



AR-IN-A-BOX

# CYBER AWARENESS GAME

Online Retail Hack

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](http://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](mailto: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.



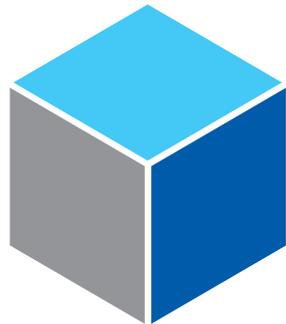
# Game Rules

- Create teams or Play Individually
  - Choose a Team Leader
  - Choose a Team Name
- Answer the Questions
- Discuss your Solution



**THE GAME STARTS HERE**

**PHASE 1**



# 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. The attackers claim that they will wipe all data, so hurry up!

**GOOD LUCK!**

# 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

# 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 News

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.

# TASK UPDATE #1

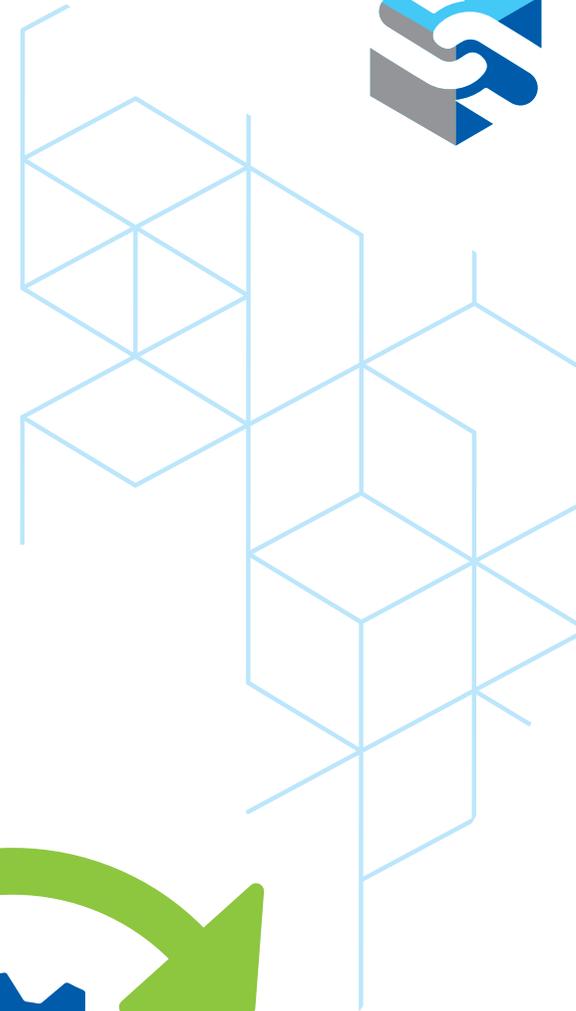
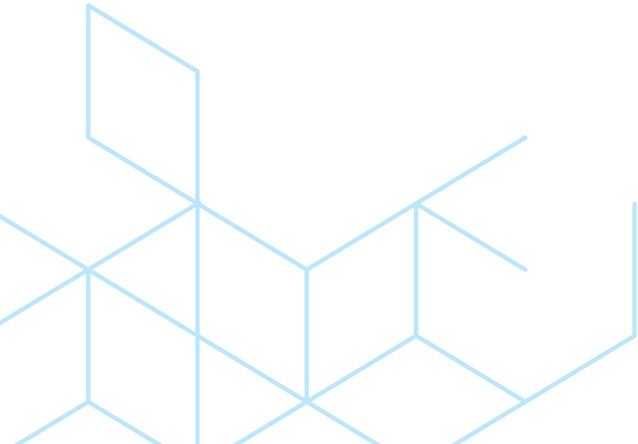
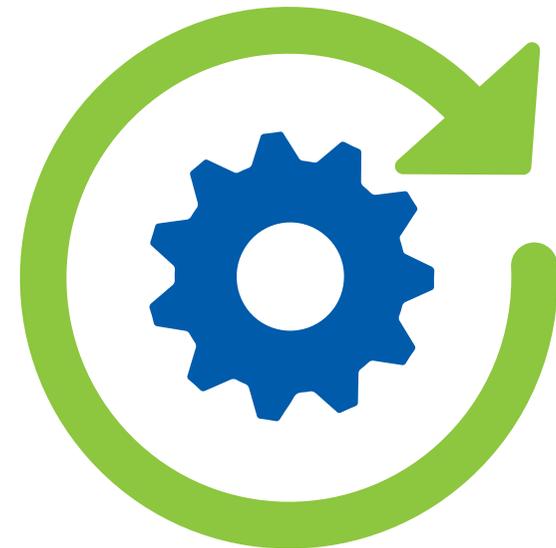
A number of suspicious emails have been recovered while investigating the hack.

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

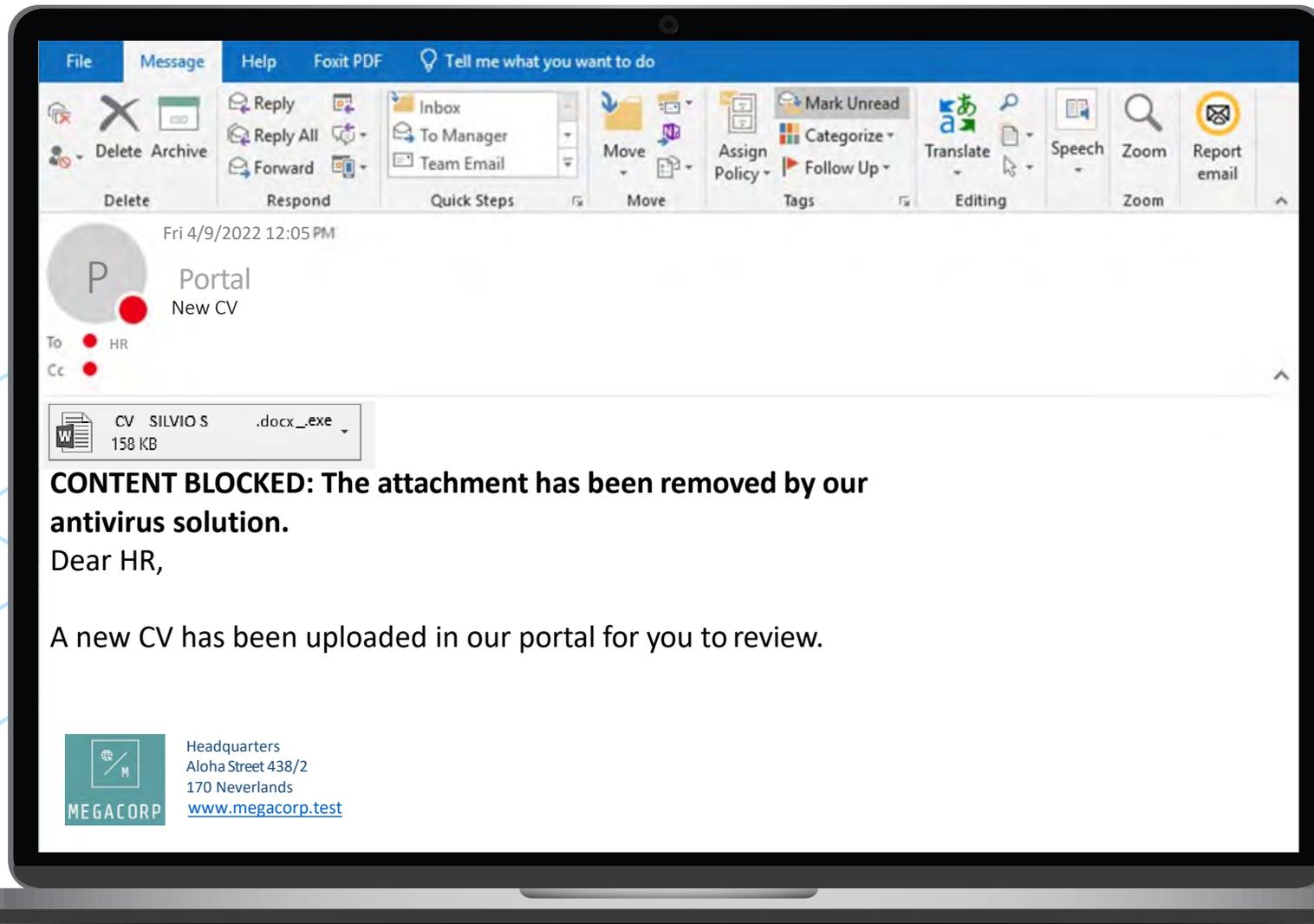
It is believed, based on our analysis, that the attacks started from a single email. That's how the hackers got access to the MEGACORP file servers.

