



MOBILE
MONEY

Ενότητα 2

Ασφάλεια και πρόληψη



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (ΕΑΕΑ). Η Ευρωπαϊκή Ένωση και ο ΕΑΕΑ δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις. Αριθμός έργου: 2023-1-RO01-KA220-ADU-000157797





Συνεργάτες



ZAVOD IZRIIS

Zavod IZRIIS, Σλοβενία

Asociația
4 CHANGE

Asociația Four Change, Ρουμανία



E-SENIORS: INITIATION DES
SENIORS AUXNTIC
ASSOCIATION, Γαλλία



GREEK UNIVERSITIES NETWORK

GUnet, Ελλάδα



NICIODATĂ SINGUR
prietenii vârstnicilor

Asociația Niciodata Singur –
Prietenii Varstnicilor, Ρουμανία

Fundación
gesmed

Fundació Gesmed Fundació de
la Comunitat Valenciana,



MOBILE
MONEY

Ενότητες

1. Βασικές δεξιότητες ψηφιακού αλφαριθμητισμού

2. Ασφάλεια και πρόληψη

3. Διαχείριση τραπεζικού λογαριασμού διαδικτυακά

4.. Διαδικτυακές λύσεις για τη λήψη και αποστολή χρημάτων

5. Χρήση πιστωτικής κάρτας για την αγορά αγαθών και υπηρεσιών από το διαδίκτυο

6. Επεξεργασία ηλεκτρονικών πληρωμών για φόρους και λογαριασμούς



Μονάδα 1

Εισαγωγή

Στόχοι

Με την ολοκλήρωση αυτής της ενότητας, θα ενημερωθείτε σχετικά με

- ✓ τους μαθησιακούς στόχους και το εκπαιδευτικό περιεχόμενο αυτής της ενότητας
- ✓ τη μεθοδολογία κατάρτισης που χρησιμοποιείται και η διάρκεια αυτής της ενότητας





Ικανότητες

Μετά την ολοκλήρωση αυτής της ενότητας, θα:

- Αποκτήσετε τις απαραίτητες δεξιότητες για την ασφαλή και σίγουρη χρήση λύσεων κινητών χρημάτων:
 - ✓ Κατανοείτε τι είναι η διαδικτυακή ασφάλεια.
 - ✓ Κατανοείτε τι είναι προσωπικά και ευαίσθητα δεδομένα.
 - ✓ Κατανοείτε τις έννοιες της ιδιωτικότητας και της ασφάλειας.
 - ✓ Γνωρίζετε τι είναι το spamming και το phishing και πώς να απαντάτε σε αυτά.
 - ✓ Γνωρίζετε τα κριτήρια για να αποφασίσετε ποιοι σύνδεσμοι είναι ασφαλείς για επίσκεψη
 - ✓ Γνωρίζετε τα διαδικτυακά δικαιώματά σας
 - ✓ Κατανοείτε τι είναι ο GDPR και γιατί τον χρειαζόμαστε
 - ✓ Γνωρίζετε πώς να εφαρμόζετε μέτρα ασφαλείας και προληπτικά μέτρα

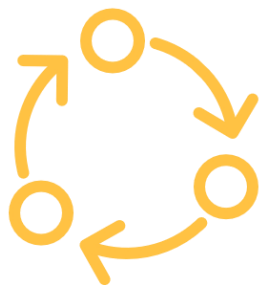


Περιεχόμενο κατάρτισης



MOBILE
MONEY

1. Εισαγωγή της συνεδρίας: διάρκεια, στόχοι, περιεχόμενο και μεθοδολογία
2. Διαδικτυακή ασφάλεια, προσωπικά δεδομένα, ευαίσθητα δεδομένα, ιδιωτικότητα και ασφάλεια
3. Αναγνώριση του spam και του phishing και τι πρέπει να κάνετε γι' αυτά
4. Γνωρίζοντας τα διαδικτυακά δικαιώματά σας, το παράδειγμα του GDPR
5. Προστασία του εαυτού σας στο διαδίκτυο
6. Κουίζ: ελέγξτε τις γνώσεις σας



