is MiniBiz CEO.
- Maria main concerns is to deliver quality service and built customer loyalty. She deals with personal data, employee personal data, accounting software and client data.
- She uses emails, SaaS solutions for development and static webpage where she indicates her services, team, projects and contact information
- Risks she is aware of: phishing, ransomware, weak passwords
- IT resources: development tools, office collaboration tools, on prem servers, antivirus, accounting software, web dev software.
- Challenges: Limited broadband capacity on the corporate network, prompting staff to use personal devices/email when travelling or working from home.
- MiniBiz never had security issues but is concerned about ransomware as Maria heard about friends losing their data. She doesn't believe she would lose client data as it is deployed at client servers after project completion, nor accounting data as an external accountant is taking care of it.

EMAIL ATTACK

PHASE 1

TASK UPDATE #1

Several **suspicious emails** have been recovered while investigating the hack.

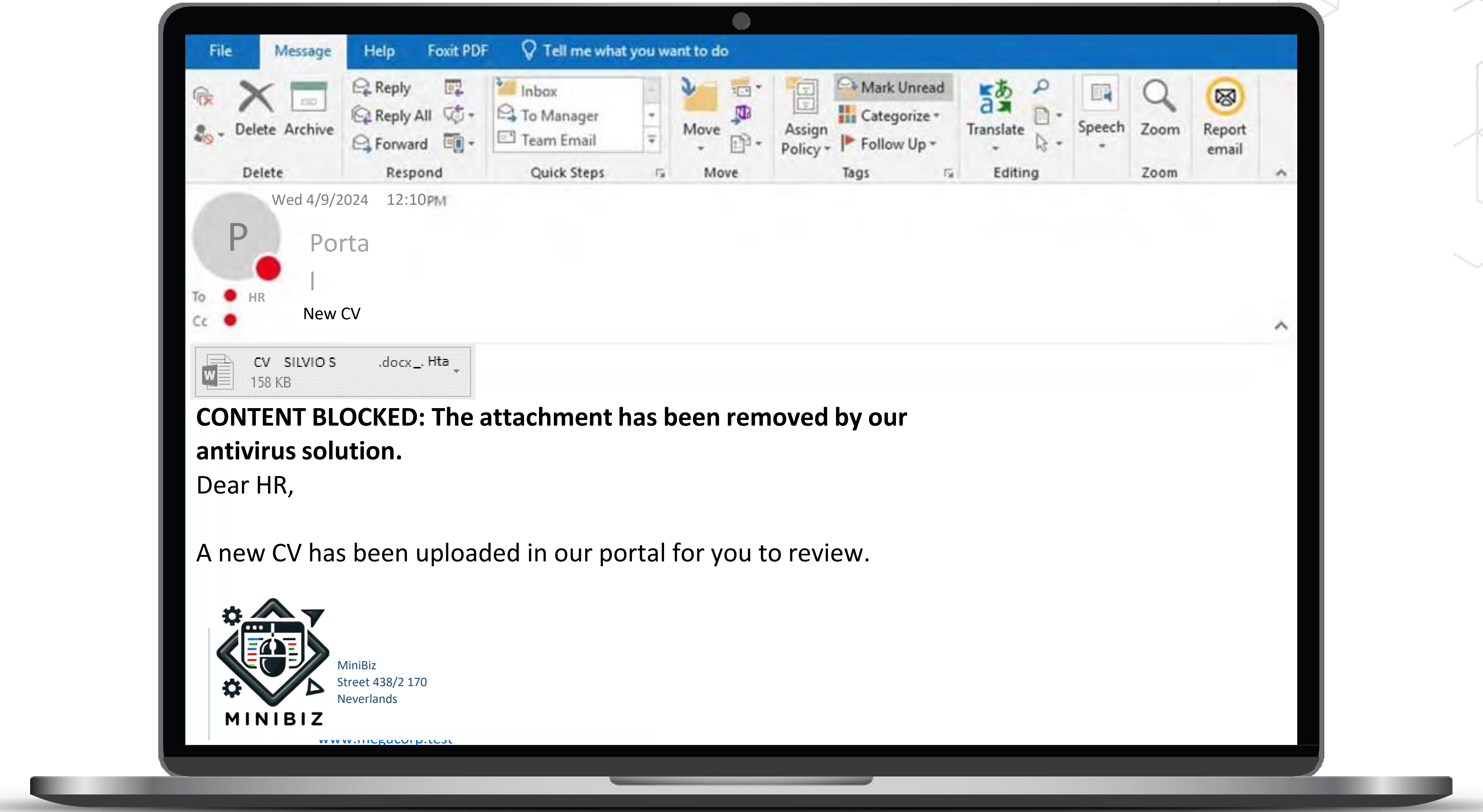
Your task is to go through the **communications of various individuals and identify the perpetrator and possible victims.**

It is believed, based on our analysis, that the attacks **started from a single attack - a social engineering with an email**. That’s how the hackers got access to the **MiniBiz internal systems**.

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

Good Luck,
The Management

SUSPICIOUS MAIL



Wed 4/9/2024 12:10PM

Porta

To HR

Cc

New CV

CV SILVIO S .docx_. Hta
158 KB

CONTENT BLOCKED: The attachment has been removed by our antivirus solution.

Dear HR,

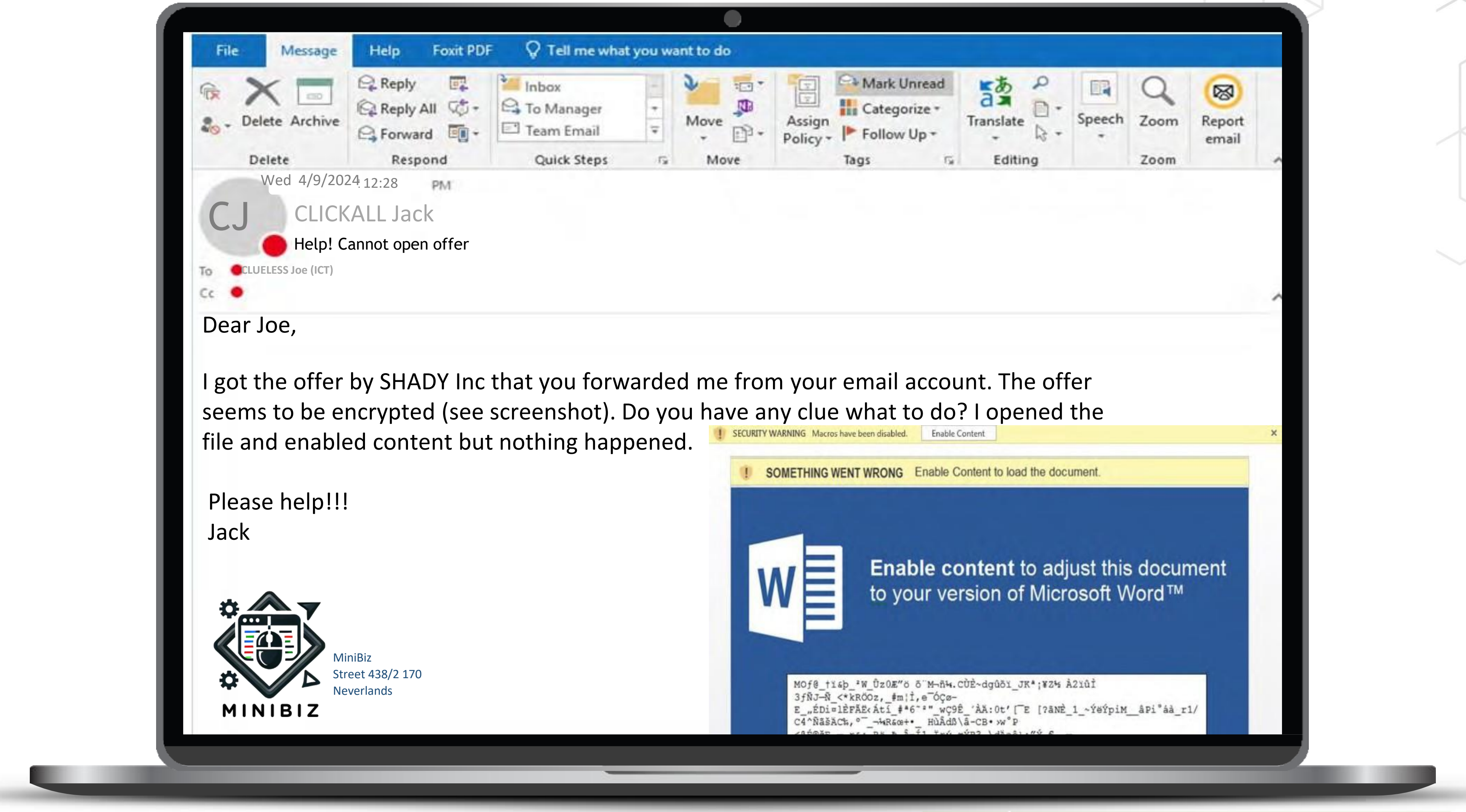
A new CV has been uploaded in our portal for you to review.

