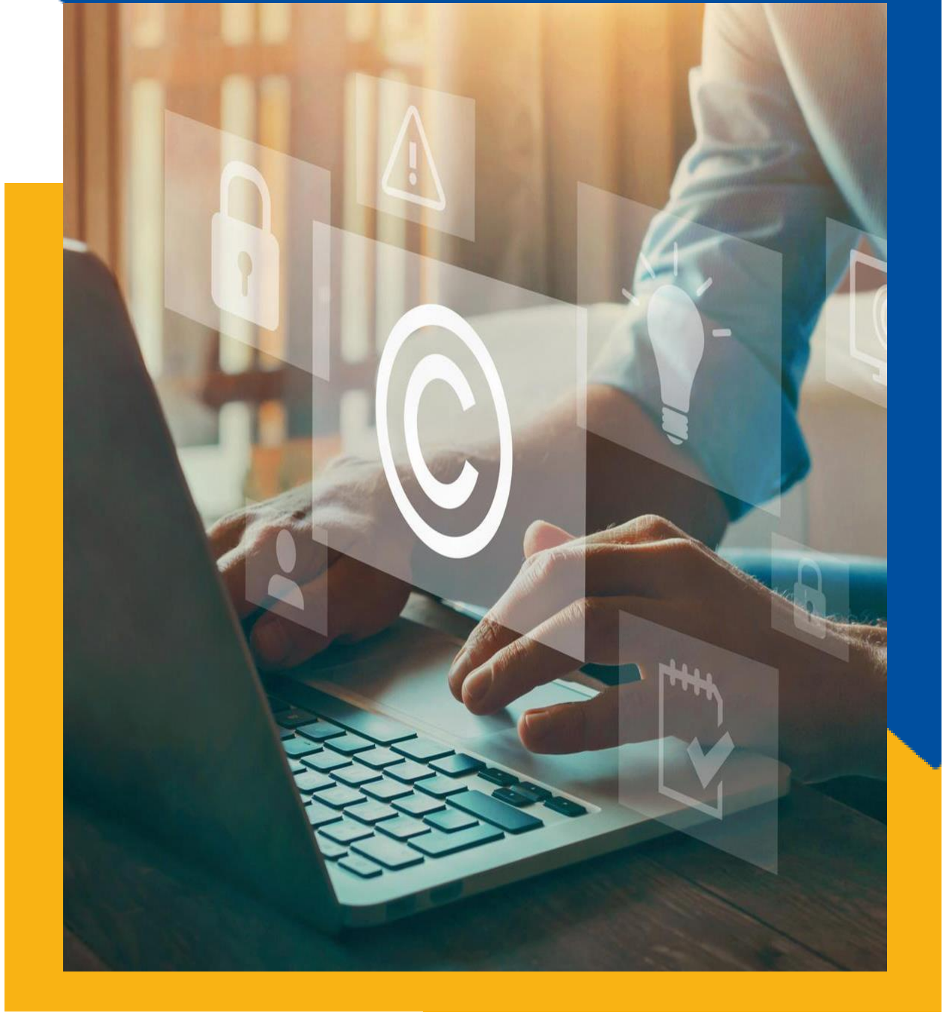
AR-IN-A-BOX

SMEs Edition

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

AR-in-a-BOX SME Edition

BE PREPARED REDUCE THE IMPACT



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 Crisis Communication Toolbox, 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.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

WHY SME CYBERSECURITY

With increasing reliance on technology, cybersecurity became crucial for maintaining SMEs business operations and protecting their data.

80% of SMEs surveyed by ENISA state that cybersecurity issues would have a serious negative impact on their business, 57% say they could likely go out of business.

Social engineering attacks grew significantly in 2023, with 30% of attacks targeting the general public. 90% of security incidents start with phishing. Awareness and preparedness are key counter-measures.

SMEs edition

Prepare to avoid disaster

Train to empower & modernise

Measure to assure effectiveness

AR-IN-A-BOX STARTING POINT

- **Template for a custom awareness programmes** for internal use within an organisation.
- **Examples of Key Performance Indicators to evaluate the effectiveness of a programme or campaign.**
- **A step-by-step** guide for the development of internal and external **cyber crisis communication plans.**
- **An awareness raising quiz** to test comprehension and retention of key information.
- **An awareness raising game,** along with a guide on how to play.
- ***Instructions on selecting the appropriate tools and channels to effectively reach the target audience.***
- ***A guideline on creating targeted awareness campaigns for external stakeholders.***
- ***A guide for the development of a communication strategy, crucial for achieving awareness objectives.***