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

Good Luck,  
The Management

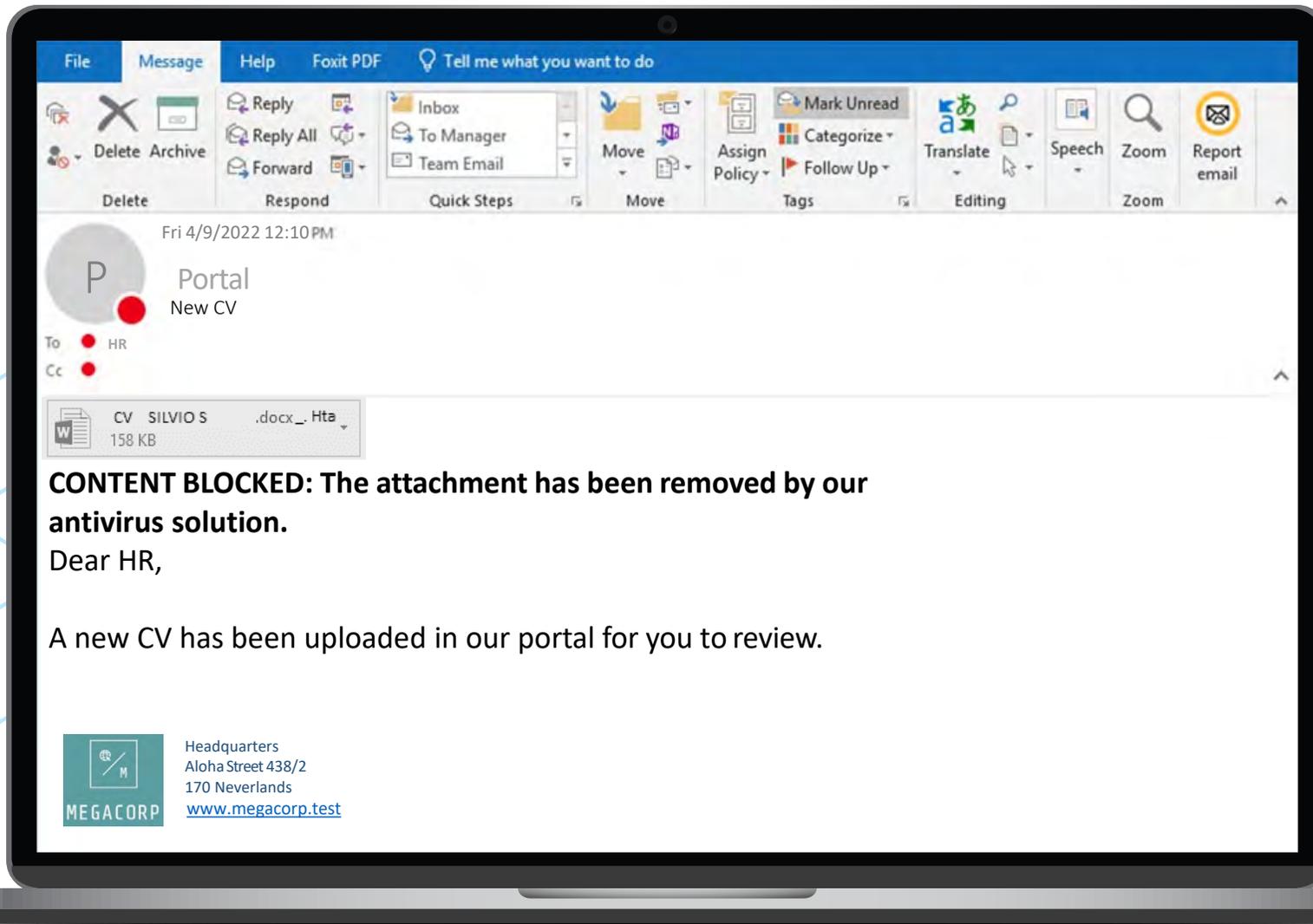


# SUSPICIOUS MAIL



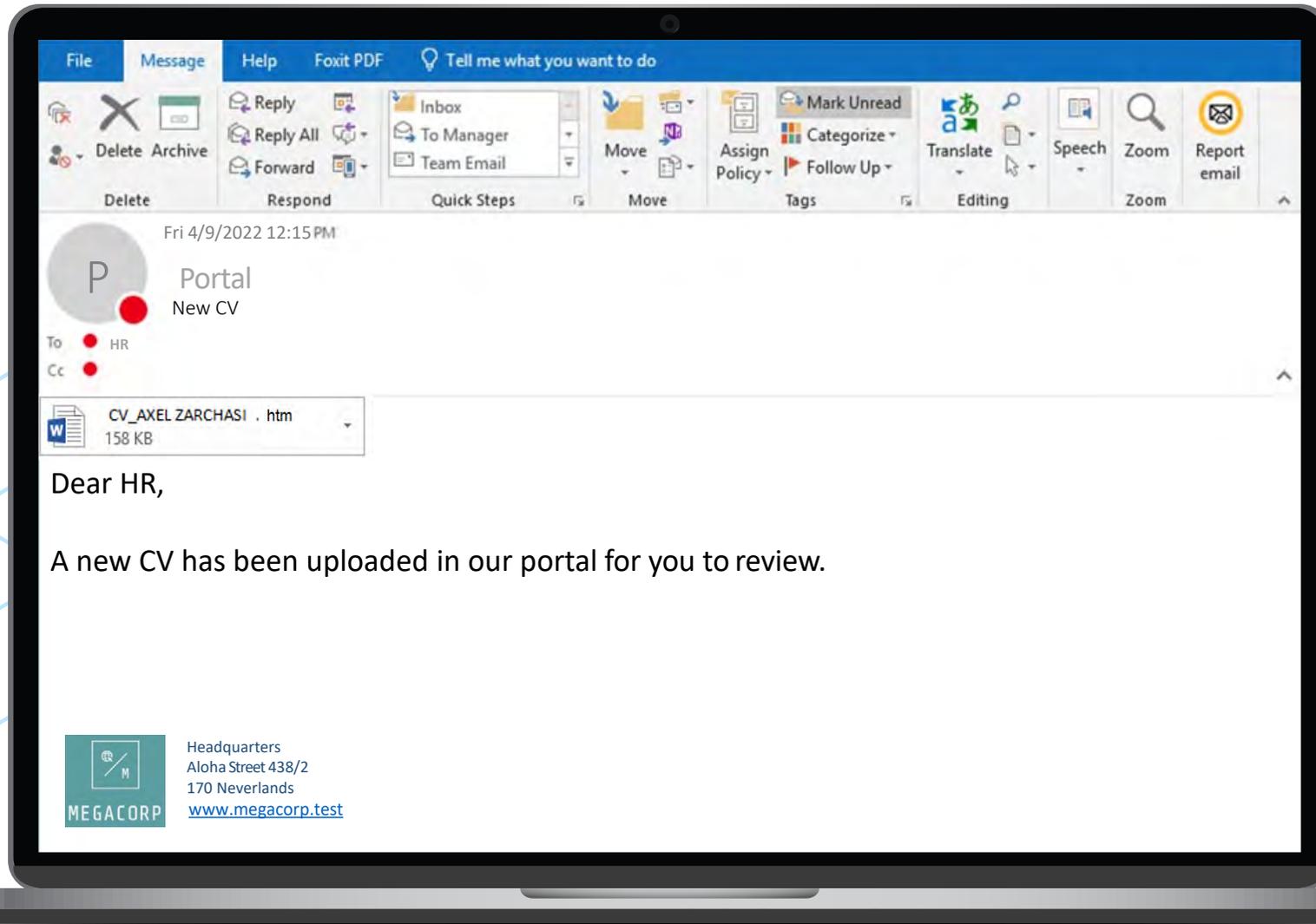
PHISHING ATTACK

# SUSPICIOUS MAIL



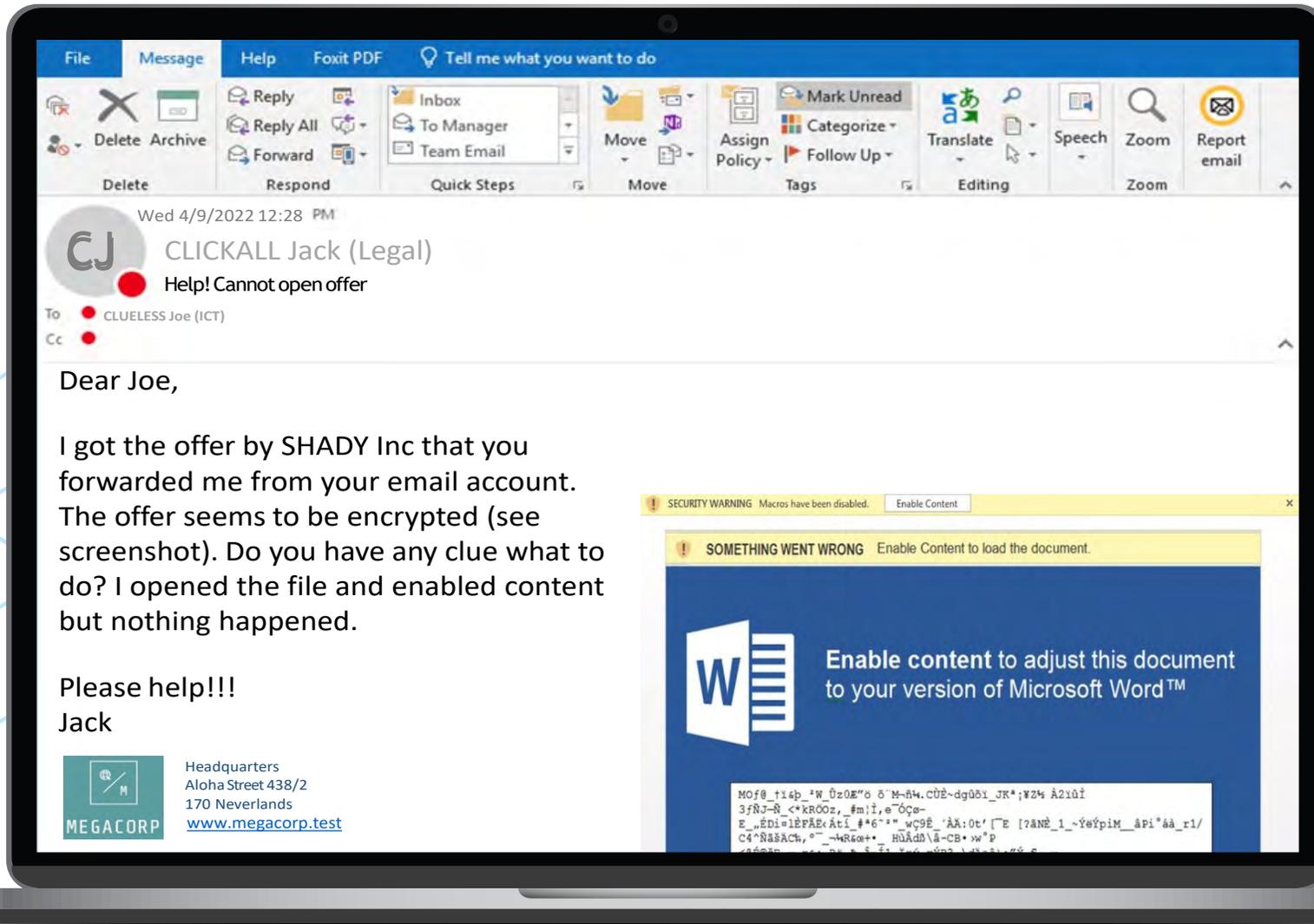
**PHISHING ATTACK**

# SUSPICIOUS MAIL



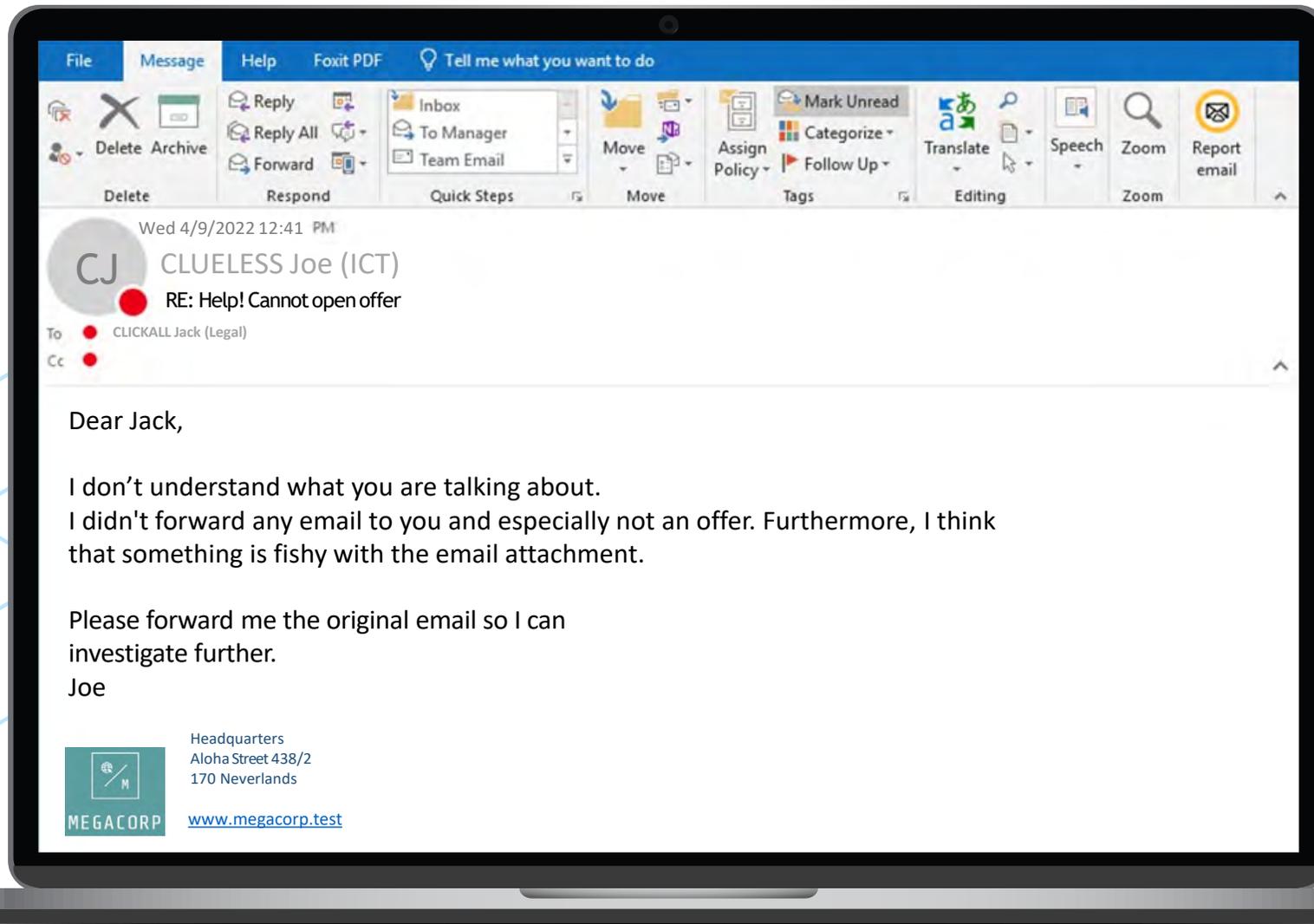
**PHISHING ATTACK**

# SUSPICIOUS MAIL



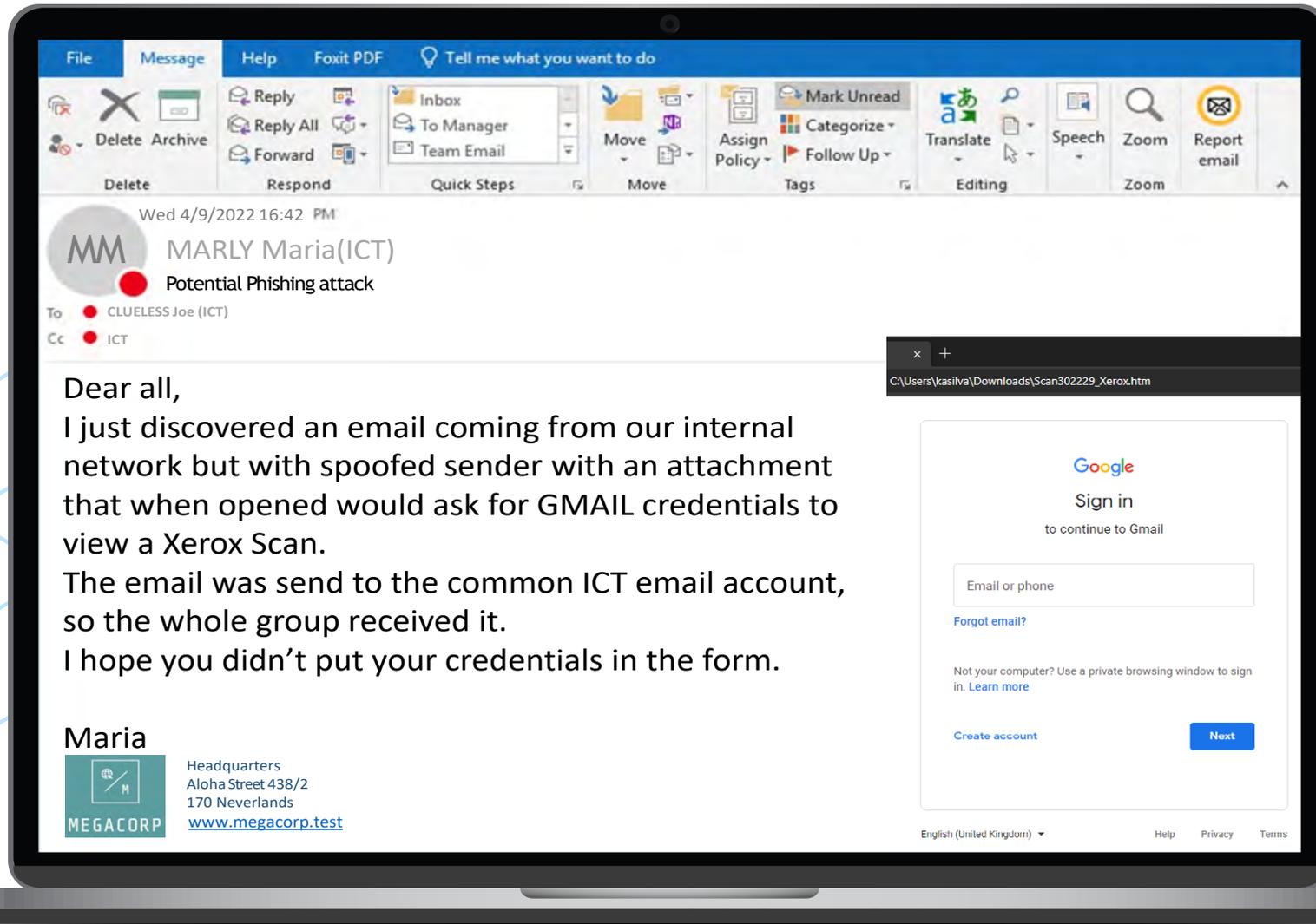