MiniBiz
Street 438/2 170
Neverlands

www.megacorp.test

PHISHING ATTACK

SUSPICIOUS MAIL



Wed 4/9/2024 12:28 PM

CLICKALL Jack

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

MINIBIZ

MiniBiz
Street 438/2 170
Neverlands

SECURITY WARNING Macros have been disabled. Enable Content

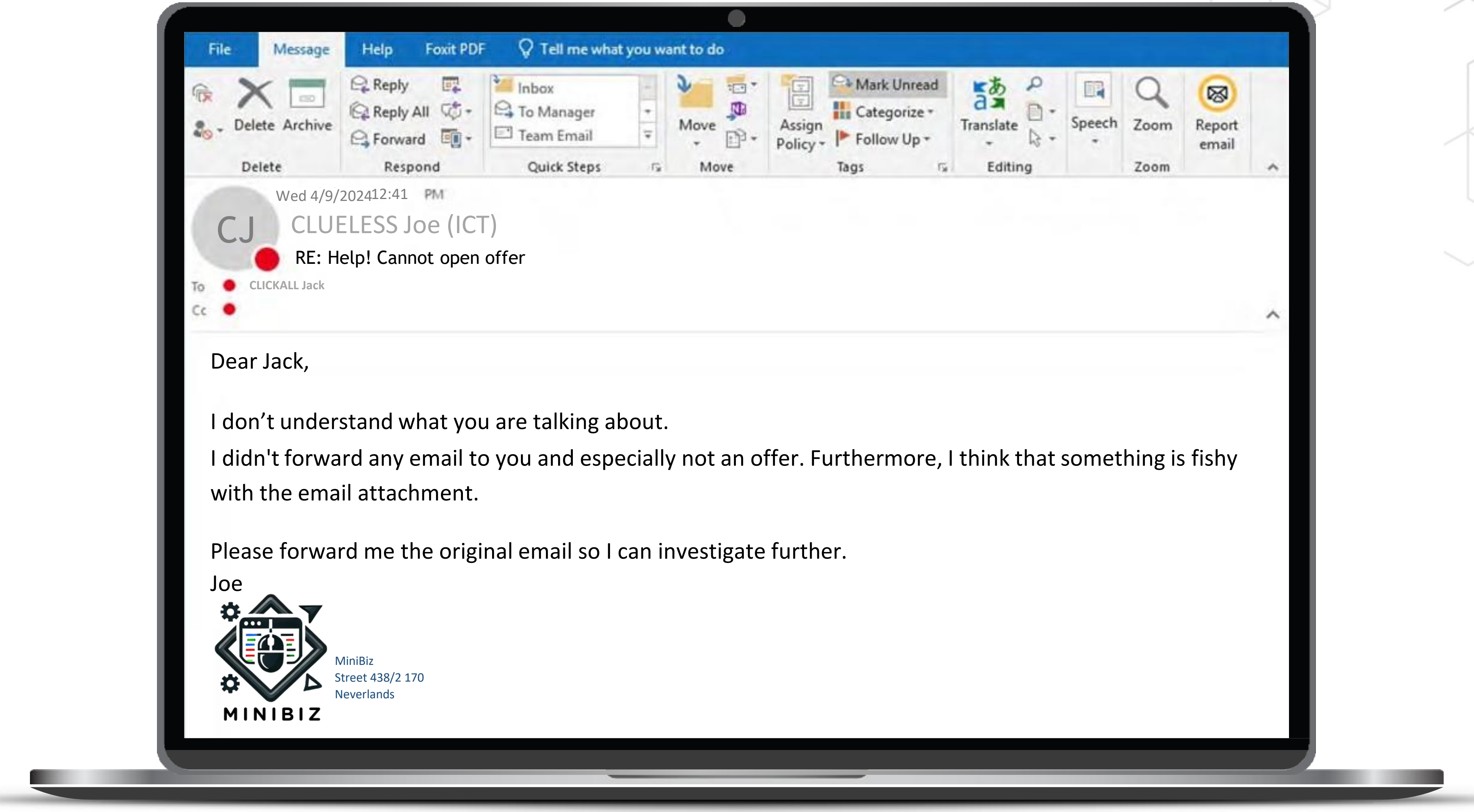
SOMETHING WENT WRONG Enable Content to load the document.

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

```
MOf@_†Ï&þ_²W_Ûz0Æ”ö ö¨M¬ñ¼.CÙÈ~dgûõÏ_JKª;¥Z½ À2ÏûÌ
3fÑJ—Ñ_<*kRÖOz,_#m¦Ì,e¯ÓÇø-
E_„ÉDi¤lÈFÃË‹Átí_#ª6¯²"_wÇ9Ê_´ÀÄ:0t’[¯E [?ãNÈ_1_~ÝëÝpiM__âPi°áà_r1/
C4^ÑãšÃC‰,°¯_¬¼R&œ+•_ HùÂdß\ã-CB•›w°P
```

PHISHING ATTACK

SUSPICIOUS MAIL



Wed 4/9/202412:41 PM

CLUELESS Joe (ICT)

RE: Help! Cannot open offer

To CLICKALL Jack

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.

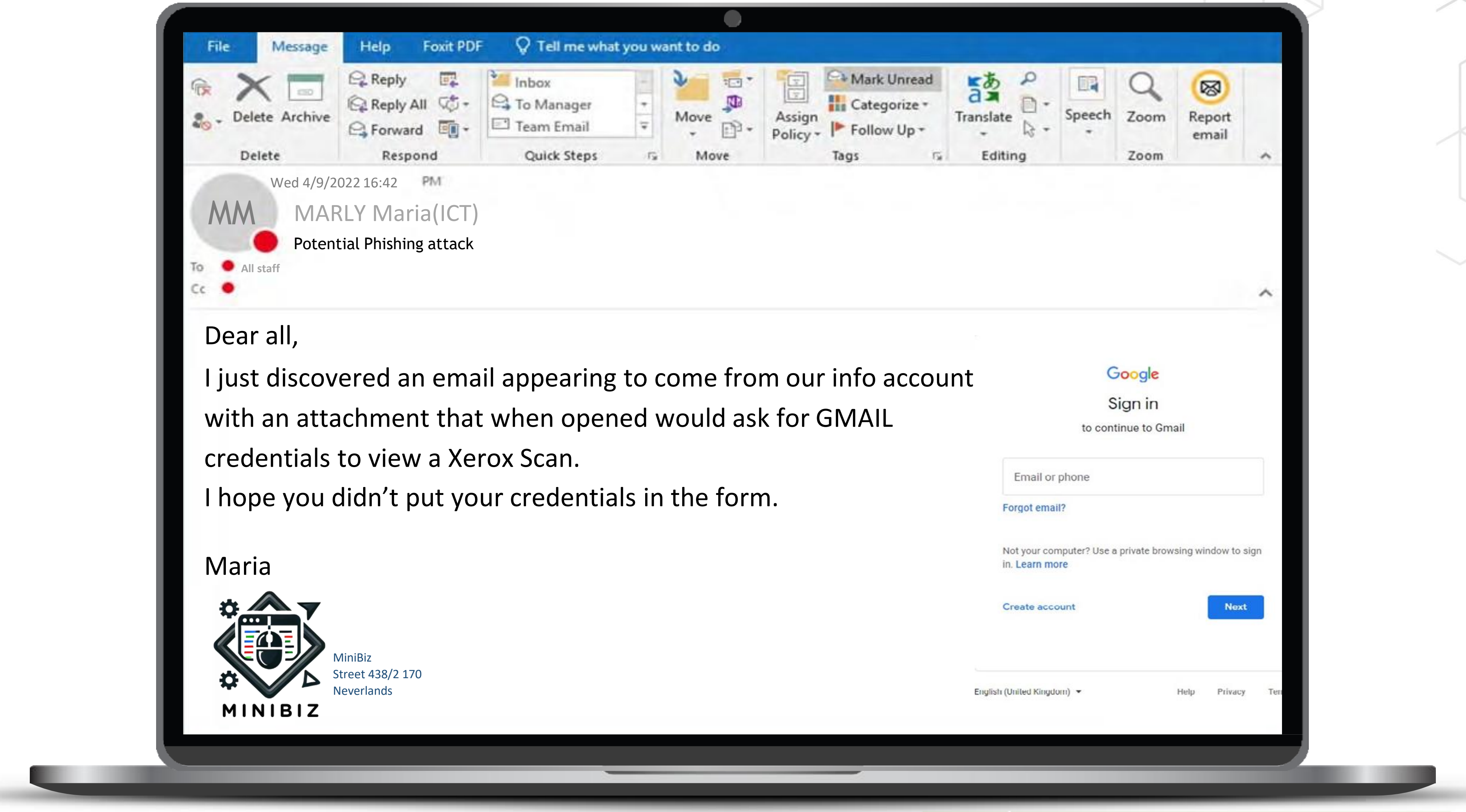
Please forward me the original email so I can investigate further.

Joe

MiniBiz
Street 438/2 170
Neverlands

PHISHING ATTACK

SUSPICIOUS MAIL



Wed 4/9/2022 16:42 PM

MARLY Maria(ICT)

Potential Phishing attack

To All staff

Cc

Dear all,

I just discovered an email appearing to come from our info account with an attachment that when opened would ask for GMAIL credentials to view a Xerox Scan.