SME EDITION

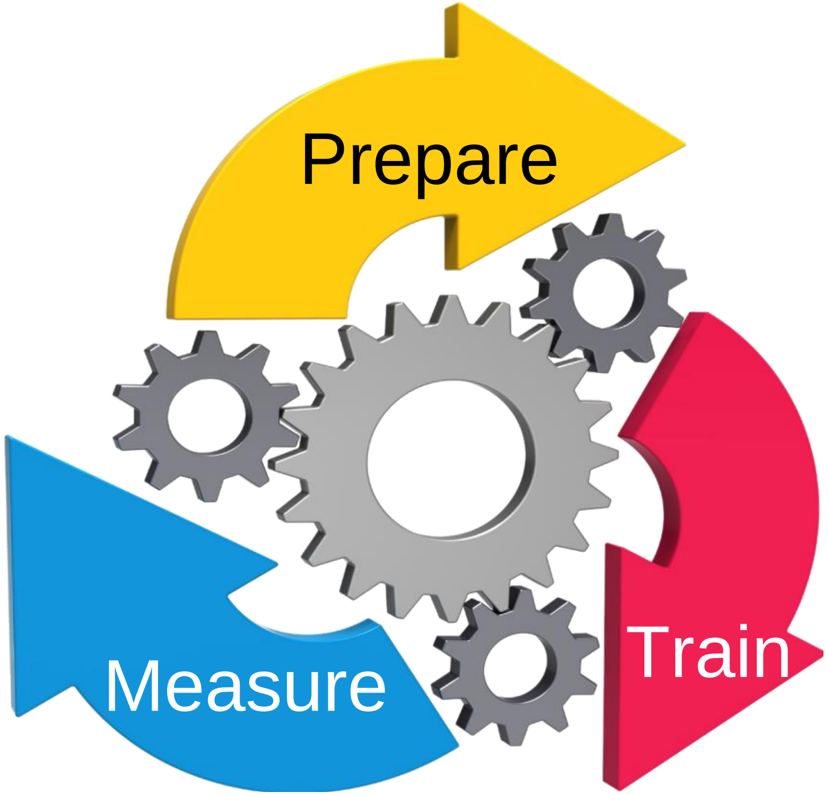
1. **Objective:** Create a customised AR in a box for SMEs

2. **Use case:** Phishing and ransomware attack are still Number 1 threat to SMEs, focus on small and micro enterprises, ensure adapted roles

3. **Format:** scenario driven, based on real events, visual, based on key steps / process

Repeat

Follow up on results, indicators and improvement opportunities in the other boxes.



Annual awareness programme template

Crisis communication plan

Annual awareness programme template

Awareness raising game

Awareness raising quiz

Key Performance Indicators

An awareness raising quiz

Crisis communication measurement objectives

Risk, Situation, Effectiveness assessment

ANNUAL CYBER AWARENESS PROGRAMME TEMPLATE

Consider and Formalise:

Who: Knowledge level
What: Topics
How: Method/Tool
Measure: KPI, Metrics, Means of measure
Why: Desired outcome
Result: Outcome and next steps
Timing: Month/date, duration
Cost: Budget, time

Examples of

KPIs, measures, objectives

Further ressources

Links, how to use tips

KPI EXAMPLES PROPOSED

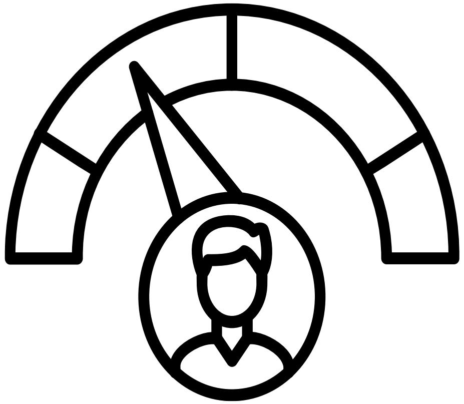
KPIs are proposed as examples to identify:

The ultimate objective of the awareness campaign

Depending on the objectives, the length, size, target, and content will differ.

Indicators to measure whether the KPI is achieved

Useful to measure the success of the awareness program and adapt when and where needed. Defining the indicators ahead will enable to design a ‘measurable’ campaign.



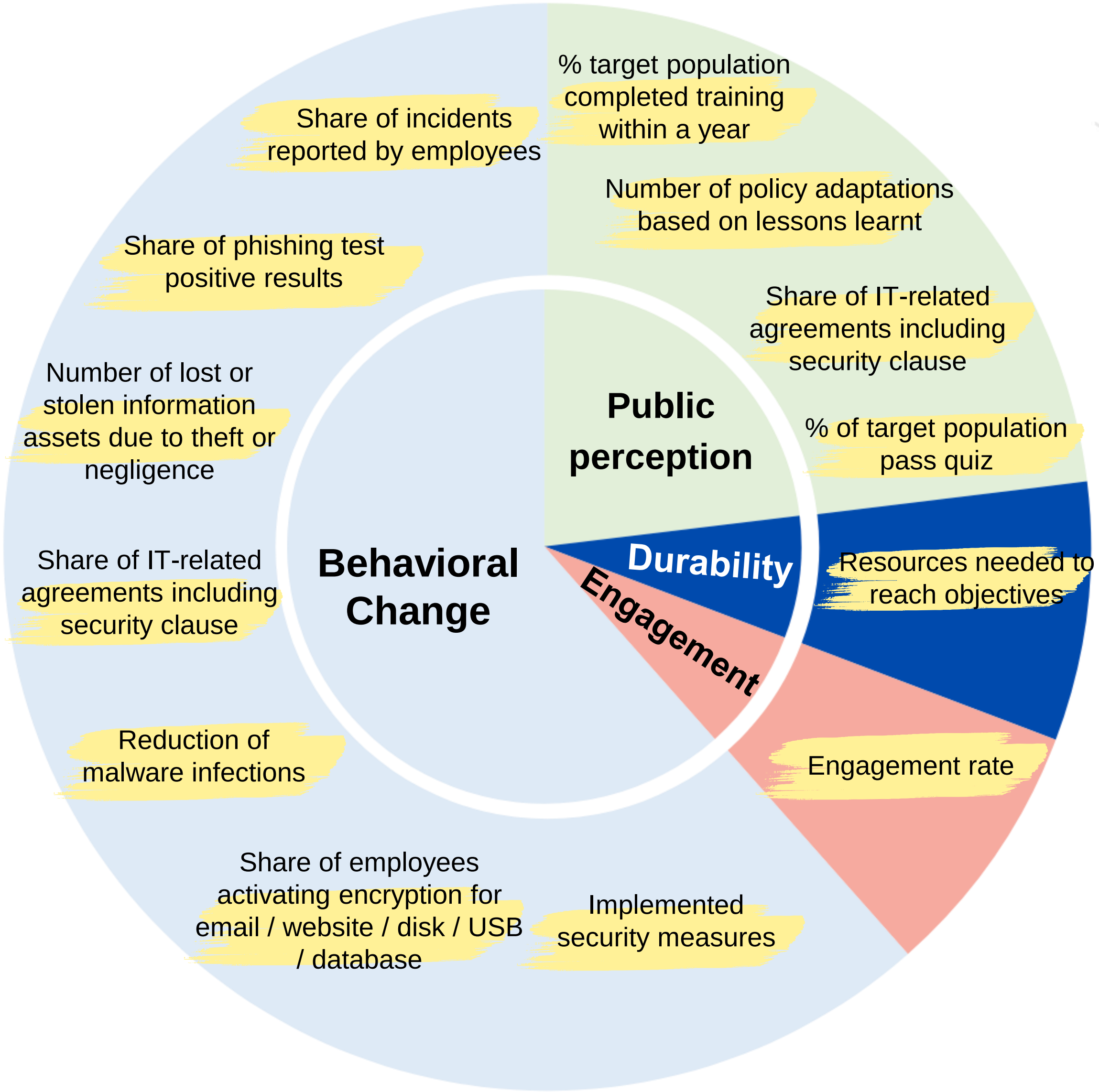
Principles

- **S**pecific
- **M**easurable
- **A**chievable
- **R**ealistic
- **T**ime bound

KPI EXAMPLES PROPOSED

KPI	Behavioral change								Scale of outreach			Public perception	Durability
Indicator	Share of incidents reported by employees	Share of phishing test positive results	Number of lost or stolen information assets due to theft or negligence	Share of IT-related agreements including security clause	Reduction of malware infections	Share of employees activating encryption for email / website / disk / USB / database	Number of instances of personal or sensitive information shared with unauthorized recipients	Implemented security measures	% of target population completed training within a year	Number of policy adaptations based on lessons learnt	% of target population pass quiz	Engagement rate (e.g. short survey)	Resources needed to reach objectives
Example of objective	90% of security incidents were reported by employees within 24 hours in the last 12 months. NB: this KPI implies that there is a defined channel for incident notification by employees	50% of employees report a phishing simulation email during the last campaign	No lost or stolen information assets due to theft or negligence in the last 12 months	80% of the IT-related agreements completed within the last 12 months include a security clause	The number of malware infections in the last 12 months is lower than the previous 12 months	100% of employees activated encryption on communication channels or storage spaces.	No such instances recorded in the last 12 months.	Number of people who have enabled multifactor authentication (MFA), configured automatic updates, installed antimalware or used a (reputable) virtual private network (VPN).	At least 90% of the targeted employees completed at least 1 cyber awareness training	At least 1 lesson learnt from the last exercise / tabletop feeds into a policy update	At least 80% of the target population successfully passed a quiz within the last 12 months	At least 70% of the survey respondents have positive feedback on the awareness campaign	Budget per person spent to meet KPIs / metric in the last 12 months

KPI EXAMPLES PROPOSED



Behavioral Change

- Share of incidents reported by employees
- Share of phishing test positive results
- Number of lost or stolen information assets due to theft or negligence
- Share of IT-related agreements including security clause
- Reduction of malware infections
- Share of employees activating encryption for email / website / disk / USB / database
- Implemented security measures

Public perception

- % target population completed training within a year
- Number of policy adaptations based on lessons learnt
- Share of IT-related agreements including security clause
- % of target population pass quiz

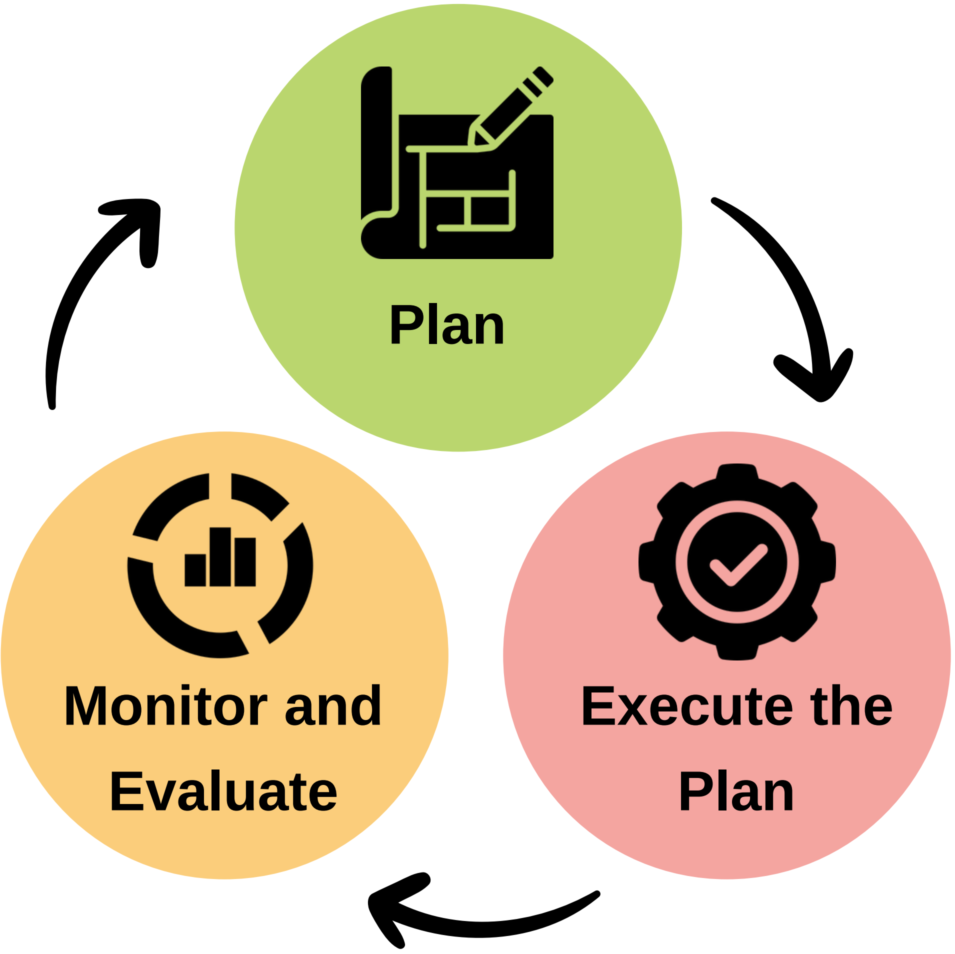
Durability

- Resources needed to reach objectives

Engagement

- Engagement rate

CYBER CRISIS COMMUNICATION GUIDE



Plan

1. **Risk, situation, target of communication** assessment
2. **Clear target, messages, roles** and communication **protocols**

