EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AR-IN-A-BOX : BUILDING A CUSTOM CYBER AWARENESS PROGRAM

Dimitra Liveri
Team Leader for Awareness raising and Education

12 | 10 | 2022

CYBER AWARENESS PROGRAM

A **plan** encompassing multiple awareness raising activities over a long period of time following the **organizational strategy for cybersecurity**

- Teaches employees **how to mitigate the impact of cyber threats**.
- Incorporates activities, materials and training to promote a **culture of cyber security**.

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?

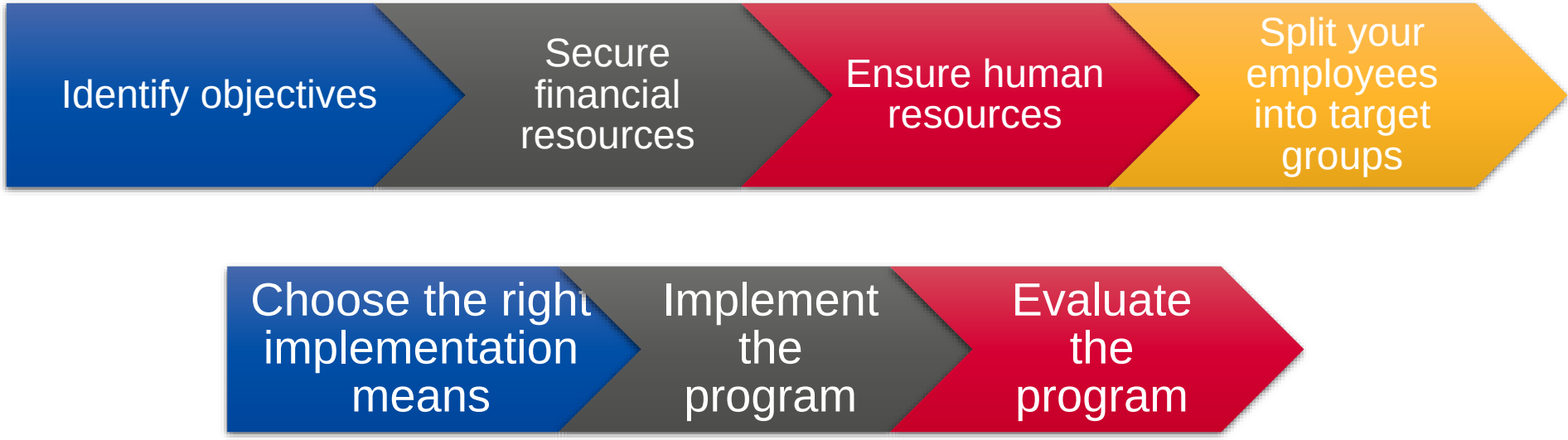
ISO 27001/2 & Information Security Awareness Training

For ISO 27001 compliance, it is essential to comply with **clause 7.2.2**.

The ISO 27001/2 clause 7.2.2 states:

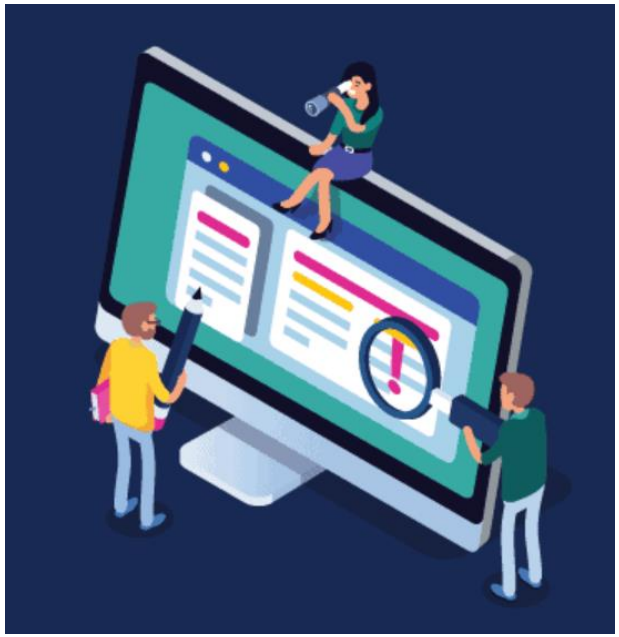
> *'Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function'.*

HOW TO BUILD THE PROGRAM



IDENTIFY OBJECTIVES

- Evaluate the threat landscape and identifying your top risks.
- Find or develop the right training.
- Every organization has a different threat profile.
- Be sure to cover: phishing, malware, and poor security practices.
- Phishing is behind 71% of all cyber attacks worldwide.