PHISHING ATTACK

# SUSPICIOUS MAIL



PHISHING ATTACK

# SUSPICIOUS MAIL

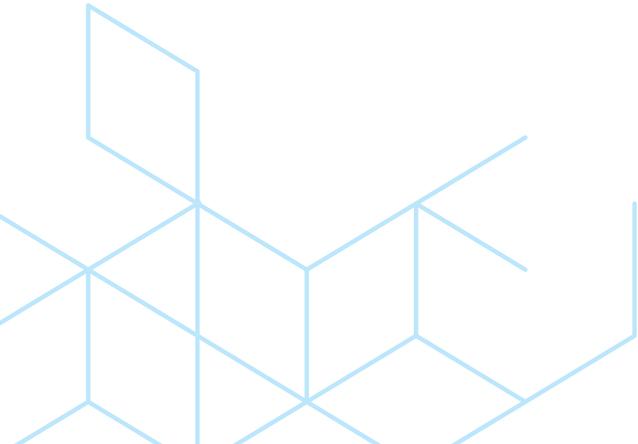


PHISHING ATTACK

# Action Time

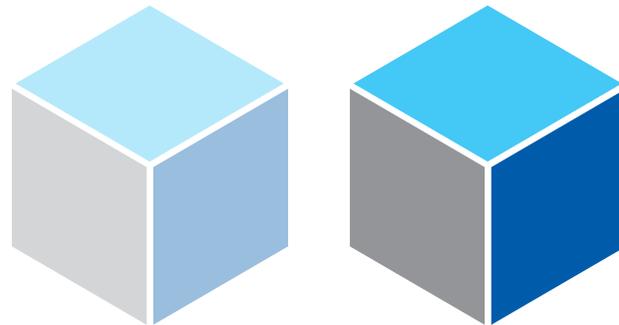
Based on your experience can you please draft some answers on the following questions:

- **Q1.** Which type of attack most likely took place?
- **Q2.** Can you explain the attacker's steps so far?
- **Q3.** Was the email Antivirus configured correctly?