Execute the Plan

1. **How to communicate** about a cyber crisis
2. **How to manage media inquiries**
3. **How to test the plan**

Monitor and Evaluate

1. **What to measure and monitor, and how**
2. **How to draw lessons learnt** from internal or other players’ in your sector cyber crisis experiences

BASIC PRINCIPLES

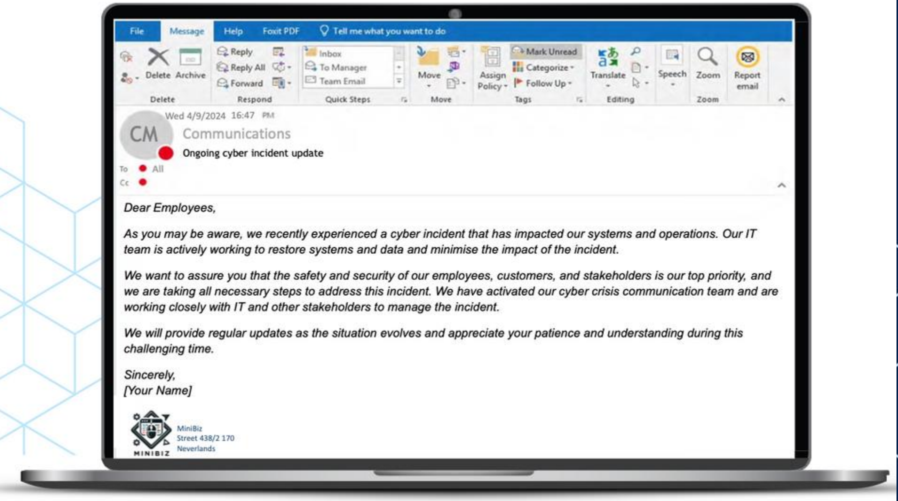
✓

1. Do conduct regular risk assessments to identify potential vulnerabilities and threats.
2. Do establish clear communication protocols and roles.
3. Do communicate timely, clearly and transparently with stakeholders, incl. customers, partners, employees.
4. Do adapt the granularity, focus and channels for communication for each target audience.
5. Do ask for help and expert advise if in doubt.
6. Do use the crisis experience to improve your organisation, resilience, procedures.

✗

7. Don't panic. Use a set of tools, procedures, good examples developed in calm times.
8. Don't cover, ignore or omit real cybersecurity incidents.
9. Don't delay in responding to a cyber crisis or fail to communicate with stakeholders in a timely and transparent manner.
10. Don't rely solely on technology to protect your organisation from cyber threats - employee training and incident response planning are also critical components of a comprehensive cybersecurity strategy.

Example: Internal Email Communication



Wed 4/9/2024 16:47 PM

CM Communications

Ongoing cyber incident update

To All

Cc

Dear Employees,

As you may be aware, we recently experienced a cyber incident that has impacted our systems and operations. Our IT team is actively working to restore systems and data and minimise the impact of the incident.

We want to assure you that the safety and security of our employees, customers, and stakeholders is our top priority, and we are taking all necessary steps to address this incident. We have activated our cyber crisis communication team and are working closely with IT and other stakeholders to manage the incident.

We will provide regular updates as the situation evolves and appreciate your patience and understanding during this challenging time.

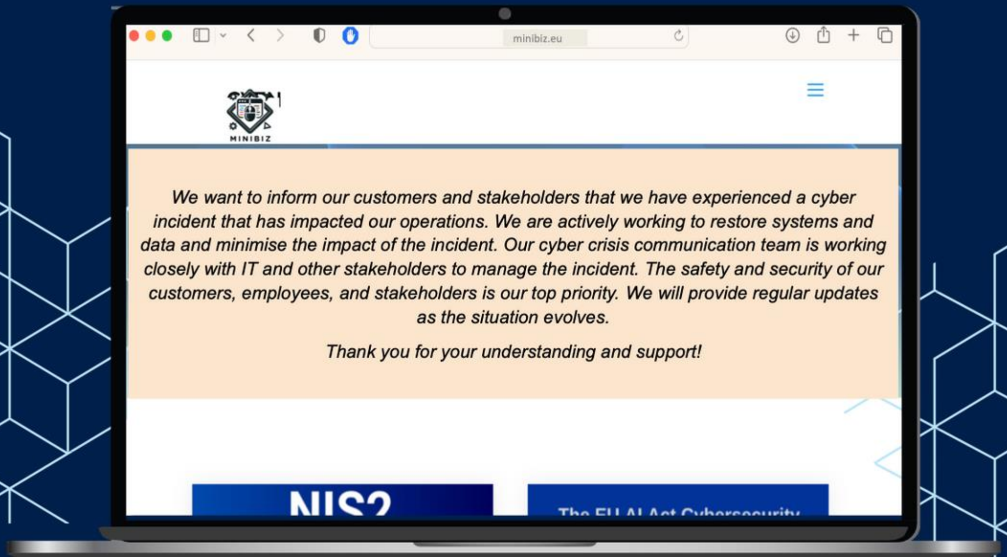
Sincerely,
[Your Name]