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

Maria

MINIBIZ

MiniBiz
Street 438/2 170
Neverlands

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

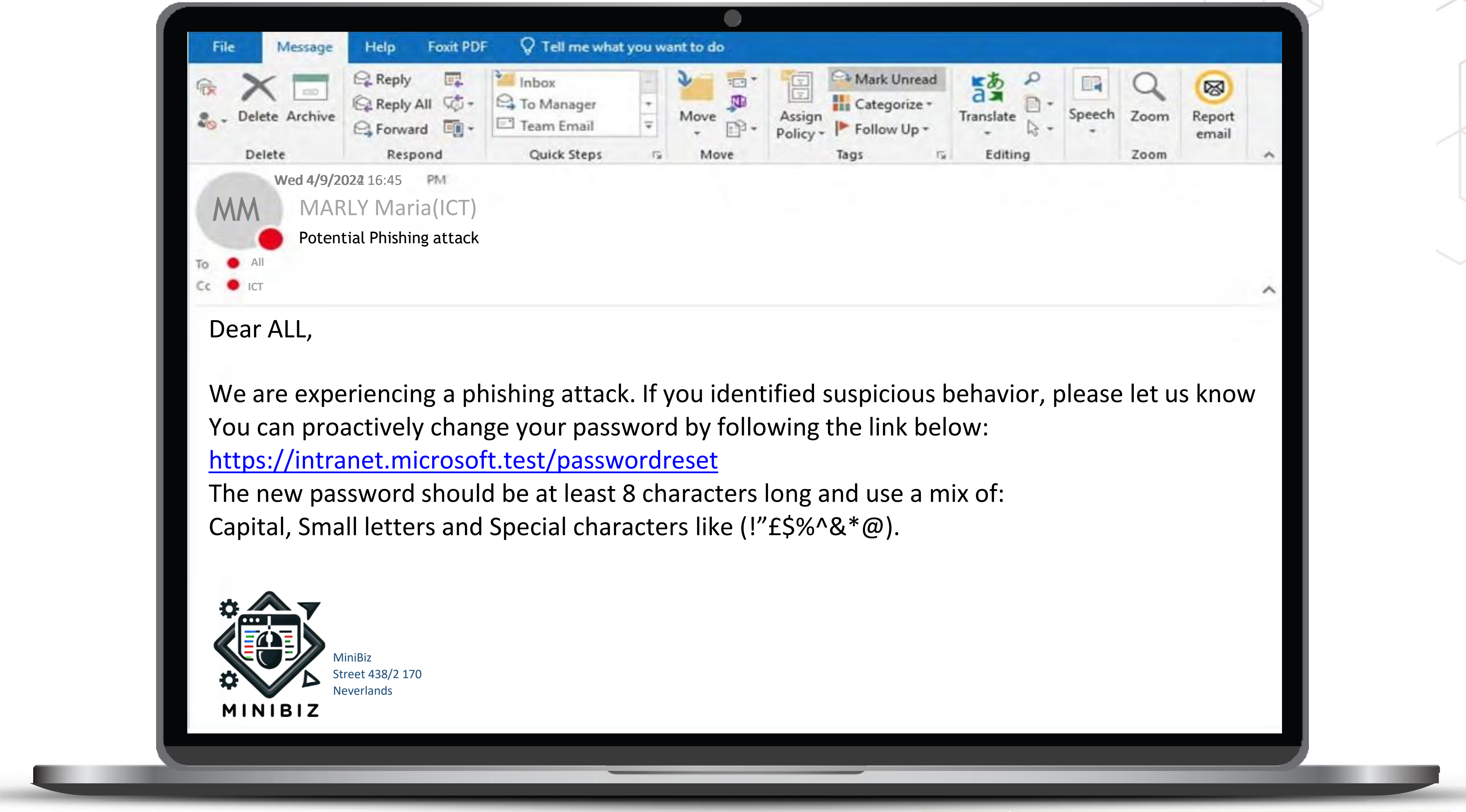
Create account

Next

English (United Kingdom) Help Privacy Ter

PHISHING ATTACK

SUSPICIOUS MAIL



Wed 4/9/2024 16:45 PM

MARLY Maria(ICT)

Potential Phishing attack

To ● All

Cc ● ICT

Dear ALL,

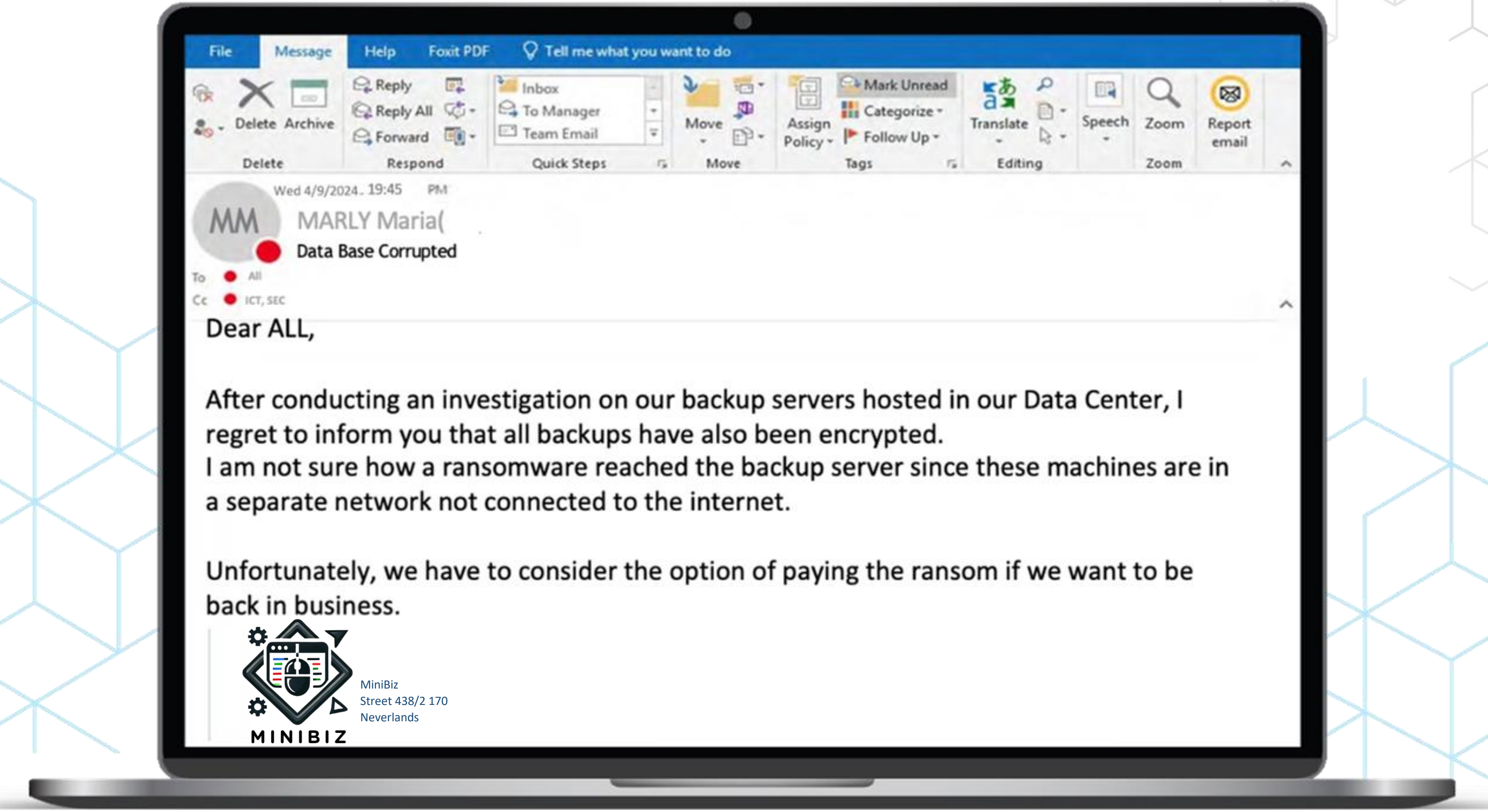
We are experiencing a phishing attack. If you identified suspicious behavior, please let us know
You can proactively change your password by following the link below:
https://intranet.microsoft.test/passwordreset
The new password should be at least 8 characters long and use a mix of:
Capital, Small letters and Special characters like (!”£$%^&*@).

MINIBIZ

MiniBiz
Street 438/2 170
Neverlands

PHISHING ATTACK

SUSPICIOUS MAIL



Wed 4/9/2024 19:45 PM

MARLY Maria(

Data Base Corrupted

To ● All

Cc ● ICT, SEC

Dear ALL,

After conducting an investigation on our backup servers hosted in our Data Center, I regret to inform you that all backups have also been encrypted.
I am not sure how a ransomware reached the backup server since these machines are in a separate network not connected to the internet.

Unfortunately, we have to consider the option of paying the ransom if we want to be back in business.

MINIBIZ

MiniBiz
Street 438/2 170
Neverlands

PHISHING ATTACK

ACTION TIME

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

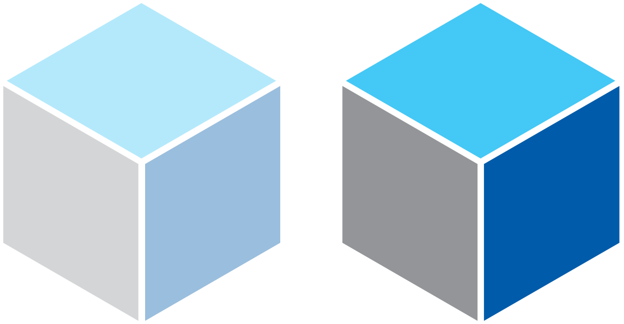
Q1. Which type of attack most likely took place?

Q2. Can you explain the attackers' steps so far?

Q3. Was the potential incident handled correctly?

