AR-IN-A-BOX

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

HOW TO BUILD YOUR CUSTOM AWARENESS RAISING PROGRAM

Alex Zacharis, Georgia Bafoutsou - ENISA

08 | 11 | 2023

CONTENT

1. What is a Cyber Awareness Program
2. ENISA AR-in-a-Box
3. Gamification and examples

1

CHAPTER

CYBER AWARENESS PROGRAM

CYBER AWARENESS PROGRAM

“An (internal) marketing strategy designed to raise ***cyber*** *security* ***awareness****.”*

- ✓ Teaches employees **how to mitigate the impact of cyber threats**.
- ✓ A plan encompassing multiple awareness-raising activities over a long period of time following the organisation’s strategy for cybersecurity.
- ✓ It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target group.

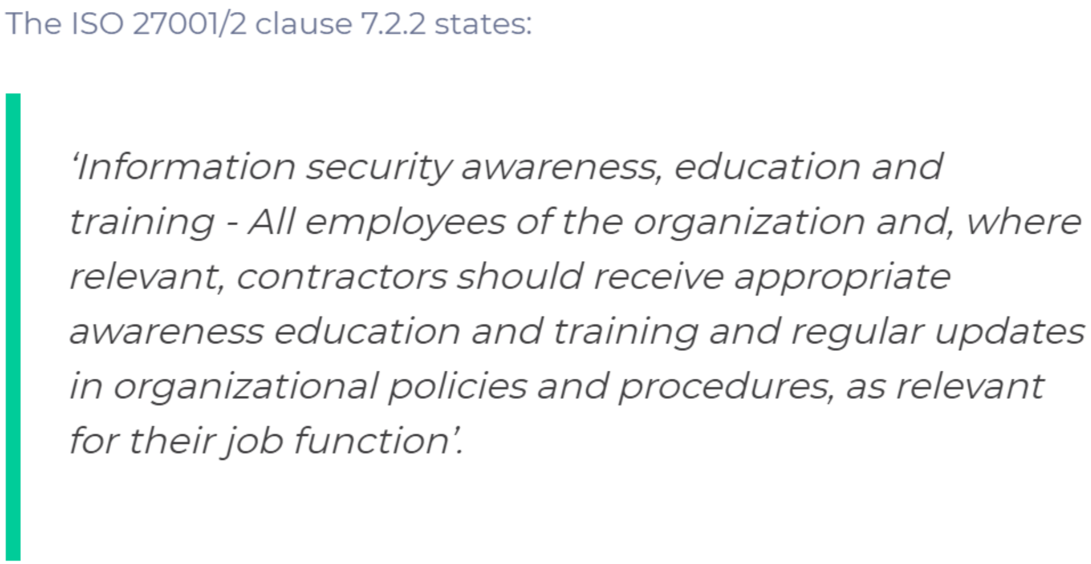
WHY HAVE ONE?

- New threats are emerging.
- Organizations can no longer just rely on their technological defenses to be safe.
- Cybercriminals use sophisticated social engineering techniques to by-pass defenses.
- All it takes is one employee to click on a malicious link and it’s game over!
- Your employees are your first line of defense.

A comprehensive Cyber Security Awareness program is the best way to educate staff and create a security-first culture.

STILL NOT SURE?

ISO 27001/2 & Information Security Awareness Training
For ISO 27001 compliance, it is essential to comply with **clause 7.2.2**.

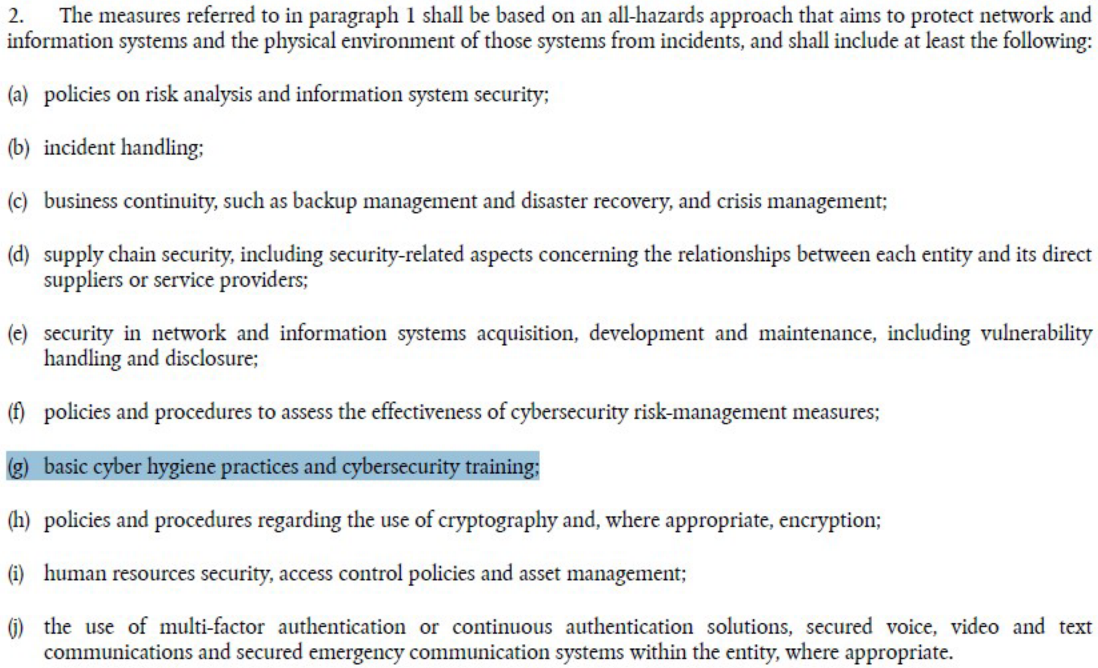


The ISO 27001/2 clause 7.2.2 states:

> *'Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function'.*

STILL NOT SURE?

