Security Awareness Training

LEDRA COLLEGE
NICOSIA

Security Awareness Training

According to the European Network and Information Security Agency, 'Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks.'

The focus of Security Awareness training is to achieve a long term shift in the attitude of employees towards security - from top management to the last employee - whilst promoting a cultural and behavioral change within an organization.

It is designed to raise awareness about information security and encourage good information security practices, in order to help prevent unintentional compromises of sensitive information and computing systems

Course Aims

After the successful completion of this course, learners should be able to:

- Identify information security threats and vulnerabilities
- Learn and practice habits that will promote a secure organizational environment
- Highlight several current attack vectors and the associated mitigating behavior
- Determine risk level of their actions while using the Internet
- Use browser protection, extensions or add-ons
- Verify the website they are going to use is authentic and malware free
- Secure their mobile devices
- Judge normal requests for information from suspicious requests

Eligible Participants

This course is targeted at all computer users of an organization, with the exception of IT specialists.

Course Duration

The total duration of this course is twenty (20) hours. Upon completion of the course, successful participants will be awarded a certification approved by the HRDA.

Course Indicative Content

NO	INDICATIVE CONTENT	DURATION (HOURS)
1	**Importance of security** The aim is to introduce the concept of information security awareness and safe computing habits, as well as the reasons why cyber criminals are now actively targeting the human element in an organization.	2
2	**Responsibilities of people in the organization** The aim is to explain how every individual in an organization is responsible for the organization's overall security. Participants will understand how their role is affecting security and that the responsibility for information security does not belong solely to the IT department.	2
3	**Policies and procedures** The aim is to present certain guidelines, policies and procedures which should be followed by the participants in order to ensure their individual and organizational safety.	2
4	**Account and password selection criteria** The aim is to stretch the importance of having strong passwords. Participants will acquire knowledge of proper password selection criteria and safe password management habits and processes.	2
5	**Social engineering prevention** The aim is to explain the meaning of social engineering and how attackers are targeting the human element to acquire valuable information, with or without the use of technological means.	2
6	**Social networking dangers** The aim is to identify and evaluate the risks and dangers involved in the social networking domain and how these can be reduced through proper social networking mentality and safe social networking habits.	2
7	**Data handling** The aim is to present proper data handling techniques and how otherwise "innocent" data can become dangerous in the hands of a cyber-criminal. Safe ways of creating, transferring, editing, handling and deleting data are presented and analysed.	2
8	**Personally identifiable information (PII)** The aim is to present and explain what kind of data falls within the category of PII. Ways of how these data should be treated and safeguarded are presented, as well as the possible consequences of not handling PII with the appropriate care.	2
9	**Mobile devices** The aim is to present how mobile devices are now one of the major targets of cyber criminals and what measures a user can take to protect the information stored and shared through his mobile device.	2
10	**Safe internet habits** The aim is to present specific procedures, techniques, guidelines and processes which can minimize the dangers an individual can come across with, while surfing the web and/or performing usual tasks through the internet.	2

Ταχύρυθμα επιχορηγημένα μαθήματα
Αρχής Ανάπτυξης Ανθρώπινου Δυναμικού (ΑΝΑΔ) 2014

Το LEDRA COLLEGE προσφέρει ταχύρυθμα επιχορηγημένα πολυεπιχειρησιακά προγράμματα σε άτομα που επιθυμούν να εμπλουτίσουν τις γνώσεις και τα επαγγελματικά τους προσόντα.

Σημαντικές πληροφορίες & κριτήρια για τα επιχορηγημένα προγράμματα της ΑΝΑΔ

- Τα μαθήματα δικαιούνται να τα παρακολουθήσουν άτομα που εργάζονται στον ιδιωτικό τομέα, σε ημικρατικούς οργανισμούς και σε δημοτικές αρχές. Εξαιρούνται από την επιχορήγηση οι κυβερνητικοί υπάλληλοι.

- Για να δικαιούται ένα άτομο να παρακολουθήσει κάποιο από τα επιχορηγημένα προγράμματα της ΑΝΑΔ, θα πρέπει να καταβάλλει εισφορές στο Ταμείο Κοινωνικών Ασφαλίσεων

- Για κάθε πρόγραμμα υπάρχουν επιπλέον συγκεκριμένα κριτήρια εισδοχής, τα οποία αναγράφονται στον οδηγό κάθε προγράμματος.

- Το ποσοστό της επιχορήγησης διαφέρει ανάλογα με το μέγεθος της επιχείρησης/οργανισμού: Αν η επιχείρηση είναι μικρού μεγέθους (κάτω των 50 ατόμων), η επιχορήγηση ανέρχεται στο 80%, αν η επιχείρηση είναι μεσαίου μεγέθους (κάτω των 250 ατόμων), η επιχορήγηση ανέρχεται στο 70% και αν είναι μεγάλου μεγέθους (άνω των 250 ατόμων), η επιχορήγηση ανέρχεται στο 60%.

- Δεν υπάρχει περιορισμός όσο αφορά τον συνολικό αριθμό των εργοδοτουμενων που μπορεί να στείλει κάθε εταιρεία για κάθε πρόγραμμα.

- Δεν υπάρχει περιορισμός όσο αφορά τον συνολικό αριθμό των προγραμμάτων που μπορεί να παρακολουθήσει κάθε ενδιαφερόμενος.

- Όλα τα μαθήματα ξεκινούν την εβδομάδα 10-16 Φεβρουαρίου 2014

LEDRA COLLEGE
NICOSIA

13 Lankada Street, Strovolos, 2023 Nicosia, Cyprus
+357 22514044 I www.ledra.ac.cy I info@ledra.ac.cy