PHONE ATTACK

PHASE 2



TASK UPDATE #2

Several **phone records** have been recovered while investigating the hack.

Your task is to **go through the communications** of **the victim** and **identify the perpetrator and identity of the victim**.

It is believed, based on our analysis, that the **attack was a complex a social engineering**, **using either an** email or **SMS or voice call, or combination of all the above methods**. That’s how the hackers **initiated a fraudulent payment**.

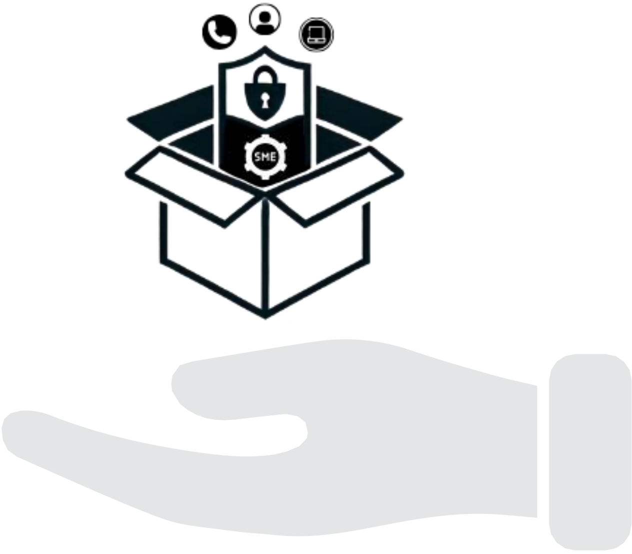
We count on you to perform the analysis **fast**.

Good Luck,
The Management

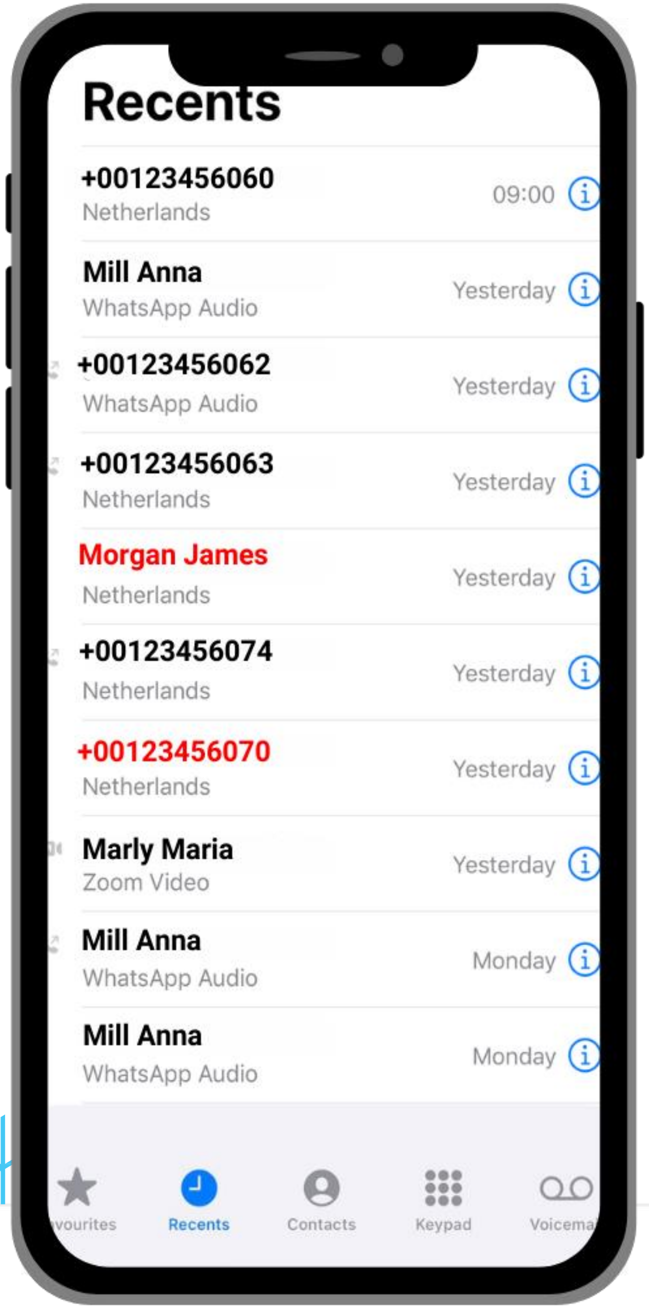
FULL EMPLOYEES LIST

Phone number	Name	Role
+00123456060	Marly Maria	CEO
+00123456061	Clickall Jack	Office Manager
+00123456062	Clueless Joe	ICT
+00123456063	Mill Anna	Sales
+00123456064	Darc Marc	Sales
+00123456065	Marly John	Sales
+00123456066	Elton Jack	Marketing
+00123456067	Morgan Monica	Developer
+00123456068	Lee Kim	Trainee
+00123456069	Cross Michael	Developer
+00123456070	Dollar Sam	Developer
+00123456071	Prince Stan	Developer
+00123456072	Maze Luke	Developer
+00123456073	Jasper Joanne	Developer
+00123456074	Frank Alex	Project Manager