NIS DIRECTIVE 2, Article 21: Cybersecurity-Risk management measures



2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

2

CHAPTER

AR-IN-A-BOX

Towards Awareness Culture

AR-IN-A-BOX CONTENT

AR-IN-A-BOX

YOUR GUIDE TO DESIGNING A CYBER-AWARENESS PROGRAMME

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

AR-IN-A-BOX

YOUR GUIDE TO DESIGNING A CYBER-AWARENESS CAMPAIGN

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

AR-IN-A-BOX

COMMUNICATION STRATEGIES FOR CYBER AWARENESS

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

AR-IN-A-BOX

PROMOTION TOOLS AND CHANNELS

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

AR-IN-A-BOX

CYBER AWARENESS – MEASURING IMPACT

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

AR-IN-A-BOX

HOW TO RUN THE CYBER-AWARENESS GAME

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

AR-IN-A-BOX

CYBER AWARENESS GAME

EnergyCorp hacked

BE THE STRONGEST LINK
BREAK THE KILLCHAIN

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

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

enisa

- A Phishing
- B Smishing
- C Vishing
- D Ransomware

DESIGNING
A CYBER-AWARENESS PROGRAMME

1. Identify objectives
2. Secure financial resources
3. Ensure human resources
4. Split employees into target groups
5. Choose the right means
6. Create a timeplan
7. Implement program
8. Evaluate the program

AR-IN-A-BOX

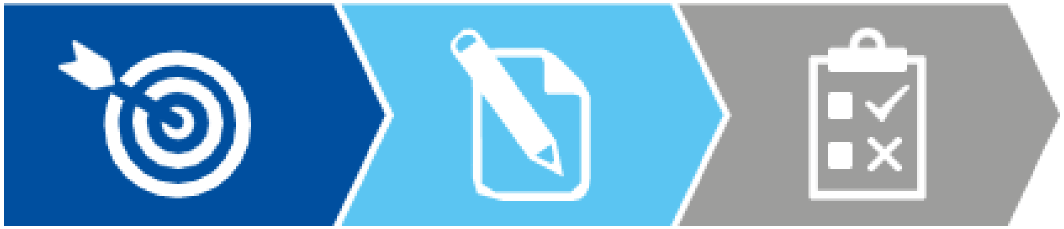
YOUR GUIDE
TO DESIGNING
A CYBER-AWARENESS
PROGRAMME

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

SETTING OBJECTIVES

1

Identify objectives



Overall goals for awareness and learning

Definition of SMART awareness objectives

Selection of specific material, tools, methods

Awareness-raising objectives stem from the risk assessment of the organization and help:

- ✓ **To promote cybersecurity education and culture**
- ✓ **To be prepared for incidents.**
- ✓ **To develop an understanding of emerging cybersecurity threats and landscape**
- ✓ **To test policies and procedures**

HERE IS AN EXAMPLE

Objective	Indicative implementation timeline
1. Raise awareness on the cyber threat of phishing. • Provide a custom training on the topic, informative material and a hands-on quiz to evaluate progress. • Utilize a phishing simulation campaign to capture before and after results. • 100 % of staff should participate in the activity.	6 months
2. Promote cybersecurity education and culture. • Provide a custom training, a reporting process in the event of an incident and a hands-on table-top exercise to evaluate lessons learned. • 80 % of the staff should participate in the activity.	1 year
3. Improve preparedness in the event of an incident. • 100 % of ICT personnel should participate in the activity. • Provide training and a hands-on technical exercise to evaluate lessons learned. • Test escalation procedures in place and identify gaps.	6 months

SOME TIPS

WHAT DO YOU WANT TO ACHIEVE?	OBJECTIVES
1. Generate awareness about cybersecurity issues and practices. 2. Raise awareness about the impact of different types of attacks, especially when they involve companies and businesses.	Awareness
3. Provide detailed information on how to react in the event of phishing and ransomware attacks. 4. Inform potential attack targets of what happens before, during and after a ransomware attack.	Information
5. Prompt the target audience to act and to eventually spread the word on what they learned from you.	Engagement
6. Promote the safer use of the internet for end users and the practice of basic cyber hygiene. 7. Promote existing cybersecurity recommendations and best practices to prevent cyberattacks.	Promotion
8. Provide users with resources to protect themselves online and prevent attacks. 9. Make people become 'human firewalls' by empowering them to play their part in preventing attacks.	Empowerment

AR-IN-A-BOX

COMMUNICATION STRATEGIES FOR CYBER AWARENESS

FINANCIAL RESOURCES

2

Secure financial resources

MANAGEMENT:

- Plays a critical role.
- Make sure they are involved in the design and the objectives-setting phase of the awareness programme from an early stage.
- Budget allocation depends on their support.

TIPS:

- ✓ Try to identify the must-do topics of your programme and the must-train employees who will minimise the risk for your organisation when trained.
- ✓ Reuse or update existing material or resources.
- ✓ Select open-source material or create it in-house.
- ✓ Exploit synergies in the community where available.

