English	Greek
Data Access	**Πρόσβαση δεδομένων**
When you store information electronically you are leaving information on resources that are easily accessible. Restricting access to non-authorised persons is vital when it comes to your data. It does not really matter what data you store, what is important is that access to the information is only granted to you (or whoever is supposed to have access). The authentication mechanism works based on 3 (most usually) elements - A user identification or piece of information that will identify the user as part of the system to access. This is usually referred to as the login or user id. It is also common to have the email of the user substitute a login due to the uniqueness of this information. - A user secret value or key (commonly referred to as password) that is used to authenticate the person attempting access. - An algorithm that somehow combines the user id with the password and produces a unique piece of information (that no other combination can produce). This information is stored in the protecting entity database and is used to verify the identity of the person attempting access. Here is how it works. When the original user created the account they selected (or were assigned) a user name and a password. The algorithm generated the unique value and it was stored. Later, for the user to gain access, they need to enter their user id and password. The protecting entity reads in the information and, using the algorithm, generates a unique value. The generated unique value is then compared with the unique value stored in the database. If the two values match, the user is authenticated and access is granted. If the two values do not match then access is denied.	Όταν αποθηκεύετε πληροφορίες ηλεκτρονικά αφήνετε πληροφορίες σε πόρους που είναι εύκολα προσβάσιμοι. Ο περιορισμός της πρόσβασης σε μη εξουσιοδοτημένα άτομα είναι ζωτικής σημασίας όσον αφορά τα δεδομένα σας. Δεν έχει σημασία τι δεδομένα αποθηκεύετε, αυτό που είναι σημαντικό είναι ότι η πρόσβαση στις πληροφορίες παρέχεται μόνο σε εσάς (ή σε όποιον υποτίθεται ότι έχει πρόσβαση). Ο μηχανισμός ελέγχου ταυτότητας λειτουργεί με βάση 3 (συνήθως) στοιχεία - Ταυτοποίηση χρήστη ή μία πληροφορία που θα προσδιορίζει τον χρήστη ως μέρος του συστήματος για πρόσβαση. Αυτό συνήθως αναφέρεται ως το όνομα χρήστη. Είναι επίσης συνηθισμένο να χρησιμοποιείται η διεύθυνση email του χρήστη λόγω της μοναδικότητας αυτής της πληροφορίας. - Μυστική τιμή ή κλειδί χρήστη (συνήθως αναφέρεται ως κωδικός πρόσβασης) που χρησιμοποιείται για τον έλεγχο ταυτότητας του ατόμου που επιχειρεί πρόσβαση. - Ένας αλγόριθμος που συνδυάζει κάπως το login με το password και παράγει μια μοναδική πληροφορία (που δεν μπορεί να παράγει άλλος συνδυασμός). Αυτή αποθηκεύεται στη βάση δεδομένων της προστατευτικής οντότητας και χρησιμοποιείται για την επαλήθευση της ταυτότητας του ατόμου που επιχειρεί πρόσβαση. Να πώς λειτουργεί. Όταν ο αρχικός χρήστης δημιούργησε το λογαριασμό, επέλεξε (ή του εκχωρήθηκε) ένα όνομα χρήστη και επέλεξε έναν κωδικό πρόσβασης. Ο αλγόριθμος παρήγαγε τη μοναδική τιμή και αυτή αποθηκεύτηκε. Αργότερα, για να αποκτήσει πρόσβαση ο χρήστης, εισάγει το αναγνωριστικό χρήστη και τον κωδικό πρόσβασης. Η προστατευτική οντότητα διαβάζει τις πληροφορίες και χρησιμοποιώντας τον αλγόριθμο δημιουργεί μια μοναδική τιμή. Στη συνέχεια, η δημιουργούμενη μοναδική τιμή συγκρίνεται με τη μοναδική τιμή που είναι ήδη αποθηκευμένη στη βάση δεδομένων. Εάν οι δύο τιμές ταιριάζουν, ο χρήστης πιστοποιείται και χορηγείται πρόσβαση. Εάν οι δύο τιμές δεν ταιριάζουν, τότε δεν επιτρέπεται η πρόσβαση.
The importance of the password	**Η σημασία του κωδικού πρόσβασης**
In everyday usage of technology we have to authenticate ourselves in order to gain access to our	Στην καθημερινή χρήση της τεχνολογίας πρέπει να πιστοποιήσουμε τον εαυτό μας προκειμένου να

data. Unlocking your mobile phone (code, fingerprint, and face recognition); logging onto windows (code, fingerprint scan); accessing online banking (code, 2-way verification); we are entering password after password in order to open machines, start applications or access services and/or resources. Choosing, using and safely keeping your multiple passwords is very important.	αποκτήσουμε πρόσβαση στα δεδομένα μας. Ξεκλείδωμα του κινητού μας τηλεφώνου (κωδικός, δακτυλικό αποτύπωμα και αναγνώριση προσώπου). σύνδεση στο λειτουργικό windows (κωδικός, σάρωση δακτυλικών αποτυπωμάτων). πρόσβαση σε διαδικτυακές τραπεζικές συναλλαγές (κωδικός, αμφίδρομη επαλήθευση) · εισάγουμε διάφορους κωδικούς πρόσβασης για να ανοίξουμε μηχανήματα, να ξεκινήσουμε εφαρμογές ή να προσπελάσουμε υπηρεσίες ή / και πόρους. Η επιλογή, χρήση και ασφαλής διατήρηση των πολλαπλών κωδικών πρόσβασης είναι πολύ σημαντική.
<u>Choosing a password</u>	<u>Επιλογή κωδικού πρόσβασης</u>
Many systems can generate and supply a password (usually difficult to remember) or they will allow you to select your own but can request that the selected password must meet certain requirements. Usual restrictions include: - Length of the password. The longer the password the more difficult it is to guess. A usual restriction is a minimum of 8 characters - Including lower as well as uppercase letters. Passwords are **always** case sensitive so using lowercase and uppercase complicates the password more - Including at least one digit. Mixing letters and digits further complicates the password, thus making guessing more difficult - Including symbols (like !, _, @, #, %, &,), (, [etc.). Incorporating (one or more) symbols complicates the password more. Choosing a password is important. Combining letters (upper and/or lower case) and digits and symbols ensure a high complexity password. The more complicated the password is the more difficult it is for it to be guessed / discovered.	Πολλά συστήματα μπορούν να δημιουργήσουν και να παρέχουν έναν κωδικό πρόσβασης (συνήθως δύσκολο να τον θυμόμαστε) ή θα σας επιτρέψουν να επιλέξετε τον δικό σας, αλλά μπορούν να ζητήσουν ο επιλεγμένος κωδικός πρόσβασης να πληροί συγκεκριμένες απαιτήσεις. Οι συνήθεις περιορισμοί περιλαμβάνουν: - Μήκος του κωδικού πρόσβασης. Όσο μεγαλύτερος είναι ο κωδικός πρόσβασης τόσο πιο δύσκολο είναι για κάποιον να τον μαντέψει. Ένας συνηθισμένος περιορισμός είναι τουλάχιστον 8 χαρακτήρες - Συμπερίληψη μικρών και κεφαλαίων γραμμάτων. Στους κωδικούς πρόσβασης μικρά και κεφαλαία είναι διαφορετικά και έτσι η χρήση μικρών και κεφαλαίων περιπλέκει περισσότερο τον κωδικό πρόσβασης - Συμπερίληψη τουλάχιστον ενός ψηφίου. Ο συνδυασμός γραμμάτων και ψηφίων περιπλέκει τον κωδικό πρόσβασης περισσότερο, καθιστώντας έτσι δύσκολο να τον μαντέψει κάποιος - Συμπερίληψη συμβόλων (όπως: !, _, @, #, %, &,), (, [κλπ.). Με την ενσωμάτωση (ενός ή περισσοτέρων) συμβόλων περιπλέκεται ο κωδικός πρόσβασης περισσότερο. Η επιλογή ενός κωδικού πρόσβασης είναι σημαντική. Ο συνδυασμός γραμμάτων (κεφαλαίων και / ή μικρών) και ψηφίων και συμβόλων διασφαλίζει έναν κωδικό πρόσβασης υψηλής πολυπλοκότητας. Όσο πιο περίπλοκος είναι ο κωδικός πρόσβασης τόσο πιο δύσκολο είναι να εικαστεί / ανακαλυφθεί.
<u>Using passwords</u>	<u>Χρήση κωδικών πρόσβασης</u>
It is a fact that in modern society users are required to remember and use a considerable number of passwords. It is tempting to use and reuse the same password(s) for a number of applications and services. However,	Είναι γεγονός ότι στη σύγχρονη κοινωνία οι χρήστες πρέπει να θυμούνται και να χρησιμοποιούν σημαντικό αριθμό κωδικών πρόσβασης. Είναι δελεαστικό να χρησιμοποιείτε και να επαναχρησιμοποιείτε τους ίδιους κωδικούς

such a practice is not advisable. If your password is discovered then your accounts are in danger. Modern computer systems and browsers can store your passwords and use them when you visit specific pages. This is something that can be used but only if you are the only one using the computer. If you are using a shared computer in a lab or an office then you should not allow any application to store your passwords. One more approach is to write down your passwords either in a hard copy file (on paper) or in electronic format and save it in a location that you are aware. Both these approaches are **not advisable** since the information can be compromised.	πρόσβασης για ορισμένες εφαρμογές και υπηρεσίες. Ωστόσο, μια τέτοια πρακτική δεν συνιστάται. Εάν εντοπιστεί ο κωδικός πρόσβασής σας, τότε οι λογαριασμοί σας βρίσκονται σε κίνδυνο. Σύγχρονα συστήματα υπολογιστών και προγράμματα περιήγησης μπορούν να αποθηκεύουν τους κωδικούς πρόσβασης και να τους χρησιμοποιούν όταν επισκέπτεστε συγκεκριμένες σελίδες. Αυτό είναι κάτι που μπορεί να χρησιμοποιηθεί, αλλά μόνο εάν είστε ο μόνος που χρησιμοποιείτε τον υπολογιστή. Εάν χρησιμοποιείτε κοινόχρηστο υπολογιστή σε εργαστήριο ή γραφείο, τότε δεν πρέπει να επιτρέπετε σε καμία εφαρμογή να αποθηκεύει τους κωδικούς πρόσβασής σας. Μια ακόμη προσέγγιση είναι να γράψετε τους κωδικούς πρόσβασής σας είτε σε έντυπο αντίγραφο (σε χαρτί) είτε σε ηλεκτρονική μορφή και να τον αποθηκεύσετε σε μια τοποθεσία που γνωρίζετε. Και οι δύο αυτές προσεγγίσεις **δεν συνιστώνται** καθώς οι πληροφορίες μπορούν να τεθούν σε κίνδυνο.
<u>Safe keeping passwords</u>	<u>Ασφαλής τήρηση κωδικών πρόσβασης</u>
Due to the number of passwords that must be remembered, a common approach to use is to install some password management software application. Applications like these give you the ability to save as many passwords as you like in a database and look them up whenever you need them. Password management applications use what is called a 'master' password, which is needed in order to start up the application and access the database (and remaining passwords). One other, a little bit more manual approach, is to create a file to store your passwords and then either encrypt the file using some encryption application or add the file to a compress archive and use a password to protect the file.	Λόγω του αριθμού των κωδικών πρόσβασης που πρέπει να θυμάστε, μια κοινή προσέγγιση για χρήση είναι η εγκατάσταση κάποιας εφαρμογής λογισμικού διαχείρισης κωδικών πρόσβασης. Εφαρμογές όπως αυτές σας δίνουν τη δυνατότητα να αποθηκεύετε όσους κωδικούς πρόσβασης θέλετε σε μια βάση δεδομένων και να τους αναζητάτε όποτε τους χρειάζεστε. Οι εφαρμογές διαχείρισης κωδικού πρόσβασης χρησιμοποιούν αυτό που ονομάζεται «κυρίως» κωδικός πρόσβασης που απαιτείται για την εκκίνηση της εφαρμογής και την πρόσβαση στη βάση δεδομένων (και τους υπόλοιπους κωδικούς πρόσβασης). Μία άλλη, λίγο πιο χειροκίνητη προσέγγιση, είναι να δημιουργήσετε ένα αρχείο για να αποθηκεύσετε τους κωδικούς πρόσβασής σας και στη συνέχεια είτε να κρυπτογραφήσετε το αρχείο χρησιμοποιώντας κάποια εφαρμογή κρυπτογράφησης ή να προσθέσετε το αρχείο σε ένα αρχείο συμπίεσης και να χρησιμοποιήσετε έναν κωδικό πρόσβασης για την προστασία του αρχείου.