SOCIAL ENGINEERING



SUSPICIOUS PHONE LOGS



Recents

+00123456060
Netherlands
09:00

Mill Anna
WhatsApp Audio
Yesterday

+00123456062
WhatsApp Audio
Yesterday

+00123456063
Netherlands
Yesterday

Morgan James
Netherlands
Yesterday

+00123456074
Netherlands
Yesterday

+00123456070
Netherlands
Yesterday

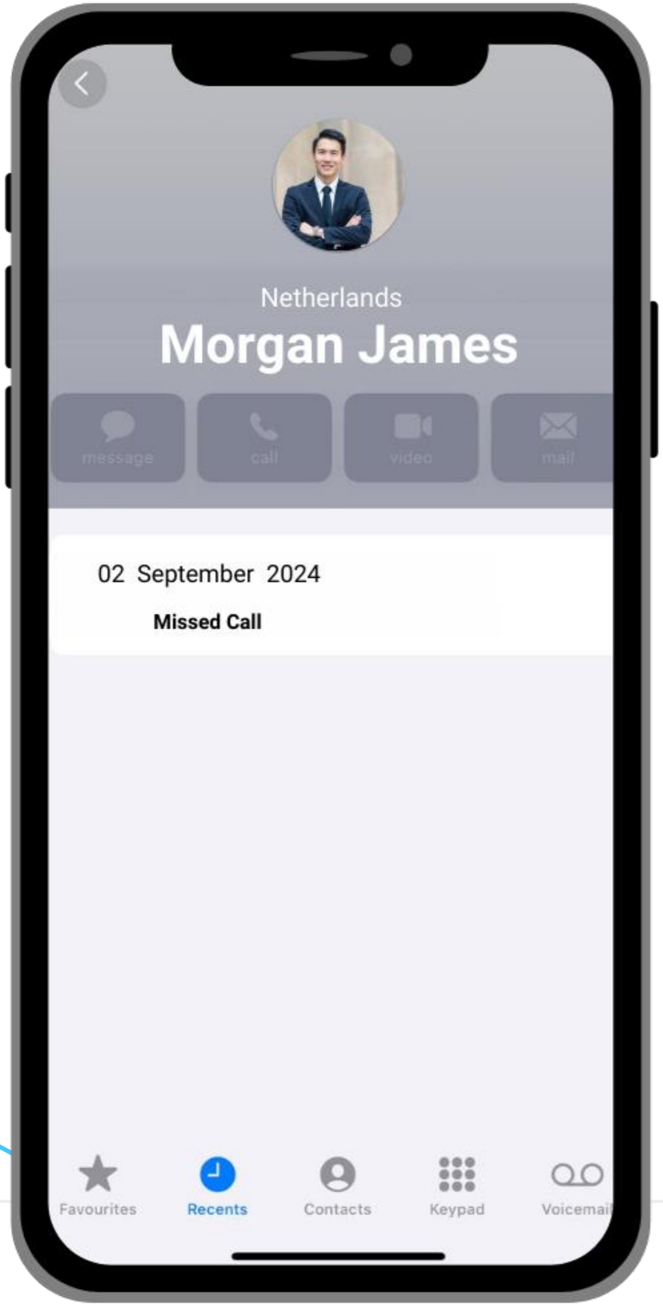
Marly Maria
Zoom Video
Yesterday

Mill Anna
WhatsApp Audio
Monday

Mill Anna
WhatsApp Audio
Monday

VISHING ATTACK

SUSPICIOUS PHONE LOGS



Netherlands

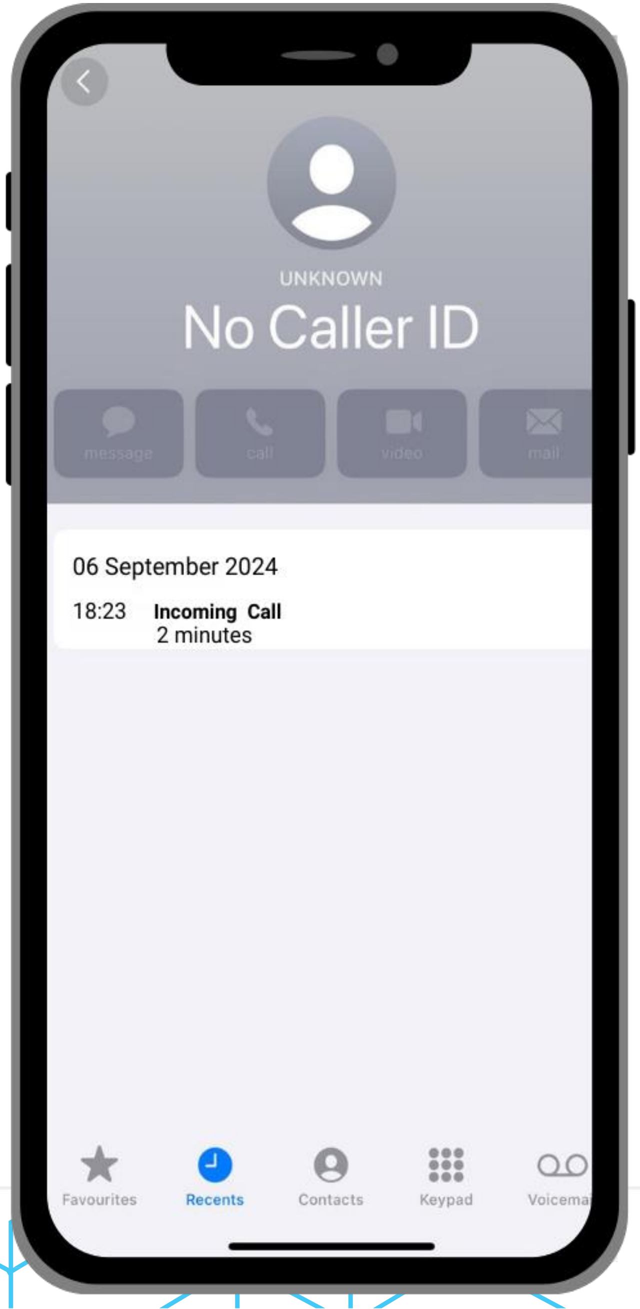
Morgan James

02 September 2024

Missed Call

VISHING ATTACK

SUSPICIOUS PHONE LOGS



UNKNOWN

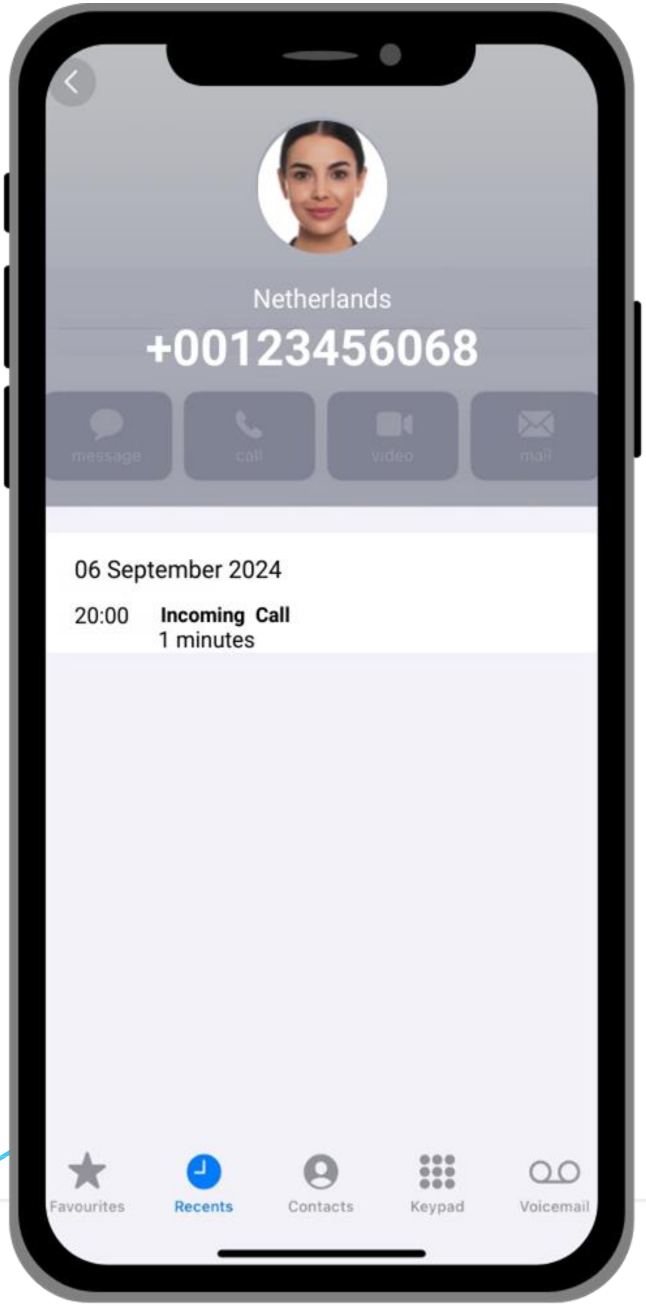
No Caller ID

06 September 2024

18:23 **Incoming Call**
2 minutes

VISHING ATTACK

SUSPICIOUS PHONE LOGS



Netherlands

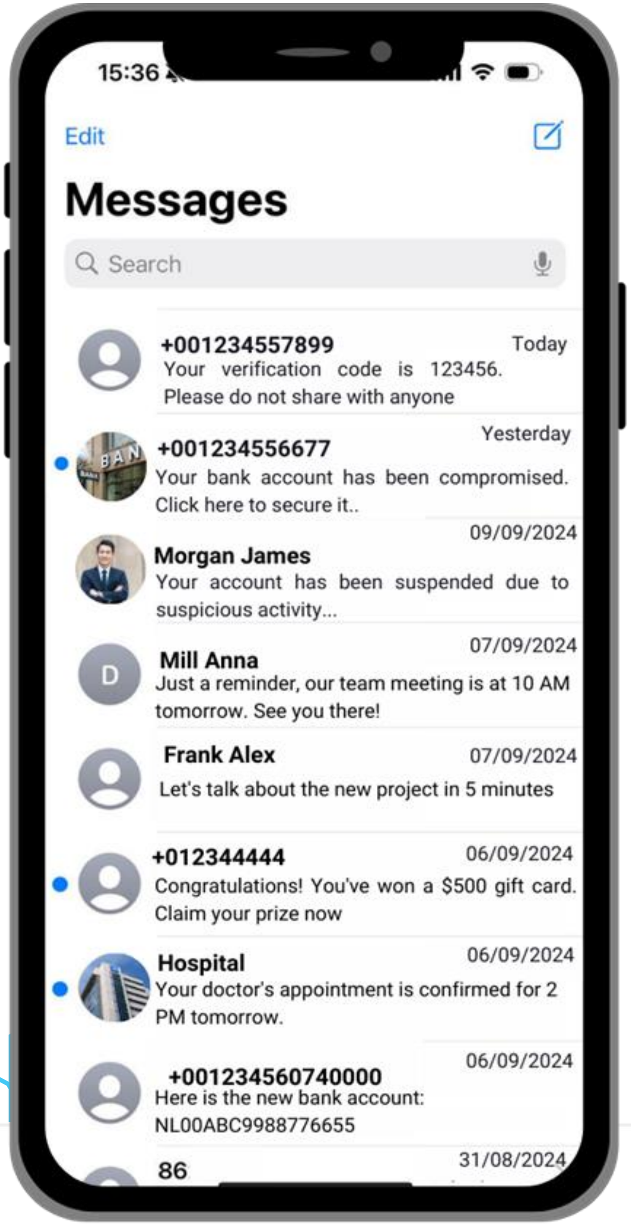
+00123456068

06 September 2024

20:00 **Incoming Call**
1 minutes

VISHING ATTACK

SUSPICIOUS PHONE LOGS



Messages

+001234557899 Today
Your verification code is 123456. Please do not share with anyone

+001234556677 Yesterday
Your bank account has been compromised. Click here to secure it..

Morgan James 09/09/2024
Your account has been suspended due to suspicious activity...

Mill Anna 07/09/2024
Just a reminder, our team meeting is at 10 AM tomorrow. See you there!

Frank Alex 07/09/2024
Let's talk about the new project in 5 minutes

+012344444 06/09/2024
Congratulations! You've won a $500 gift card. Claim your prize now

Hospital 06/09/2024
Your doctor's appointment is confirmed for 2 PM tomorrow.

+001234560740000 06/09/2024
Here is the new bank account: NL00ABC9988776655

86 31/08/2024

SMISHING ATTACK

ACTION TIME

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

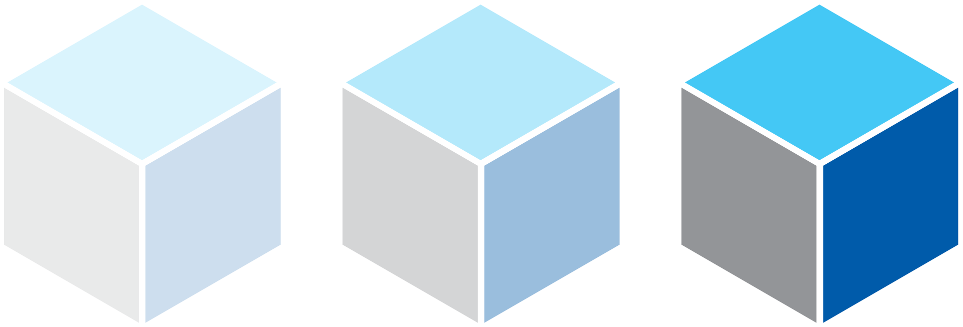
Q4. Which type of attack most likely took place?