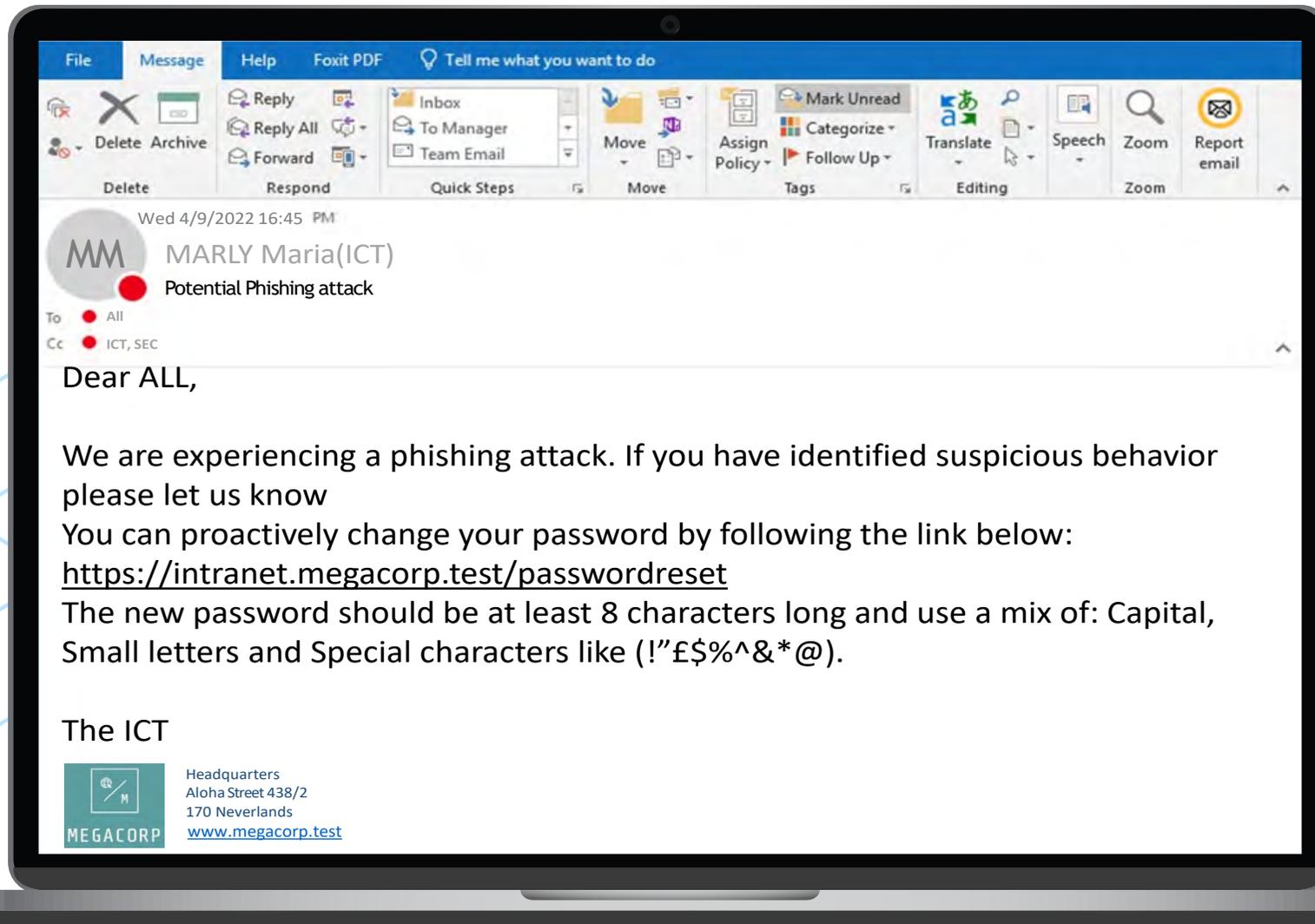


**THE GAME STARTS HERE**

**PHASE 2**

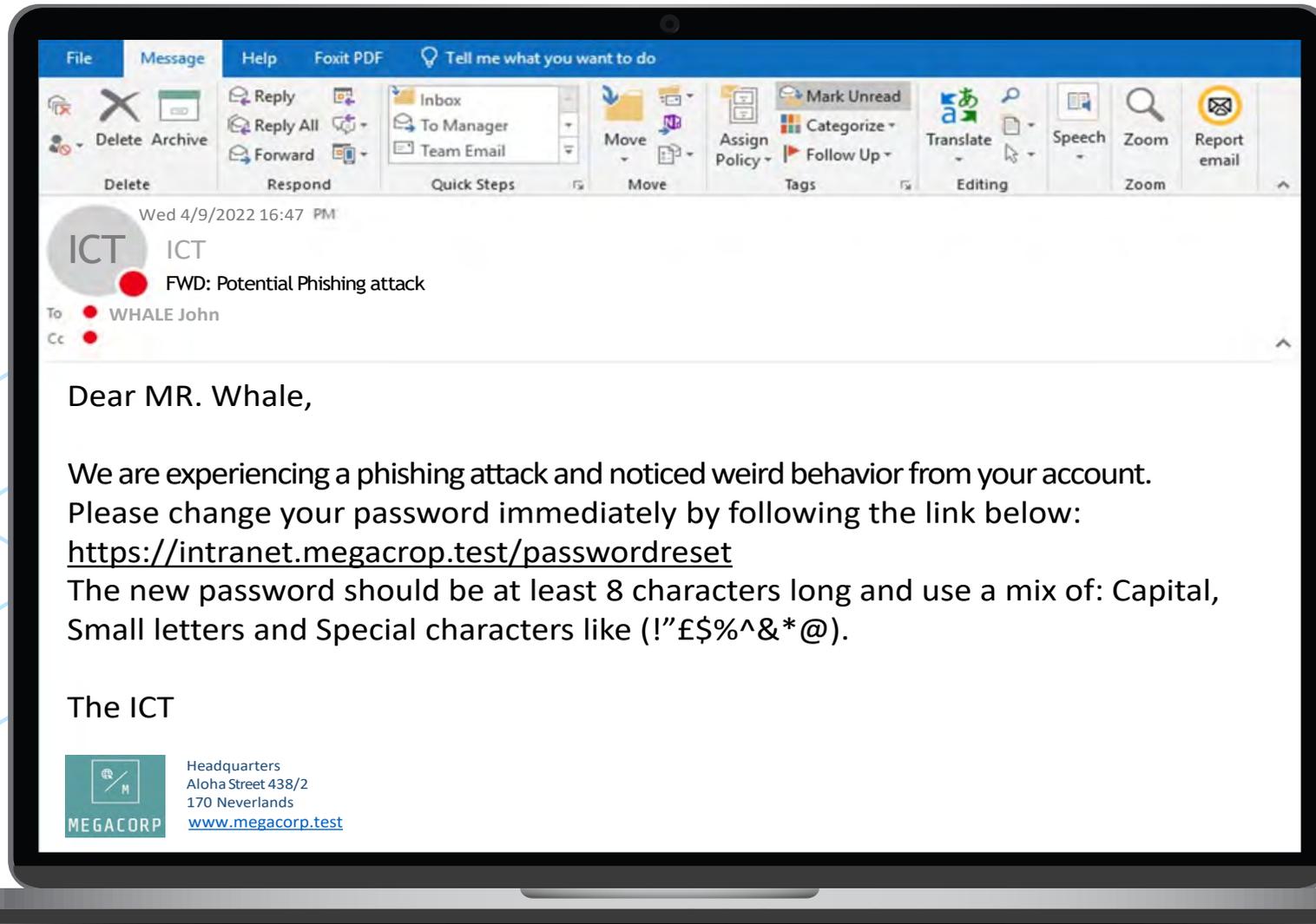


# SUSPICIOUS MAIL



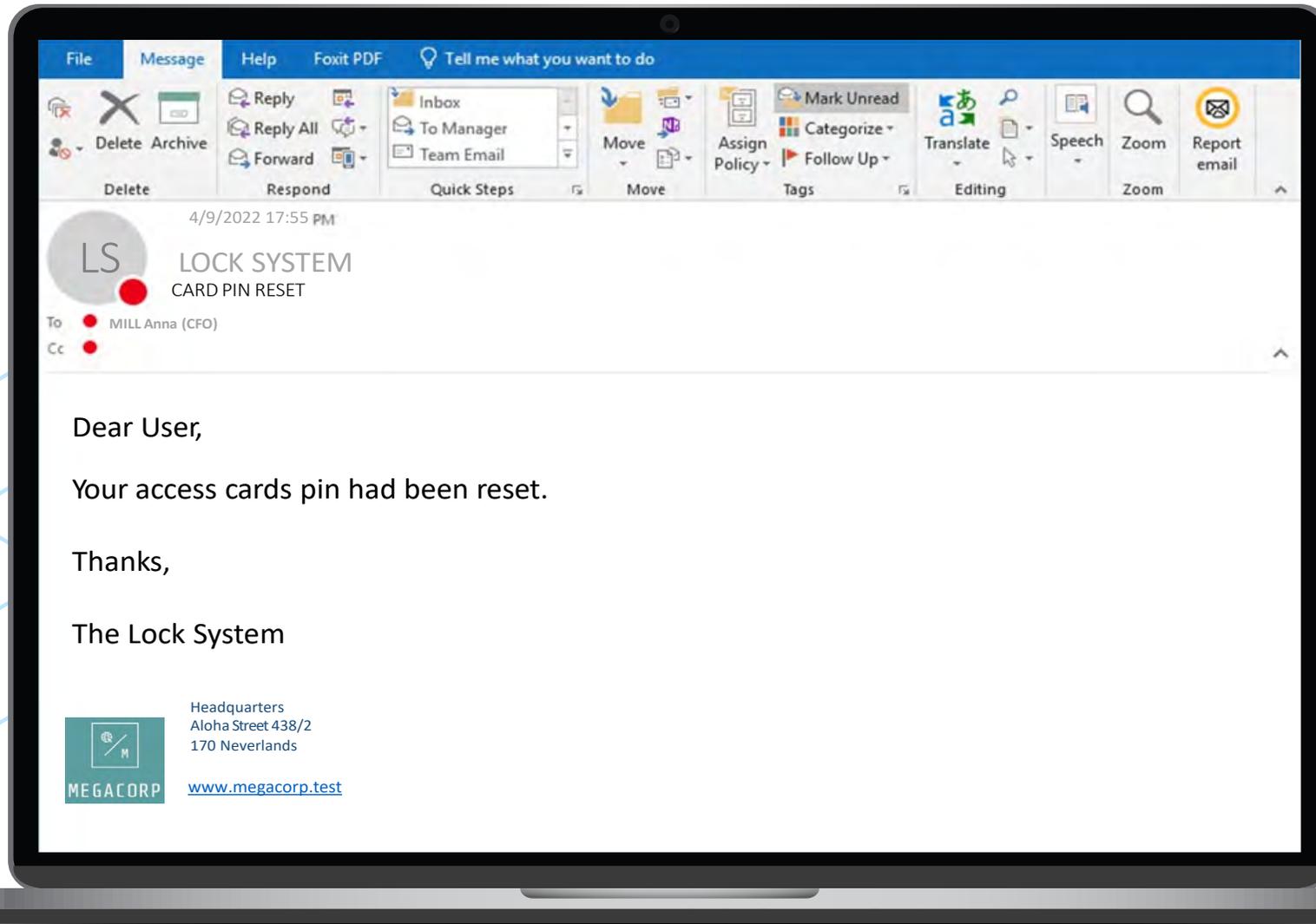
PHISHING ATTACK

# SUSPICIOUS MAIL



PHISHING ATTACK

# SUSPICIOUS MAIL



PHISHING ATTACK

# MORE SOCIAL MEDIA POSTS



# Action Time

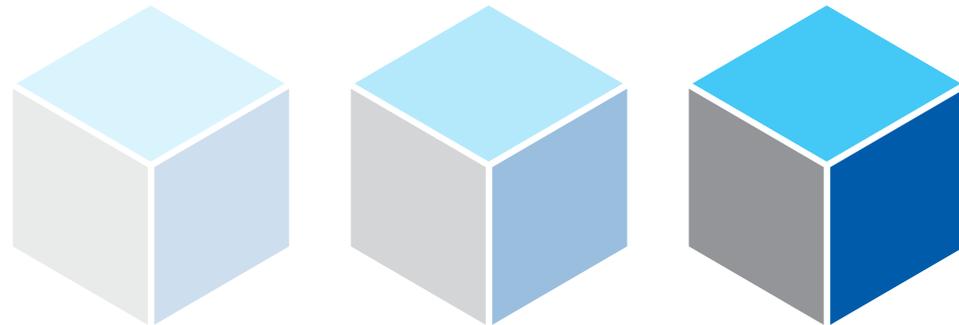
Based on your experience can you please draft some answers on the following questions:

- **Q4.** Can you spot a bad practice in password management?
- **Q5.** Is there anything else suspicious in the emails?  
More attacks maybe?



**THE GAME STARTS HERE**

**PHASE 3**

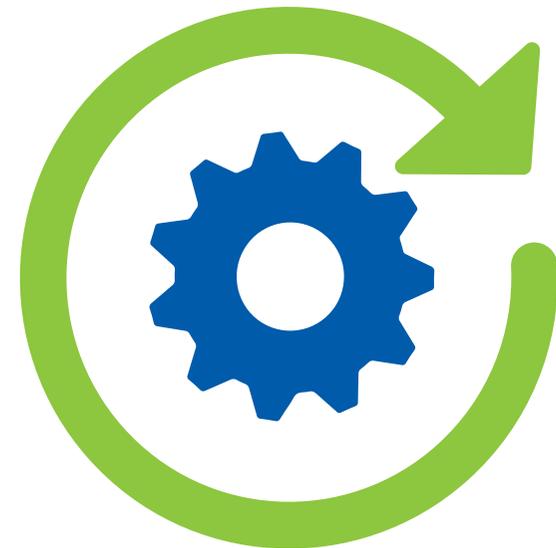


# TASK UPDATE #1

Suspicious activity has been detected in MEGACORP HQ. 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's. Dig into the logs to identify the SECURITY breach that lead to stolen the info and the ransomware infection. We count on you to perform the analysis as fast as possible.

Good Luck!