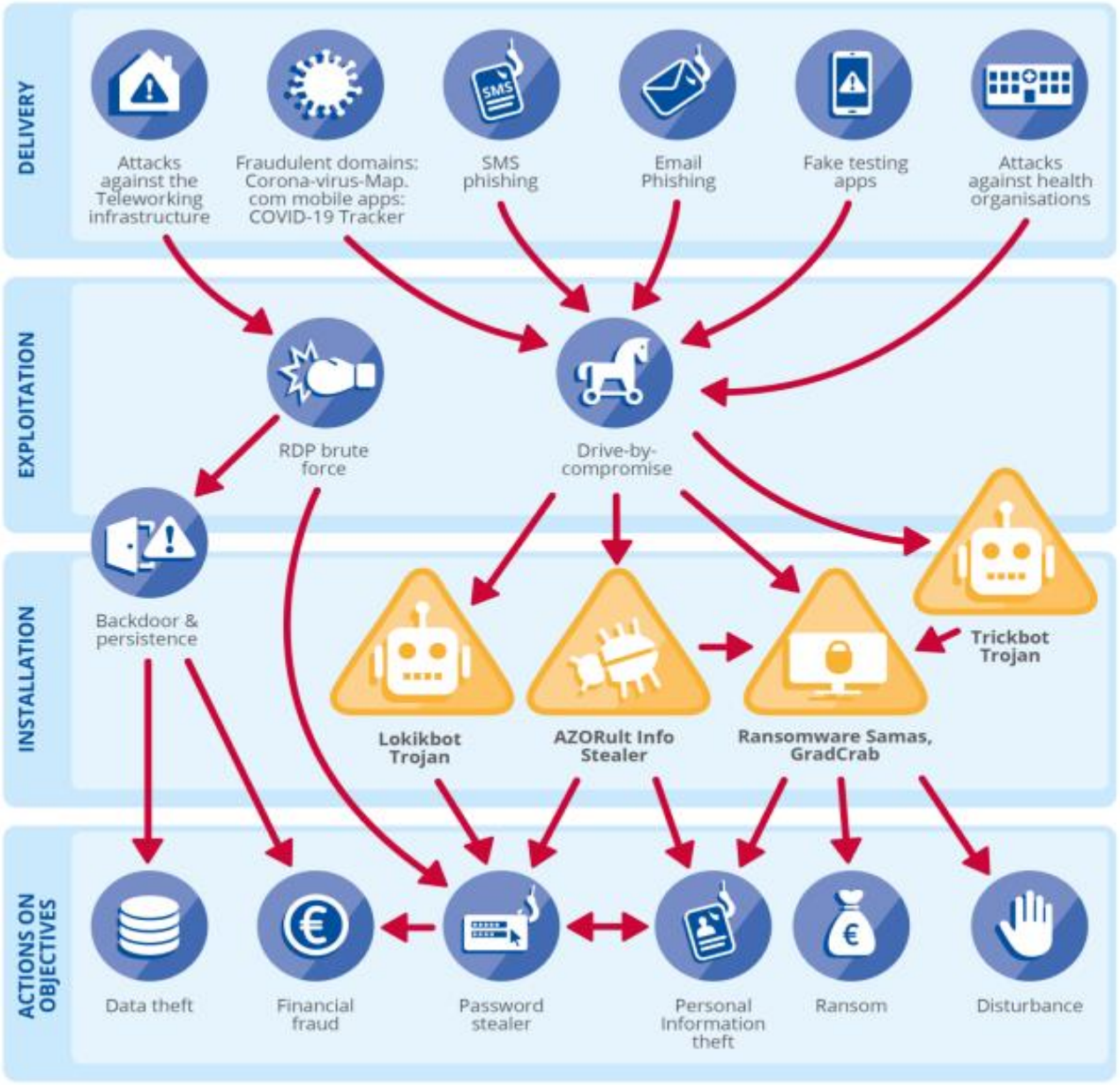


Threat Landscape — ENISA (europa.eu)

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREAT LANDSCAPE MAPPING

Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.

