

AR-in-a-BOX SME Edition

TECHNOLOGICAL INNOVATIONS OF THE FUTURE

BE PREPARED REDUCE THE IMPACT

DISCLAIMER

Copyright © European Union Agency for Cybersecurity (ENISA), 2024

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.

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



Objective: Create a customised AR in a box for SMEs



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



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.

Key Performance Indicators

An awareness raising quiz

Crisis communication measurement objectives

Risk, Situation, Effectiveness assessment



Annual awareness programme template

Crisis communication plan



Annual awareness programme template

Awareness raising game

Awareness raising quiz

ANNUAL CYBER AWARENESS PROGRAMME TEMPLATE

Consider and Formalise:

Who: Knowledge level

What: Topics

How: Method/Tool

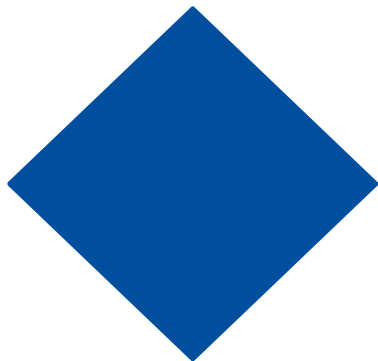
Measure: KPI, Metrics, Means of measure

Why: Desired outcome

Result: Outcome and next steps

Timing: Month/date, duration

Cost: Budget, time



Examples of
KPIs, measures, objectives

Further resources
Links, how to use tips

KPI EXAMPLES PROPOSED

KPIs are proposed as examples to identify:



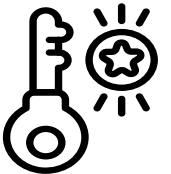
The ultimate objective of the awareness campaign

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



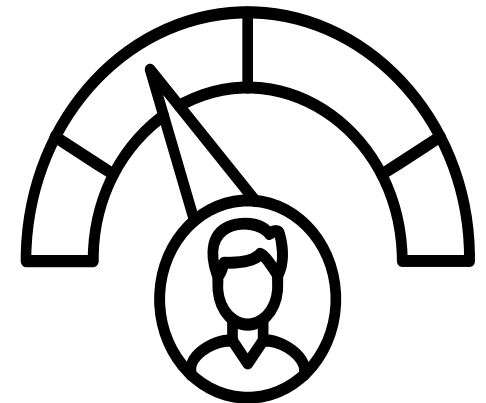
Indicators to measure whether the KPI is achieved