Good Luck,  
The Management



# ACCESS LOGS – MEGACORP



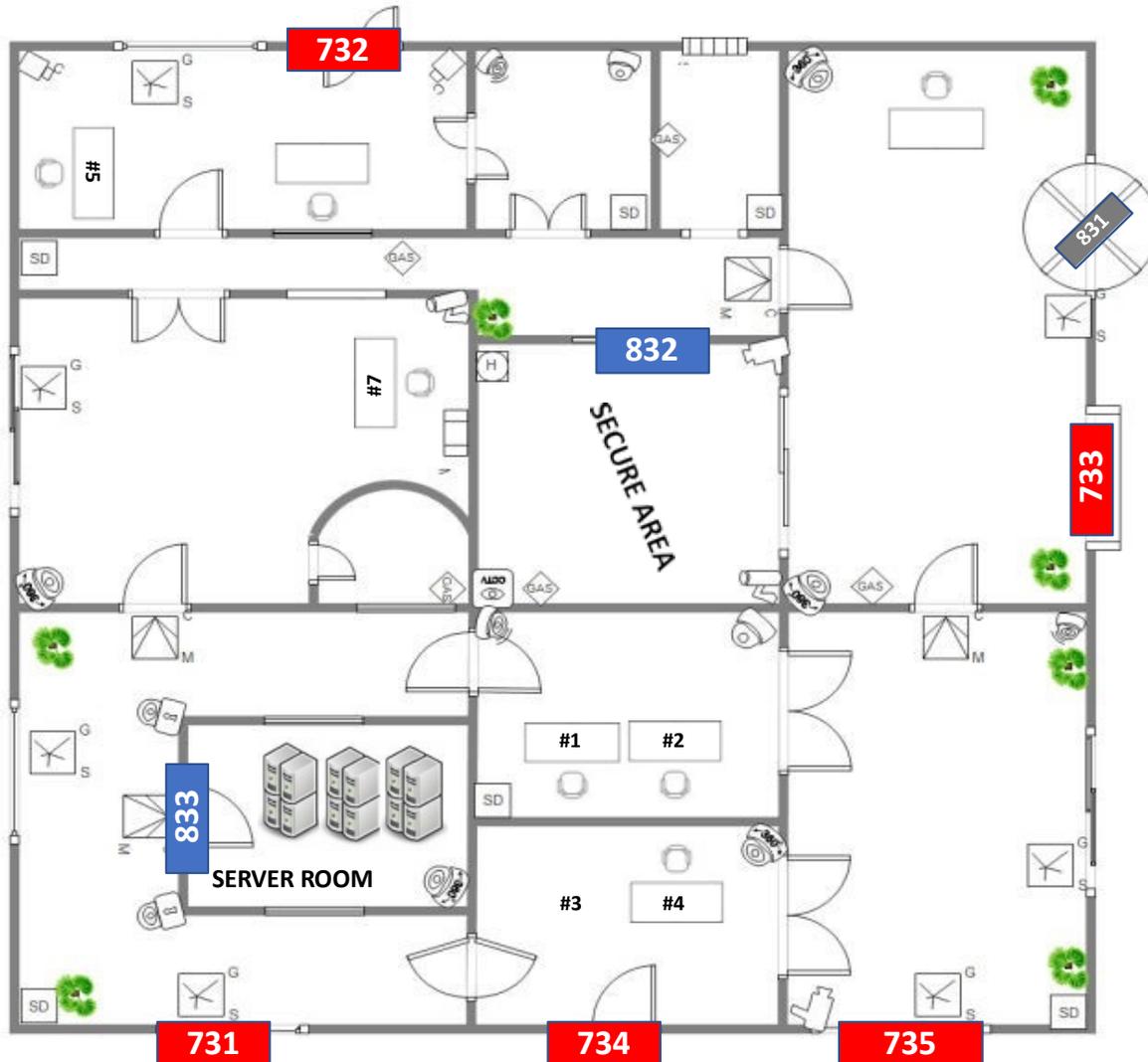
| BADGE ID | Name          | READER ID | Date       | TIME  |
|----------|---------------|-----------|------------|-------|
| FA23RN1  | Mill Anna     | 831       | 04/09/2022 | 8:30  |
| IT23RL2  | Clueless Joe  | 831       | 04/09/2022 | 8:38  |
| AL3XZA4  | Clickall Jack | 831       | 04/09/2022 | 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