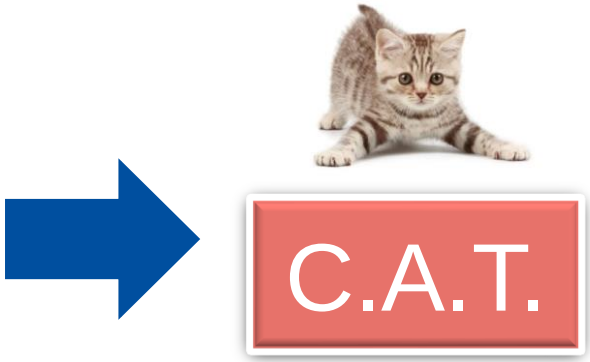


ROLES

Creating a team of Experts cultivates Culture

Use rolling roles!

- Management
- Cyber Security Officer
- Heads of Departments
- Public Relations
- ICT
- HR
- DPO / LEGAL



IDENTIFY TARGET AUDIENCE

	Audience groups	Clustered audiences
1	Generic Employee	Generic Employee
2	Contractor	
3	HR	
4	Communications & Marketing	
5	Legal	
6	Operations & R&D	C-Level, Decision Makers, Handling budgets
7	Finance & Procurement	
8	Managers, Officers	
9	Head of Unit, Directors	
10	Cybersecurity professionals	Professionals / Horizontal implementors of cybersecurity actions and users of cybersecurity solutions, working for organisations and/or individuals
11	IT professionals	

CHANGE BEHAVIOR

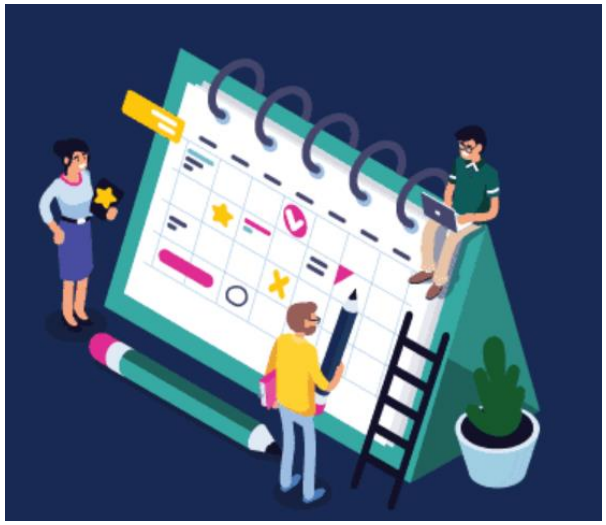
- We are not in the ’00, forget boring classrooms. Employees need to be engaged
- Training needs to be role-specific, tailored, fun, and address daily challenges
- **Make it Audience Specific**
- Provide easily consumable content (videos, realistic scenarios, quizzes, policies and real-world phishing simulation tests)
- Utilize communications & marketing tools such as blogs, awareness posters
- Break the culture barrier that cyber security is an IT thing

CHOOSE THE RIGHT CHANNEL

#	Mechanism/Activity	Category	Target Audience			Occurrence	Delivery Method	Expected level of Impact	Measurability	Resources
			General	*Specific*	*Target Group*			*1-3*	*1-3*	*1-3*
1	Videos	Media	X	X	Youth (incl. Students), Kids	Ad hoc, On request	Online	2	1	2
2	Webinar/Seminar	Training	X			Annual, On request	Online, Instructor led	2	3	3
3	Communication Calendar	Material	X	X	National AR Authorities, SMEs, Large Organizations	Annual	Online	2	2	1
4	Workshop	Training	X			On request	Instructor led, Online	3	3	3
5	Cybersecurity in a Box	Material	X	X	National AR Authorities	On request	Online	3	2	3
6	Surveys/Quizzes	Training	X			Annual	Online	2	3	1
7	Social Media	Media		X	Youth (incl. Students), Employees, Cyber Ignorant, Cyber Savvy	Annual	Online	2	3	1
8	Computer Based Training (CBT)	Training		X	Employees, SMEs, Large Organizations	On request	Online	2	3	2
9	Champions Network	Material		X	SMEs, Large Organizations	Annual	Conventional	3	1	1
10	Physical Material	Material	X			Annual	Conventional	2	1	1
11	One-Day Campaign	Event	X			On request	Conventional	2	2	3