HUMAN RESOURCES

3

Ensure human resources

- ✓ **Management**
- ✓ **Cyber Security Officer**
  - identifies the target audience and the most relevant topics
  - steers the effort
- ✓ **Public Relations & Communications**
  - disseminate the right message internally
  - engage the right target employee groups via the proper channels
- ✓ **ICT**
  - can customise the content based on the operation reality of each organization
- ✓ **Incident response teams (security operations centres):**
  - have a good overview of the vulnerabilities, monitor traffic and handle potential incidents.
  - can feed the awareness programme with information and tailor it to the needs of the staff or to the trending threats

HUMAN RESOURCES

3

Ensure human resources

✓ **HR**

- are responsible for promoting but also engaging the different target audiences to all relevant activities.

✓ **DPO / Legal**

- Privacy, personal data topics, regulatory obligations can be part of the awareness-raising training agenda.

✓ **Instructors:**

- are responsible for delivering the programme content to the target audience
- can be external entities or employees of the organisation with a specialised background

TARGET GROUPS

4

Split employees into target groups

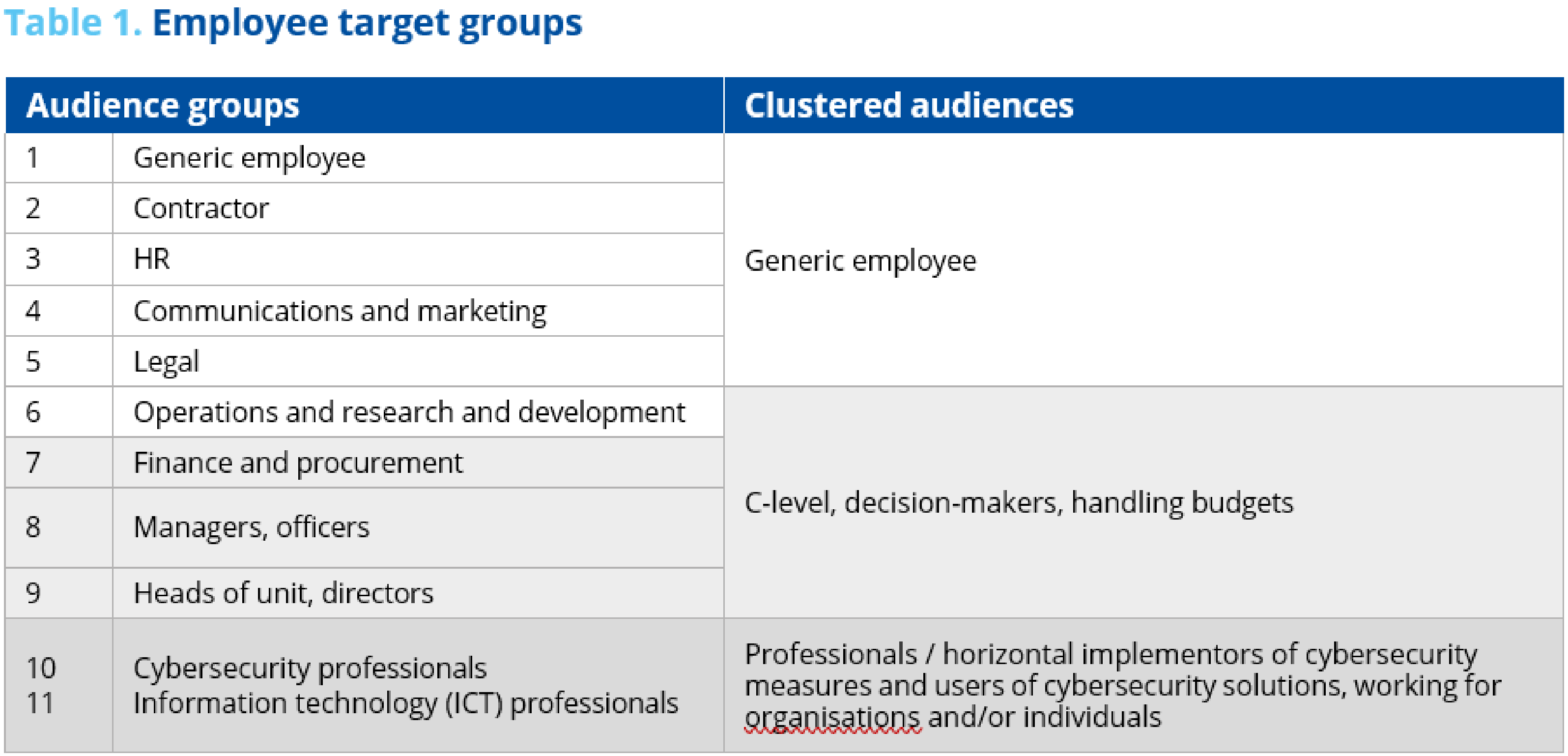


Table 1. Employee target groups

Audience groups		Clustered audiences
1	Generic employee	Generic employee
2	Contractor	
3	HR	
4	Communications and marketing	
5	Legal	
6	Operations and research and development	C-level, decision-makers, handling budgets
7	Finance and procurement	
8	Managers, officers	
9	Heads of unit, directors	
10 11	Cybersecurity professionals Information technology (ICT) professionals	Professionals / horizontal implementors of cybersecurity measures and users of cybersecurity solutions, working for organisations and/or individuals

SELECTING THE RIGHT TOOLS

5

Choose the right means

Infographics – Posters

Easy to deploy physically, e.g. in elevators, common spaces

Ads – Videos

Able to hold and convey a lot of information

TOOLS FOR AWARENESS RAISING

Puzzles – Quizzes

Ensure and test understanding of concepts

Live presentations

Direct interactions with participants

SELECTING THE RIGHT TOOLS FOR THE RIGHT AUDIENCE

5

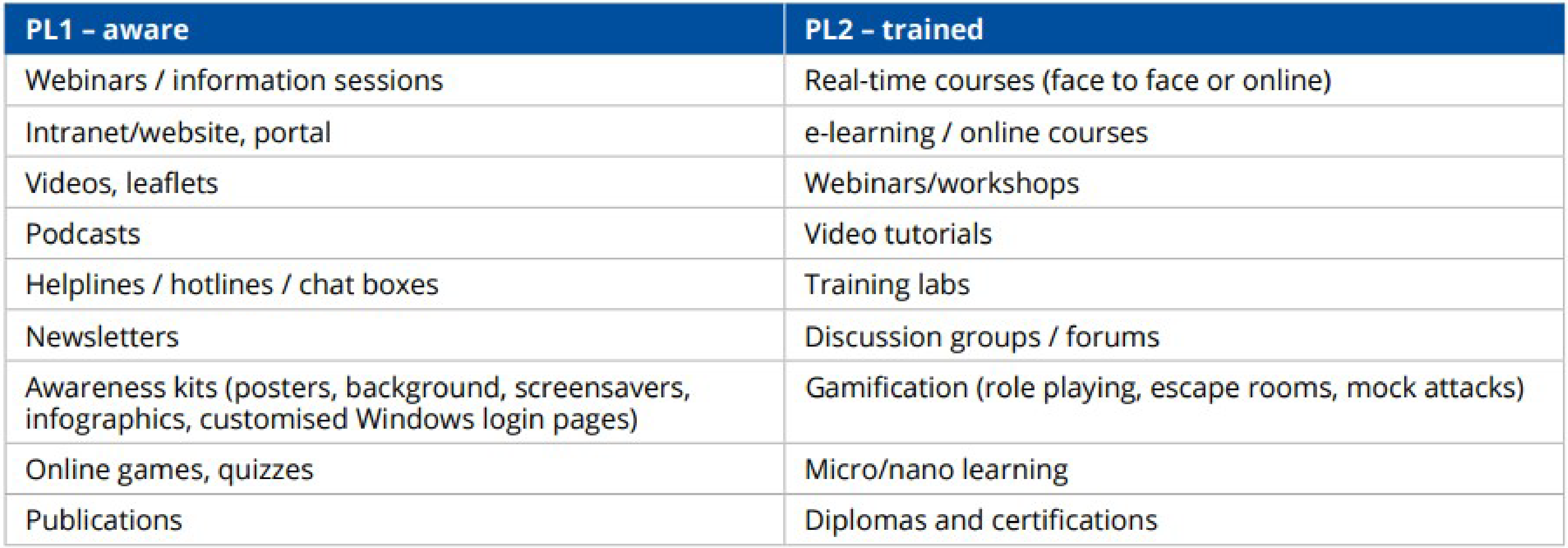
Choose the right means

- **Aware – proficiency level 1 (PL1)**
- **Trained – proficiency level 2 (PL2)**
- **Experienced – proficiency level 3 (PL3)**

PL drop down per audience group and topic category		Audience groups		
		Generic employee	C-level	ICT and security professionals
Topic categories	Cyberbullying	PL1		
	Online gaming	PL1		
	Online pornography	PL1		
	Safe internet	PL1	PL1	
	Sexting	PL1		
	Fake news	PL1		
	Privacy and data protection	PL1	PL1	
	Financial scams	PL1		
	Mobile banking	PL1		
	Device safety	PL1	PL1	
	Email spam	PL1	PL1	
	Business email compromise fraud	PL1	PL1	
	Password attacks	PL1	PL1	
	Data breach	PL1	PL1	PL2
	Malware	PL1	PL1	PL2
	Phishing	PL1	PL1	
	Ransomware	PL1	PL1	PL2
	Cyber upskilling	PL1		PL2
	Cyberterrorism		PL1	
	Certifications			PL2

