ECDL Foundation

PeopleCert
All talents, certified.

Ασφάλεια Πληροφοριακών Συστημάτων

(IT Security)

Syllabus Version 2.0

ecdl.gr

PeopleCert
All talents, certified.

Αποποίηση
Παρ' όλα τα μέτρα που έχουν ληφθεί από το Ίδρυμα ECDL για την προετοιμασία αυτής της έκδοσης, καμία εγγύηση δεν παρέχεται από το Ίδρυμα ECDL, ως εκδότη, για την πληρότητα των πληροφοριών που περιέχονται εντός αυτής. Επίσης, το Ίδρυμα ECDL δεν είναι υπεύθυνο ή υπόχρεο για οποιαδήποτε απώλεια, βλάβη, φθορά, οποιουδήποτε είδους προκύψει λόγω πληροφοριών, οδηγιών ή συμβουλών που περιέχονται σε αυτό το έγγραφο. Το Ίδρυμα ECDL διατηρεί το δικαίωμά του να πραγματοποιεί αλλαγές μονομερώς και κατά τη διακριτική του ευχέρεια οποτεδήποτε χωρίς προηγούμενη γνωστοποίηση.

Ενότητα Ασφάλεια Πληροφοριακών Συστημάτων (IT Security)

Η ενότητα αυτή παραθέτει τις κύριες έννοιες που διέπουν την ασφαλή χρήση των Τεχνολογιών Πληροφορίας και Επικοινωνιών (Πληροφορικής και Επικοινωνιών - ΤΠΕ) στην καθημερινή ζωή καθώς και τις δεξιότητες που απαιτούνται για την υλοποίηση και συντήρηση ασφαλών συνδέσεων δικτύου, την ασφαλή σύνδεση στο Διαδίκτυο, καθώς και τη σωστή διαχείριση δεδομένων και πληροφοριών.

Στόχοι Ενότητας

Ο υποψήφιος θα πρέπει να είναι σε θέση να:

- Κατανοεί τη σημασία της ασφαλούς διατήρησης πληροφοριών και δεδομένων, και να αναγνωρίζει τις βασικές αρχές προστασίας ιδιωτικότητας, διατήρησης, και ελέγχου δεδομένων.
- Αναγνωρίζει απειλές στο σύστημα ασφαλείας τού από κλοπή ταυτότητας και πιθανές απειλές στα δεδομένα που προκύπτουν από τη χρήση υπολογιστικής νέφους.
- Χρησιμοποιεί κωδικούς πρόσβασης και κρυπτογράφηση για να προστατεύει αρχεία και δεδομένα.
- Αναγνωρίζει απειλές, να προστατεύει έναν υπολογιστή, μια συσκευή ή ένα δίκτυο από λογισμικό κακόβουλης χρήσης (malware) και να αντιμετωπίζει επιθέσεις κακόβουλου λογισμικού
- Αναγνωρίζει τους τύπους δικτύων, τους τύπους ασύρματης ασφάλειας και να χρησιμοποιεί τείχη προστασίας και hotspot
- Προστατεύει έναν υπολογιστή, μια συσκευή από μη εξουσιοδοτημένη πρόσβαση, να διαχειρίζεται με ασφάλεια και να ενημερώνει τους κωδικούς πρόσβασης.
- Χρησιμοποιεί τις κατάλληλες ρυθμίσεις πλοήγησης στον Ιστό, να κατανοεί τον τρόπο πιστοποίησης της αυθεντικότητας ενός Ιστότοπου και να περιηγείται στον Ιστό με ασφάλεια.
- Κατανοεί τα θέματα ασφαλείας που σχετίζονται με την επικοινωνία και μπορούν να προκύψουν από τη χρήση ηλεκτρονικού ταχυδρομείου, κοινωνικών δικτύων, υπηρεσιών VOIP, άμεσων μηνυμάτων και κινητών συσκευών.
- Δημιουργεί αντίγραφα ασφαλείας (backup) και να επαναφέρει (restore) δεδομένα σωστά και με ασφάλεια, σε τοπικές θέσεις αλλά και στο νέφος (cloud), καθώς και να διαγράφει δεδομένα και συσκευές με ασφάλεια.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
1 Έννοιες Ασφαλείας	1.1 Απειλές κατά των Δεδομένων (Data Threats)	1.1.1	Κατανόηση της διαφοράς μεταξύ δεδομένων και πληροφοριών.
		1.1.2	Κατανόηση του όρου ηλεκτρονικό έγκλημα/έγκλημα στον κυβερνοχώρο (cybercrime), hacking (πληροφορική πειρατεία - εισβολών σε μη εξουσιοδοτημένα δίκτυα για αναγνώριση – αναφορά αδυναμιών ασφαλείας).
		1.1.3	Αναγνώριση τυχαίων, κακόβουλων απειλών κατά των δεδομένων από μεμονωμένα άτομα, παρόχους υπηρεσιών και εξωτερικούς οργανισμούς.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		1.1.4	Αναγνώριση απειλών κατά των δεδομένων από ανωτέρα βία, όπως: φωτιά, πλημμύρες, πόλεμος, σεισμός.
		1.1.5	Αναγνώριση απειλών κατά των δεδομένων από τη χρήση νεφελοϋπολογιστικής (cloud computing) όπως: έλεγχος των δεδομένων, πιθανή απώλεια ιδιωτικότητας.
	1.2 Αξία της Πληροφορίας	1.2.1	Κατανόηση βασικών χαρακτηριστικών ασφάλειας πληροφοριών, όπως: εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity), διαθεσιμότητα (availability).
		1.2.2	Κατανόηση των λόγων προστασίας εμπορικώς ευαίσθητων στοιχείων/πληροφοριών, όπως: πρόληψη κλοπής ταυτότητας (identity theft), απάτη, Διατήρηση της ιδιωτικότητας
		1.2.3	Κατανόηση των λόγων προστασίας εργασιακές πληροφορίες που υπάρχου σε υπολογιστές και συσκευές, όπως: πρόληψη κλοπής ή κακής χρήσης των στοιχείων, τυχαία απώλεια δεδομένων, σαμποτάζ.
		1.2.4	Προσδιορισμός των κύριων απαιτήσεων προστασίας, διατήρησης και ελέγχου δεδομένων/ιδιωτικότητας όπως: διαφάνεια, νομικοί λόγοι χρήσης, αναλογικότητα .
		1.2.5	Κατανόηση των όρων κάτοχοι δεδομένων (data subjects) και διαχειριστές δεδομένων (data controllers). Κατανόηση του τρόπου εφαρμογής των αρχών προστασίας ιδιωτικότητας, διατήρησης, και ελέγχου δεδομένων στους κατόχους και στους διαχειριστές δεδομένων.
		1.2.6	Κατανόηση της σημασίας της τήρησης οδηγιών και πολιτικών για τη χρήση των ΤΠΕ και του τρόπου πρόσβασής τους.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
	1.3 Προσωπική Ασφάλεια	1.3.1	Κατανόηση του όρου κοινωνική μηχανική (social engineering) καθώς και των συνεπειών της, όπως: μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές ή/και συσκευές, μη εξουσιοδοτημένη συλλογή πληροφοριών, ηλεκτρονική απάτη.