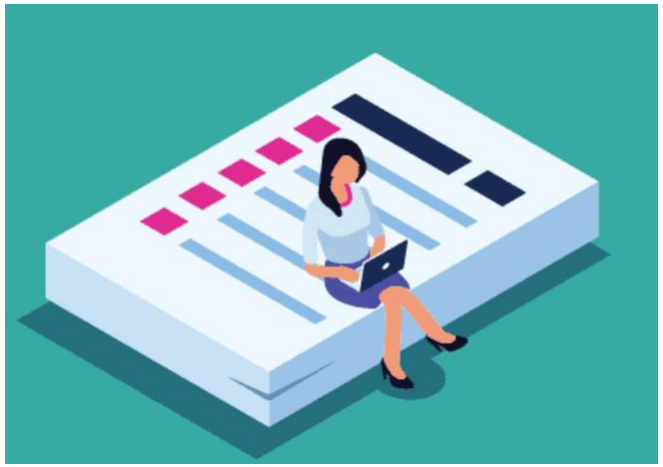
SCHEDULE DELIVERY

- Security awareness training should be an ongoing process conducted at regular intervals throughout the year.
- Cybercriminals launch scams to coincide with seasonal events, so learn to recognize the devious new attack methods
- Create an annual security awareness campaign
- Keep them wondering when the next test will hit them



TEST EFFECTIVENESS

- Conduct an initial baseline assessment to determine where the risks lie.
- Execute regular phishing simulations to identify staff that require additional training.
- Execute controlled simulation exercises
- Quizzes and tests can be added to the end of training videos to help reinforce the key messaging and reduce risk.



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)

MEASURING IMPACT

SCALE OF OUTREACH (KPI)				
Metrics	Number of participating countries	Number of reached individuals	Number of communication partners	Number of mentions in media
FACILITATING THE MULTIPLIERS (KPI)				
Metrics	Number of multipliers	Number of multipliers that contributed to the campaign	Number of multipliers that downloaded the material	
LEVEL OF BEHAVIOURAL CHANGE ACHIEVED (KPI)				
Metrics	Percentage decrease of incidents	Number of reported incidents	Number of positive test results	Level of increased knowledge
	Qualitative feedback on security good practices			
PUBLIC PERCEPTION (KPI)				
Metrics	Qualitative feedback on activities from the participants (on level of satisfaction)	Qualitative feedback from the participating Member States (on level of satisfaction)	Engagement rate (e.g., followers, likes)	
DURABILITY (KPI)				
Metrics	Level of reusability (for example ranging from 1-5)	Resources needed to reach objectives	Costs - Contribution partners/stakeholders	