Μεθοδολογία και διάρκεια κατάρτισης

Διάρκεια: Διάρκεια: 4 ώρες

- Πρόσωπο με πρόσωπο: 2 ώρες
- Διαδικτυακή εκπαίδευση: 2 ώρες

Μεθοδολογία

- Ενεργό και συμμετοχικό
- Εκπαίδευση πρόσωπο με πρόσωπο:
 - ✓ Διάλογος
 - ✓ Παιχνίδι ρόλων
 - ✓ Ομαδική εργασία
- Διαδικτυακή εκπαίδευση:
 - ✓ Επιλεγμένα ή δικής τους παραγωγής βίντεο
 - ✓ Πρακτική εφαρμογή ορισμένων συμβουλών που συμφωνήθηκαν στην τάξη
 - ✓ Κάποια συνεργατική εργασία
 - ✓ Προσομοίωση

Υποενότητα 2

Διαδικτυακή ασφάλεια και προσωπικά δεδομένα

Στόχοι

Με την ολοκλήρωση αυτής της υποενότητας θα γνωρίζετε:

- ✓ Τι είναι η διαδικτυακή ασφάλεια
- ✓ Τι είναι τα προσωπικά δεδομένα και παραδείγματα αυτών



Διαδικτυακή ασφάλεια

Η παρουσία στο διαδίκτυο εκθέτει τους χρήστες του Διαδικτύου **σε διαδικτυακές απειλές ασφαλείας**. Από τη στιγμή που ένας χρήστης στέλνει δεδομένα μέσω του Διαδικτύου (πακέτα κλήσεων βίντεο ή φωνής, συνομιλίες, ηλεκτρονικό ταχυδρομείο ή αριθμούς πιστωτικών καρτών, ιστότοπους) **δεν έχει κανέναν έλεγχο για το ποιος μπορεί να έχει πρόσβαση στα δεδομένα**. Τα δεδομένα περνούν μέσα από πολλούς διακομιστές, δρομολογητές και συσκευές όπου οποιοσδήποτε χάκερ, πάροχος υπηρεσιών ή κυβερνητικός πράκτορας μπορεί να έχει πρόσβαση και να τα διαβάσει.

Συνεπώς, είναι εξαιρετικά σημαντικό οι χρήστες του Διαδικτύου να λαμβάνουν μέτρα για:

- Προστασία **των ευαίσθητων προσωπικών** τους **δεδομένων**,
- Χρησιμοποιούν διαδικτυακά εργαλεία και υπηρεσίες, όπως η κρυπτογράφηση δεδομένων, που **διασφαλίζουν το απόρρητο και την ασφάλεια** των πληροφοριών των πελατών τους όταν επικοινωνούν μαζί τους στο διαδίκτυο.



Τι είναι τα προσωπικά δεδομένα;

Δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αφορά ένα **ζωντανό, ταυτοποιημένο ή αναγνωρίσιμο άτομο**.

Διάφορες πληροφορίες που μαζί μπορούν να χρησιμοποιηθούν για **την ταυτοποίηση ενός συγκεκριμένου ατόμου** είναι επίσης προσωπικά δεδομένα.



Παραδείγματα προσωπικών δεδομένων

Παραδείγματα προσωπικών δεδομένων είναι τα εξής:

- Όνομα και επώνυμο,
- Διεύθυνση κατοικίας,
- Διεύθυνση ηλεκτρονικού ταχυδρομείου όπως
name.surname@company.com,
- Δεδομένα τοποθεσίας, όπως η λειτουργία δεδομένων τοποθεσίας ενός κινητού τηλεφώνου),
- Αριθμός δελτίου ταυτότητας,
- Διεύθυνση πρωτοκόλλου Internet (IP),
- Ένα αναγνωριστικό cookie,
- Το αναγνωριστικό διαφήμισης του τηλεφώνου σας,
- Δεδομένα που τηρούνται από ένα νοσοκομείο ή έναν γιατρό, τα οποία μπορεί να είναι ένα σύμβολο που ταυτοποιεί μοναδικά ένα άτομο.



Υποενότητα 3

Ευαίσθητα δεδομένα, ιδιωτικότητα και ασφάλεια

Στόχοι

Με την ολοκλήρωση αυτής της υποενότητας θα γνωρίζετε:

- ✓ Ποια προσωπικά δεδομένα θεωρούνται ευαίσθητα
- ✓ Τι είναι τα ευαίσθητα προσωπικά και οικονομικά δεδομένα
- ✓ Τις έννοιες της ιδιωτικότητας και της ασφάλειας
- ✓ Τι είναι το διαδικτυακό απόρρητο και πώς να είστε ασφαλείς στο διαδίκτυο



Ποια δεδομένα προσωπικού χαρακτήρα θεωρούνται ευαίσθητα;

Ευαίσθητα προσωπικά δεδομένα

Τα ακόλουθα δεδομένα προσωπικού χαρακτήρα θεωρούνται "ευαίσθητα" και υπόκεινται σε ειδικούς όρους επεξεργασίας:

- Προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- Φωτογραφίες, βίντεο
- Συμμετοχή σε συνδικαλιστικές οργανώσεις
- Γενετικά δεδομένα, βιομετρικά δεδομένα που υποβάλλονται σε επεξεργασία αποκλειστικά με σκοπό την ταυτοποίηση ενός ανθρώπου
- Δεδομένα σχετικά με την υγεία
- Δεδομένα που αφορούν τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό ενός προσώπου.



Ευαίσθητα οικονομικά δεδομένα

- Λογαριασμός και κωδικός πρόσβασης για ένα σύστημα e-banking
- CCV, ημερομηνία λήξης της πιστωτικής ή χρεωστικής κάρτας
- Ο κωδικός PIN του κινητού σας τηλεφώνου

→ Παραδείγματα και άσκηση



Εικόνα από redgreystock στο Freepik



Τι είναι το απόρρητο;

Το απόρρητο αφορά:

- Πώς **ελέγχουμε** τα προσωπικά μας δεδομένα, και
- πώς **χρησιμοποιούνται** από τα τρίτα μέρη που τα έχουν λάβει, με ασφαλή τρόπο.

Σκεφτείτε τις **πολιτικές απορρήτου** που σας ζητείται να διαβάσετε και να συμφωνήσετε όταν επισκέπτεστε έναν ιστότοπο ή κατεβάζετε μια νέα εφαρμογή για smartphone.



Τι είναι Ασφάλεια;

Η ασφάλεια αφορά **τον τρόπο με τον οποίο εξασφαλίζετε, προστατεύετε τα προσωπικά σας δεδομένα από μη εξουσιοδοτημένη πρόσβαση**, είτε στη συσκευή σας, είτε στον απομακρυσμένο διακομιστή ιστού, είτε κατά τη διάρκεια της επικοινωνίας μέσω του Διαδικτύου.

Χρησιμοποιούμε **ελέγχους ασφαλείας** σε τεχνικό επίπεδο για να περιορίσουμε το ποιος μπορεί να έχει πρόσβαση στις πληροφορίες. Αυτοί οι έλεγχοι εφαρμόζονται:

- Στις συσκευές μας (PC, tablet, κινητό τηλέφωνο), δηλαδή, εφαρμόζοντας ενημερώσεις λειτουργικού συστήματος και λογισμικού, χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης,
- Στον απομακρυσμένο διακομιστή ιστού, δηλαδή, χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης,
- Κατά την υποβολή πληροφοριών μέσω του Διαδικτύου, δηλαδή, χρησιμοποιήστε το ασφαλές πρωτόκολλο **https**.



Ασφάλεια και προστασία προσωπικών δεδομένων

- Η ασφάλεια αφορά την **προστασία των δεδομένων**, ενώ η ιδιωτικότητα αφορά την **προστασία της ταυτότητας των χρηστών**.