		1.3.2	Προσδιορισμός μεθόδων κοινωνικής μηχανικής, όπως: τηλεφωνικές κλήσεις, ηλεκτρονική υφαρπαγή προσωπικών δεδομένων (phishing), κρυφοκοίταγμα (shoulder surfing).
		1.3.3	Κατανόηση του όρου κλοπή στοιχείων ταυτότητας (identity theft) και των επιπτώσεών της: προσωπικές, οικονομικές, επιχειρηματικές, νομικές.
		1.3.4	Προσδιορισμός μεθόδων κλοπής στοιχείων ταυτότητας, όπως: ανάκτηση δεδομένων από διάφορα έγγραφα – πχ πεταμένους λογαριασμούς (information diving), ηλεκτρονική υφαρπαγή δεδομένων, αποθηκευμένων σε μαγνητικά μέσα, όπως τραπεζικές κάρτες, και δημιουργία κλωνοποιημένων καρτών ή «ξάφρισμα» (skimming), δημιουργία ψευδών συνθηκών για απόσπαση δεδομένων/πληροφοριών (pretexting).
	1.4 Ασφάλεια Αρχείων	1.4.1	Κατανόηση της επίδρασης της ενεργοποίησης/απενεργοποίησης των ρυθμίσεων ασφαλείας μακροεντολών.
		1.4.2	Κατανόηση των πλεονεκτημάτων και των περιορισμών της κρυπτογράφησης (encryption). Επίγνωση της σημασίας μη-αποκάλυψης ή απώλειας του κωδικού πρόσβασης κρυπτογράφησης, κλειδιού, πιστοποιητικού.
		1.4.3	Κρυπτογράφηση ενός αρχείου, φακέλου, δίσκου.
		1.4.4	Ορισμός κωδικού πρόσβασης (password) σε αρχεία, όπως: έγγραφα, υπολογιστικά φύλλα, συμπιεσμένα αρχεία.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
2 Λογισμικό Κακόβουλης Χρήσης (Malware)	2.1 Τύποι και Μέθοδοι Λειτουργίας	2.1.1	Κατανόηση του όρου λογισμικό κακόβουλης χρήσης (malware). Αναγνώριση διάφορων μεθόδων απόκρυψης του κακόβουλου λογισμικού σε υπολογιστές ή συσκευές, όπως: Δούρειοι ίπποι (Trojans), ιών σε επίπεδο λειτουργικού συστήματος (rootkits) και κερκόπορτες/"πίσω πόρτες" (back doors).
		2.1.2	Αναγνώριση διάφορων τύπων μολυσματικών κακόβουλων λογισμικών και κατανόηση της λειτουργίας τους, όπως: ιοί (viruses), σκουλήκια (worms).
		2.1.3	Αναγνώριση τύπων κλοπής δεδομένων, κερδοσκοπικού/εκβιαστικού κακόβουλου λογισμικού και κατανόηση της λειτουργίας τους, όπως: λογισμικό ανεπιθύμητης διαφήμισης (adware), κακόβουλο λογισμικό ransomware (απαίτηση λύτρων), λογισμικό παρακολούθησης (spyware), δίκτυα μολυσμένων υπολογιστών (botnets), καταγραφέας πληκτρολογίου (keystroke logging) και λογισμικό ανεπιθύμητων κλήσεων (diallers).
	2.2 Προστασία	2.2.1	Κατανόηση του πώς λειτουργεί το λογισμικό προστασίας από ιούς (anti-virus) και των περιορισμών του.
		2.2.2	Κατανόηση ότι το λογισμικό προστασίας από ιούς θα πρέπει να είναι εγκατεστημένο σε υπολογιστές και συσκευές.
		2.2.3	Κατανόηση της σημασία της τακτικής ενημέρωσης λογισμικού όπως: προστασίας από τους ιούς (anti-virus), περιηγητής Ιστού, πρόσθετο (plug-in), εφαρμογή, λειτουργικό σύστημα
		2.2.4	Σάρωση συγκεκριμένης μονάδας δίσκου, συγκεκριμένων φακέλων ή αρχείων χρησιμοποιώντας λογισμικό προστασίας από ιούς. Προγραμματισμός σάρωσης χρησιμοποιώντας ένα λογισμικό προστασίας από ιούς.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		2.2.5	Κατανόηση των κινδύνων που προκύπτουν από τη χρήση απαρχαιωμένου και μη υποστηριζόμενου λογισμικού όπως: αύξηση των απειλών από κακόβουλο λογισμικό (increased malware threats), μη συμβατότητα (incompatibility).
	2.3 Επίλυση και Αφαίρεση	2.3.1	Κατανόηση του όρου καραντίνα (quarantine) και της επίπτωσης της απομόνωσης μολυσμένων/ύποπτων αρχείων.
		2.3.2	Καραντίνα, διαγραφή μολυσμένων/ύποπτων αρχείων.
		2.3.3	Κατανόηση του ότι μια επίθεση κακόβουλου λογισμικού μπορεί να διαγνωστεί και να επιλυθεί με τη χρήση διαδικτυακών πόρων όπως: ιστότοποι παροχής λειτουργικών συστημάτων, ιστότοποι παροχής λογισμικού προστασίας από ιούς (anti-virus), ιστότοποι παροχής λογισμικού περιήγησης στον Ιστό, ιστότοποι σχετικών αρχών.