Q5. Can you explain the attackers' steps so far?

Q6. Was the payment initiation process defined correctly?

UNAUTHORISED ACTIVITY

PHASE 3



TASK UPDATE #3

Suspicious activity has been detected in **MiniBiz**. 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. **Dig into the logs to identify the SECURITY breach that led to the ransomware infection**. We count on you to perform the analysis as fast as possible.

Good Luck!
The Management

ICT SYSTEM ACCESS LOGS – MINIBIZ

Name	Activity	Date	TIME
Mill Anna	Login	04/09/2024	8:30
Clueless Joe	Login	04/09/2024	8:38
Clickall Jack	Login	04/09/2024	9:00
Darc Marc	Login	04/09/2024	9:05
Darc Marc	Password update	04/09/2024	12:20
Clueless Joe	High privilege activated	04/09/2024	13:48
Marly Maria	Login	04/09/2024	14:00
Mill Anna	Logout	04/09/2024	16:45
Marly Maria	Logout	04/09/2024	17:03
Marly Maria	Logout	04/09/2024	17:08
Darc Marc	Logout	04/09/2024	17:58
Marly Maria	Password reset	04/09/2024	17:59
Mill Anna	Failed authentication	04/09/2024	18:01
Mill Anna	Login	04/09/2024	18:04
Clickall Jack	Logout	04/09/2024	18:20
Clueless Joe	Logout	04/09/2024	18:30

UNAUTHORISED ACTIVITY

ACTION TIME

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

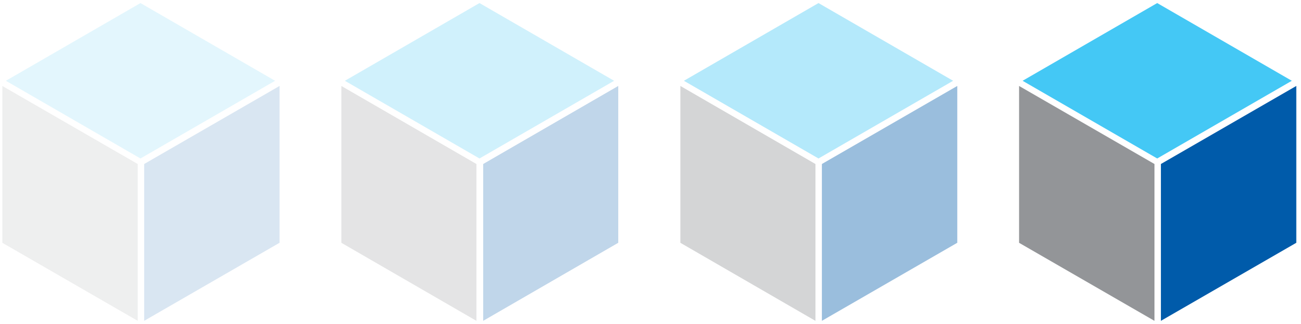
Q7. What could have been a measure taken that could have saved your data for the scenario presented, making paying the ransom obsolete?

Q8. What would be the correct steps to follow in case of **a suspected** hack (identity compromise)?

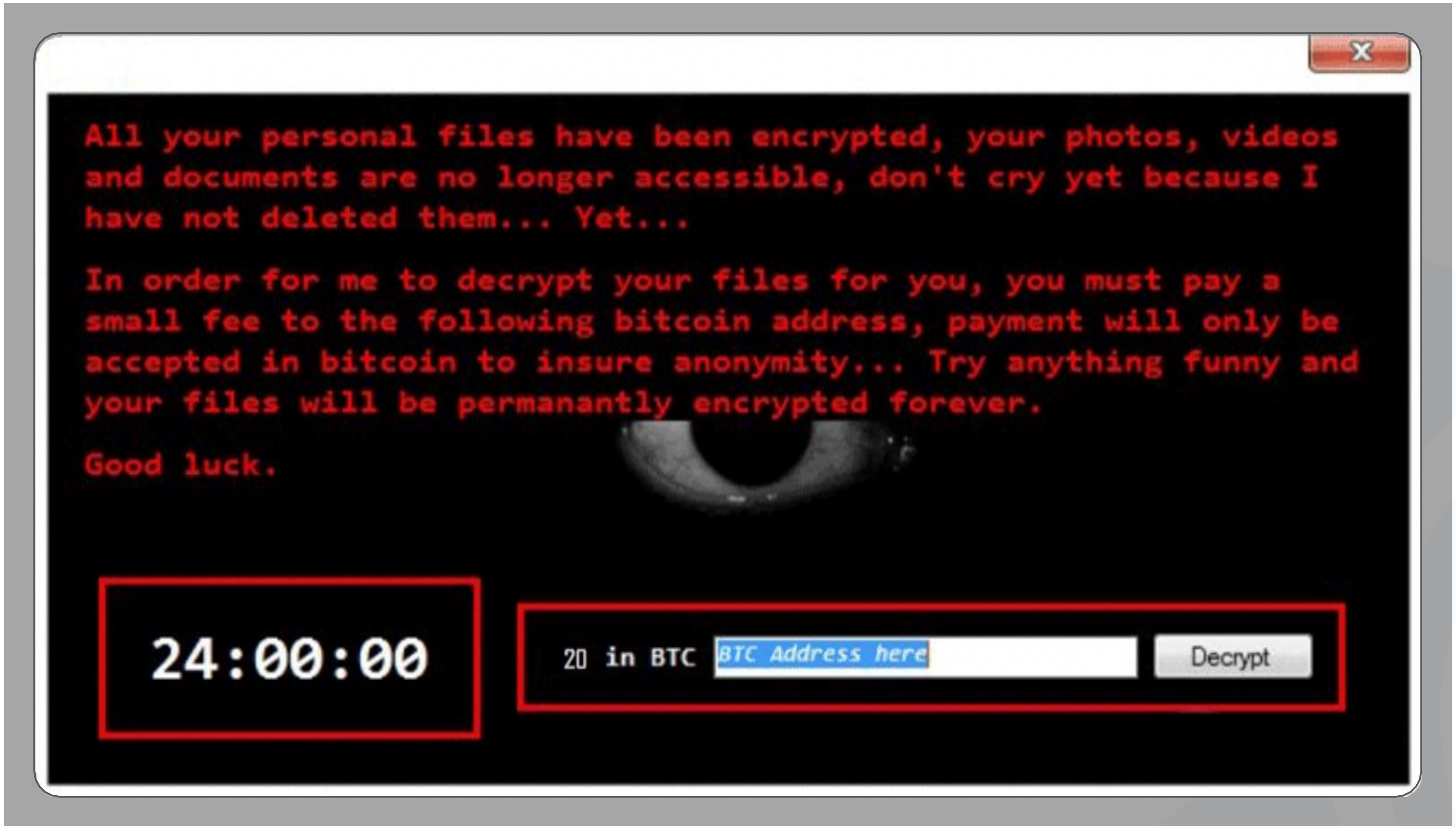
Q9. What would be the steps to follow in case of **a ransomware claim** against your company?

RANSOMWARE

PHASE 4



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.

24:00:00

20 in BTC BTC Address here

File to unlock:

UPKWBPWEW.db

Decrypt the FILENAME using the correct key

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:

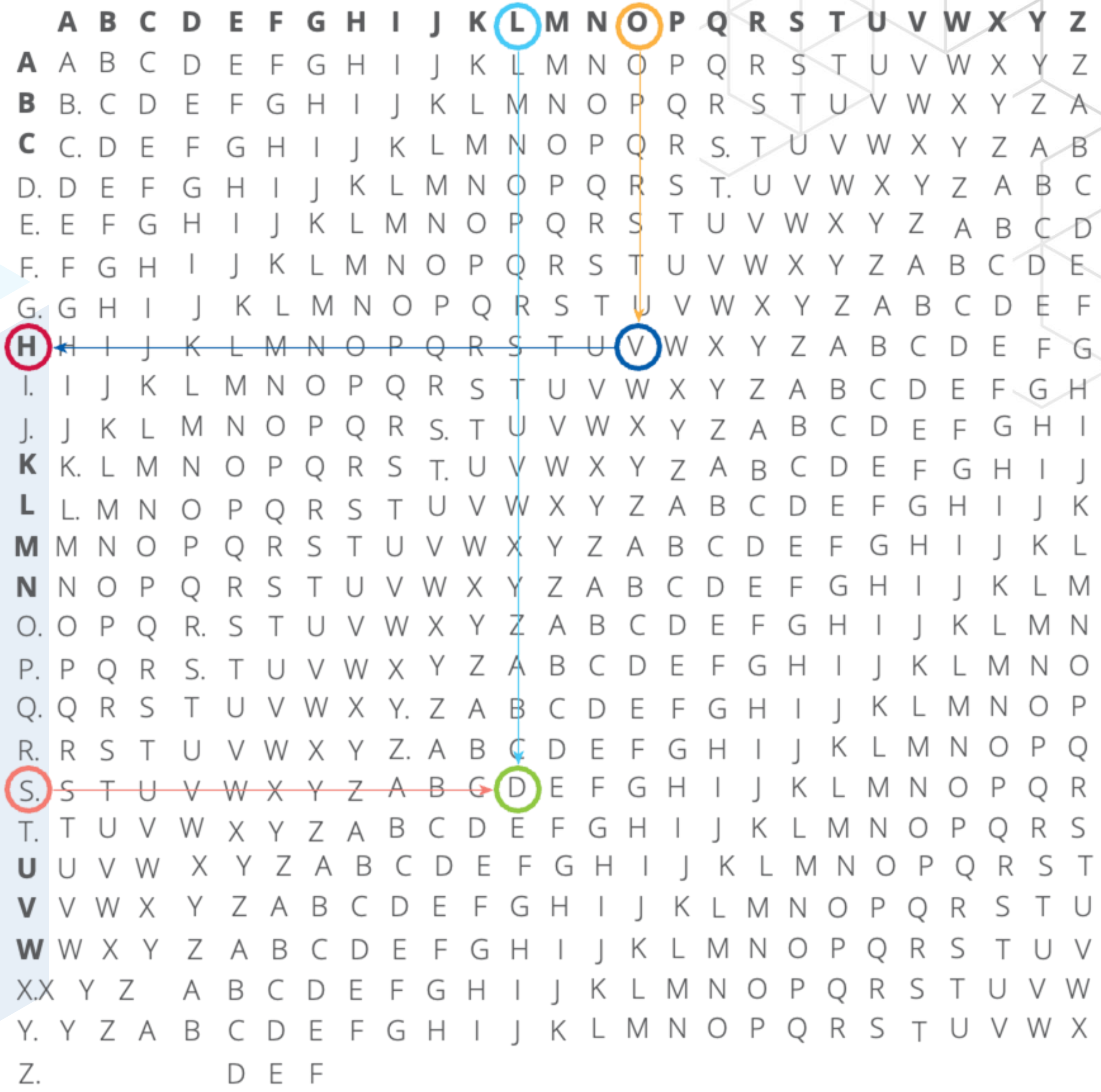
LOCKME

DECRYPTION MECHANISM:

L O C K M E L O C K M E

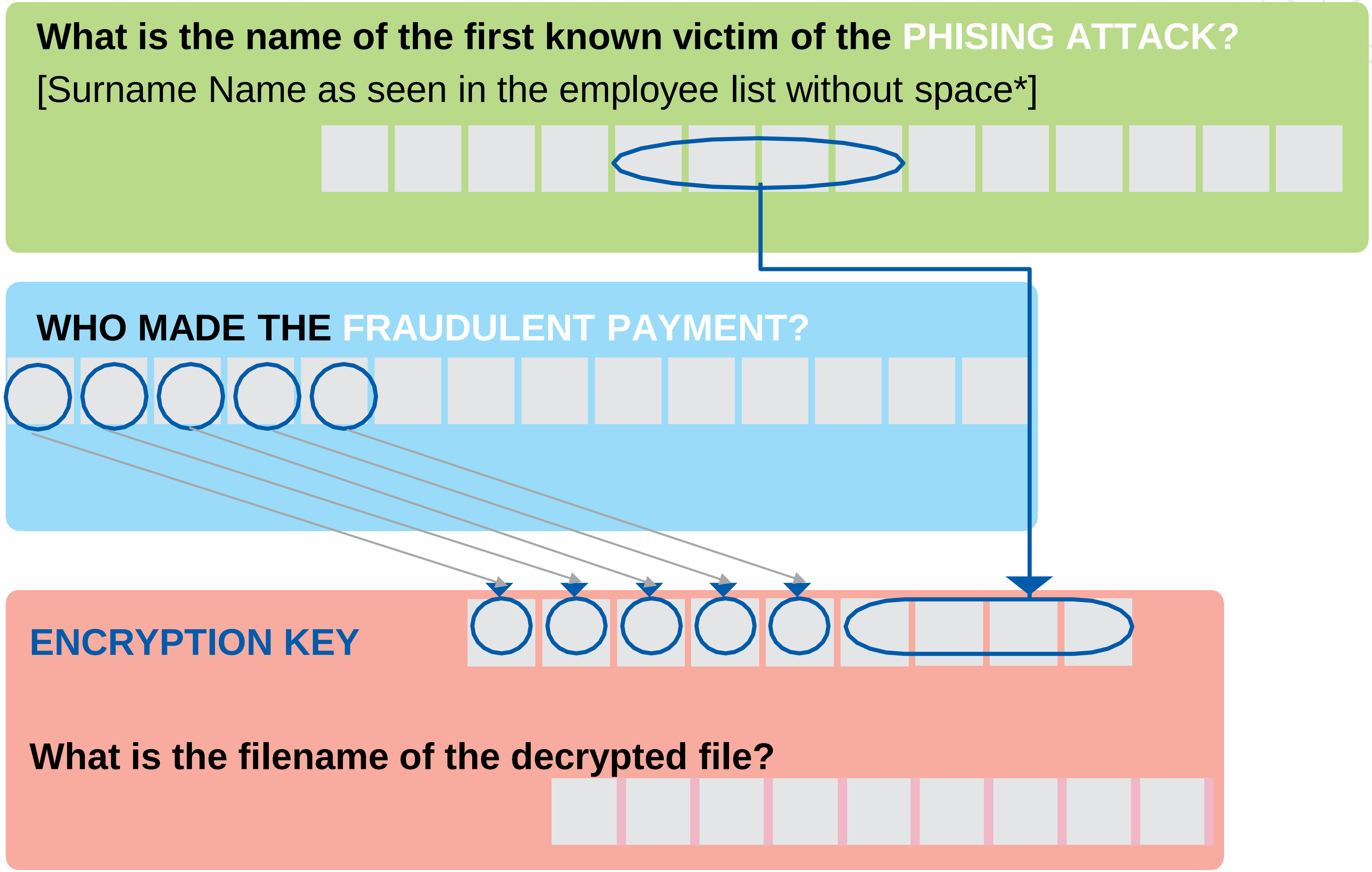
D S E B Q X A V T K E I

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.					D	E	F																			

ANSWER SHEET



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

[Surname Name as seen in the employee list without space*]

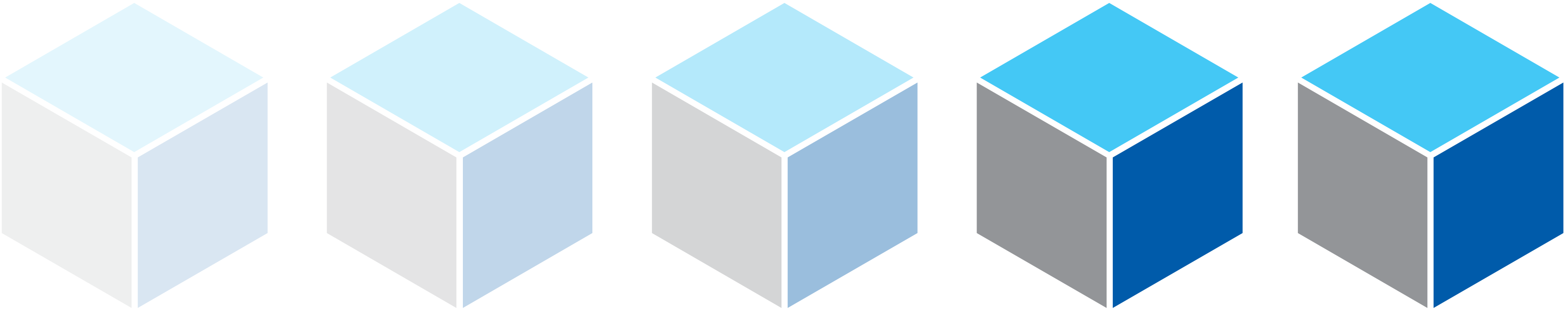
WHO MADE THE FRAUDULENT PAYMENT?

ENCRYPTION KEY

What is the filename of the decrypted file?

LESSONS LEARNT

PHASE 5



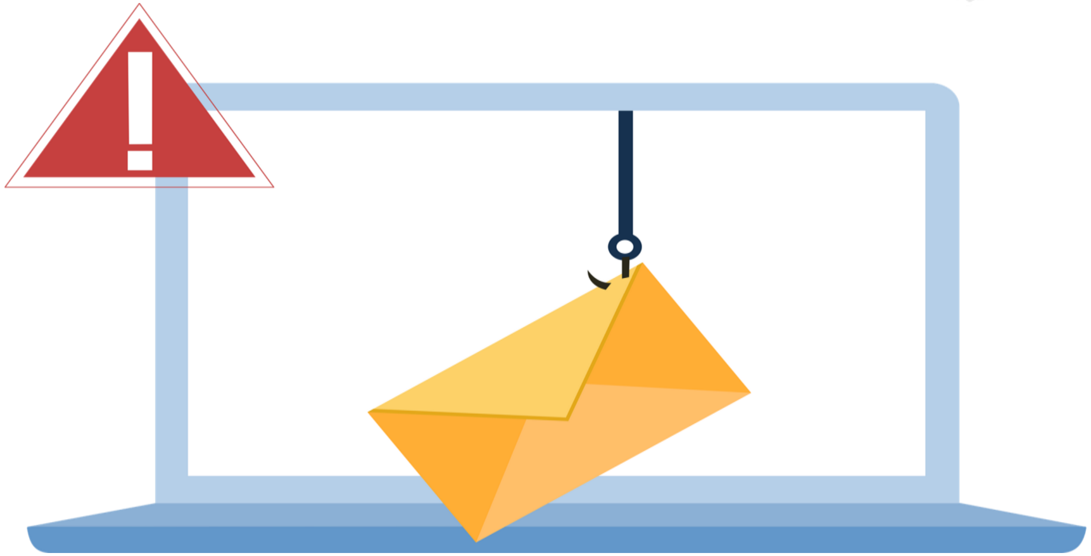
1. WHICH TYPE OF CYBER-ATTACK IS COMMONLY PERFORMED THROUGH EMAIL?