Για παράδειγμα, το προσωπικό των νοσοκομείων και των κλινικών χρησιμοποιεί ασφαλή συστήματα για να επικοινωνεί με τους ασθενείς σχετικά με την υγεία τους, αντί να στέλνει πληροφορίες μέσω προσωπικών λογαριασμών ηλεκτρονικού ταχυδρομείου. Αυτός ο τύπος επικοινωνίας αποτελεί παράδειγμα ασφάλειας.

- Από την άλλη πλευρά, η πολιτική και η διάταξη περί προστασίας των προσωπικών δεδομένων μπορεί να περιορίζουν την πρόσβαση στα αρχεία υγείας των ασθενών σε **ορισμένα μέλη του προσωπικού του νοσοκομείου**, όπως γιατρούς, νοσηλευτές και ιατρικούς βοηθούς.

- **Είναι δυνατόν να υπάρχει ασφάλεια χωρίς ιδιωτικότητα.**

Πράγματι, για παράδειγμα, τα προσωπικά δεδομένα μπορούν να μεταδίδονται με ασφάλεια και να αποθηκεύονται με ασφάλεια σε έναν ιστότοπο, αλλά ο ιστότοπος εξακολουθεί να τα πωλεί.

- **Δεν είναι δυνατόν να υπάρχει ιδιωτικότητα χωρίς ασφάλεια.**

Πράγματι, για παράδειγμα, ένας χάκερ θα μπορούσε να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στη συσκευή σας, στον διακομιστή ιστού ή στα δεδομένα που μεταδίδονται και να κλέψει τα προσωπικά σας δεδομένα.



Υποενότητα 3

Spam και phishing

Στόχοι

Με την ολοκλήρωση αυτής της υποενότητας θα γνωρίζετε:

- ✓ Τι είναι το spam και το phishing
- ✓ Πώς να αναγνωρίζετε το spam
- ✓ Πότε ένας σύνδεσμος είναι ασφαλής για επίσκεψη



Τι είναι το spam και το phishing

Μπορεί να έχετε λάβει ενοχλητικά μηνύματα ηλεκτρονικού ταχυδρομείου από **άγνωστο αποστολέα**, συνήθως εμπορικής φύσης.

Επιπλέον, τα **μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να είναι επικίνδυνα, επειδή** μπορεί να περιέχουν συνδέσμους που οδηγούν σε ιστότοπους phishing ή σε ιστότοπους που φιλοξενούν κακόβουλο λογισμικό ή περιέχουν κακόβουλο λογισμικό ως συνημμένο.

Επομένως, **μην ανοίγετε συνημμένα αρχεία και μην κάνετε κλικ σε συνδέσμους**. Και ποτέ μην δίνετε τα προσωπικά σας δεδομένα, τα στοιχεία του λογαριασμού σας e-banking (όνομα χρήστη, κωδικό πρόσβασης) ή τα στοιχεία της πιστωτικής/χρεωστικής σας κάρτας, όπως η ημερομηνία λήξης και το τριψήφιο CCV.

Αυτό ονομάζεται **phishing**: οι εγκληματίες στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου που μοιάζουν επίσημα για να σας εξαπατήσουν ώστε να αποκαλύψετε στοιχεία που μπορούν να χρησιμοποιηθούν για κλοπή ταυτότητας.



Πώς μπορώ να αναγνωρίσω το spam;

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου είναι ύποπτο εάν περιέχει ένα ή περισσότερα από τα ακόλουθα

- Λάθη γραμματικής και ορθογραφίας
- Μηνύματα σε ξένη γλώσσα
- Το όνομα του αποστολέα λείπει
- Επείγουσα ανάγκη για δράση - ιδίως σε συνδυασμό με απειλή



- Προτροπή για εισαγωγή προσωπικών δεδομένων (π.χ. PIN ή TAN)
- Αίτηση για να ανοίξετε ένα αρχείο
- Δεν έλαβα ποτέ κανένα email από την τράπεζα ή από πελάτη



Τι να κάνετε ή να μην κάνετε;

- ✓ Αποφεύγετε να ανοίγετε συνημμένα αρχεία, εκτός εάν έχουν σαρωθεί από πρόγραμμα προστασίας από ιούς.
- ✓ Θυμηθείτε να αποσυνδεθείτε, ειδικά αν χρησιμοποιείτε κοινόχρηστο δημόσιο υπολογιστή.
- ✓ Διαγράψτε όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστα άτομα.
- ✓ Ποτέ μην απαντάτε σε spam!
- ✓ Μην κάνετε κλικ σε συνδέσμους σε μηνύματα spam.