3 Ασφάλεια Δικτύου	3.1 Δίκτυα και Συνδέσεις Δικτύου	3.1.1	Κατανόηση του όρου δίκτυο και αναγνώριση των συνήθων τύπων δικτύου, όπως: Τοπικό Δίκτυο (Local Area Network - LAN), Ασύρματο Δίκτυο Τοπικής Περιοχής (WLAN), Δίκτυο Ευρείας Περιοχής (Wide Area Network - WAN), Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network - VPN).
		3.1.2	Κατανόηση ότι ο τρόπος σύνδεσης σ' ένα δίκτυο έχει επιπτώσεις για την ασφάλεια, όπως: κακόβουλο λογισμικό, πρόσβαση σε δεδομένα χωρίς άδεια, διατήρηση ιδιωτικότητας.
		3.1.3	Κατανόηση του ρόλου του διαχειριστή δικτύου (network administrator) στη διαχείριση της ταυτοποίησης (authentication), της εξουσιοδότησης (authorisation),και των λογαριασμών (accounting) των χρηστών σ' ένα δίκτυο, στην εγκατάσταση ενημερώσεων, στην παρακολούθηση της κινητικότητας του δικτύου και στην αντιμετώπιση κακόβουλου λογισμικού εντός ενός δικτύου.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		3.1.4	Κατανόηση της λειτουργίας και των περιορισμών ενός τείχους προστασίας (firewall) σε προσωπικό/οικιακό, εργασιακό περιβάλλον.
		3.1.5	Ενεργοποίηση και απενεργοποίηση του τείχους προστασίας (firewall). Παροχή πρόσβασης, κατάργηση πρόσβασης σε εφαρμογή, υπηρεσία/δυνατότητα πέρα από το τείχος προστασίας.
	3.2 Ασύρματη Ασφάλεια	3.2.1	Αναγνώριση διαφορετικών τύπων ασύρματης προστασίας / κρυπτογράφησης και των περιορισμών τους, όπως: Πρωτόκολλο WEP (WEP), Πρωτόκολλο WPA(Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2), Φιλτράρισμα μέσω διεύθυνσης MAC (Media Access Control), Απόκρυψη του SSID (Service Set Identifier).
		3.2.2	Επίγνωση ότι η χρήση ενός μη-προστατευμένου ασύρματου δικτύου μπορεί να οδηγήσει σε επιθέσεις όπως: υποκλοπές των προσωπικών σας δεδομένων (eavesdroppers), μη εξουσιοδοτημένη χρήση του δικτύου σας (network hijacking), μεσάζοντας (man in the middle).
		3.2.3	Κατανόηση του όρου προσωπικό hotspot (σημείο αναμετάδοσης).
		3.2.4	Ενεργοποίηση, απενεργοποίηση ενός ασφαλούς προσωπικού hotspot και ασφαλής σύνδεση/αποσύνδεση συσκευών σε προσωπικό hotspot.
4 Έλεγχος Πρόσβασης (Access Control)	4.1 Μέθοδοι	4.1.1	Αναγνώριση μέτρων προστασίας από μη εξουσιοδοτημένη πρόσβαση σε δεδομένα όπως: όνομα χρήστη (user name), χρήση κωδικών πρόσβασης (passwords), προσωπικός κωδικός ασφαλείας PIN, κρυπτογράφηση (encryption), εξουσιοδότηση πολλαπλών παραγόντων (multi-factor authentication).
		4.1.2	Κατανόηση του όρου κωδικός πρόσβασης μίας χρήσης (one-time password).
		4.1.3	Κατανόηση του σκοπού ύπαρξης λογαριασμού δικτύου.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		4.1.4	Κατανόηση του ότι ένας λογαριασμός δικτύου πρέπει να: ανοίγει με χρήση ονόματος χρήστη (user name) και κωδικού πρόσβασης (password) και να κλειδώνεται ή να αποσυνδέεται όταν δεν χρησιμοποιείται.
		4.1.5	Αναγνώριση συνήθων βιομετρικών τεχνικών ασφαλείας που χρησιμοποιούνται για τον έλεγχο πρόσβασης, όπως: δακτυλικό αποτύπωμα (fingerprint), σάρωση οφθαλμών (eye scanning), αναγνώριση προσώπου (face recognition), γεωμετρία χειρός (hand geometry).
	4.2 Διαχείριση Κωδικών Ασφαλείας (Password Management)	4.2.1	Αναγνώριση ορθών πολιτικών κωδικών πρόσβασης, όπως: μη-αποκάλυψη κωδικών, τακτική αλλαγή κωδικών, επαρκές πλήθος χαρακτήρων κωδικού, κατάλληλη μίξη χαρακτήρων (γράμματα, αριθμοί και ειδικοί χαρακτήρες), διαφορετικοί κωδικοί πρόσβασης για κάθε υπηρεσία.
		4.2.2	Κατανόηση της λειτουργίας και των περιορισμών του λογισμικού διαχείρισης κωδικών (password manager software).
5 Ασφαλής Χρήση του Ιστού	5.1 Ρυθμίσεις Φυλλομετρητή Ιστού.	5.1.1	Επιλογή κατάλληλων ρυθμίσεων για την ενεργοποίηση, απενεργοποίηση της αυτόματης συμπλήρωσης, αυτόματης αποθήκευσης κατά τη συμπλήρωση μίας φόρμας.