MINIBIZ

MiniBiz
Street 438/2 170
Neverlands

EMAIL TEMPLATE

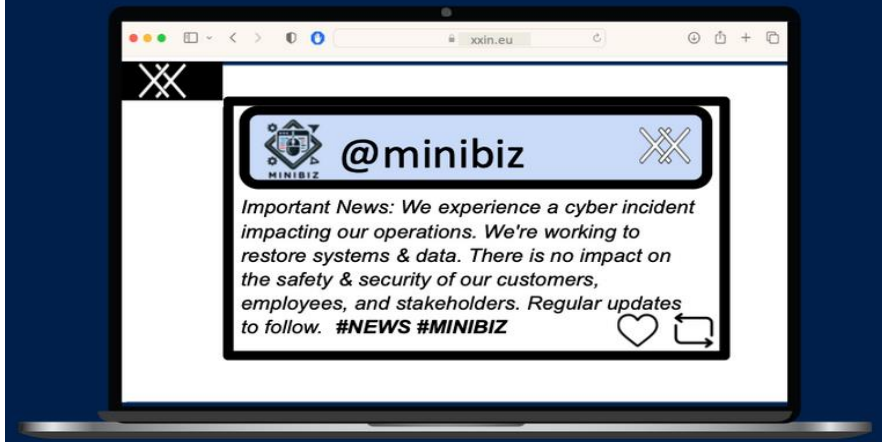
Example: Website News Communication



We want to inform our customers and stakeholders that we have experienced a cyber incident that has impacted our operations. We are actively working to restore systems and data and minimise the impact of the incident. Our cyber crisis communication team is working closely with IT and other stakeholders to manage the incident. The safety and security of our customers, employees, and stakeholders is our top priority. We will provide regular updates as the situation evolves.

Thank you for your understanding and support!

Example: Social Media



Important News: We experience a cyber incident impacting our operations. We're working to restore systems & data. There is no impact on the safety & security of our customers, employees, and stakeholders. Regular updates to follow. ***#NEWS #MINIBIZ***

NEWS TEMPLATE

1 Tailored messages

2 Action-oriented

3 Show empathy

4 Ongoing updates

GAME TIME

start!

Awareness raising game

Realistic

SME profile, personae, real cases

Relevant

Key threats:

phishing, smishing, vishing, ransomware

Decryption

Rich in visuals

Visual clues, vigenere game

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

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 o**r 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