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

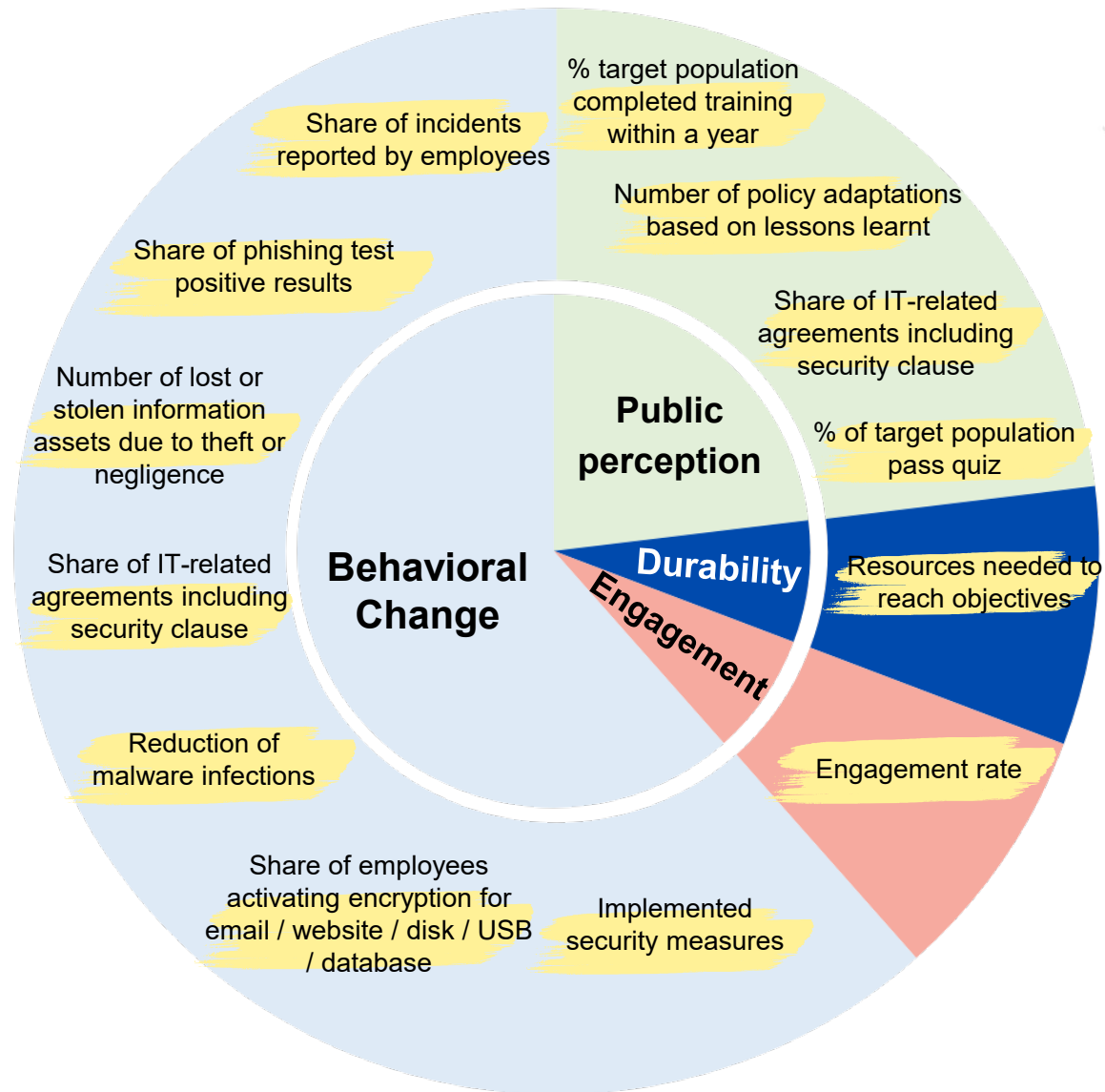


KPI EXAMPLES PROPOSED

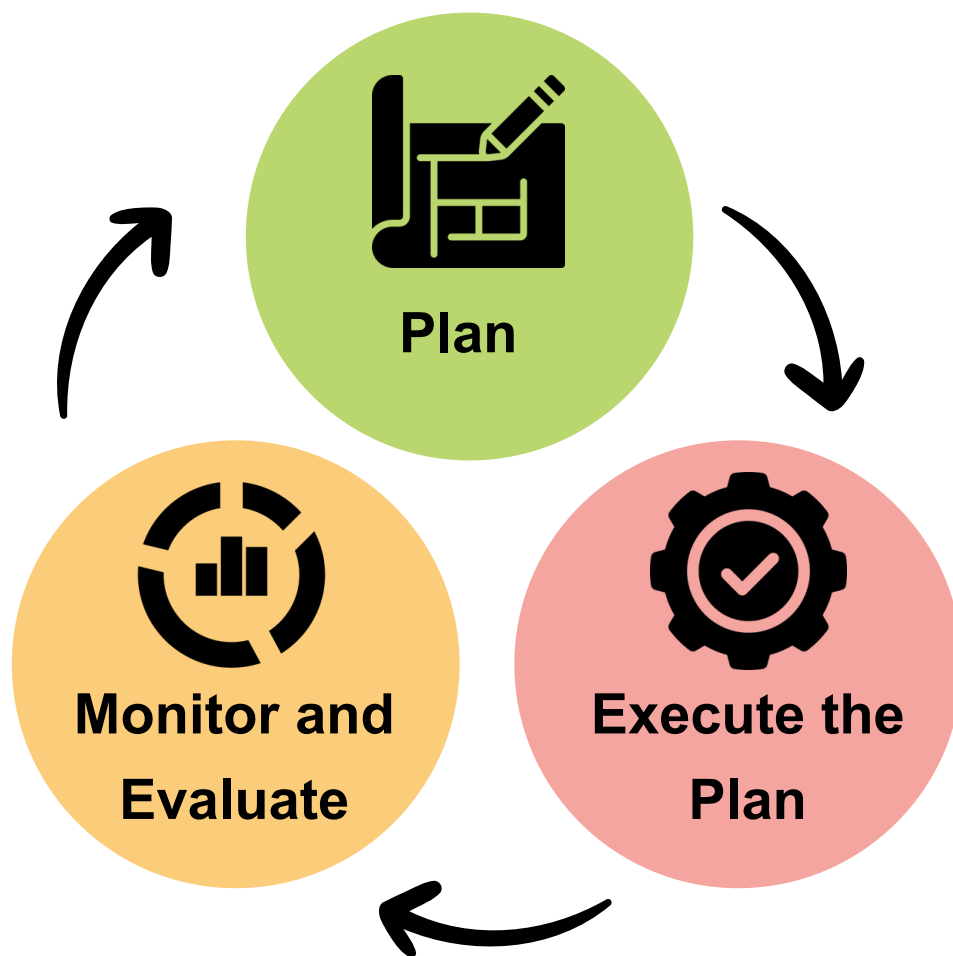
KPI	Behavioral change								Scale of outreach			Public perception	Durability
Indicator	Share of incidents reported by employees	Share of phishing test positive results	Number of lost or stolen information assets due to theft or negligence	Share of IT-related agreements including security clause	Reduction 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