HERE’S AN EXAMPLE

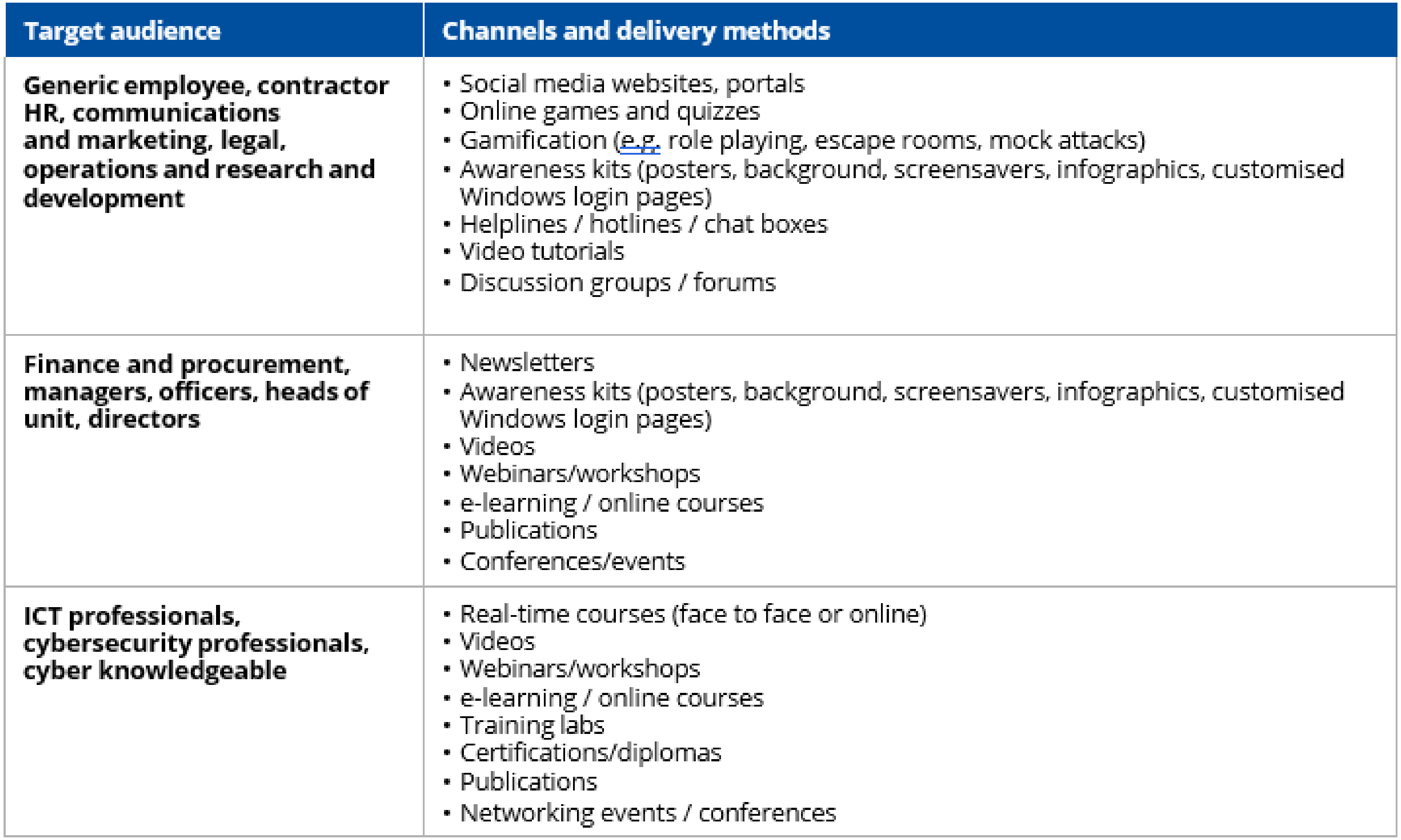
Suggested programme delivery methods according to proficiency level target



PL1 – aware	PL2 – trained
Webinars / information sessions	Real-time courses (face to face or online)
Intranet/website, portal	e-learning / online courses
Videos, leaflets	Webinars/workshops
Podcasts	Video tutorials
Helplines / hotlines / chat boxes	Training labs
Newsletters	Discussion groups / forums
Awareness kits (posters, background, screensavers, infographics, customised Windows login pages)	Gamification (role playing, escape rooms, mock attacks)
Online games, quizzes	Micro/nano learning
Publications	Diplomas and certifications

HERE’S AN EXAMPLE

Suggested delivery methods per target group



Target audience	Channels and delivery methods
Generic employee, contractor HR, communications and marketing, legal, operations and research and development	• Social media websites, portals • Online games and quizzes • Gamification (e.g. role playing, escape rooms, mock attacks) • Awareness kits (posters, background, screensavers, infographics, customised Windows login pages) • Helplines / hotlines / chat boxes • Video tutorials • Discussion groups / forums
Finance and procurement, managers, officers, heads of unit, directors	• Newsletters • Awareness kits (posters, background, screensavers, infographics, customised Windows login pages) • Videos • Webinars/workshops • e-learning / online courses • Publications • Conferences/events
ICT professionals, cybersecurity professionals, cyber knowledgeable	• Real-time courses (face to face or online) • Videos • Webinars/workshops • e-learning / online courses • Training labs • Certifications/diplomas • Publications • Networking events / conferences

PLANNING

6

Create a timeplan

January	February	March	April
Baseline quiz	Training topic	Videos and dissemination material	Videos and dissemination material
May	**June**	**July**	**August**
Training topic 2	Simulation exercise	HOLIDAYS	HOLIDAYS
September	**October**	**November**	**December**
Back-to-school training	Games/test/quiz	Insights collections	Report to management

IMPLEMENTATION

7

Implement program

Cybersecurity training is an ongoing process.
Ensure that your security posture is as mature as it can be, even as your company and the cybersecurity landscape grows and evolves.

Three periods are considered relevant for delivering cybersecurity-awareness training to your employees:

- ✓ When they join the organisation as part of the induction process
- ✓ After an incident, in order to indicate the procedures, roles and responsibilities in place;
- ✓ At regular intervals throughout the year (see calendar)

EVALUATION

8

Evaluate the program

A KPI is a value that measures a component of an awareness-raising campaign or programme.

There are five reasons why KPIs fail to improve performance:

1. the KPIs are poorly defined;
2. they lack accountability;
3. they are not achievable;
4. they are not specific enough;
5. they are too hard to measure.