A Phishing

B Smishing

C Vishing

D Ransomware



Correct Answer

Ⓐ Phishing

The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).

2. What clues a typical phishing email presents?

A **There is a typographical error** (e.g. ‘www.yourbanc.com’)

B **The email address is not a professional email account, such as @company.com**

C **Requires an urgent action by clicking on a URL link**

D **It is something unexpected, e.g. an invoice you have not authorised or a package you have not ordered**

E **Any of the above**

Correct Answer

A **Any of the above**

To recognize a phishing e/mail it is a good idea to ask yourself if the sender account is correct and authentic (matches the ‘Name’ and is corporate account), if it contains urgent and unexpected requests (if something urgent is requested from you, would they email it to you?), if the content is grammatically correct. In case you think there is something suspicious, never open or click on attached documents, do not send money to bank accounts and don’t share personal data! If in doubt, contact directly the ‘sender’ through their official channel to verify the request.

3. WHAT KIND OF PASSWORD DO YOU THINK IS THE MOST SECURE FOR ACCOUNTS AND DEVICES?

- A One word that is meaningful to the user
- B A long list of random words combined with numbers and symbols
- C A series of numbers, such as a telephone number, that is meaningful to the user
- D A short, easy to remember combination of random words and symbols

Correct Answer

B **A long list of random words combined with numbers and symbols**

The longer the password, the less likely it is to be hacked. Security experts suggest using a very long list of random words strung together. Bear in mind that #&5%@>$ is no more difficult than "pancake" for a computer program to decipher, and most hackers don't try to figure out passwords on their own. Instead, they use software to try o steal passwords.

4. WHAT IS A GOOD EXAMPLE OF CYBER-HYGIENE PRACTICES?

A Keep a clean desk, without sensitive information visible

B Don’t let the web browser save passwords

C Don’t use the personal mobile to handle professional information

D A short, easy to remember combination of random words & symbols

E All of the above

Correct Answer

E All of the above

When it comes to cyber-hygiene, it's about practicing routine cyber-cleaning habits in not just one, but several key cybersecurity areas: avoid phishing andemail scams, protect data and devices, browse safely, keep systems updated and connect safely to public Wi-Fi networks.

5. YOU HAVE BEEN A VICTIM OF A RANSOMWARE ATTACK. WHAT SHOULD YOU DO FIRST?

A Discuss with the attacker to bargain the ransom

B Pay the ransom

C Quarantine affected systems, lock down access to backup systems until after the infection gets removed

D Do nothing

Correct Answer

C

Quarantine affected systems, lock down access to backup systems until after the infection gets removed

The goal is to remove the ransomware from infected systems, restore systems and files from a legitimate trusted site (ideally from backups), and patch vulnerabilities (if the ransomware has used such an entry vector).

6.WHAT KINDS OF RANSOMWARE EXIST?

A Encrypt, Delete

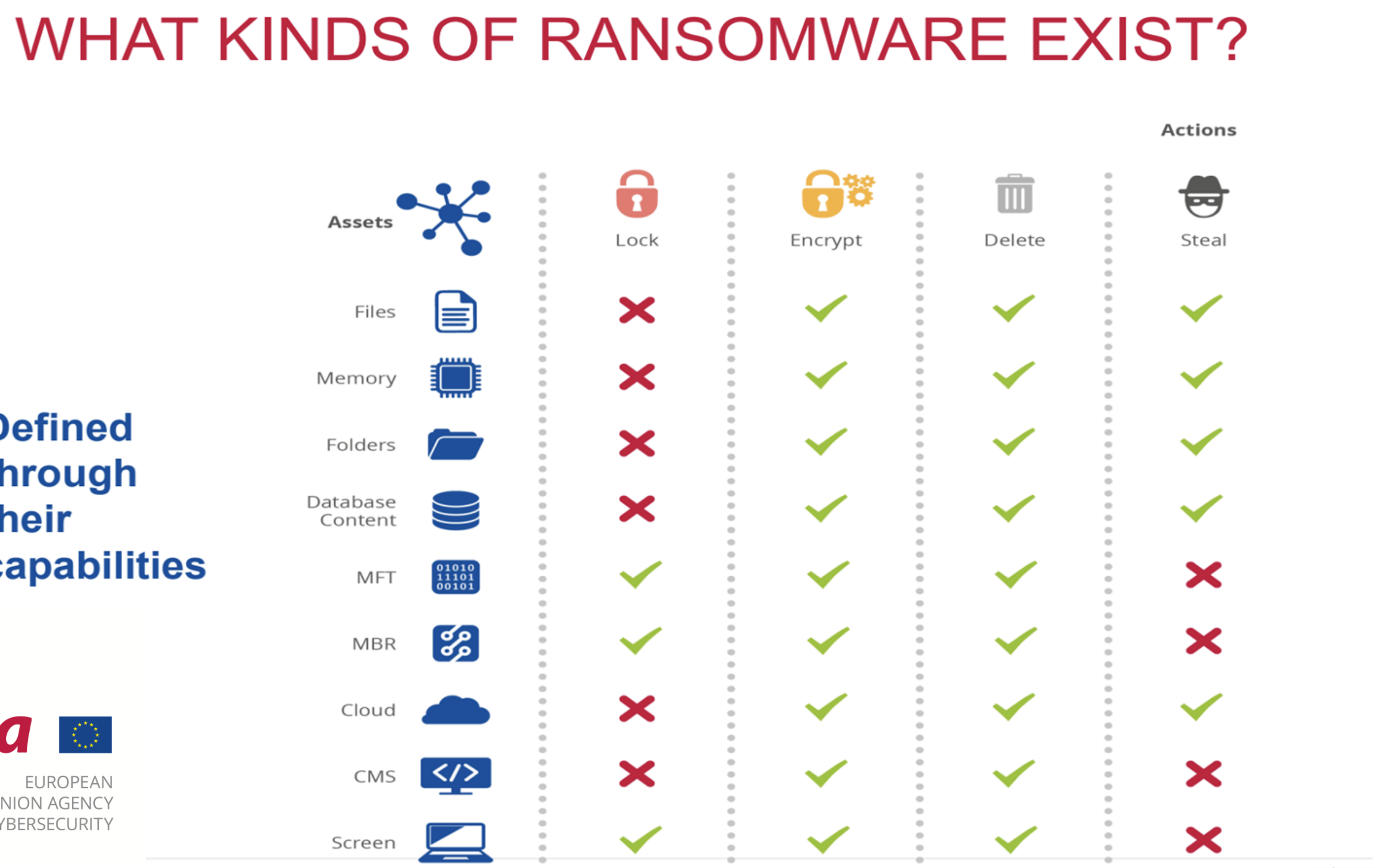
B Lock, Encrypt, Delete

C Lock, Encrypt, Delete, Steal

D Encrypt, Delete, Steal, Create

QUIZ
Correct Answer

C



WHAT KINDS OF RANSOMWARE EXIST?

	Actions			
Assets	Lock	Encrypt	Delete	Steal
Files	✗	✓	✓	✓
Memory	✗	✓	✓	✓
Folders	✗	✓	✓	✓
Database Content	✗	✓	✓	✓
MFT	✓	✓	✓	✗
MBR	✓	✓	✓	✗
Cloud	✗	✓	✓	✓
CMS	✗	✓	✓	✗
Screen	✓	✓	✓	✗

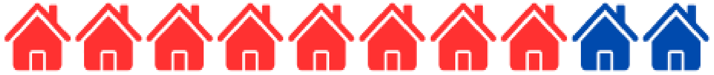
Defined through their capabilities

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Recent Statistics

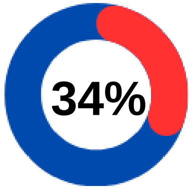
Over 80% of the SMEs surveyed by ENISA stated that cybersecurity issues would have a **serious negative impact on their business** within a week of the cybersecurity incident happening.

SMEs



57% say they would most likely become bankrupt or go out of business**.**

Ransomware remains the most prevalent danger, making up **34%** of all threats in the European Union.



The demanded ransom in Europe grew from €13m in 2019 to **€62m** in 2021.

Ransomware targeted various sectors, with **manufacturing** (14%) & **health** (13%) topping the list, followed by **public administration** (11%) & **services** (9%)**.**

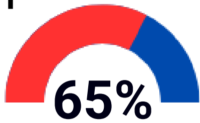
The average downtime a company experienced in 2021 after a ransomware attack was 23 days.

23 days

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Recent Statistics

European healthcare services disruption in the period **January 2021 - March 2023** was related to ransomware threats  of the cases.

Social engineering attacks grew significantly in 2023 with **Artificial Intelligence (AI)** and new types of techniques are emerging, but **phishing** still remains the top attack vector.

Out of the **observed events related to social engineering**, **30 percent were aimed at the general public**, 18 percent at public administration, and 8 percent at all sectors.

SOLUTION

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

[Surname Name as seen in the employee list without space*]

C	L	U	E	L	E	S	S	J	O	E			

WHO MADE THE FRAUDULENT PAYMENT?

C	L	I	C	K	A	L	L	J	A	C	K		

ENCRYPTION KEY

C	L	I	C	K	L	E	S	S

What is the filename of the decrypted file?

S	E	C	U	R	E	S	M	E