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

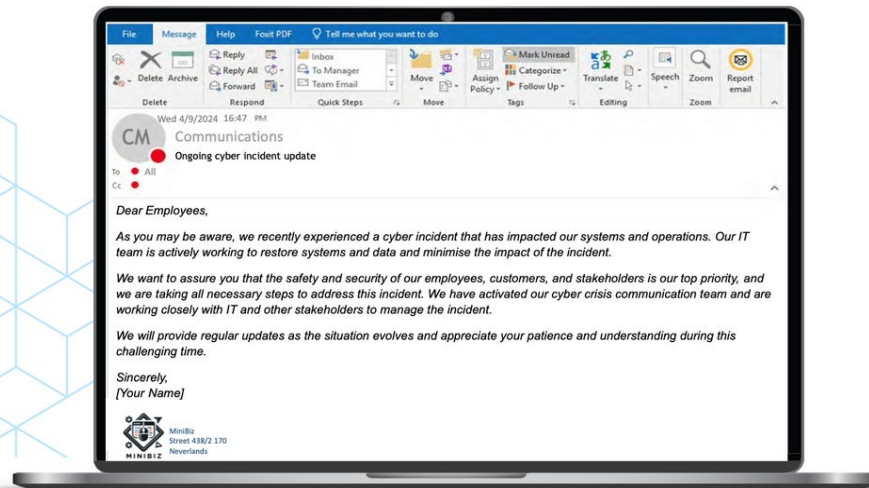


1. **Do conduct regular risk assessments** to identify potential vulnerabilities and threats.
2. **Do establish clear communication protocols and roles.**
3. **Do communicate timely, clearly and transparently** with stakeholders, incl. customers, partners, employees.
4. **Do adapt the granularity, focus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



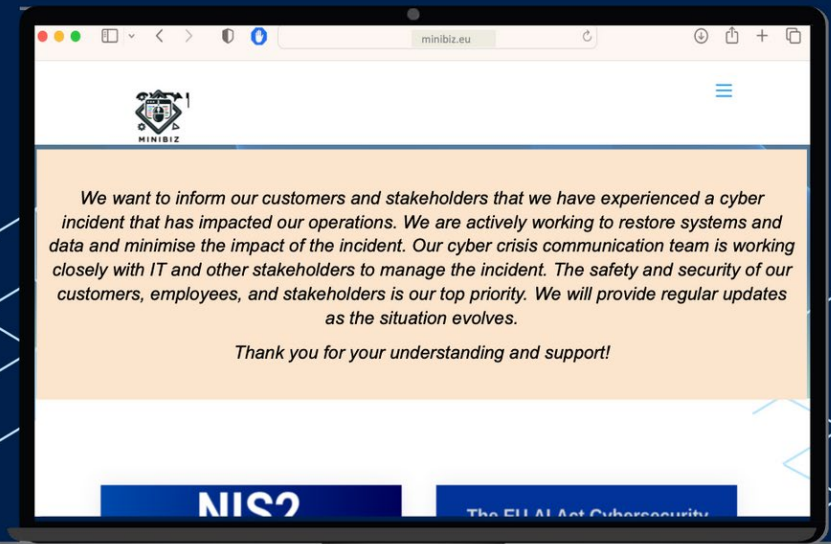
7. **Don't panic.** Use a set of tools, procedures, good examples developed in calm times.
8. **Don't cover, ignore or omit** real cybersecurity incidents.
9. **Don't delay in responding** to a cyber crisis or fail to communicate with stakeholders in a timely and transparent manner.
10. **Don't rely 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



EMAIL TEMPLATE

Example: Website News Communication



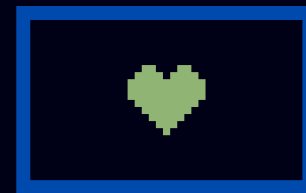
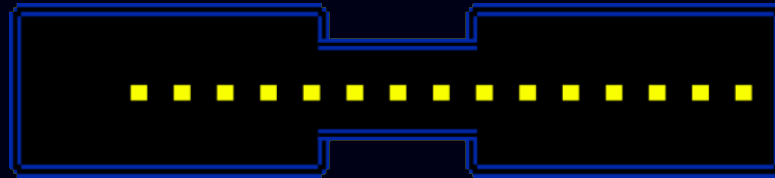
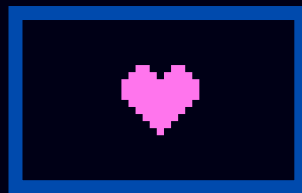
Example: Social Media



NEWS TEMPLATE

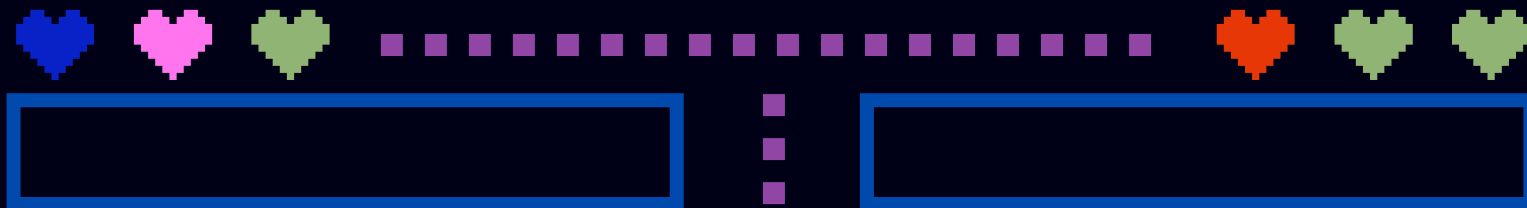
- 1 Tailored messages
- 2 Action-oriented
- 3 Show empathy
- 4 Ongoing updates





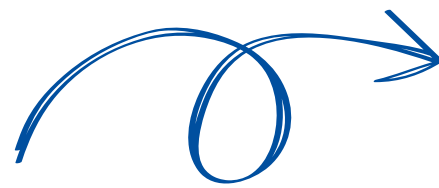
GAME TIME

start!



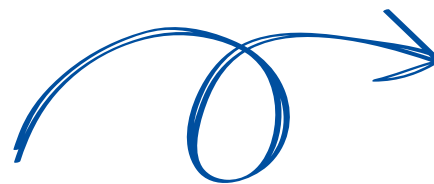
Awareness raising game

Realistic



SME profile, personae, real cases

Relevant



Key threats:
phishing, smishing, vishing,
ransomware
Decryption



Visual clues, vigenere game

Rich in visuals



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 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