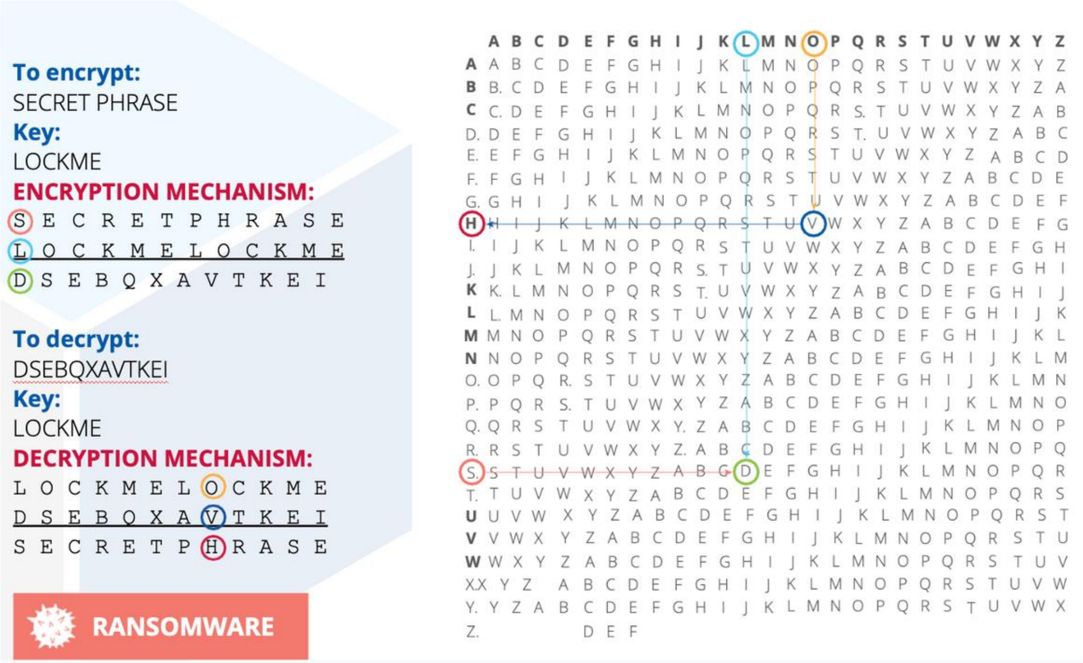
TASK UPDATE #3

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

Ransomware techniques played out



To encrypt:
SECRET PHRASE
Key:
LOCKME
ENCRYPTION MECHANISM:

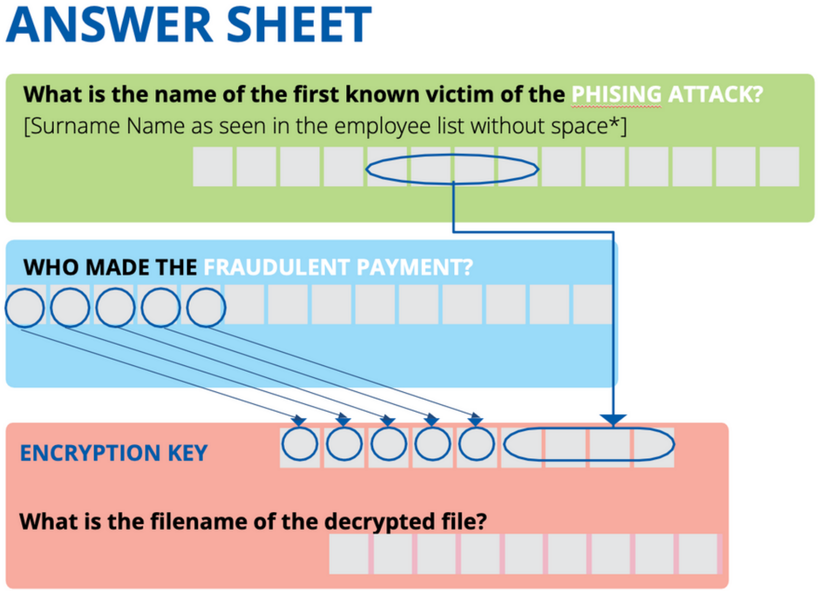
S E C R E T P H R A S E
L O C K M E L O C K M E
D S E B Q X A V T K E I

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	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
XX	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																							

RANSOMWARE



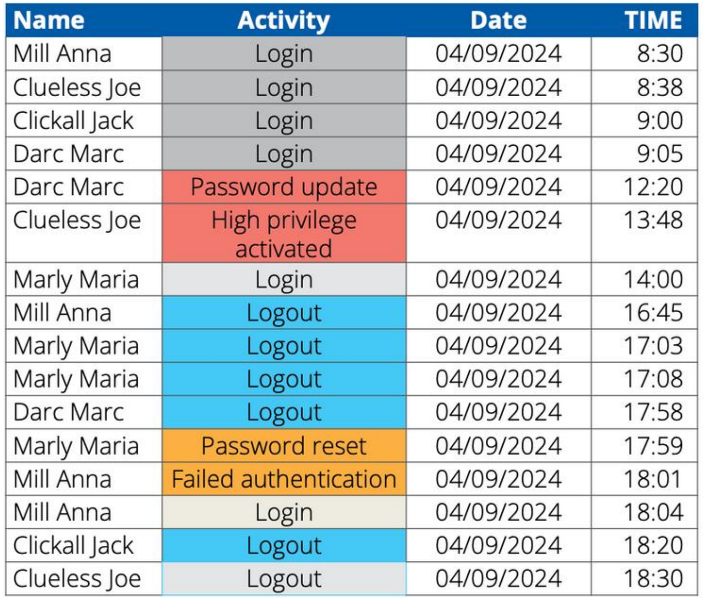
ANSWER SHEET

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

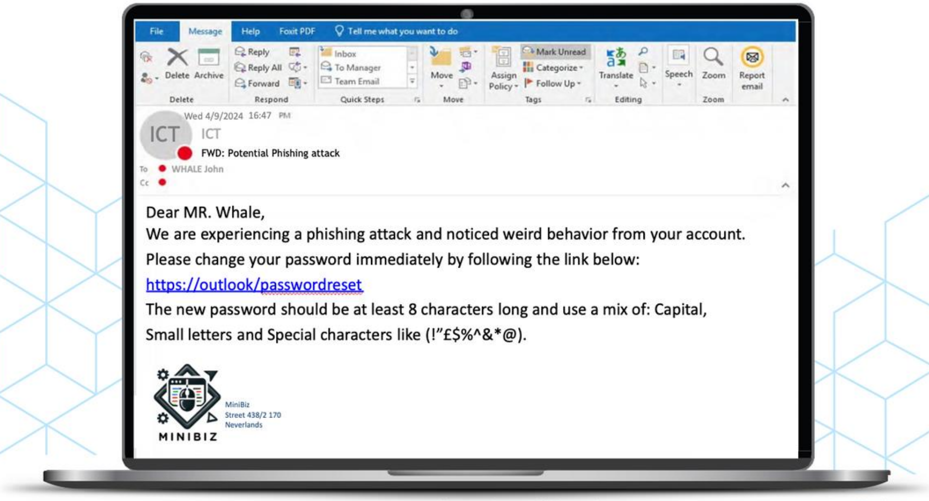
What is the filename of the decrypted file?



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

SUSPICIOUS MAIL



Wed 4/9/2024 16:47 PM

ICT

FWD: Potential Phishing attack

To WHALE John

Cc

Dear MR. Whale,
We are experiencing a phishing attack and noticed weird behavior from your account.
Please change your password immediately by following the link below:
https://outlook/passwordreset
The new password should be at least 8 characters long and use a mix of: Capital,
Small letters and Special characters like (!"£$%^&*@).

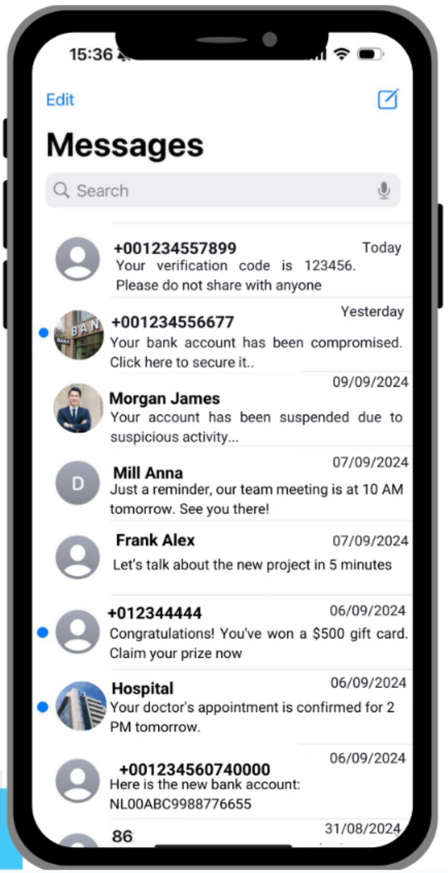
MINIBIZ

MiniBiz
Street 438/2 170
Neverlands

PHISHING ATTACK

3 types of social engineering visualised

SMISHING ATTACK



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

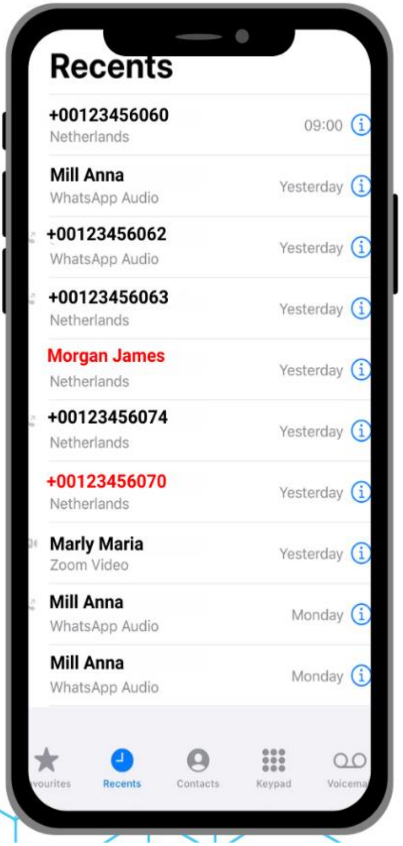
+012344444 06/09/2024
Congratulations! You've won a $500 gift card. Claim your prize now

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

+00123456074000 06/09/2024
Here is the new bank account: NL00ABC9988776655

86 31/08/2024

VISHING ATTACK



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

THANK YOU

Ethnikis Antistaseos 72, Chalandri 15231, Attiki,
Greece

info@enisa.europa.eu