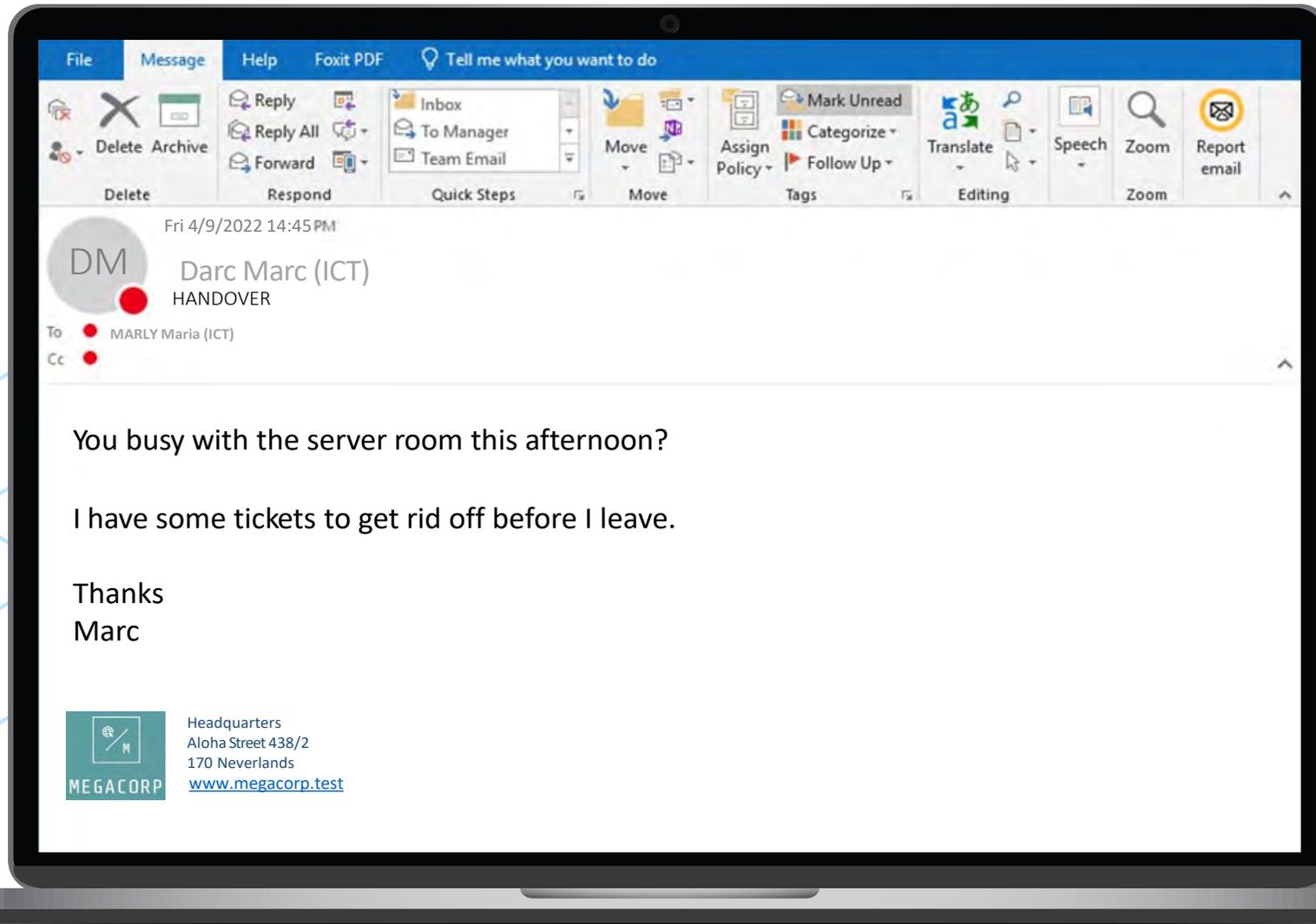
**MILL Anna**  
CFO  
ID: FA23RN1

**DARC Marc**  
ICT - Contractor  
ID: IT21NO6

**MARLY Maria**  
ICT  
ID: IT11NI9

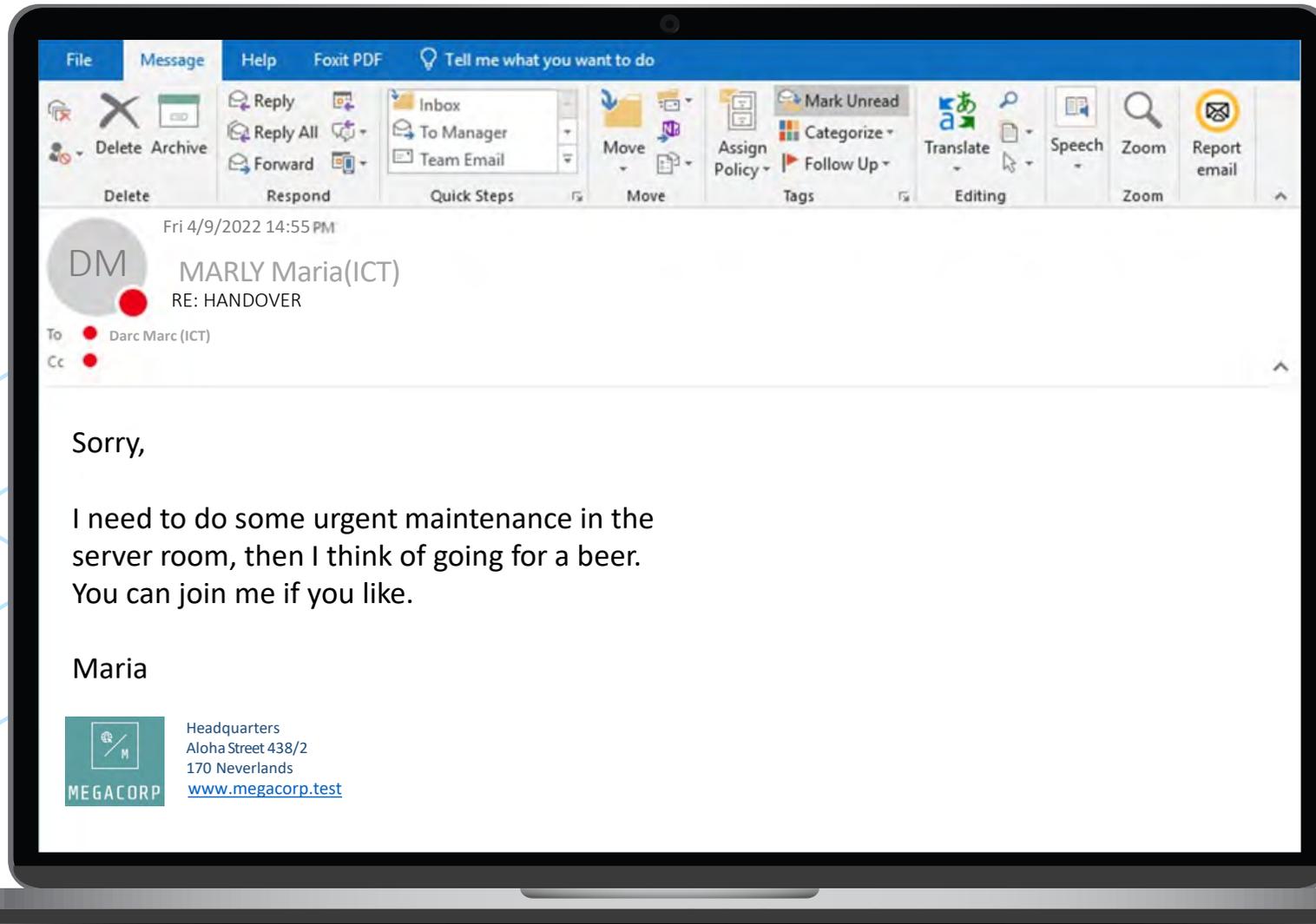
UNAUTHORISED ACCESS

# SUSPICIOUS MAIL



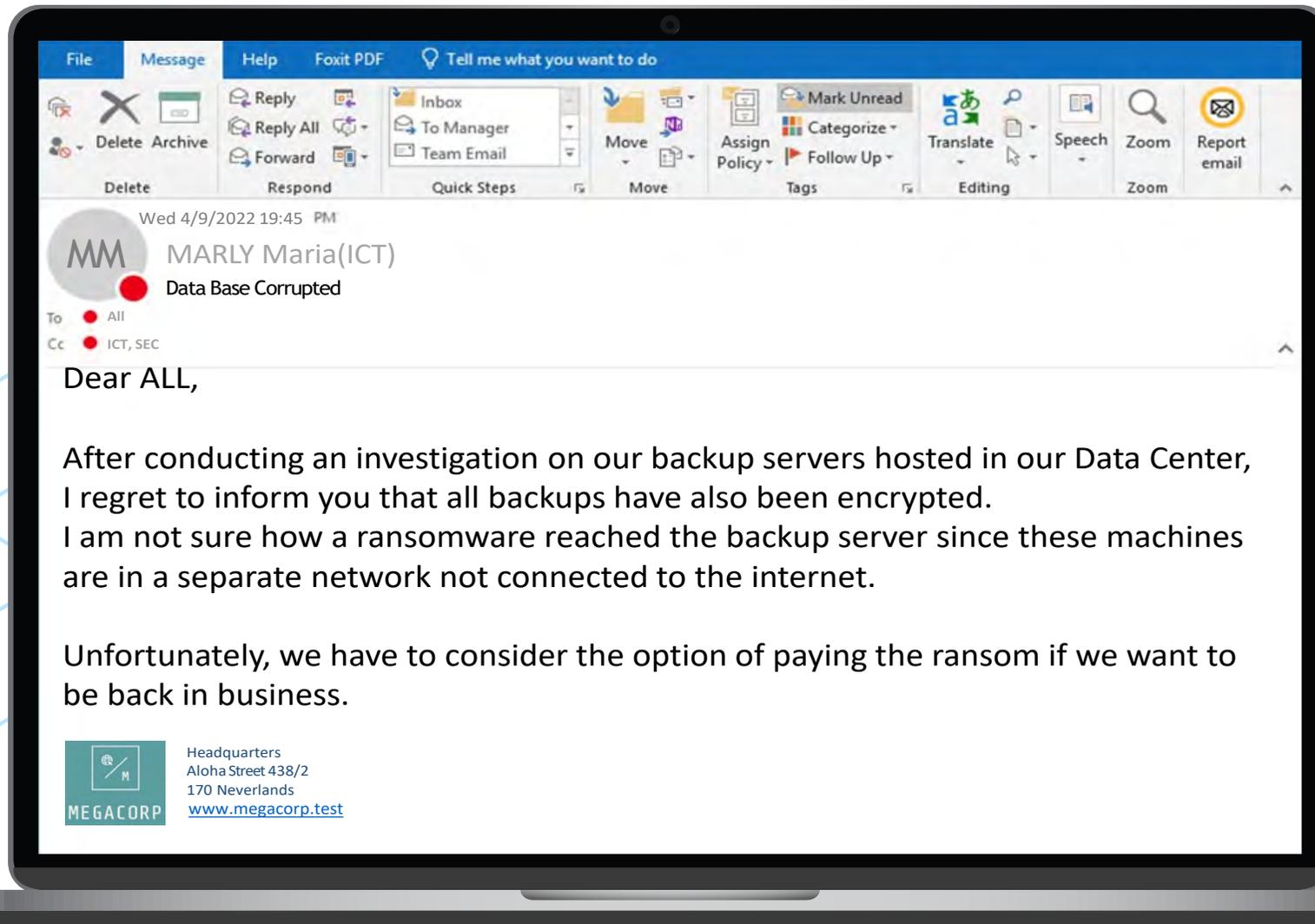
PHISHING ATTACK

# 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

**LIVE** breakyourownnews.com



**BREAKING NEWS** MEGACORP

**MEGACORP CAUGHT REDHANDED**

**16:05** USERS FURIOUS AFTER MEGACORP LEAKED DATA EXPOSE SALE OF PERSONAL INFO TO

 **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

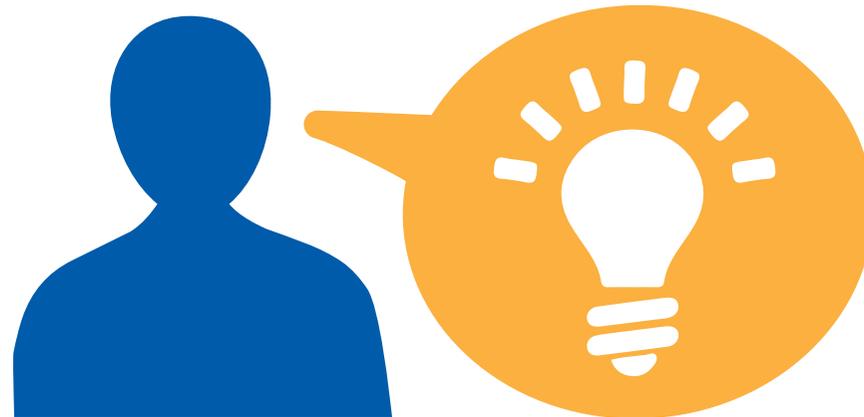