Δραστηριότητα: Είναι ασφαλής η επίσκεψη του συνδέσμου;

Αποφασίστε, αν ο σύνδεσμος είναι ασφαλής για να τον επισκεφθείτε:

Ας υποθέσουμε ότι λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια τράπεζα που σας ζητά να κάνετε κλικ σε έναν σύνδεσμο όπως ο παρακάτω και να υποβάλετε προσωπικά δεδομένα, όπως όνομα χρήστη, κωδικούς πρόσβασης και στοιχεία πιστωτικής κάρτας.

<http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRIk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpny-asDvdv>

1. Μη βιάζεστε, σκεφτείτε το καλά και αποφασίστε αν ο σύνδεσμος αυτοί να τον επισκεφθείτε.
2. Σκεφτείτε τους λόγους.





Δραστηριότητα: Είναι ασφαλής η επίσκεψη του συνδέσμου; (2)

Η απάντηση. Αυτός ο σύνδεσμος δεν είναι ασφαλής για διάφορους λόγους:

- Χρησιμοποιεί http αντί για https.
- Το όνομα τομέα δεν σχετίζεται με το επίσημο όνομα της τράπεζας.
- Ο σύνδεσμος είναι ύποπτα μακρύς.
- Το όνομα τομέα του συνδέσμου είναι διαφορετικό από το όνομα τομέα της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα.
- Μια πραγματική τράπεζα δεν θα ζητήσει ποτέ ονόματα χρηστών, κωδικούς πρόσβασης ή στοιχεία πιστωτικών καρτών.



Υποενότητα 4

Ποια είναι τα διαδικτυακά σας δικαιώματα

Στόχοι

Με την ολοκλήρωση αυτής της υποενότητας θα γνωρίζετε:

- ✓ Ποια είναι τα ψηφιακά σας δικαιώματα και υποχρεώσεις
- ✓ Τι είναι ο GDPR και γιατί τον χρειαζόμαστε



Είμαστε ψηφιακοί πολίτες

Οι ψηφιακοί πολίτες μπορούν να απολαμβάνουν δικαιώματα προστασίας της ιδιωτικής ζωής, ασφάλειας, πρόσβασης και ένταξης, ελευθερία της έκφρασης και πολλά άλλα.

Ωστόσο, μαζί με αυτά τα δικαιώματα έρχονται και ορισμένες ευθύνες, όπως η ηθική και η ενσυναίσθηση και άλλες ευθύνες για την εξασφάλιση ενός ασφαλούς και υπεύθυνου ψηφιακού περιβάλλοντος για όλους.



*Όλοι είμαστε πλέον
συνδεδεμένοι μέσω του
Διαδικτύου, σαν νευρώνες σε
έναν τεράστιο εγκέφαλο.*



Τι είναι ο ΓΚΠΔ και ποιος πρέπει να συμμορφωθεί με αυτόν;

Τι είναι ο ΓΚΠΔ;

- Ο **Γενικός Κανονισμός για την Προστασία Δεδομένων** είναι ένας νόμος της Ευρωπαϊκής Ένωσης που τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 και απαιτεί από τους οργανισμούς να διασφαλίζουν τα προσωπικά δεδομένα και να προασπίζουν τα δικαιώματα προστασίας της ιδιωτικής ζωής οποιουδήποτε βρίσκεται στην επικράτεια της ΕΕ.

Ποιος πρέπει να συμμορφωθεί με τον ΓΚΠΔ;

- Κάθε οργανισμός που επεξεργάζεται προσωπικά δεδομένα ατόμων στην ΕΕ πρέπει να συμμορφώνεται με τον ΓΚΠΔ.
- Η "**επεξεργασία**" είναι ένας ευρύς όρος που καλύπτει σχεδόν οτιδήποτε μπορείτε να κάνετε με δεδομένα: συλλογή, αποθήκευση, διαβίβαση, ανάλυση κ.λπ.
- "**Προσωπικά δεδομένα**" είναι κάθε πληροφορία που αφορά ένα άτομο, όπως ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις IP, χρώμα ματιών, πολιτικές πεποιθήσεις κ.λπ.



Ποιος πρέπει να συμμορφωθεί με αυτό;

Ακόμη και αν ένας οργανισμός δεν έχει καμία σχέση με την ΕΕ αλλά επεξεργάζεται προσωπικά δεδομένα ατόμων στην ΕΕ (για παράδειγμα, μέσω της παρακολούθησης στον ιστότοπό του), πρέπει να συμμορφώνεται με τον ΓΚΠΔ.

Ο ΓΚΠΔ δεν περιορίζεται στις κερδοσκοπικές εταιρείες.



Είναι ο ΓΚΠΔ κάτι θετικό;

- Ο ΓΚΠΔ υπάρχει για να προστατεύει τα δικαιώματά σας ως χρήστης.
- Είναι καλό να γνωρίζετε σε τι συναινείτε και τι σημαίνουν τα cookies.
- Η σωστή διαχείριση των ευάλωτων πελατών δεν είναι μόνο κάτι που αναμένει ο νόμος, αλλά και το σωστό κοινωνικά και μια έξυπνη επιχειρηματική κίνηση.



Υποενότητα 5

Πώς μπορείτε να προστατευτείτε εκ των προτέρων

Στόχοι

Με την ολοκλήρωση αυτής της υποενότητας θα γνωρίζετε:

- ✓ Πώς μπορείτε να προστατεύσετε τον εαυτό σας
εντοπίζοντας ασφαλείς ιστότοπους, συνδέσμους, cookies,
συναινέσεις



Μερικά παραδείγματα για να είστε ασφαλείς (1/3)

- Αποφύγετε να πληρώνετε οποιονδήποτε μέσω εμβάσματος, Western Union, εντολής πληρωμής ή δωροκάρτας. Οι απατεώνες συχνά ζητούν αυτούς τους τύπους πληρωμών, καθώς δεν αφήνουν ανιχνεύσιμα ίχνη χαρτιού.
- Ποτέ μην μοιράζεστε τους κωδικούς πρόσβασής σας με κανέναν στο διαδίκτυο. Μόνο με ένα έμπιστο πρόσωπο, όπως ένα καθημερινό μέλος.
- Να είστε επιφυλακτικοί σε οτιδήποτε επείγον. Οι απατεώνες συχνά θέλουν να δράσετε πριν προλάβετε να σκεφτείτε κριτικά την κατάσταση. Θυμηθείτε να κάνετε μια παύση και ίσως να απομακρυνθείτε από τον υπολογιστή αντί να πανικοβληθείτε, αν νομίζετε ότι κάτι είναι ύποπτο και δεν είστε σίγουροι πώς να προχωρήσετε.
- Κάντε αμέσως κλικ στο Χ ή στο Όχι για να κλείσετε τυχόν ιστότοπους ή αναδυόμενα παράθυρα σχετικά με ιούς ή κληρώσεις.



Μερικά παραδείγματα για να είστε ασφαλείς (2/3)

- Καλέστε ένα αγαπημένο σας πρόσωπο ή αναζητήστε συμβουλές στο διαδίκτυο (π.χ. πληκτρολογώντας "Χρειάζομαστε επείγοντως υποστήριξη..")
- Ελέγξτε στο Google για να δείτε αν άλλοι άνθρωποι έχουν αναφέρει τέτοιες απάτες.
- Βεβαιωθείτε ότι οι ιστότοποι έχουν μπροστά τους τη διεύθυνση <https://>. Το "s" υποδηλώνει ότι ο ιστότοπος είναι ασφαλής. Το όνομα θα πρέπει επίσης να έχει μια μικρή κλειδαριά δίπλα του.
- Να είστε επιφυλακτικοί με οτιδήποτε φαίνεται πολύ καλό για να είναι αληθινό.
- Εξετάστε το ενδεχόμενο να ενεργοποιήσετε τον έλεγχο ταυτότητας πολλαπλών παραγόντων. Αυτό απαιτεί είτε την εισαγωγή ενός κωδικού (που αποστέλλεται μέσω γραπτού μηνύματος ή ηλεκτρονικού ταχυδρομείου) είτε τη χρήση μιας εφαρμογής για να συνδεθείτε σε ορισμένους από τους λογαριασμούς σας, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης ή των τραπεζικών πυλών. Αυτό μπορεί να αποτρέψει τους χάκερ από το να συνδεθούν.



Μερικά παραδείγματα για να είστε ασφαλείς (3/3)

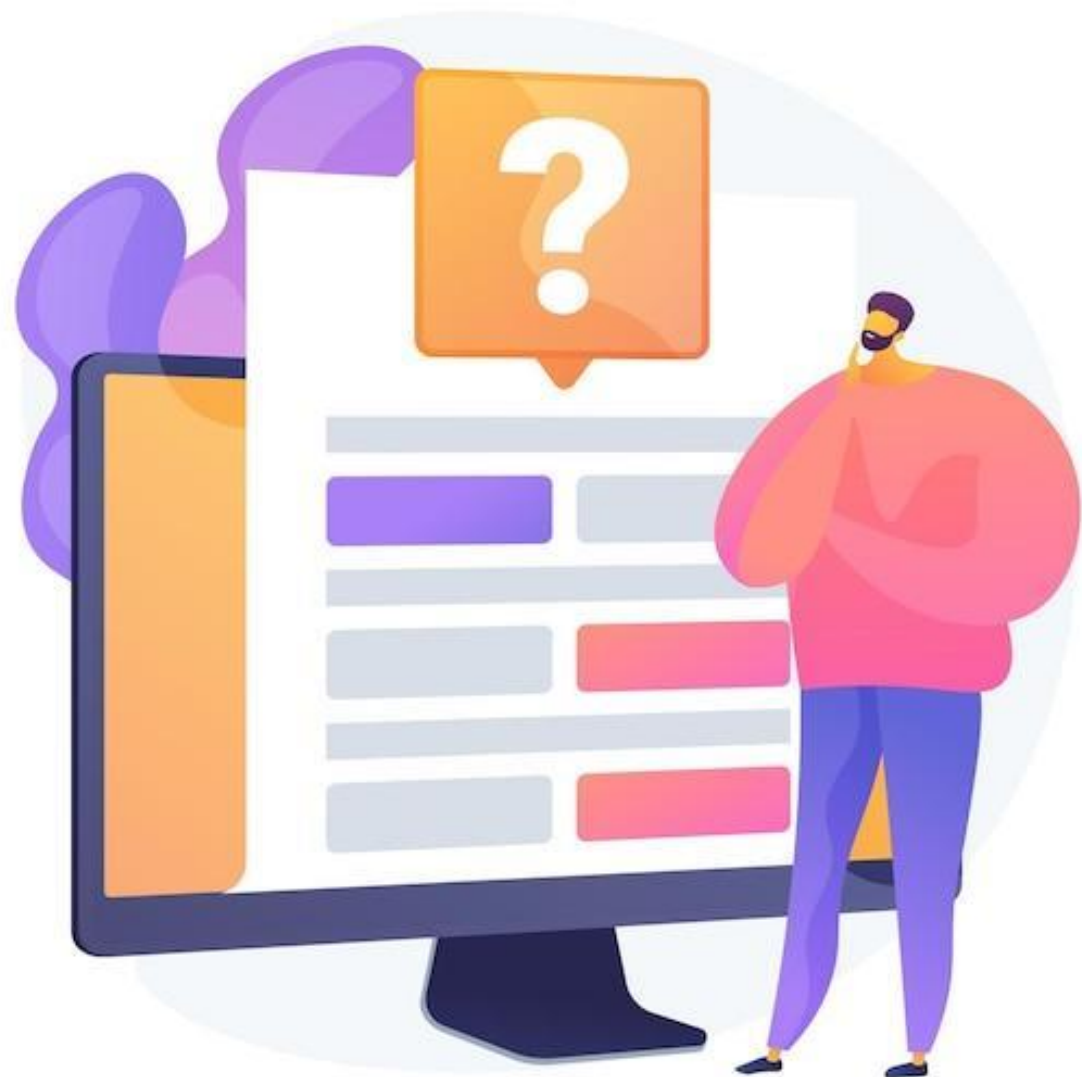
- Μπορείτε να λάβετε περισσότερες προφυλάξεις για να αποφύγετε τις απάτες.
- Κανείς δεν χρειάζεται να φοβάται να συνεχίσει να χρησιμοποιεί το διαδίκτυο, αρκεί να είναι εφοδιασμένος με τις γνώσεις για το πώς να το χρησιμοποιεί με ασφάλεια.
- Βρείτε έναν ασφαλή χώρο στην κοινότητά σας ή στον κοινωνικό σας κύκλο όπου μπορείτε να νιώσετε άνετα να συζητήσετε αυτά τα θέματα χωρίς να φοβάστε ότι θα σας κρίνουν.