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



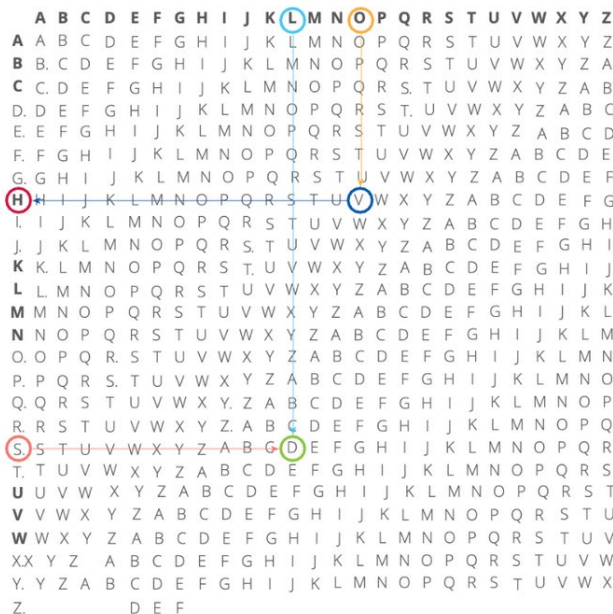
To encrypt:
SECRET PHRASE

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



ANSWER SHEET

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

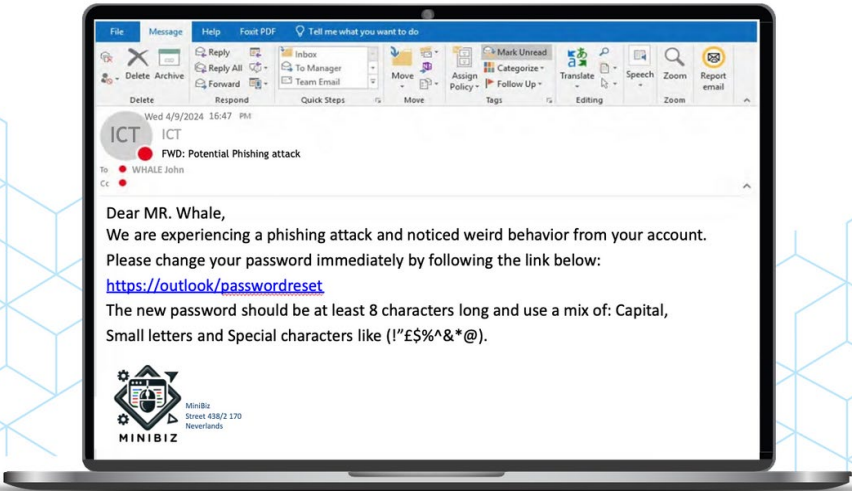
Ransomware techniques played out

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

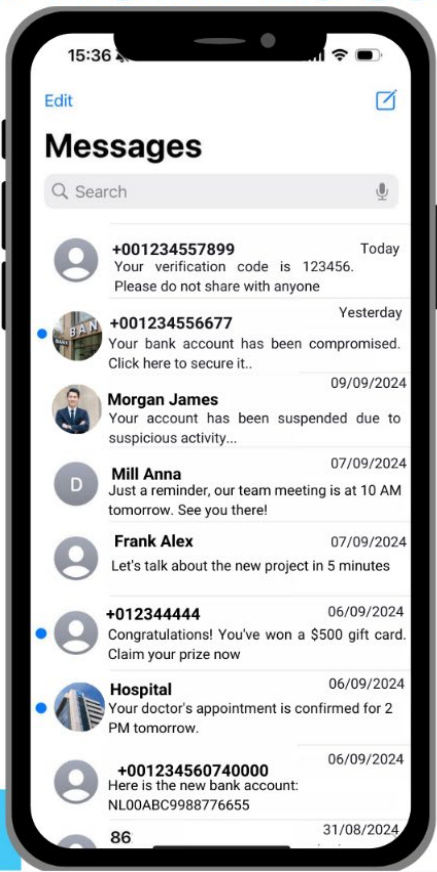
SUSPICIOUS MAIL



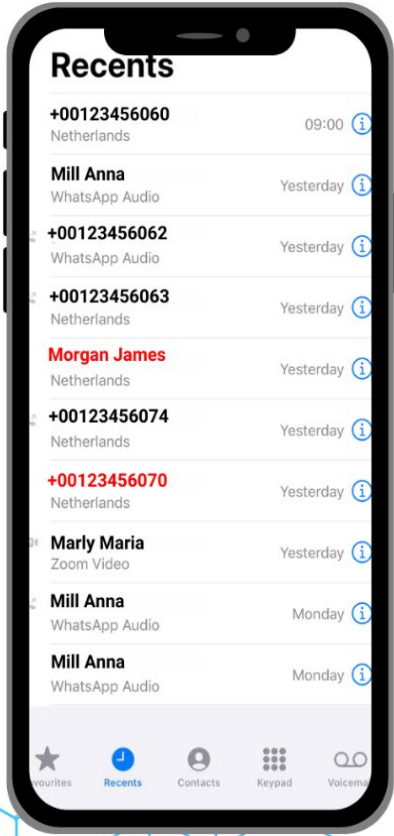
 PHISHING ATTACK



SMISHING ATTACK



VISHING ATTACK



3 types of
social engineering
visualised

THANK YOU



NA



| arinabox@enisa.europa.eu |



| <https://www.enisa.europa.eu>