AR-IN-A-BOX

CYBER AWARENESS – MEASURING IMPACT

enisa

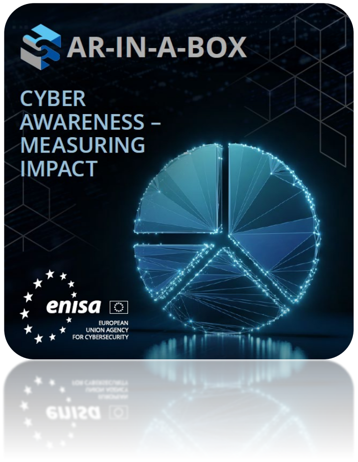
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EVALUATION

8

Evaluate the program

A KPI is a value that measures a component of an awareness-raising campaign or programme.


AR-IN-A-BOX

CYBER AWARENESS – MEASURING IMPACT

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

Examples of KPIs

1. Scale of outreach
Metric: Number of reached individuals
2. Level of behavioural change achieved
Metrics: Percentage decrease of incidents, Number of positive test results
3. Durability (process is long lasting, continuous and cost efficient)
Metrics: Level of reusability (for example ranging from 1 to 5)
Resources needed to reach objectives

AR-IN-A-BOX: METHODS OF DELIVERY

1 Training-at-your-own-pace

Set Up: Online access to Material
Content: AR-in-a-Box — ENISA (europa.eu)

SCAN ME

2 Virtual or Physical Workshop

Set Up: 1-2 days Workshop
Content:

- ➢ Theory of building an Awareness Raising Program
- ➢ Use of Communications dept in real life
- ➢ How ENISA supporting tools can be best utilized to deal with cyber crisis.

Delivery upon Request

3

PRACTICE MAKES PERFECT

3

CHAPTER

GAMIFICATION AND EXAMPLES

CYBER AWARENESS GAMES

Gamification helps!

- ✓ Determine how your team will react to a theoretical cyber attack and how effective your plan is.
- ✓ Identify flaws or gaps in the organization’s response and make adjustments
- ✓ Testing consequences in a safe environment
- ✓ Coordination between different departments
- ✓ Save money

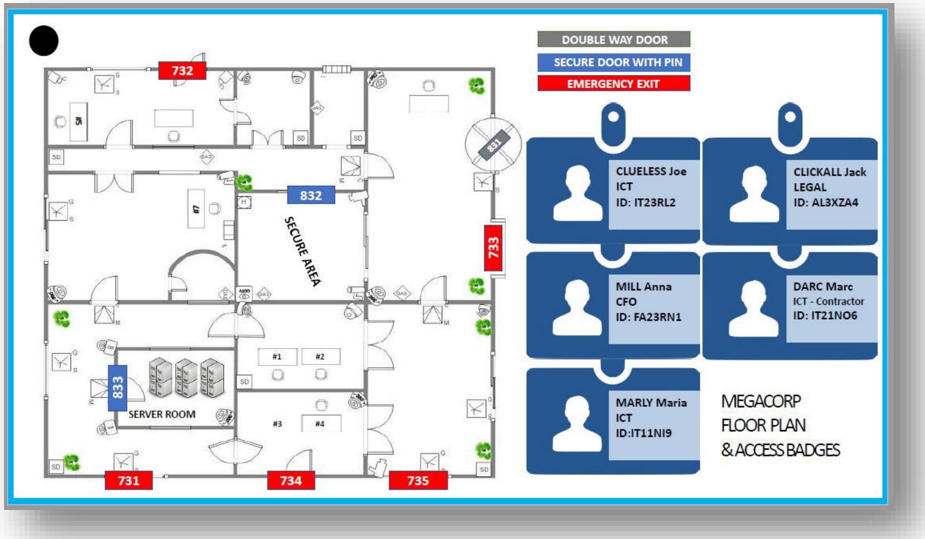
AR-IN-A-BOX

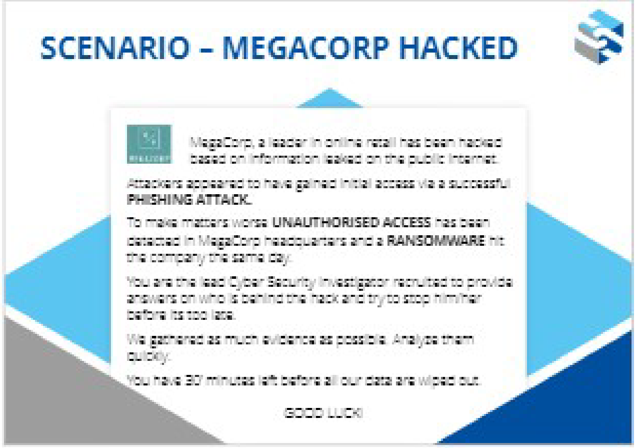
HOW TO RUN THE CYBER-AWARENESS GAME

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

CYBER AWARENESS GAMES





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.**

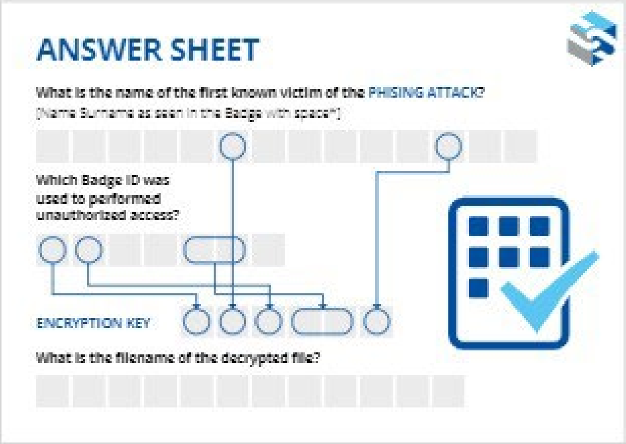
To make matters worse **UNAUTHORISED ACCESS** has been detected in MegaCorp headquarters and a **RANSOMWARE** hit the company the same day.