**FAKE NEWS**

# Action Time

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

- **Q6.** What could have been a measure taken that could have saved your data for the scenario presented, making paying the ransom obsolete?
- **Q7.** What would be the correct steps to follow in case of public leakages of your clients DB after a hack?
- **Q8.** What would be the steps to follow in case of defamation (fake news) against your company after a hack?



# DRAFT YOUR SOCIAL MEDIA RESPONSE



MEGACORP

@Megacorp



0/280 characters

12:00 PM · Jun 1, 2021

[Click to add client...](#)

Retweets

Quote Tweets

Likes

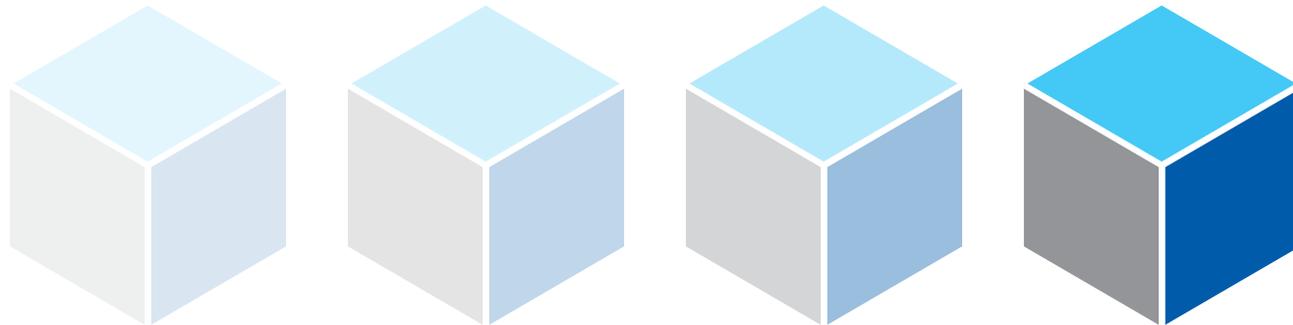
[Randomize all](#)