		5.1.2	Διαγραφή προσωπικών δεδομένων από έναν φυλλομετρητή ιστού, όπως: ιστορικό περιήγησης (browsing history), ιστορικό λήψεων (download history), προσωρινά αποθηκευμένα αρχεία διαδικτύου (cached internet files), κωδικών ασφαλείας (passwords), λανθανόντων αρχείων καταγραφής δεδομένων (cookies), δεδομένων αυτόματης συμπλήρωσης (autocomplete data).
	5.2 Ασφαλής Περιήγηση στον Ιστό (Secure Browsing)	5.2.1	Επίγνωση ότι συγκεκριμένες ηλεκτρονικές δραστηριότητες (αγορές, χρηματοοικονομικές συναλλαγές) θα πρέπει να πραγματοποιούνται μόνο σε ασφαλείς ιστοσελίδες χρησιμοποιώντας ασφαλή σύνδεση στο δίκτυο.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		5.2.2	Αναγνώριση τρόπων επιβεβαίωσης της αυθεντικότητας ενός ιστότοπου όπως: ποιότητα περιεχομένου, επίκαιρη ενημέρωση, έγκυρο URL, πληροφορίες ιδιοκτήτη ή εταιρίας, πληροφορίες επικοινωνίας, επικυρωμένος τομέας ιδιοκτήτη, πιστοποιητικό ασφαλείας.
		5.2.3	Επίγνωση της διαδικασίας παραπλάνησης (pharming).
		5.2.4	Κατανόηση του σκοπού, της λειτουργίας και των τύπων του λογισμικού ελέγχου-περιεχομένου (content-control software), όπως: λογισμικό φιλτραρίσματος διαδικτυακού περιεχομένου (Internet filtering), λογισμικού γονικού ελέγχου (parental control).
6 Επικοινωνίες	6.1 E- Ηλεκτρονικό Ταχυδρομείο (E-Mail)	6.1.1	Κατανόηση του σκοπού της κρυπτογράφησης, αποκρυπτογράφησης ενός μηνύματος ηλεκτρονικού ταχυδρομείου.
		6.1.2	Κατανόηση του όρου ψηφιακή υπογραφή (digital signature).
		6.1.3	Αναγνώριση της πιθανότητας λήψης δόλιων / απρόσμενων και αυτόκλητων μηνυμάτων.
		6.1.4	Αναγνώριση των συνήθων χαρακτηριστικών της ηλεκτρονικής υφαρπαγής προσωπικών δεδομένων, όπως: χρήση ονομάτων υπαρχόντων οργανισμών, ατόμων, ψευδών διαδικτυακών τοποθεσιών, λογότυπων, επωνυμιών, παρότρυνση αποκάλυψης προσωπικών πληροφοριών.
		6.1.5	Επίγνωση της δυνατότητας αναφοράς απόπειρας υφαρπαγής προσωπικών δεδομένων στους νόμιμους οργανισμούς, αρμόδιες αρχές.
		6.1.6	Επίγνωση του κινδύνου μόλυνσης του Η/Υ ή της συσκευής με κακόβουλο λογισμικό (malware) που προήλθε από άνοιγμα επισυναπτόμενου αρχείου που περιέχει μια μακροεντολή ή ένα εκτελέσιμο αρχείο.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
	6.2 Κοινωνική Δικτύωση (Social Networking)	6.2.1	Κατανόηση της σημασίας μη-αποκάλυψης εμπιστευτικών πληροφοριών ή προσωπικών δεδομένων σε διαδικτυακές τοποθεσίες κοινωνικής δικτύωσης (social networking).
		6.2.2	Επίγνωση της ανάγκης εφαρμογής και συνεχής ανανέωσης των κατάλληλων ρυθμίσεων σε λογαριασμούς κοινωνικής δικτύωσης όπως: απόρρητο λογαριασμού, τοποθεσία.
		6.2.3	Εφαρμογή ρυθμίσεων σε λογαριασμούς κοινωνικής δικτύωσης όπως: απόρρητο λογαριασμού (privacy), τοποθεσία (location).
		6.2.4	Κατανόηση πιθανών κινδύνων κατά τη χρήση διαδικτυακών τοποθεσιών κοινωνικής δικτύωσης, όπως: εκφοβισμός στον κυβερνοχώρο (cyber bullying), προσέγγιση πλασματικής φιλίας με απώτερο σκοπό την διαδικτυακή σεξουαλική παρενόχληση ή αποπλάνηση ανηλίκου (grooming), κακόβουλη αποκάλυψη του προσωπικού περιεχομένου (malicious disclosure of personal content), ψευδείς ταυτότητες (false identities), ψευδείς σύνδεσμοι, περιεχόμενα ή μηνύματα απάτης.
		6.2.5	Επίγνωση της δυνατότητας αναφοράς (report) ακατάλληλης χρήσης των κοινωνικών δικτύων ή απρεπής συμπεριφοράς στον αντίστοιχο φορέα υπηρεσίας, στις αρμόδιές αρχές.
	6.3 Διαδικτυακή Τηλεφωνία (VoIP) και Άμεσα Μηνύματα (Instant Messaging)	6.3.1	Κατανόηση των αδυναμιών ασφαλείας των εφαρμογών ανταλλαγής άμεσων μηνυμάτων (IM) και Διαδικτυακής Τηλεφωνίας (Voice Over IP – VoIP), όπως: λογισμικό κακόβουλης χρήσης (malware), πρόσβαση μέσω κερκόπορτας/"πίσω πόρτας" (backdoor access), πρόσβαση σε αρχεία, υποκλοπές των προσωπικών δεδομένων (eavesdropping).

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		6.3.2	Αναγνώριση μεθόδων εξασφάλισης της εμπιστευτικότητας κατά τη χρήση εφαρμογών ανταλλαγής άμεσων μηνυμάτων (IM) και Διαδικτυακής Τηλεφωνίας (Voice Over IP – VoIP), όπως: κρυπτογράφηση (encryption), μη-αποκάλυψη σημαντικών πληροφοριών, περιορισμός στο διαμοιρασμό αρχείων (file sharing).
	6.4 Κινητό (Mobile)	6.4.1	Κατανόηση των πιθανών επιπτώσεων της χρήσης εφαρμογών που προέρχονται από ανεπίσημα ηλεκτρονικά καταστήματα εφαρμογών όπως: λογισμικό κακόβουλης χρήσης κινητών συσκευών(mobile malware), περιττή χρήση πόρων (unnecessary resource utilization), πρόσβαση σε προσωπικά δεδομένα (access to personal data), κακή ποιότητα (poor quality), κρυμμένες χρεώσεις (hidden costs).
		6.4.2	Κατανόηση του όρου άδεια εφαρμογής (application permissions).
		6.4.3	Επίγνωση ότι οι εφαρμογές κινητών μπορούν να εξάγουν προσωπικές πληροφορίες από την κινητή συσκευή όπως: λεπτομέρειες επαφών (contact details), ιστορικό τοποθεσιών (location history), εικόνες (images).
		6.4.4	Επίγνωση των μέτρων έκτακτης ανάγκης και πρόληψης σε περίπτωση απώλειας συσκευής, όπως: απενεργοποίηση από απόσταση (remote disable), αφαίρεση αρχείων από απόσταση (remote wipe), εύρεση της τοποθεσίας της συσκευής (locate device).
7 Ασφαλή Διαχείριση Δεδομένων	7.1 Διασφάλιση και Δημιουργία Αντιγράφων Ασφαλείας Δεδομένων	7.1.1	Αναγνώριση τρόπων εξασφάλισης φυσικής ασφάλειας υπολογιστών και συσκευών, όπως: να μην αφήνονται χωρίς επίβλεψη οι υπολογιστές και οι συσκευές, καταγραφή της θέσης και των λεπτομερειών μιας συσκευής, χρήση καλωδίων κλειδώματος/κλειδαριές συρματόσχοινου (cable locks), έλεγχος πρόσβασης.