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!



ANSWER SHEET

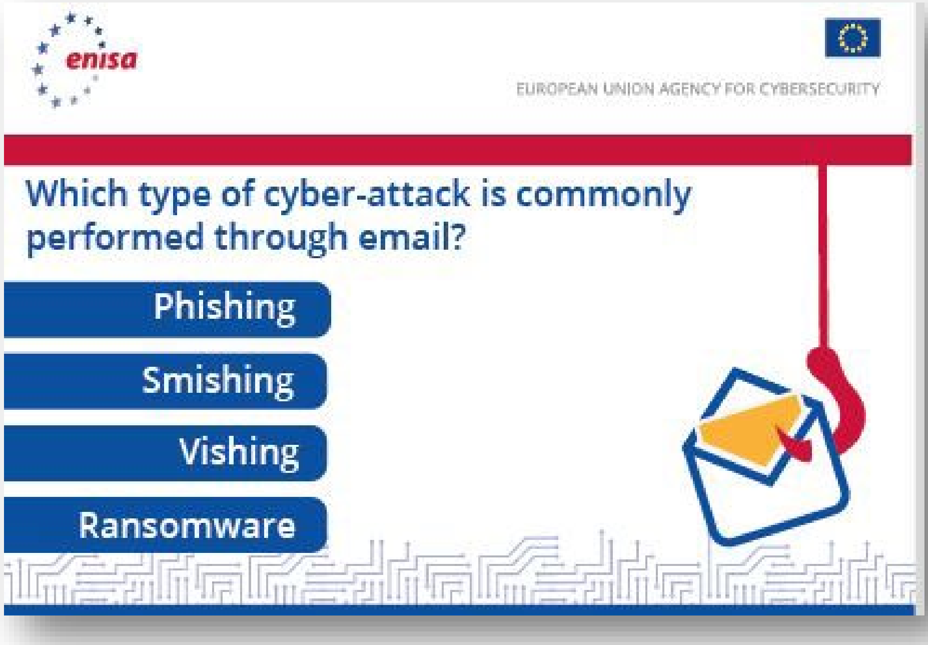
What is the name of the first known victim of the PHISING ATTACK?
[Name Surname as seen in the Badge with space*]

Which Badge ID was used to performed unauthorized access?

ENCRYPTION KEY

What is the filename of the decrypted file?

QUIZZES


enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

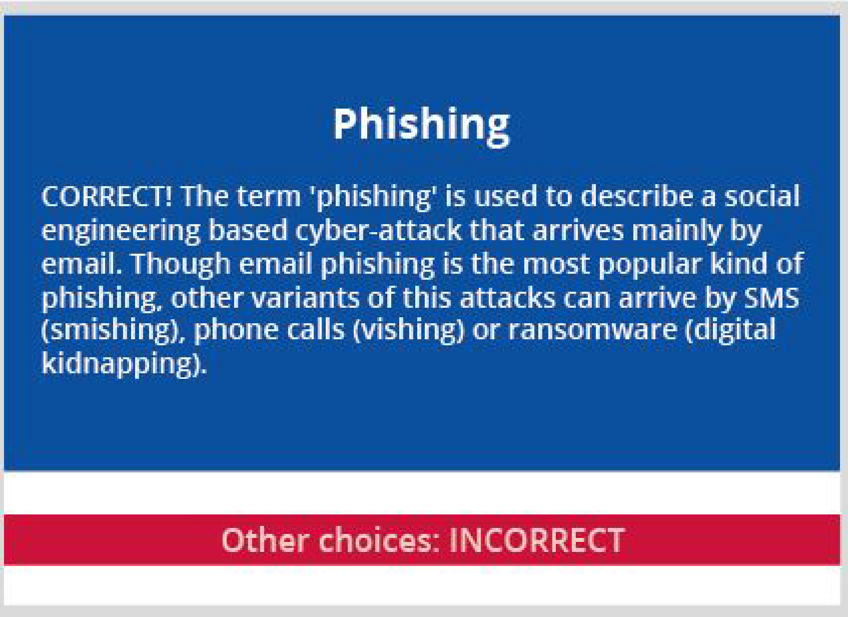
Which type of cyber-attack is commonly performed through email?

Phishing

Smishing

Vishing

Ransomware


Phishing

CORRECT! 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).