**FAKE NEWS**

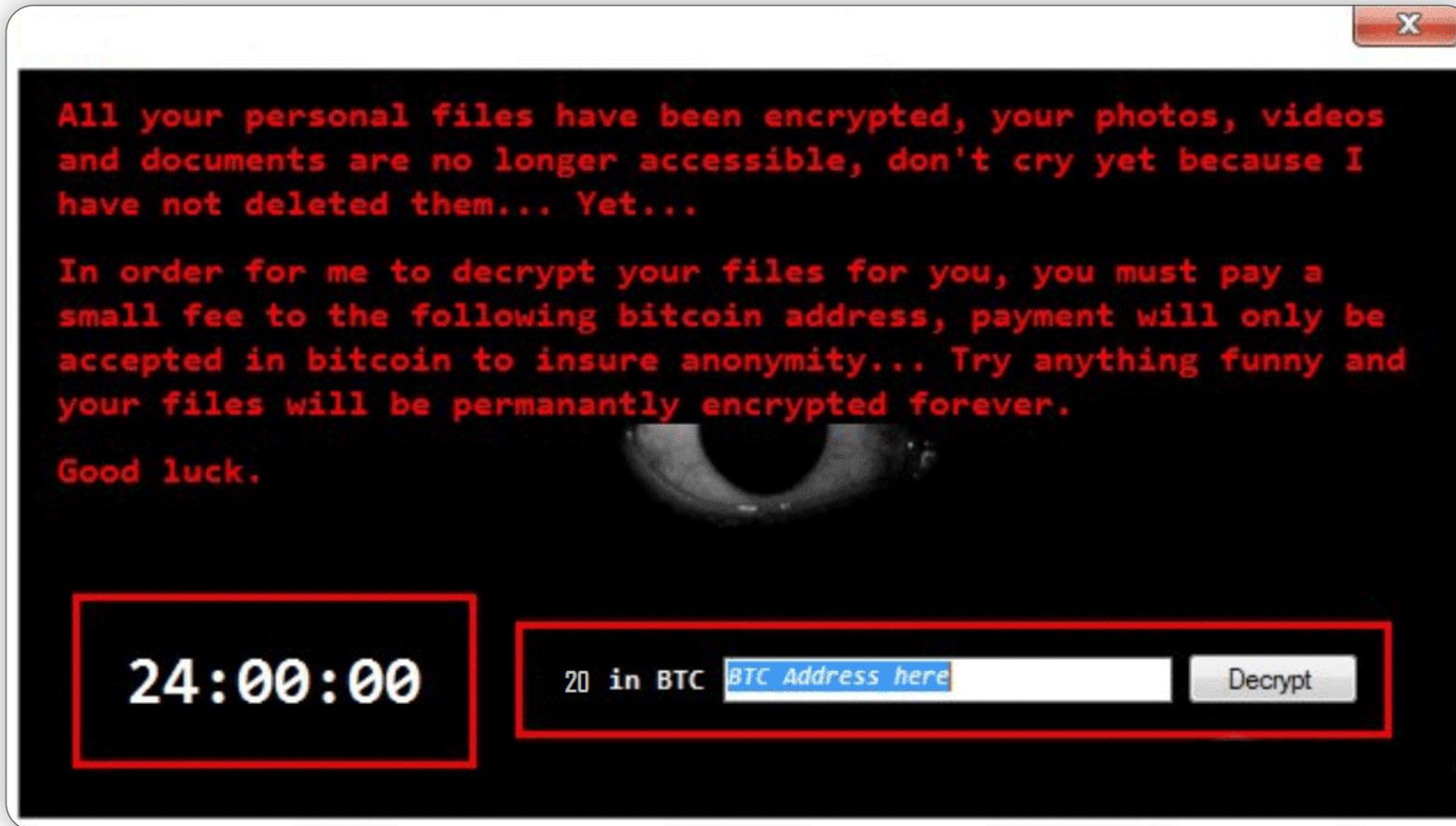
**THE GAME STARTS HERE**

**PHASE 4**





# THE RANSOMWARE NOTE



File to unlock:



**UVOAQQY 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

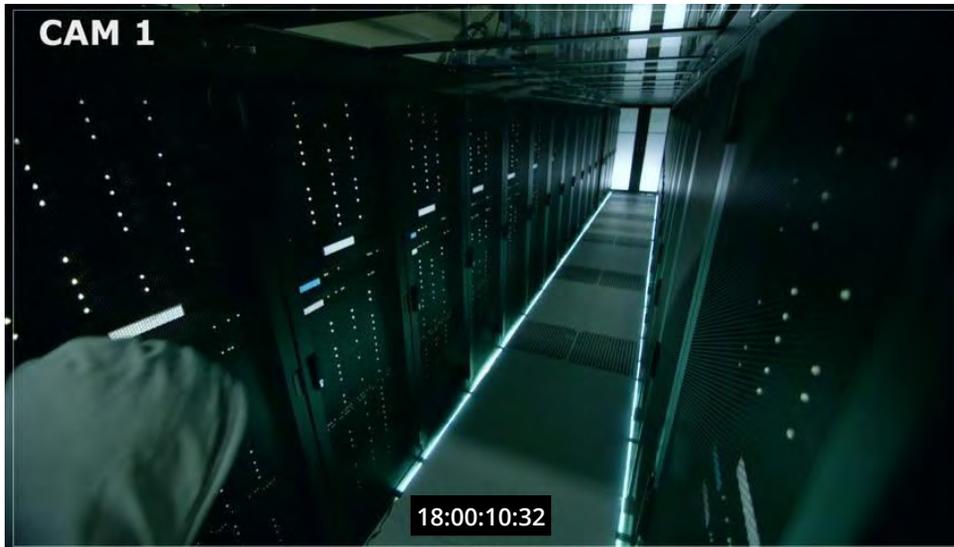
**DECRYPTION MECHANISM:**

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 |



# Server Room: Camera Footage



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

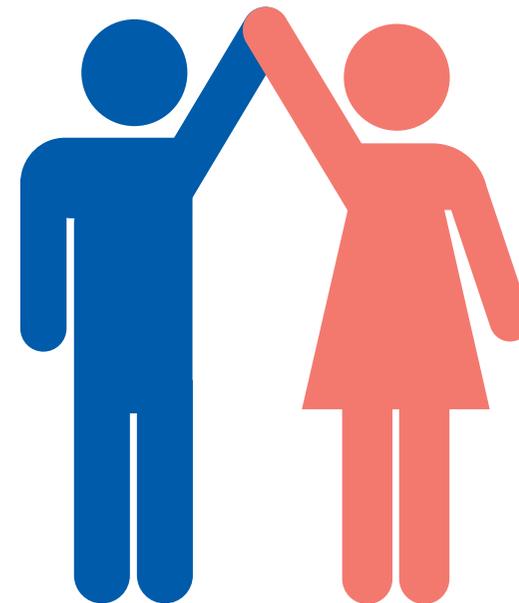
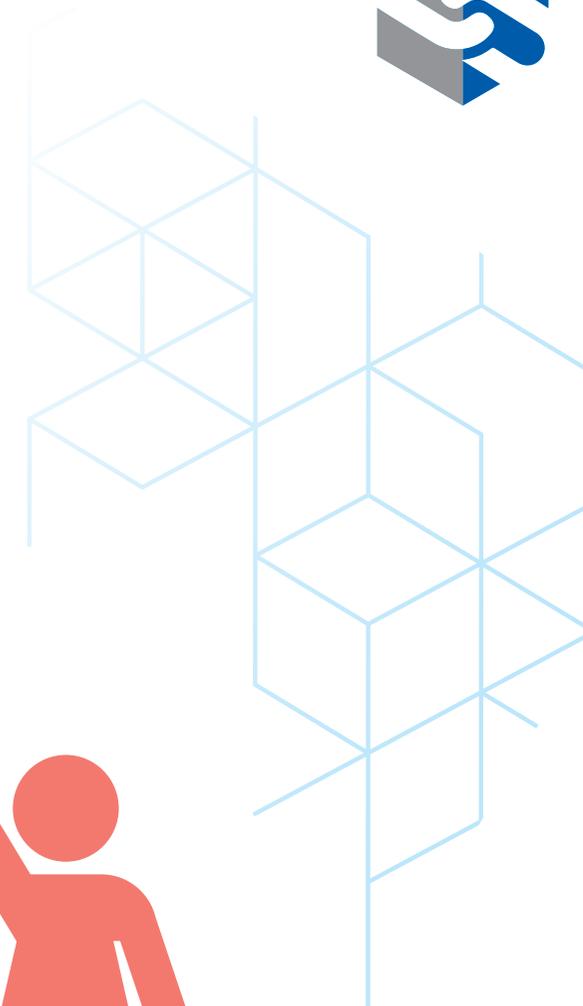


UNAUTHORISED ACCESS

# Almost there

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

- **Q9.** What was the name of the INSIDER that was behind the attacks
- **Q10.** Would you have paid the ransom?



# ANSWER SHEET



**What is the name of the first known victim of the PHISHING 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?**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|



# SOLUTION

What is the name of the first known victim of the PHISHING 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