ACTUAL MEASUREMENT IS IMPORTANT

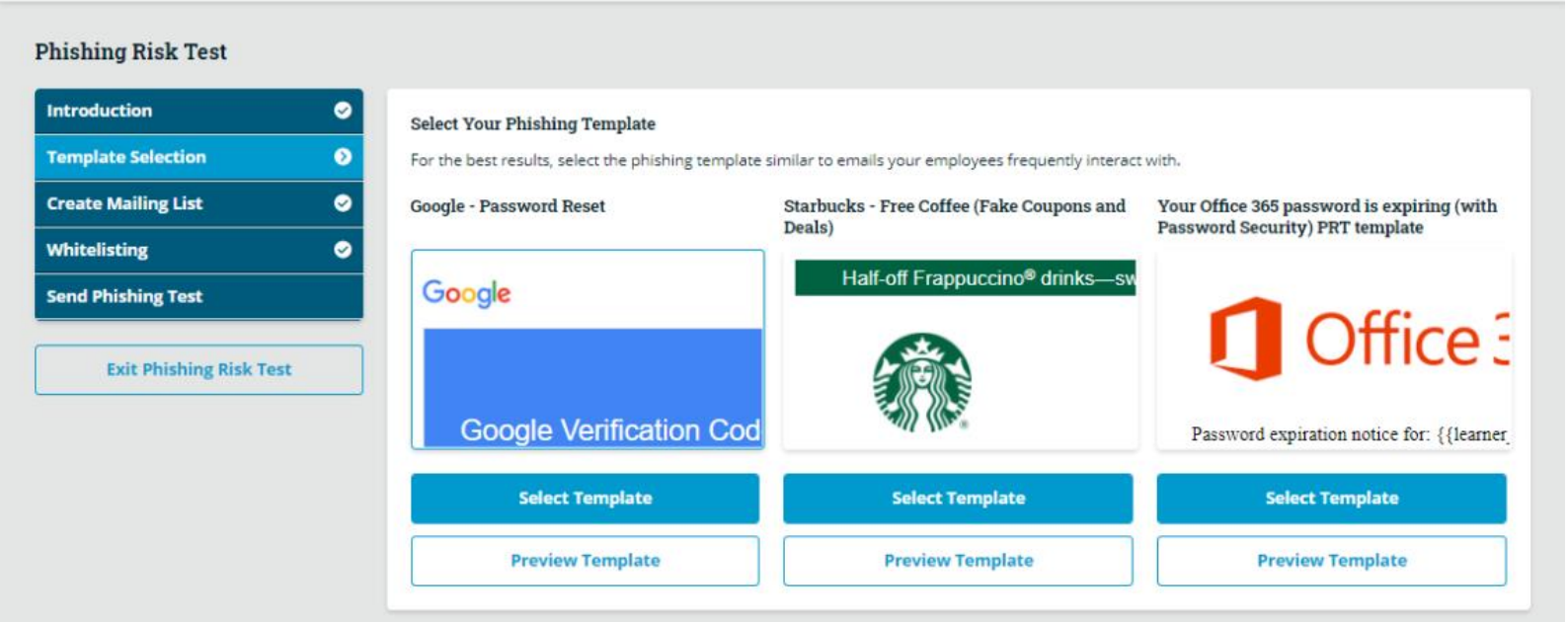
Number of reached individuals

Indicators	- Social media impressions and engagement with campaign posts. - Number of people participating in the locally deployed activities and events (i.e., physical vs. online). Possibly on a more fine-grained level with attention to the number of participants of specific target audiences.
Means of Measurement	- Social media analytics provided by the platform (e.g., Twitter, Facebook, Instagram, LinkedIn). - Media monitoring tool. - Measure the number of views, likes, clicks, and shares. - Information from the communication partners on how many people they reach.
Strengths	- Effective way of measuring outreach on a large scale. - Quantitative information to measure the number of citizens or professionals engaged and participating. This is a proof of interest in the security topics discussed.
Limitations	- The use of the appropriate Social Media to disseminate the campaigns according to the target (other than existing accounts on Facebook, LinkedIn, and Twitter). - Media monitoring tool can be costly. - This can only be achieved if the participating Member States collect the information from the events and activities.
Innovative Suggestions	- Ask partners and customers to benchmark activities and track campaigns and the number of individuals reached. Reporting on national activities—and pointing to gaps in that reporting—might motivate less-active entities to increase their efforts.

