AR-IN-A-BOX

How to Build your Custom Awareness Program

Evangelos Kantas, Cybersecurity Expert, ENISA

BE THE STRONGEST LINK
BREAK THE KILLCHAIN

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

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'.*

AR-IN-A-BOX REVIEW

DESIGNING A CYBER-AWARENESS PROGRAMME

SETTING OBJECTIVES

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 promote cybersecurity culture and hygiene
- ✓ To test policies and procedures

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

- ✓ **Management**
- ✓ **Cyber Security Officer**
- ✓ **Public Relations & Communications**
- ✓ **ICT**
- ✓ **HR**
- ✓ **DPO / Legal**
- ✓ **Content Developers**
- ✓ **Instructors**

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

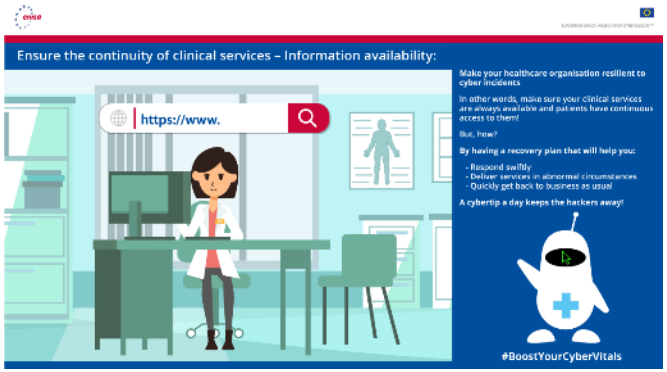
Puzzles – Quizzes

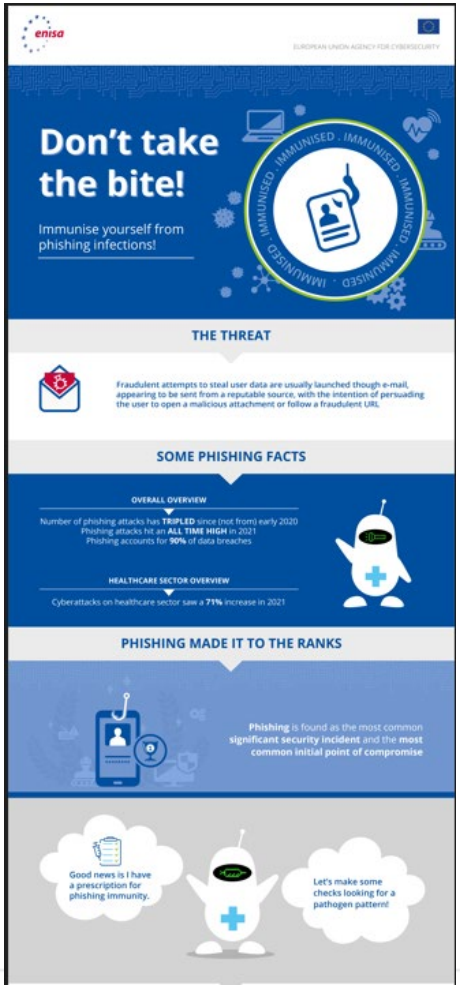
Ensure and test understanding of concepts