Εάν έχει ήδη διαπραχθεί απάτη, μπορείτε να λάβετε ορισμένα μέτρα που μπορούν να αναληφθούν:

- Καλέστε την τράπεζά σας. Μπορούν να παγώσουν το λογαριασμό σας ώστε να μην μπορεί κανείς να έχει πρόσβαση στα χρήματά σας και να σας εκδώσουν νέα χρεωστική κάρτα. Αν έχουν ήδη κλαπεί χρήματα, μπορείτε να δείτε αν η τράπεζα μπορεί να ακυρώσει τις συναλλαγές αυτές και να σας επιστρέψει τα χρήματά σας.
- Εξετάστε το ενδεχόμενο να καταθέσετε αναφορά στην αστυνομία.



Ελέγξτε τις γνώσεις
σας!



1. Ποιος από τους ακόλουθους κωδικούς πρόσβασης είναι ισχυρότερος;

Μόνο μία απάντηση είναι σωστή!

A. John1234

B. John1990

Γ. John051190

Δ. J0Hn!2nO



2. Ποια από τα ακόλουθα είναι προσωπικά δεδομένα

Μόνο μία απάντηση είναι σωστή!

A. Διεύθυνση IP

B. Διεύθυνση ηλεκτρονικού ταχυδρομείου

Γ. Όλοι τους

Δ. Cookies IDs στο πρόγραμμα περιήγησης



3. Όταν το σύμβολο κλειδαριάς εμφανίζεται στο πρόγραμμα περιήγησης σημαίνει ότι το πρόγραμμα περιήγησης έχει κλειδώσει τη σελίδα επειδή δεν είναι ασφαλής.

Ναι, η δήλωση είναι σωστή.

Όχι, η δήλωση είναι λανθασμένη.



4. Ποιο από τα ακόλουθα ΔΕΝ είναι ευαίσθητα προσωπικά δεδομένα

Μόνο μία απάντηση είναι σωστή!

A. Φωτογραφίες

B. Διεύθυνση κατοικίας

Γ. Δεδομένα σχετικά με την υγεία

Δ. Πολιτικές απόψεις



5. Μπορεί ο αποστολέας να αποτελεί ένδειξη για το αν ένα email είναι spam;

Ναι

Όχι



6. Τι δεν πρέπει ποτέ να κάνετε αν λάβετε ένα υποτιθέμενο spam-mail;

Μόνο μία απάντηση είναι σωστή!

A. Διαγράψτε το e-mail

B. Ελέγξτε τον αποστολέα

Γ. Ελέγξτε τη γραμμή αναφοράς

Δ. Απαντήστε και ρωτήστε αν πρόκειται για spam-mail





IMOBILE
MONEY

Συγχαρητήρια!
Ολοκληρώσατε αυτό το θέμα!



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.
Αριθμός έργου: 2023-1-RO01-KA220-ADU-000157797