Κατηγορία	ΣΥΝΟΛΟ ΔΕΞΙΟΤΗΤΩΝ	ΑΝΑΦ.	ΑΜΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		7.1.2	Αναγνώριση της σημασίας ύπαρξης διαδικασίας δημιουργίας αντιγράφων ασφαλείας για τις περιπτώσεις απώλειας δεδομένων από υπολογιστές και συσκευές.
		7.1.3	Προσδιορισμός χαρακτηριστικών διαδικασίας δημιουργίας αντιγράφων ασφαλείας, όπως: τακτικότητα/συχνότητα, προγραμματισμός/χρονοδιάγραμμα, τοποθεσία αποθήκευσης, συμπίεση δεδομένων (data compression).
		7.1.4	Δημιουργία αντιγράφων ασφαλείας δεδομένων (backup) σε μια τοποθεσία όπως: τοπικός δίσκος, εξωτερικός δίσκος/μέσο, υπηρεσία νέφους (cloud service).
		7.1.5	Ανάκτηση (restore) δεδομένων από μια τοποθεσία αποθήκευσης αντιγράφων ασφαλείας, όπως: τοπικός δίσκος, εξωτερικός δίσκος/μέσο, υπηρεσία νέφους (cloud service).
	7.2 Ασφαλής Διαγραφή και Καταστροφή	7.2.1	Διάκριση μεταξύ διαγραφής και μόνιμης διαγραφής δεδομένων.
		7.2.2	Κατανόηση αιτιών μόνιμης διαγραφής δεδομένων από μονάδες δίσκου ή άλλες συσκευές.
		7.2.3	Επίγνωση ότι η διαγραφή περιεχομένου μπορεί να μην είναι μόνιμη σε υπηρεσίες, όπως: ιστοσελίδες κοινωνικής δικτύωσης (social network), ιστολόγιο (blog), ιστοσελίδες ομαδικών συζητήσεων (forum), υπηρεσίες νέφους (cloud services)
		7.2.4	Προσδιορισμός συνήθων μεθόδων μόνιμης **διαγραφής** δεδομένων, όπως: καταστροφή αρχείων (shredding), καταστροφή δίσκου/μέσου, απομαγνητισμός (degaussing), χρήση βοηθητικών προγραμμάτων καταστροφής δεδομένων.