Other choices: INCORRECT

RAILWAYS CAMPAIGN

#CyberOnTrack — ENISA (europa.eu)

#CyberOnTrack

- Physical security
- Phishing
- Qrishing
- Vishing
- CyberHygiene
- Ransomware

RAILWAYS CAMPAIGN

[#CyberOnTrack — ENISA (europa.eu)]

#CyberOnTrack

RAILWAYS CAMPAIGN

PHISHING

Your attention, please
Take care!
Whenever you receive
an email...
Stop & Check

RAILWAYS CAMPAIGN

PHYSICAL SECURITY

Keep your distances

Mind the CyberSec Gap: Everyone must access the premises with their own **access card** & **third parties must always be accompanied.**

#CyberOnTrack

RESTRICTED AREA
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

RAILWAYS CAMPAIGN

If you see something, say something

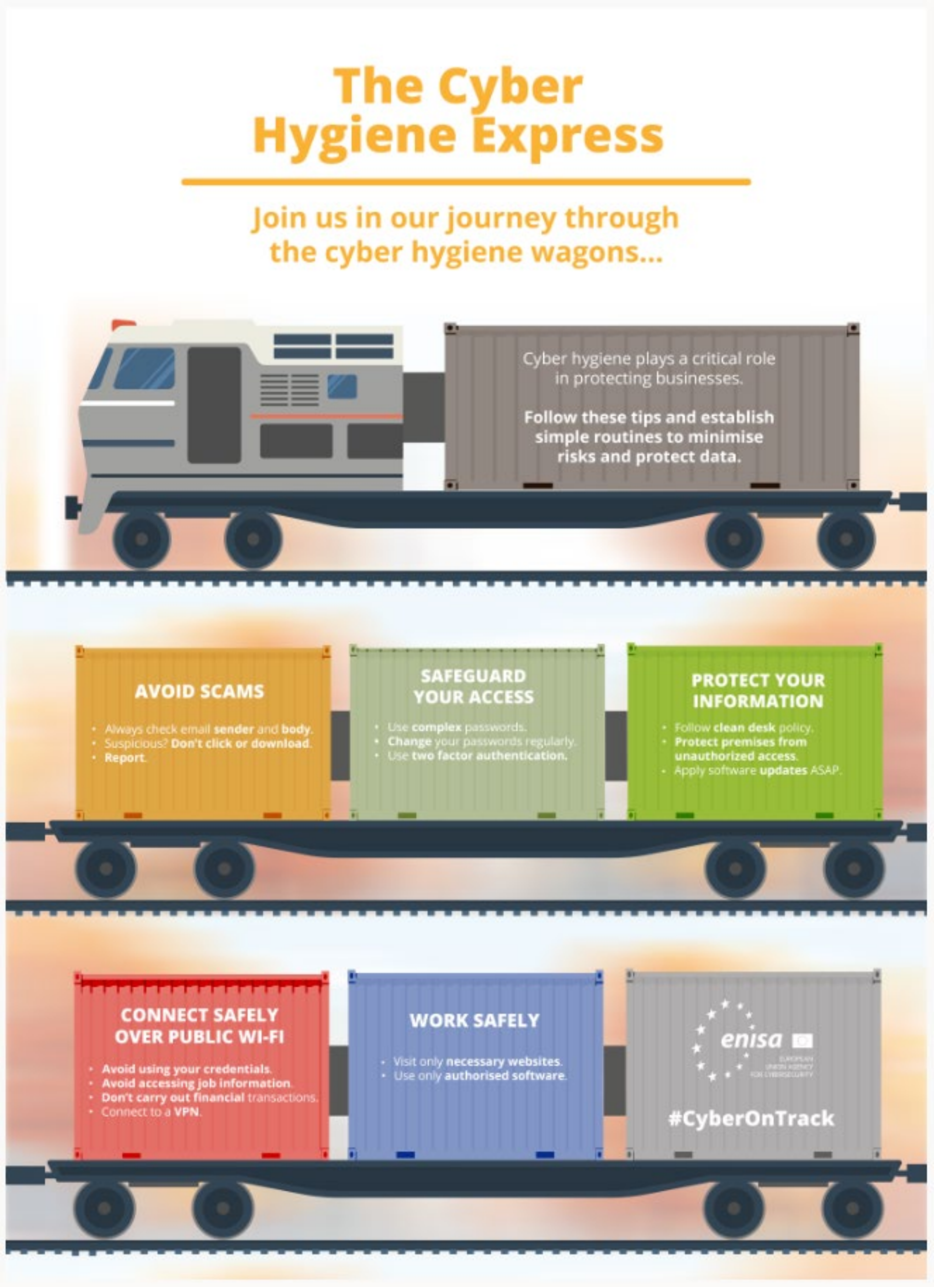
Mind the CyberSec Gap: If you suspect something, say something! Alert the security team.

Sharing is not always caring

Mind the CyberSec Gap: Remember your access cards and codes are personal and unique, do not share them!

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
SAM
#CyberOnTrack

RAILWAYS CAMPAIGN



The Cyber Hygiene Express

Join us in our journey through the cyber hygiene wagons...

Cyber hygiene plays a critical role in protecting businesses.

Follow these tips and establish simple routines to minimise risks and protect data.

AVOID SCAMS

- Always check email **sender** and **body**.
- Suspicious? **Don't click or download**.
- **Report**.

SAFEGUARD YOUR ACCESS

- Use **complex** passwords.
- **Change** your passwords regularly.
- Use **two factor authentication.**

PROTECT YOUR INFORMATION

- Follow **clean desk** policy.
- **Protect premises from unauthorized access**.
- Apply software **updates** ASAP.

CONNECT SAFELY OVER PUBLIC WI-FI

- **Avoid using your credentials**.
- **Avoid accessing job information**.
- **Don't carry out financial** transactions.
- Connect to a **VPN**.

WORK SAFELY

- Visit only **necessary websites**.
- Use only **authorised software**.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

#CyberOnTrack

aet@enisa.europa.eu | enisa.europa.eu