YOUR CYBER AWARENESS PROGRAM

O1. Raise awareness on the cyber threat of Phishing (6 months)					
Target audience	Message/Desired Skills	Means	Materials/Tools	Timeframe	Evaluation
All staff	How aware are we?	Phishing simulation	Email	Jan	
All staff	"Do not open suspicious emails"	Custom training	- Webinar (video tutorial) - Workshops	Jan - Mar	Survey/Quiz
All staff	Do not get phished!	Informative material	- Posters - Stickers	Apr	Survey/Quiz
All staff	What did we learn so far?	Gamification	Quiz	May	Survey/Quiz
All staff	How aware are we now?	Phishing simulation		June	Survey/Quiz
All clientele	"We will never ask for your password via email"	Informative material	Newsletter, videos, leaflets	Mar - Jul	
Business Clients	"We will never ask your credentials via email, sms or call"	Informative material	Newsletter, videos, leaflets	Mar - Jul	
O2. Promote cybersecurity education and culture (1 year)					
Target audience	Message/Desired Skills	Means	Materials/Tools	Timeframe	Evaluation
Public relations team	Actions to follow in case of incident	Custom training	Hands-on table-top exercise	Mar (repeat in Oct)	Survey/Quiz
Financial Dep	Advanced Phishing Attacks	Custom training	- Webinar (video tutorial)	Mar (repeat in Oct)	
New employees	Cyber Hygiene Best Practices	Informative session	Presentation	Every interval	
Board of directors	Whaling Attacks aka Attacks against the C-Level	Custom training	Webinar (video tutorial)	Oct	

PHISHING SIMULATION



- Think of phishing simulation as a fire drill
- Phishing simulation as part of security awareness training
- Phishing simulation as a security control

EXAMPLE:

Gophish - Open Source Phishing Framework (getgophish.com)

CYBER GAMES

(Tabletop) Games help:

- 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
    - Finding missing links in the chain-of-command
    - Ensuring documentation of response plans
    - Finding gaps in your recovery processes
- Testing consequences in a safe environment
- Coordination between different departments
- Save money

CUSTOM VS READY-MADE AWARENESS PROGRAMS

CUSTOM

Pros:

- Fits Organizations needs only
- Engages Employees to collaborate
- Enhances the cyber security culture
- Is cheaper

Cons:

- Requires time & some expertise
- Material is less professional
- Does not scale fast

READY-MADE

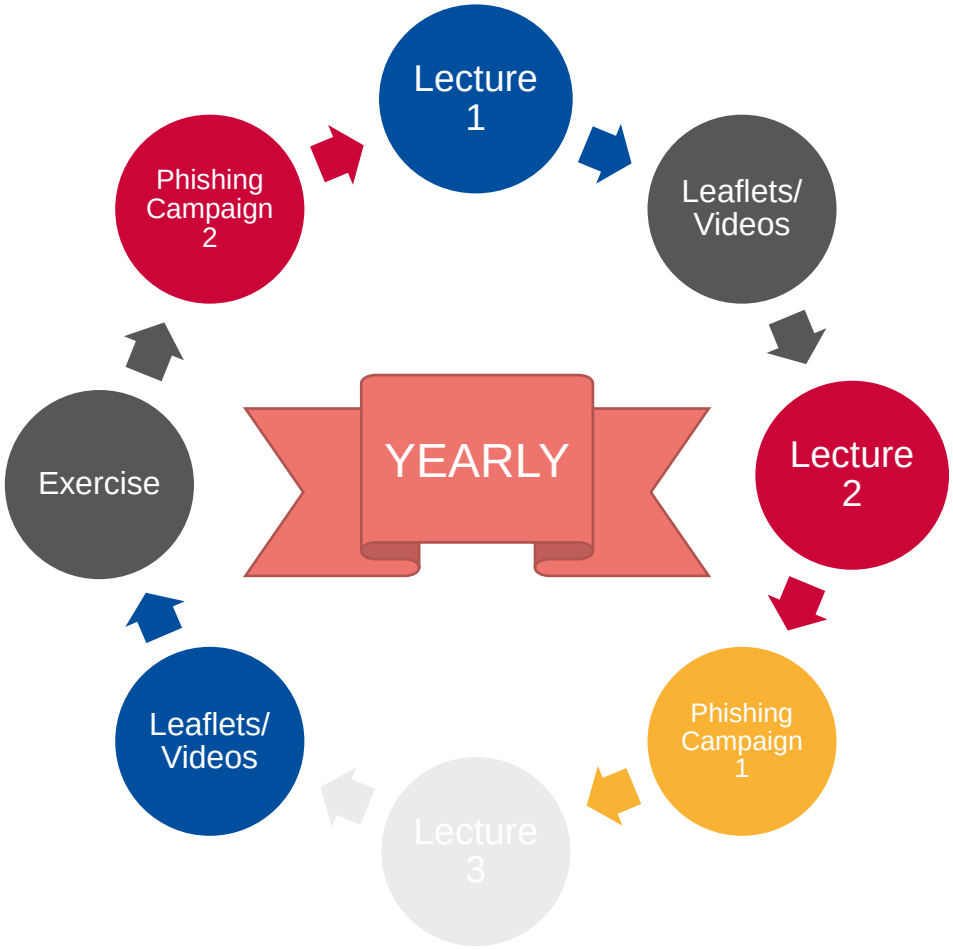
Pros:

- Deploy & Scale Fast
- Ready Metrics
- Medium Expertise needed
- Updated to current trends

Cons:

- Expensive
- Not very personalized by default
- Market research is needed to find the suitable product

AWARENESS ACTIVITY LIFECYCLE

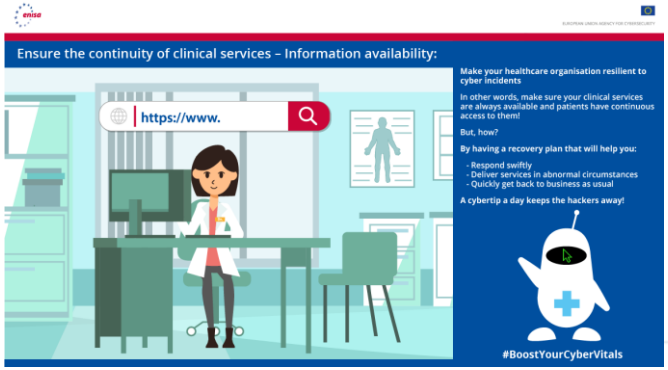


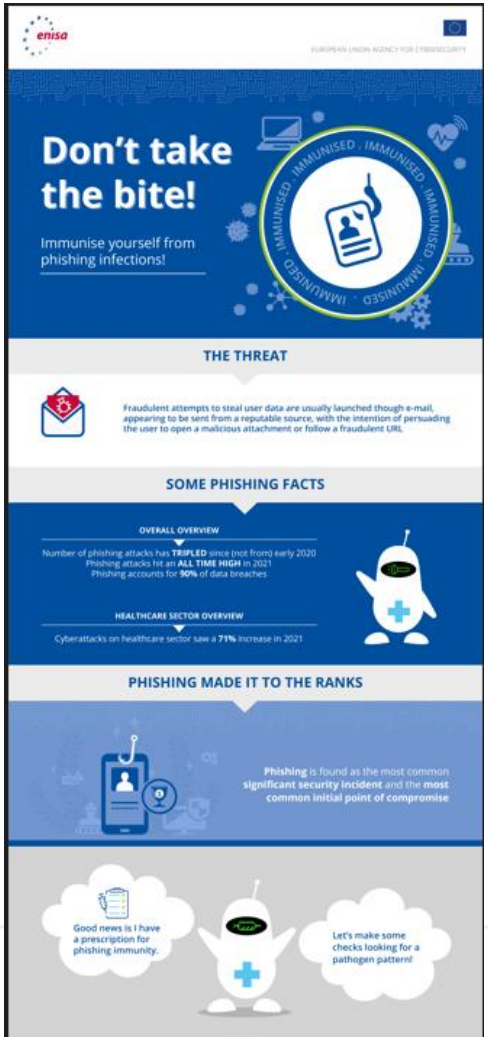
HEALTHCARE SECTOR EXAMPLE'S

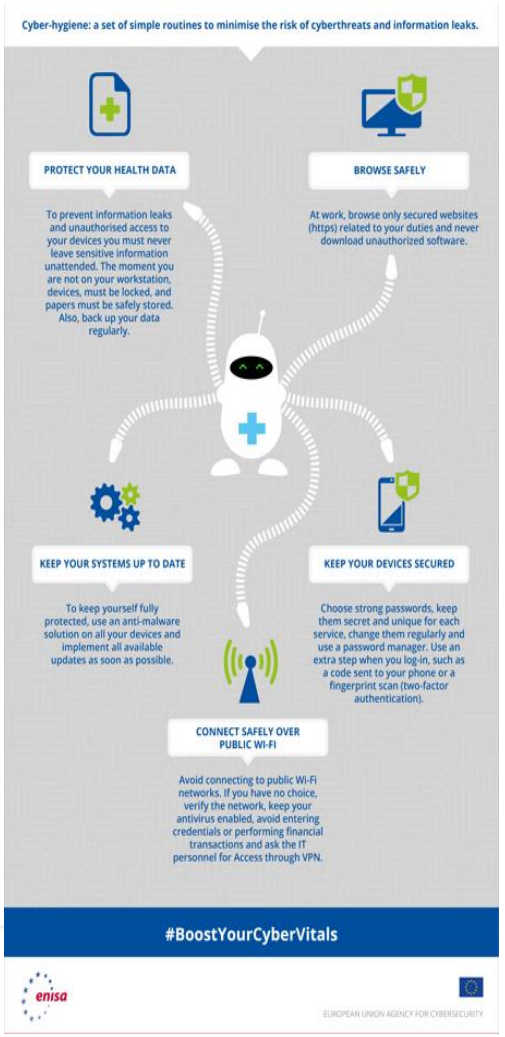
Cyber Health Week 2022