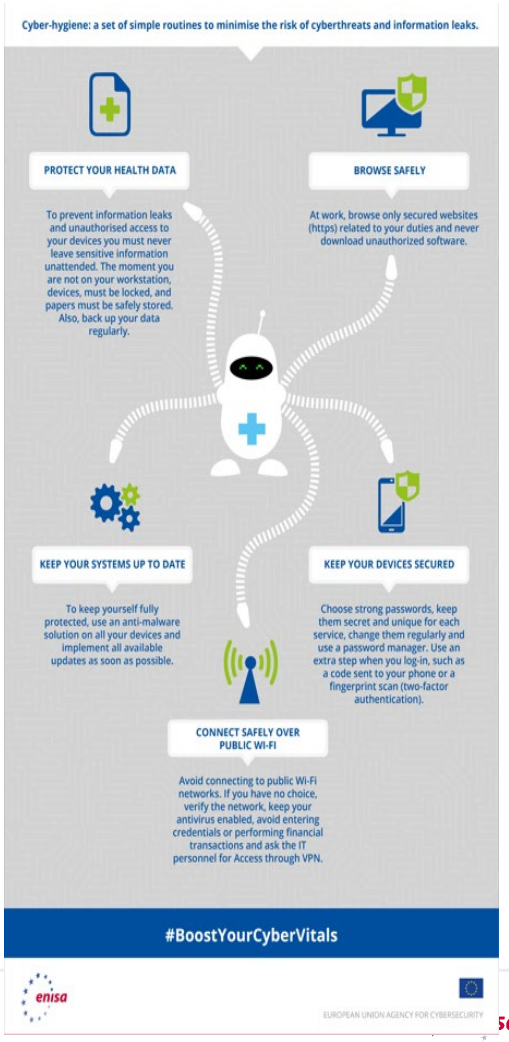
Live presentations

Direct interactions with participants

HEALTHCARE SECTOR CAMPAIGN

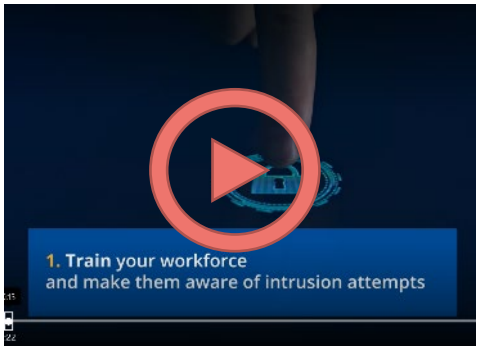


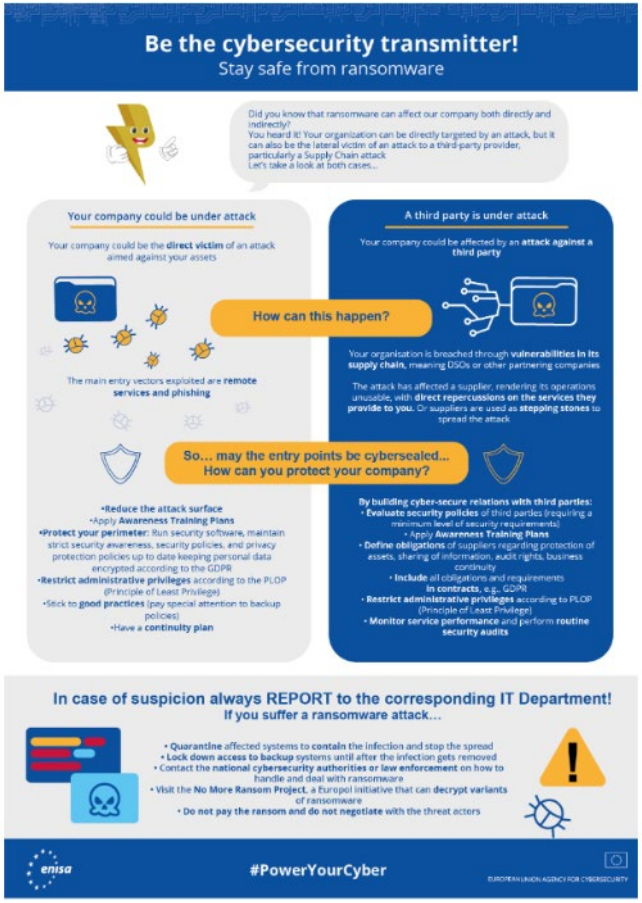




 [Cyber Health Week — ENISA (europa.eu)]

ENERGY CAMPAIGN TO TRANSMISSION SYSTEM OPERATORS





[Cyber Energy Week — ENISA (europa.eu)]

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

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:

1. when they join the organisation as part of the induction process
2. after an incident, in order to indicate the procedures, roles and responsibilities in place;
3. at regular intervals throughout the year (see calendar)

EVALUATION

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.

MAGNIFY THE EFFECT

- Quick wins count
- Keep it simple
- Identify strategies to magnify the effects of your program
- Train-a-Trainer
- Cyber Awareness Champions
- Inject Cyber Awareness in other events (Ex. team building events)

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

QUIZZES


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
Which type of cyber-attack is commonly performed through email?
Phishing
Smishing
Vishing
Ransomware

