ECS
EUROPEAN CYBER SECURITY ORGANISATION

JULY EDITION
AWARENESS CALENDAR

Social engineering

Awareness Calendar **CYBERSECURITY**

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO Members' and Partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2022 are planned as follows:

- January – Cybersecurity certification
- February – Internet of Things
- March – Gender diversity in cyber
- April – Artificial Intelligence
- May – Cyber ranges & range-enabled services
- June – Cybersecurity for verticals
- July – Social engineering
- August – Privacy & data security
- September – Organisational resilience
- October – Cyber hygiene & readiness
- November – Cloud computing
- December – Threat & vulnerability management

DID YOU KNOW?

- Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons. Though such form of trickery has always existed, it has significantly evolved with ICT technologies. Any organisation should identify its critical assets and implement the appropriate security policies and protocols. When necessary, these should be reinforced through the use of technology.
- As a countermeasure ENISA recommends the following:
  - frequent awareness campaigns: posters, presentations, emails, information notes;
  - staff training and exercising;
  - penetration tests to determine an organisation's susceptibility to social engineering attacks, reporting and acting upon the results.

READ MORE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

Phishing Awareness Program

CYS4 created an innovative service that helps companies gain KPI visibility of their workforce's phishing awareness. Humans are the weakest link in the security chain, so we aim to improve their resilience against phishing attacks.
We keep testing employees with tailor-made phishing campaigns based on real-world attacks, helping them recognise phishing emails over time.
Real-time learning Pills appear upon a wrong behavior, describing phishing technics & providing recommendations to avoid falling victim to cybercriminals.
CYS4 draws up a final report with the information collected that is securely processed and anonymised, aggregating the metrics by departments, and identifying the ones needing further training on phishing topics.
Phishing campaigns are performed regularly, embracing the continuous learning approach, allowing companies to constantly measure their workforce, and acting in time to educate personnel and protect the company's data.
READ MORE.

CyberSEAS

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

Social engineering and the importance of a knowledge culture

Social Engineering (SE) is one of the most difficult cyber threats to counter. IT is extremely effective as it plays on people's psychology to steal information, or to induce them to do something that compromises the system security. Nowadays, solutions to effectively defend against it are not yet mature. For this reason it is important to develop a culture of knowledge to be able to prevent and counter this dangerous threat. Research projects such as DOGANA, CyberSec4Europe, and CyberSEAS aim at supporting public and private organisations to protect themselves from SE attacks by promoting an integrated approach that includes: (a) SE assessment - to measure employee resilience through the simulation of phishing e-mails and quizzes - (b) SE detection - to identify malicious e-mails - and (c) SE awareness and training - with gamification-based tools for organization’s employees.
READ MORE.

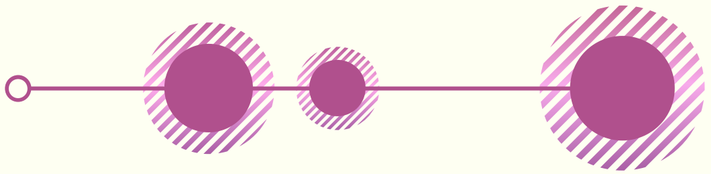
Social Engineering: the most powerful weapon of the attackers

The main threat to cyber security is represented by social engineering, the art of manipulating people for criminal purposes.
In recent times, social engineering attacks have become increasingly sophisticated. Fake websites and e-mails appear realistic enough to trick victims into disclosing data that can be used for identity theft, making social engineering one of the most common ways for hackers to breach an initial defenses company to cause further harm and danger.
Among them, Business Email Compromise (BEC) attacks are aimed at attacking CEO or CFO email accounts.
The new frontier of cyber attacks is deepfake phishing.
The Exprivia Cybersecurity Observatory highlights that the attack technique most exploited by an attacker is Phishing / Social Engineering. In 1Q2022, 389 security cases related to Phishing / Social Engineering in Italy were analysed. To learn more, download the Exprivia Threat Intelligence Report

Fake or authentic?
Learn to spot audio deepfakes!

Fraunhofer AISEC

Advances in machine learning are making deepfakes an increasingly serious threat. Whether it's Zelensky or Angela Merkel, attackers can now deceptively clone targets and put words in their mouths that they never said. This is increasingly becoming a threat to both individuals (fraud) and our society in general (fake news). Studies show that even low exposure and deepfake detection training significantly increase the resilience of listeners: Listeners can then detect deepfakes much better and more reliably. Fraunhofer AISEC has therefore developed an online demo where anyone can try it out: How well can you detect audio deepfakes? And how well do current AI-based deepfake detection methods perform compared to humans? Try it yourself!
READ MORE.



Phishing Red Flags!

Think you'll never fall for a scam? Unfortunately those that exercise social engineering techniques are very experienced, homing in on what they know works - taking time to improve their 'hit rate' and they are very good at it. Keep personal data private, don't disclose information that others can use against you or to gain your trust. It's hard to distinguish the genuine from the malicious, we know. So sign up for our short course on phishing to learn some of the common 'red flags' to look out for. It is one in a series of seven mini courses that accompany the GCA Cybersecurity Toolkit for Small Business.

HSLU Lucerne University of Applied Sciences and Arts

eBanking but secure!

Do you recognise phishing?

Phishing is the most widespread social engineering method. Do you recognise phishing? Take the test!

READ MORE.

incibe_

SPANISH NATIONAL CYBERSECURITY INSTITUTE

Fighting the art of hacking the human: knowledge as a weapon against social engineering

For children and educators: Through the infographic "Objective: zero online fraud" we share a series of recommendations with which we will avoid being victims of online fraud and how cybercriminals carry out actions based on social engineering. READ MORE.

At home: In the campaign "Social engineering, don't be fooled" we explain through videos, articles, infographics and games, which techniques are the most used by cybercriminals and how to avoid them. READ MORE.

For SME's: All you need to know to fight against social engineering in your business: real cases, clues to identify it and steps to make your employees human firewalls. READ MORE.

SECURITY MADEIN.LU | Cybersecurity Agency for the Luxembourg Economy and Municipalities

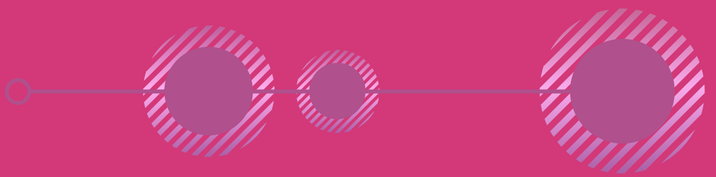
Social Engineering: The Art of Manipulating People

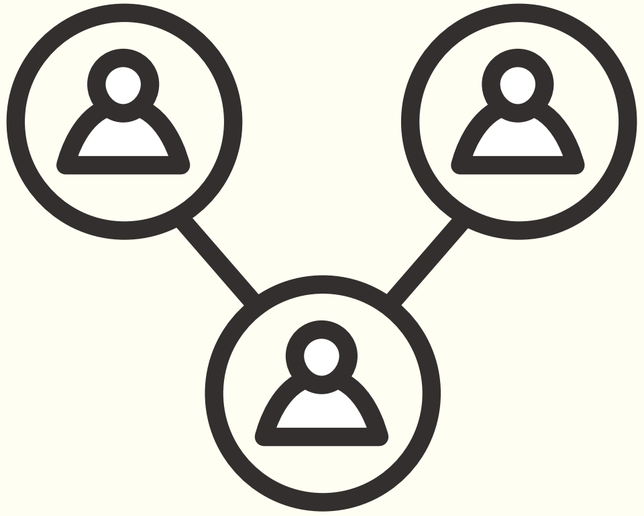
Facts & Figures

- 98% of cyber attacks rely on social engineering
- New employees are the most susceptible to socially engineered attacks
- 21% of current or former employees use social engineering to gain a financial advantage
- The number one type of social engineering attack is phishing
- 30% of phishing messages get opened by targeted users
- 45% of employees click emails they consider to be suspicious “just in case it’s important”
- 50% of phishing sites now using HTTPS
- 66% of malware is installed via malicious email attachments
- Over 18 million websites are infected with malware at a given time each week
- 43% of cyber attacks target small business
- 67% of financial institutions reported an increase in cyber attacks over the past year
- 70 – 90 % of breaches are caused by social engineering
- READ MORE.

A large-scale phishing study by WithSecure

WithSecure (formerly F-Secure Business) conducted a large-scale email phishing study, seeking to explore why phishing continues to be the paramount access method of malicious cyber actors. 82,402 individuals participated in the study, which we believe is the largest so far to explore which tactics are most effective in driving clicks on phishing emails. We hope the study findings will help security teams plan and take effective actions to better protect their organisations. READ MORE.





RESOURCES FROM THE COMMUNITY

Industrial cyber security: protect information, production and supply chain

HWG
A Cyber Security Company

From Industry 4.0 to production line automation: with digitisation, cyber security is now the priority of the industrial sector as well. The topic of cybersecurity has made its overbearing entry onto the industry agenda, placing it among the priorities that companies must give themselves to protect their business model. READ MORE.

Employee awareness to combat social engineering

Sababa
Security

What is the best defence against social engineering? Employee awareness – even better if your training platform is based on gamification. One of the main hurdles that cyber security awareness programs need to overcome is getting staff members to finish the necessary steps and ensuring their participation. Find out how gamification can make this far easier to do. READ MORE.

THANK YOU

for your time!

The Cybersecurity Awareness Calendar
is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu

secretariat@ecs-org.eu