Welcome to the official page of the Cybersecurity Healthcare Week 2022!

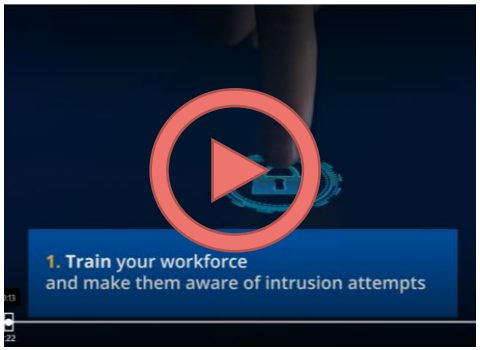
Join us for CyberHealthWeek
#BoostYourCyberVitals

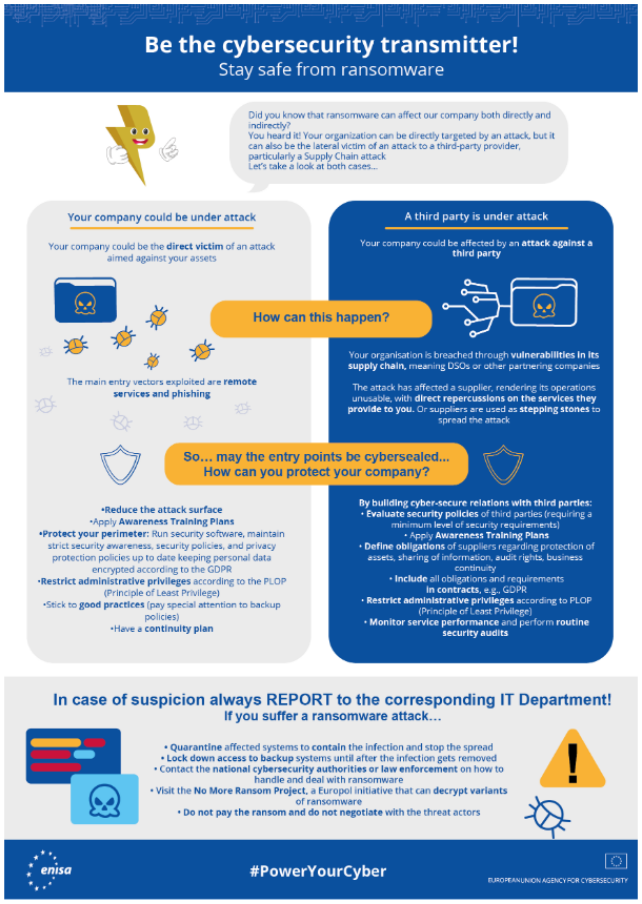






ENERGY SECTOR EXAMPLE'S





RESOURCES

- **Cyber Health Week — ENISA (europa.eu)**
- **Cyber Energy Week — ENISA (europa.eu)**

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 6972765418

Alexandros.zacharis@enisa.europa.eu

www.enisa.europa.eu