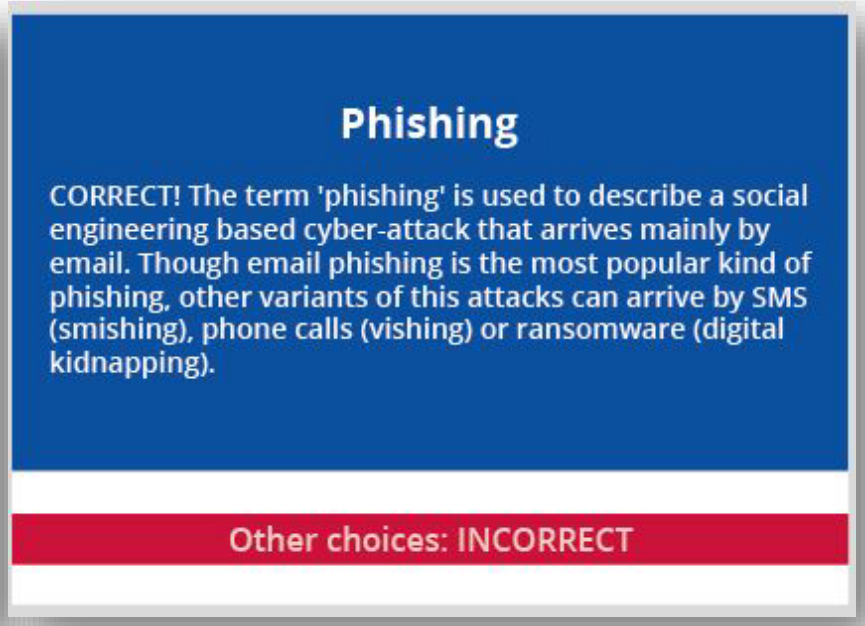
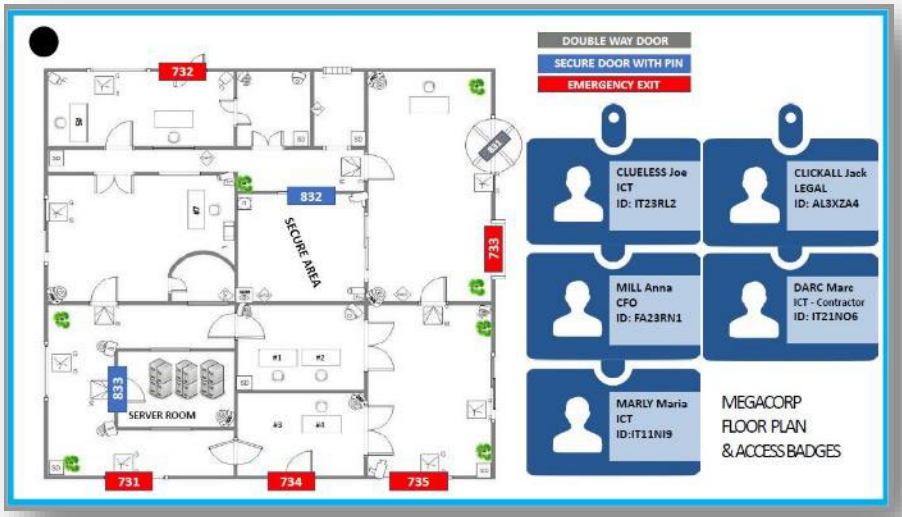
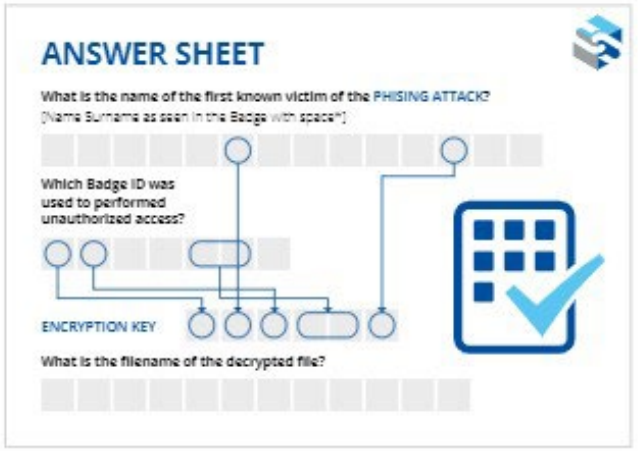

Phishing
CORRECT! The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).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

TABLE-TOP GAMES





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)

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

THE FUTURE -2023

- ✓ Crisis Communications guide
- ✓ Sector agnostic, editable, customizable material for an AR campaign on phishing and cyber-hygiene (leaflets, posters, videos, quizzes, etc)
- ✓ Expansion packs for Game including other kinds of threats/incidents (e.g. BYOD, DDOS)
- ✓ Online version of the Game
- ✓ Translations

GIVE US SOME FEEDBACK!

SCAN ME

EUSurvey - Survey (europa.eu)


AR-IN-A-BOX
Thank you
BE THE STRONGEST LINK
BREAK THE KILLCHAIN
enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY