ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Από τους φοιτητές : Αρζουμάν Άγγελος, Κορώνη Ευάγγελος, Δημήτριος Λαμπίρης

1.ΕΙΣΑΓΩΓΗ

2.ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

3.ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΣΤΗΝ ΕΛΛΑΔΑ

4.ΠΟΥ ΥΠΑΡΧΟΥΝ ΟΙ ΚΙΝΔΥΝΟΙ

5.ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

6.ΠΡΟΒΛΗΜΑΤΑ ΣΤΟΥΣ ΝΕΟΥΣ

ΚΕΦΑΛΑΙΟ 1

[**Προσωπικά δεδομένα**](http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL) είναι κάθε πληροφορία που αναφέρεται στο πρόσωπο του κάθε ατόμου, όπως: το όνομα και το επάγγελμά του, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες

**Ευαίσθητα προσωπικά δεδομένα**

Από τα παραπάνω προσωπικά δεδομένα πολλά είναι [**ευαίσθητα**](http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL), έχουν δηλαδή ιδιαίτερη βαρύτητα για το σχηματισμό της εικόνας της προσωπικότητάς του ατόμου. Αυτά είναι η φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, η υγεία, η κοινωνική πρόνοια και η ερωτική ζωή καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.

### Υποκείμενο των δεδομένων

Ως [**Υποκείμενο των δεδομένων**](http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL) ορίζεται το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

### Επεξεργασία δεδομένων προσωπικού χαρακτήρα

**Επεξεργασία δεδομένων προσωπικού χαρακτήρα** λέγεται κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.

**Προσωπικά δεδομένα χρησιμοποιούνται εναντίον**

Είναι δυνατό τα προσωπικά μου δεδομένα να χρησιμοποιηθούν... εναντίον μου; Αν δεν προσέξεις πώς και πού τα δημοσιοποιείς ή αν πέσουν σε λάθος χέρια, τα προσωπικά σου δεδομένα μπορούν να χρησιμοποιηθούν από κάποιους για να σε δυσφημίσουν ή να σε φέρουν σε δύσκολη θέση, αποκαλύπτοντας ιδιωτικές σου στιγμές... Οι πληροφορίες αυτές είναι δυνατόν να δυσκολέψουν τη ζωή σου στο μέλλον, π.χ. όταν θα ψάχνεις για δουλειά ή θα θες να σπουδάσεις στο πανεπιστήμιο ή να πάρεις δάνειο από μία τράπεζα. Σε ακραίες περιπτώσεις μπορεί να πέσεις ακόμα και θύμα υποκλοπής ταυτότητας (δηλαδή κάποιος που έχει τα δεδομένα σου μπορεί να προσποιείται ότι είσαι εσύ) ή θύμα παρενόχλησης και εξαπάτησης.

ΚΕΦΑΛΑΙΟ 2

Κοινοτική Οδηγία 95/46/Ε.Ε

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών έχει διπλό στόχο: την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής του ατόμου και την εξασφάλιση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, για την επίτευξη οικονομικής και κοινωνικής προόδου και συνεργασίας, καθώς και τεχνικής και επιστημονικής συνεργασίας στην ολοένα αναπτυσσόμενη κοινωνία της πληροφορικής και των τηλεπικοινωνιών. Η Οδηγία 95/46/ΕΚ αποτελεί το κείμενο αναφοράς, σε ευρωπαϊκό επίπεδο, στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα. Θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση. Η εν λόγω Οδηγία ορίζει ως «δεδομένα προσωπικού χαρακτήρα» κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί το πρόσωπο στο οποίο αναφέρονται τα δεδομένα. Οι διατάξεις της παρούσας οδηγίας εφαρμόζονται στην αυτοματοποιημένη, εν όλο ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. πληροφοριακή βάση δεδομένων πελατών) καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο (παραδοσιακά αρχεία σε χαρτί). Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει δυνάμει της παρούσας οδηγίας σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον η επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Συνεπώς η Ελλάδα είναι υπεύθυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται οι οργανισμοί ηλεκτρονικού εμπορίου που είναι εγκατεστημένοι στα γεωγραφικά όρια της Ελλάδας. Στη συνέχεια ακολουθούν κάποιες γενικές προϋποθέσεις, που ορίζει η Οδηγία 95/46/ΕΚ, σχετικά με τη θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα:

Αρχές που Πρέπει να Τηρούνται ως Προς την Ποιότητα των Δεδομένων

Τα κράτη μέλη καθορίζουν τις προϋποθέσεις υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη. Προβλέπεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται σύννομη και θεμιτή επεξεργασία και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Θα πρέπει εξάλλου τα δεδομένα αυτά να είναι ακριβή και, αν χρειάζεται, να ενημερώνονται.

Βασικές Αρχές της Νόμιμης Επεξεργασίας Δεδομένων

Τα κράτη μέλη προβλέπουν ότι επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται μόνον εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή αν η επεξεργασία είναι απαραίτητη:1. Για την εκτέλεση σύμβασης της οποίας το υπόψη πρόσωπο αποτελεί συμβαλλόμενο μέρος. 2. Για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας. 3. Για τη διαφύλαξη ζωτικού συμφέροντος του υπόψη προσώπου.4. Για την εκτέλεση αποστολής δημόσιου συμφέροντος.  Για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.

Ειδικές Κατηγορίες Επεξεργασίας

Τα κράτη μέλη απαγορεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Η διάταξη αυτή συνοδεύεται από επιφυλάξεις που αφορούν π.χ. την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του υπόψη προσώπου ή για σκοπούς προληπτικής ιατρικής και ιατρικής διάγνωσης.

Εξαιρέσεις και Περιορισμοί

Τα κράτη μέλη μπορούν να περιορίζουν με νομοθετικά μέτρα την εμβέλεια των υποχρεώσεων και δικαιωμάτων που προβλέπονται στην παρούσα οδηγία όταν ο περιορισμός αυτός απαιτείται για τη διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημόσιας ασφάλειας και της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης παραβάσεων του ποινικού νόμου ή της δεοντολογίας των νομοθετικά κατοχυρωμένων επαγγελμάτων.

Κοινοτική Οδηγία 2002/58/Ε.Ε..

Η Οδηγία 2002/58/ΕΚ αναθεωρεί και αναπροσαρμόζει την προηγούμενη Οδηγία 97/96/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, προκειμένου να ληφθούν υπόψη οι νέες υπηρεσίες και τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ αποτελεί βασικό στοιχείο του κανονιστικού πλαισίου που επιδιώκει να εξασφαλίσει τη συνέχιση της ανάπτυξης του τομέα ηλεκτρονικών επικοινωνιών, με οφέλη για το σύνολο των εταιρειών και των ιδιωτών που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικών επικοινωνιών.. Η εν λόγω Οδηγία επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία 2002/58/ΕΚ εναρμονίζονται οι διατάξεις των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση. Η Οδηγία λοιπόν για την προστασία προσωπικών δεδομένων στηρίζεται στις εξής βασικές αρχές:

Η επεξεργασία προσωπικών δεδομένων πρέπει να είναι πάντοτε θεμιτή και νόμιμη. 1. Τα προσωπικά δεδομένα πρέπει πάντα να συλλέγοντας για ρητώς καθορισμένους και νόμιμους σκοπούς και να χρησιμοποιούνται ανάλογα. 2. Τα προσωπικά δεδομένα πρέπει να είναι κατάλληλα και να μην υπερβαίνουν τα απολύτως αναγκαία για τους σκοπούς της επεξεργασίας τους 3. Τα δεδομένα που αποκαλύπτουν την ταυτότητα των προσώπων δεν πρέπει να φυλάσσονται για περισσότερο χρόνο απ' όσο είναι απαραίτητο 4.Τα δεδομένα πρέπει να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται •5.Οι κάτοχοι δεδομένων οφείλουν να παρέχουν στα πρόσωπα που αφορούν τα δεδομένα αυτά εύλογα μέσα για τη διόρθωση, τη διαγραφή ή τη δέσμευση ανακριβών δεδομένων 6.Πρέπει να λαμβάνονται τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα για την αποτροπή της παράνομης ή χωρίς άδεια επεξεργασίας προσωπικών δεδομένων 7.Τα προσωπικά δεδομένα δεν πρέπει να μεταφέρονται σε χώρες ή επικράτειες εκτός του Ευρωπαϊκού Οικονομικού Χώρου, εκτός εάν αυτές εγγυώνται "επαρκές επίπεδο προστασίας" για τα πρόσωπα που αφορούν τα δεδομένα

Η οδηγία επιβάλλει επίσης στα κράτη μέλη την υποχρέωση να συστήσουν μία η περισσότερες ανεξάρτητες εποπτικές Αρχές για να παρακολουθούν την εφαρμογή της. Ένα από τα καθήκοντα αυτών των Αρχών είναι να τηρούν ενημερωμένο δημόσιο μητρώο, ώστε το κοινό να μπορεί να γνωρίζει τα ονόματα όλων των κατόχων προσωπικών δεδομένων και το είδος της επεξεργασίας στην οποία τα υποβάλλουν. Επίσης ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οφείλει να λαμβάνει από κοινού με τους φορείς παροχής δημόσιων δικτύων επικοινωνιών, καθόσον αφορά την ασφάλεια του δικτύου, τα ενδεδειγμένα τεχνικά και οργανωτικά μέσα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Οι εν λόγω φορείς υποχρεώνονται να ενημερώνουν τους συνδρομητές σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος για την ασφάλεια του δικτύου.

ΚΕΦΑΛΑΙΟ 3

Προστασία Προσωπικών Δεδομένων Στην Ελλάδα

Στην Ελλάδα έχει ιδρυθεί και λειτουργεί από το Νοέμβριο του 1997 ως ανεξάρτητη διοικητική υπηρεσία η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με βάση το Νόμο 2472/97. Αποστολή της Αρχής Προστασίας Δεδομένων είναι η εποπτεία της εφαρμογής των νόμων και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα που συλλέγουν οι οργανισμοί ηλεκτρονικού εμπορίου για τους πελάτες τους, στα πλαίσια πραγματοποίησης ηλεκτρονικών συναλλαγών, αποτελούν προσωπικά δεδομένα και συνεπώς προστατεύονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Συγκεκριμένα κάθε οργανισμός ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την εν λόγω Αρχή.

Η Αρχή αυτή έχει τις εξής αρμοδιότητες:1. Να εκδίδει οδηγίες και κανονιστικές πράξεις για την εφαρμογή των διατάξεων που αφορούν στην προστασία προσωπικών δεδομένων και να γνωμοδοτεί για σχετικά θέματα. 2. Να απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και να επιβάλλει/βοηθάει όσους διατηρούν αρχεία να καταρτίζουν κώδικες δεοντολογίας. 3. Να καταγγέλλει τις παραβάσεις στις αρμόδιες διοικητικές και δικαστικές αρχές αλλά και να επιβάλλει κυρώσεις.4. Να ενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, ελέγχους σε κάθε αρχείο.

Στη χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97), ενώ ο Νόμος 2774/1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα καταργήθηκε στις 29 Ιουλίου 2006. Ο Νόμος 2472/97 ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ και αναφέρεται στην "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Με λίγα λόγια καθορίζει τις υποχρεώσεις των φορέων και των υπηρεσιών που "εκτελούν την επεξεργασία" και θέτει τα δικαιώματα προστασίας των ατόμων, όσον αφορά την προστασία και διαφύλαξη των προσωπικών τους δεδομένων. Με βάση το νόμο 2472/97:1. Η επεξεργασία προσωπικών πληροφοριών είναι επιτρεπτή μόνο στις περιπτώσεις που ο νόμος προσδιορίζει περιοριστικά και δεσμευτικά.2. Η επεξεργασία επιτρέπεται μόνο για νόμιμους, θεμιτούς και εξειδικευμένους σκοπούς που είναι γνωστοί στον πολίτη. 3. Αναγνωρίζονται και κατοχυρώνονται νέα δικαιώματα των πολιτών για να αμύνονται έναντι των προσβολών της ιδιωτικής ζωής και της προσωπικότητας τους (δικαίωμα προηγούμενης πληροφόρησης, διόρθωσης, αποζημίωσης). Οι ρυθμίσεις του νόμου 2472/97 συμπληρώθηκαν από το Νόμο 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών). Ο νόμος αυτός κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών.

Κανονισμοί Α.Δ.Α.Ε..

Η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) είναι ένας νέος φορέας που λειτουργεί με βάσει το Ν. 3115/2003 με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών. Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαμβάνει διοικητικής αυτοτέλειας. Έδρα της ΑΔΑΕ είναι η Αθήνα, αλλά μπορεί με απόφαση της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της ΑΔΑΕ κοινοποιούνται στον Υπουργό Δικαιοσύνης και στο τέλος κάθε χρόνου υποβάλλεται έκθεση των πεπραγμένων της στη Βουλή. Η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον κανονισμό της Βουλής. Η ΑΔΑΕ για την εκπλήρωση της αποστολής της έχει τις ακόλουθες αρμοδιότητες:1. Διενέργεια αυτεπάγγελτων ελέγχων σε επιχειρήσεις και υπηρεσίες που έχουν γενικό αντικείμενο την επικοινωνία.  Κατάσχεση ψηφιακών πειστηρίων, καταστροφή στοιχείων που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών. 2. Εξέταση καταγγελιών σχετικά με την προστασία των δικαιωμάτων των αιτούντων.3. Συνεργασία με άλλες αρχές της χώρας και με αντίστοιχες αρχές άλλων κρατών, για θέματα ασφάλειας επικοινωνιών. 4. Έκδοση κανονισμού εσωτερικής λειτουργίας, ο οποίος δημοσιεύεται στην εφημερίδα της Κυβερνήσεως.5. Έκδοση κανονιστικών πράξεων, μέσω των οποίων ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις αρμοδιότητες της Αρχής. 6. Σύνταξη, μια φορά το χρόνο, έκθεσης πεπραγμένων, στην οποία περιγράφεται το έργο της Αρχής, διατυπώνονται παρατηρήσεις και προτείνονται νομοθετικές μεταβολές στον τομέα διασφάλισης του απορρήτου των επικοινωνιών. Το ηλεκτρονικό εμπόριο βασίζεται στην επικοινωνία των πελατών με τους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου. Για να γίνει μια ηλεκτρονική συναλλαγή, πρέπει πρώτα να επικοινωνήσει ο πελάτης με τον έμπορα, να δώσει τα προσωπικά του στοιχεία, τον αριθμό της πιστωτικής του κάρτας και να λάβει πληροφορίες σχετικές με τη συναλλαγή. Είναι προφανές ότι η επικοινωνία αυτή πρέπει να είναι απόρρητη, αφού σε καμιά περίπτωση τα προσωπικά στοιχεία του πελάτη και ιδιαίτερα οι αριθμοί των πιστωτικών του καρτών δεν πρέπει να γνωστοποιούνται σε τρίτους. Όπως αναφέρθηκε πιο πάνω, σκοπός της ΑΔΑΕ είναι η προστασία του απορρήτου των επικοινωνιών. Συνεπώς κάθε οργανισμός ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την ΑΔΑΕ. Η ΑΔΑΕ έχει εκδώσει κάποιους κανονισμούς για τη διασφάλιση του απορρήτου των επικοινωνιών και κάθε οργανισμός ηλεκτρονικού εμπορίου, σύμφωνα με τα παραπάνω, πρέπει να τους ακολουθεί. Η ΑΔΑΕ ελέγχει τους οργανισμούς ηλεκτρονικού εμπορίου για την τήρηση των κανόνων, και η ίδια ελέγχεται από το κράτος. Η ΑΔΑΕ έχει εκδώσει και δημοσιεύσει στην εφημερίδα της κυβερνήσεως κανονισμούς ασφαλείας για το διαδίκτυο, τη διασφάλιση απορρήτου τηλεπικοινωνιακής υποδομής, την κινητή και σταθερή τηλεφωνία, το θεσμικό πλαίσιο για την ασφάλεια, καθώς και την ασφάλεια για αυτόματες τραπεζικές συναλλαγές. Με δεδομένο ότι το μεγαλύτερο μέρος του ηλεκτρονικού εμπορίου πραγματοποιείται μέσω του διαδικτύου, κάθε οργανισμός ηλεκτρονικού εμπορίου πρέπει να συμμορφώνεται και να τηρεί τους κανονισμούς ασφαλείας για το διαδίκτυο. Συγκεκριμένα θα πρέπει να ακολουθεί τουλάχιστον τους κανονισμούς που περιγράφονται στη συνέχεια με λεπτομέρεια, οι οποίοι δημοσιεύθηκαν στις 26 Ιανουαρίου 2005 στην εφημερίδα της κυβερνήσεως.

ΚΕΦΑΛΑΙΟ 4

ΣΤΑ EMAIL

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική και ταχύτατη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο, όμως ακόμα και σήμερα τα περισσότερα προγράμματα αποστολής και λήψης e-mail δεν εγγυώνται σε καμία περίπτωση τη διασφάλιση του προσωπικού απορρήτου του χρήστη ούτε και την ακεραιότητα της λειτουργίας του συστήματός του. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών. Πιο συγκεκριμένα κύριος φορέας των μηνυμάτων e-mail είναι το πρωτόκολλο επικοινωνίας SMTP (Simple Mail Transfer Protocol). Το SMTP αναλαμβάνει τη μεταφορά μηνυμάτων από το μηχάνημα του χρήστη σε ένα διακομιστή αλληλογραφίας (mail server), καθώς και την προώθησή του από έναν mail server σε κάποιον άλλο. Κάθε εταιρεία παροχής ιντερνετικών υπηρεσιών (Internet Service Provider, ISP) διαθέτει έναν ή περισσότερους διακομιστές αλληλογραφίας, οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την αποστολή των μηνυμάτων. Όταν ένας χρήστης συνδέεται τηλεφωνικά (dialup) με τον ISP του, μπορεί να «κατεβάσει» την αλληλογραφία του από τον mail server του ISP στον υπολογιστή του, με τη βοήθεια του πρωτοκόλλου POP (Post Office Protocol) ή του IMAP (Internet Message Access Protocol). Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι ιδιαίτερα σημαντικό να διαχειριστεί τη διεύθυνση της ηλεκτρονικής του αλληλογραφίας με την ίδια προσοχή που διαχειρίζεται τον αριθμό του τηλεφώνου του.

Στις ηλεκτρονικές συναλλαγές

Σε μια ηλεκτρονική επικοινωνία η εμπιστοσύνη μεταξύ των συναλλασσόμενων μερών είναι πολύ σημαντική, για αυτό και θα πρέπει να δίδεται ιδιαίτερη έμφαση στο θερμά της ασφάλειας των συναλλαγών. Σήμερα, η τεχνολογία παρέχει πολύ προηγμένες λύσεις στο θέμα αυτό. Ένα ηλεκτρονικό κατάστημα που μεριμνά για την ασφάλεια των πελατών του θα πρέπει να χρησιμοποιεί και να αναφέρει ρητά όλα τα απαραίτητα συστήματα ασφάλειας καθώς και θα πρέπει να παρέχει τις απαραίτητες πληροφορίες για την πιστοποίηση της ταυτότητάς του.

Στις Ηλεκτρονικές Πληρωμές

Με τη συνεχώς αυξανόμενη εμπορευματοποίηση του Internet και τη χρήση του Web πολλές επιχειρήσεις έχουν οδηγηθεί στην υλοποίηση συστημάτων και μεθόδων ηλεκτρονικών πληρωμών προκειμένου να υποστηρίξουν πρακτικά την ανάπτυξη του ηλεκτρονικού εμπορίου στο σύγχρονο επιχειρησιακό περιβάλλον. Έτσι όχι μόνο δεν θεωρείται αρκετή η ανάπτυξη ηλεκτρονικών επιχειρήσεων χωρίς την ανάπτυξη και την εξέλιξη τέτοιων συστημάτων πληρωμών μέσα στο διαδίκτυο, αλλά είναι αδύνατο να υπάρξει ηλεκτρονικό εμπόριο χωρίς έναν τρόπο μεταφοράς χρηματικών πόρων (πληρωμής) μέσω της ψηφιακής υποδομής. Στα πρώτα στάδια ανάπτυξης του ηλεκτρονικού εμπορίου οι πληρωμές γίνονταν εκτός του διαδικτύου με καταβολή των ποσών σε κάποια τράπεζα. Ο αναχρονιστικός όμως αυτός τρόπος χρηματικής εκκαθάρισης των διαδικτυακών συναλλαγών δε συμβάδιζε με την ταχύτητα και την αξιοπιστία που απαιτούν οι σύγχρονες διαδικτυακές συναλλαγές. Για το λόγο αυτό μια σειρά από συστήματα ηλεκτρονικών πληρωμών αναπτύχθηκε σταδιακά. Τα συστήματα αυτά είτε αποτελούσαν μια μεταφορά παραδοσιακών πρακτικών του πραγματικού κόσμου στο διαδίκτυο όπως είναι η περίπτωση on-line πληρωμών με πιστωτική κάρτα, είτε οι δημιουργοί τους προχώρησαν σε καινοτομικές λύσεις που εκμεταλλεύονται τα χαρακτηριστικά του διαδικτύου προκειμένου να προτείνουν πρωτοποριακές λύσεις όπως οι πληρωμές με ηλεκτρονικό χρήμα. Οι ηλεκτρονικές πληρωμές αποτελούν αναπόσπαστο τμήμα του ηλεκτρονικού εμπορίου. Στη γενική του μορφή, ο όρος ηλεκτρονικές πληρωμές (electronic payments) περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες, ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις, οι οποίες εκτελούνται με τη μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας. Κάθε ηλεκτρονική πληρωμή γίνεται εξ αποστάσεως χωρίς τη φυσική παρουσία του πληρωτή και φυσικά δεν περιλαμβάνει μετρητά. Το περιεχόμενο αυτής της πληρωμής έχει τη μορφή κάποιου ψηφιακού οικονομικού μέσου (π.χ. κρυπτογραφημένους αριθμούς πιστωτικών καρτών, ηλεκτρονικές επιταγές, ή ψηφιακό χρήμα) το οποίο μέσο υποστηρίζεται από κάποιον χρηματοπιστωτικό οργανισμό, τράπεζα ή άλλον ενδιάμεσο φορέα.

μέσω τηλεφώνου: Οι πληρωμές μέσω του τηλεφωνικού δικτύου αποτελούν μια καινούργια μορφή ηλεκτρονικών πληρωμών. Στόχος είναι η εκμετάλλευση της υπάρχουσας τεχνικής υποδομής αλλά και της σημαντικής διείσδυσης που έχει το τηλέφωνο ως τεχνολογία σε όλα τα κοινωνικά στρώματα. Πολλές επιχειρήσεις, τράπεζες αλλά και δημόσιες υπηρεσίες επιτρέπουν την εξόφληση λογαριασμών μέσω τηλεφώνου. μέσω διαδικτύου: Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η εύκολη πρόσβαση στο διαδίκτυο από την πλειοψηφία του καταναλωτικού κοινού, καθιστά τα εν λόγω συστήματα ηλεκτρονικών πληρωμών ιδιαίτερα σημαντικά στην ανάπτυξη του ηλεκτρονικού εμπορίου.

μέσω κινητής τηλεφωνίας (m-payments): Η ανάπτυξη τεχνολογιών όπως το WAP επιτρέπουν την εκτέλεση βασικών χρηματικών συναλλαγών από κινητές και ασύρματες συσκευές ανεξαρτήτως χώρου και χρόνου. Πρόκειται για ένα μέσο πιο αυτόνομο ενώ η ευρεία αποδοχή και χρήση του από το καταναλωτικό κοινό καθιστά το κινητό ηλεκτρονικό εμπόριο (m-commerce) ιδιαίτερα δημοφιλή.

Πιστωτικές Κάρτες

Οι πιστωτικές κάρτες έχουν τύχει ευρείας χρήσης στο διαδίκτυο επειδή διαθέτουν σημαντικά πλεονεκτήματα έναντι των εναλλακτικών μεθόδων πληρωμής. Κατ’ αρχήν είναι διεθνώς γνωστές και αποδεκτές από τους εμπόρους, επιτρέποντας έτσι την πραγματοποίηση ακόμη και διεθνών συναλλαγών. Επιπλέον η χρήση τους στις ηλεκτρονικές συναλλαγές δεν διαφέρει και πολύ από την χρήση τους στις φυσικές συναλλαγές. Στις φυσικές συναλλαγές ο πελάτης δίνει την κάρτα του στον έμπορα για χρέωση χέρι με χέρι, ενώ στις ηλεκτρονικές συναλλαγές ο πελάτης δίνει στον έμπορα τις πληροφορίες της κάρτας του μέσω του διαδικτύου. Αυτό έχει σαν αποτέλεσμα την πραγματοποίηση συναλλαγών χωρίς σημαντικές επενδύσεις από την πλευρά των εμπόρων αλλά και χωρίς αλλαγή στη συμπεριφορά των καταναλωτών. Κατά την πληρωμή μέσω πιστωτικών καρτών στο διαδίκτυο ο πελάτης κοινοποιεί στον έμπορα τον αριθμό της πιστωτικής του κάρτας, καθώς και άλλες πληροφορίες της κάρτας όπως εκδότη, ημερομηνία λήξεως κλπ. Ο έμπορας ζητά έγκριση από την τράπεζα του η οποία σε συνεργασία με την τράπεζα του πελάτη (οργανισμό έκδοσης της κάρτας) δίνουν ή όχι έγκριση. Σε περίπτωση έγκρισης, ειδοποιείται ο έμπορος ότι η δαπάνη εγκρίθηκε και στέλνει τα προϊόντα στον πελάτη. Η τράπεζα του πελάτη προωθεί τα χρήματα στο λογαριασμό του έμπορα μέσω του διατραπεζικού συστήματος, και χρεώνει το ποσό στο λογαριασμό της πιστωτικής κάρτας του πελάτη. Σε τακτά χρονικά διαστήματα (συνήθως κάθε μήνα) η τράπεζα του πελάτη τον ειδοποιεί για τις συναλλαγές και τις δαπάνες του. Αυτός ο τρόπος πληρωμής παρέχει άμεση πρόσβαση στους τραπεζικούς λογαριασμούς του αγοραστή και του πωλητή και καταγράφει άμεσες μεταβολές στους λογαριασμούς τους. Με την εμφάνιση του ηλεκτρονικού εμπορίου έχουν γίνει μεγάλης κλίμακας απάτες, κυρίως με κλεμμένους αριθμούς πιστωτικών καρτών. Η έγκριση που απαιτείται στα συστήματα πληρωμών είναι μια μορφή προστασίας. Είναι σημαντικό οι αριθμοί των πιστωτικών καρτών (και γενικά οι πληροφορίες πληρωμής) να είναι δυσανάγνωστες σε όλους, εκτός από τον πελάτη και την τράπεζα του. Δεν υπάρχει λόγος ο έμπορας να γνωρίζει τον αριθμό της πιστωτικής κάρτας του πελάτη. Για το λόγο αυτό, τα δεδομένα πληρωμής στέλνονται κρυπτογραφημένα υπό μορφή μηνύματος μέσα στο διαδίκτυο καθώς υπάρχει πιθανότητα το μήνυμα να υποκλαπεί. Η χρήση της πιστωτικής κάρτας για αγορές σε ένα δικτυακό τόπο, αποτελεί έναν ασφαλή τρόπο πληρωμής. Για παράδειγμα, η easyJet έχει ήδη διεξάγει πολλά εκατομμύρια κρατήσεις θέσεων μέσω Διαδικτύου. Χρησιμοποιούν πολλά βήματα ασφάλειας, έτσι ώστε να μπορούν να εγγυηθούν την απόλυτη ασφάλεια των δεδομένων των πελατών τους κατά την αγορά πτήσεων της easyJet μέσω Διαδικτύου.

Ηλεκτρονικές Επιταγές

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών, που τώρα υπογράφονται και μεταβιβάζονται ηλεκτρονικά, και μπορούν να έχουν όλες τις παραλλαγές των κοινών επιταγών, όπως ταξιδιωτικές επιταγές ή πιστοποιημένες επιταγές. Μια επιταγή χρησιμοποιείται για να μεταφέρει ένα μήνυμα προς την τράπεζα του αποστολέα για τη μεταφορά ενός συγκεκριμένου χρηματικού ποσού από το λογαριασμό του αποστολέα στο λογαριασμό κάποιου άλλου. Σε αντιστοιχία με την παραδοσιακή διαδικασία η ηλεκτρονική επιταγή αποστέλλεται αρχικά στον αποδέκτη του χρηματικού ποσού, ο οποίος την υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό. Στη συνέχεια η εξοφλημένη και επικυρωμένη επιταγή επιστρέφεται στον αποστολέα ο οποίος τη χρησιμοποιεί ως απόδειξη πληρωμής. Μια ηλεκτρονική επιταγή έχει τα ίδια χαρακτηριστικά με μια έντυπη επιταγή. Είναι ένα ηλεκτρονικό έγγραφο που περιέχει τον αριθμό της επιταγής, το όνομα του πληρωτή, τον αριθμό λογαριασμού του πληρωτή και το όνομα της τράπεζας, το όνομα του δικαιούχου πληρωμής (αποδέκτη), το πληρωτέο ποσό, τη μονάδα χρήματος που χρησιμοποιείται, την ημερομηνία λήξης, την ηλεκτρονική υπογραφή του πληρωτή και την ηλεκτρονική επικύρωση του δικαιούχου πληρωμής. Οι ηλεκτρονικές επιταγές χρησιμοποιούν την τεχνολογία των ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές αναλύονται στο κεφάλαιο 8. Από πλευράς ασφάλειας η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη, αφού ο αποστολέας μπορεί να προστατέψει τον εαυτό του από μια απάτη. Κάτι τέτοιο επιτυγχάνεται με την κρυπτογράφηση του αριθμού λογαριασμού του με το δημόσιο κλειδί της τράπεζας του, με αποτέλεσμα να μην αποκαλύπτεται στον έμπορα ο αριθμός του λογαριασμού. Σε μια συναλλαγή πληρωμής με ηλεκτρονικές επιταγές ο πελάτης παραγγέλλει κάποια προϊόντα από τον έμπορα και για πληρωμή του στέλνει μια ηλεκτρονική επιταγή ψηφιακά υπογεγραμμένη. Ο έμπορας γνωρίζοντας το δημόσιο κλειδί του πληρωτή, μπορεί να επιβεβαιώσει την ορθότητα της ψηφιακής υπογραφής και έτσι να επικυρώσει τη συγκεκριμένη επιταγή. Μετά την παραλαβή και επικύρωση της επιταγής, ο έμπορας στέλνει τα προϊόντα στον πελάτη. Η τράπεζα του πελάτη αποσύρει το ποσό πώλησης από το λογαριασμό του πελάτη και μέσω του διατραπεζικού συστήματος το εν λόγω ποσό πιστώνεται στο λογαριασμό του έμπορα.

Στις Διαδικτυακές τραπεζικές συναλλαγές

Σύμφωνα με έρευνες, όλο και περισσότεροι ιδιώτες αλλά και επιχειρήσεις στην Ελλάδα προτιμούν να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω Διαδικτύου. Τα αποτελέσματα της Εθνικής Έρευνας για τις Νέες Τεχνολογίες και την Κοινωνία της Πληροφορίας δείχνουν ότι το 2001 περίπου 150.000 πελάτες (1%-1,5% του πληθυσμού) πραγματοποίησαν τραπεζικές συναλλαγές ηλεκτρονικά. Το 2002 ο αριθμός αυτός ξεπέρασε τους 250.000 (2,5% του συνολικού πληθυσμού). Σύμφωνα με εκτιμήσεις τραπεζών, το 2001 ο τζίρος από on-line τραπεζικές συναλλαγές έφθασε τα 2 δισ. ευρώ. Το 2002 το ποσό αυτό εκτιμάται ότι αυξήθηκε σε 10 δισ. ευρώ, ενώ για φέτος αναμένεται να υπερβεί τα 12 δισεκατομμύρια. Σύμφωνα με στοιχεία της Τράπεζας Πειραιώς, οι συναλλαγές μέσω Winbank Internet παρουσιάζουν ραγδαία ανάπτυξη: το 2003 οι εγχρήματες συναλλαγές αυξάνονται με ρυθμό της τάξεως του 150% έναντι του 2002. Επίσης, το 50% όλων των πληρωμών IKA πραγματοποιείται online, ενώ οι ηλεκτρονικές χρηματιστηριακές συναλλαγές υπερβαίνουν το 15% επί του συνόλου. Η εξάπλωση του e-banking είναι ραγδαία σε όλο τον κόσμο. Ειδικοί εκτιμούν ότι στο μέλλον οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών. Ενδεικτικά, στη Γερμανία το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες e-banking, στη Σουηδία το 28%, στη Βρετανία το 7%. Παρά τις εξελιγμένες μεθόδους για τη διασφάλιση των τραπεζικών συναλλαγών, η συχνότητα των ηλεκτρονικών επιθέσεων αυξάνεται τα τελευταία χρόνια. Η αύξηση αυτή προκαλεί ανησυχία στους ειδικούς, καθώς διακυβεύονται τεράστια ποσά, ειδικά στις περιπτώσεις κατά τις οποίες θύματα απάτης γίνονται επιχειρήσεις. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους για να επιτύχουν τους σκοπούς τους. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Έρευνες ειδικών σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είτε είχαν την ακούσια - συνήθως- βοήθεια και κάποιου που εργαζόταν στην τράπεζα, είτε υπέκλεψαν κωδικούς χρηστών. Οι επιχειρήσεις-πελάτες είναι συνήθως προσεκτικές και χρησιμοποιούν συστήματα ασφαλείας στα δίκτυά τους. Την ίδια "σοφία" ή προσοχή δεν δείχνουν και οι ιδιώτες πελάτες, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι απλοί χρήστες γίνονται εύκολα θύματα προγραμμάτων που στην πραγματικότητα ανοίγουν "τρύπες" ασφάλειας στο σύστημα και με τον τρόπο αυτό επιτρέπουν σε επιτήδειους να έχουν πρόσβαση σε αυτό και να κινούνται μέσα σε αυτό ανενόχλητοι.

ΚΕΦΑΛΑΙΟ 5

Firewalls

Τα δίκτυα των οργανισμών, επιχειρήσεων αλλά και τα οικιακά συνδέονται με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών. Όπως αναφέρθηκε παραπάνω, αυτό εγκυμονεί κινδύνους, αφού οι χρήστες του διαδικτύου μπορούν να προσεγγίσουν τις ιδιωτικές πληροφορίες του οργανισμού. Για έναν οργανισμό ηλεκτρονικού εμπορίου είναι πολύ σημαντικό να μπορεί να διαφυλάξει τα προσωπικά δεδομένα των πελατών του από μη εξουσιοδοτημένη πρόσβαση. Είναι επιθυμητό να υπάρχει ένα είδος διαχωρισμού ανάμεσα στο δίκτυο του οργανισμού και το διαδίκτυο. Η παρεμβολή ενός ενδιάμεσου συστήματος ανάμεσα στα δύο δίκτυα θα μπορούσε να τα διαχωρίσει. Ένα τέτοιο ενδιάμεσο σύστημα θα προστατεύει το ιδιόκτητο δίκτυο από επιθέσεις που προέρχονται από τον έξω κόσμο και θα παρέχει ένα μοναδικό σημείο ελέγχου, όπου θα ελέγχεται η κίνηση από και προς το δίκτυο. Επιπλέον το ενδιάμεσο αυτό σύστημα θα μπορούσε να χρησιμοποιηθεί και για συλλογή πληροφοριών διαχείρισης για χρήση του δικτύου, αφού μπορεί να καταγράφει οτιδήποτε διακινείται από ή προς το δίκτυο. Αυτά τα ενδιάμεσα συστήματα ονομάζονται φράγματα ασφαλείας (firewalls). Firewall είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το ιδιόκτητο δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Λειτουργεί σαν μια πύλη από την οποία περνάει όλη η κίνηση δεδομένων από και προς το εξωτερικό δίκτυο. Στην πύλη εξετάζεται και αποφασίζεται αν θα επιτραπεί ή όχι η διέλευση των δεδομένων, σύμφωνα με την πολιτική ασφάλειας που εφαρμόζει ο οργανισμός του συστήματος. Το firewall δεν είναι απλώς ένα σύνολο συνιστωσών λογισμικού ή υλικού, αλλά η τεχνική έκφραση μιας συγκεκριμένης στρατηγικής προστασίας των πόρων ενός οργανισμού. Ένα firewall είναι ουσιαστικά ένα «τείχος» ασφάλειας μεταξύ του μη ασφαλούς δημόσιου δικτύου και του ιδιόκτητου δικτύου που θεωρείται ασφαλές και αξιόπιστο. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν στο «απέναντι» δίκτυο. Ένα firewall δεν μπορεί να λειτουργήσει σωστά, ανεξαρτήτως του πως έχει σχεδιαστεί ή υλοποιηθεί, εάν δεν έχει καθοριστεί μια σαφής πολιτική ασφάλειας. Το firewall που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφάλειας που βρίσκεται κάθε φορά σε ισχύ και πρέπει να είναι συγκεκριμένη και σαφής. Το firewall αποτελεί την πρώτη γραμμή άμυνας του οργανισμού απέναντι στους επίδοξους εισβολείς, αλλά ποτέ τη μοναδική. Η χρήση ενός φράγματος ασφάλειας δεν αποτελεί πανάκεια για την ασφάλεια του δικτύου. Όπως όλα τα συστήματα ασφάλειας μπορεί να παραβιαστεί από κάποιον ικανό εισβολέα. Επιπλέον το firewall αλληλεπιδρά με το διαδίκτυο και χρειάζεται ιδιαίτερη προσοχή στην εγκατάσταση του και την σωστή διαμόρφωσή του.

# Προστασία των δεδομένων και της ιδιωτικής ζωής στο διαδίκτυο

Οι κανόνες της ΕΕ για την προστασία δεδομένων εγγυώνται την προστασία των προσωπικών σας δεδομένων οποτεδήποτε αυτά συγκεντρώνονται, π.χ. όταν αγοράζετε ένα προϊόν μέσω του διαδικτύου, υποβάλλετε αίτηση για θέση εργασίας ή ζητάτε τραπεζικό δάνειο. Οι κανόνες αυτοί **ισχύουν για επιχειρήσεις και φορείς (ιδιωτικούς ή δημόσιους) που έχουν την έδρα τους τόσο εντός όσο και εκτός της ΕΕ και προσφέρουν αγαθά ή υπηρεσίες εντός της ΕΕ**, όπως το Facebook ή το Amazon, κάθε φορά που οι εν λόγω επιχειρήσεις ή φορείς ζητούν ή επαναχρησιμοποιούν τα προσωπικά δεδομένα πολιτών της ΕΕ.

**Ανεξάρτητα από τη μορφή με την οποία παρέχονται τα δεδομένα** -ηλεκτρονικά σε σύστημα υπολογιστών ή σε έντυπο που περιλαμβάνεται σε δομημένο αρχείο- κάθε φορά που οι παρεχόμενες πληροφορίες οι οποίες σας ταυτοποιούν άμεσα ή έμμεσα αποθηκεύονται ή υποβάλλονται σε επεξεργασία, πρέπει να τηρούνται τα δικαιώματά σας σχετικά με την προστασία των δεδομένων σας.

## Πότε επιτρέπεται η επεξεργασία των δεδομένων;

Οι κανόνες της ΕΕ για την προστασία δεδομένων, γνωστοί και ως «γενικός κανονισμός της ΕΕ για την προστασία δεδομένων» (ΓΚΠΔ), περιγράφουν διαφορετικές περιπτώσεις κατά τις οποίες οι επιχειρήσεις ή οι φορείς **επιτρέπεται να συγκεντρώνουν ή να επαναχρησιμοποιούν πληροφορίες που σας αφορούν**:

* εφόσον έχουν συνάψει σύμβαση μαζί σας - για παράδειγμα μια σύμβαση για την προμήθεια αγαθών ή υπηρεσιών (π.χ. όταν αγοράζετε ένα προϊόν μέσω διαδικτύου), ή σύμβαση εργασίας
* εφόσον συμμορφώνονται με νομική υποχρέωση - π.χ. όταν η επεξεργασία των δεδομένων σας αποτελεί νομική υποχρέωση, όπως στην περίπτωση που ο εργοδότης σας παρέχει πληροφορίες σχετικά με τις μηνιαίες αποδοχές σας στον οργανισμό κοινωνικής ασφάλισης, ώστε να έχετε κοινωνική κάλυψη
* εφόσον η επεξεργασία των δεδομένων εξυπηρετεί τα ζωτικά συμφέροντά σας - π.χ. όταν πρόκειται για την προστασία της ζωής σας
* εφόσον αυτό απαιτείται για την ολοκλήρωση μιας δημόσιας αποστολής - που εντάσσεται κυρίως στα καθήκοντα δημόσιων υπηρεσιών, όπως σχολεία, νοσοκομεία και δήμοι
* εφόσον υπάρχουν έννομα συμφέροντα - π.χ. εάν η τράπεζά σας χρησιμοποιεί τα προσωπικά δεδομένα σας για να ελέγξει κατά πόσον μπορείτε να διαθέτετε αποταμιευτικό λογαριασμό με υψηλότερο επιτόκιο

Σε όλες τις άλλες περιπτώσεις, η επιχείρηση ή ο φορέας **οφείλει να ζητήσει τη σύμφωνη γνώμη σας** (συγκατάθεση) προτού συγκεντρώσει ή επαναχρησιμοποιήσει τα προσωπικά σας δεδομένα

## Ανάκληση της συγκατάθεσης για χρήση προσωπικών δεδομένων και δικαίωμα απαγόρευσης της επεξεργασίας τους

Αν δώσατε κάποια στιγμή τη συγκατάθεσή σας σε επιχείρηση ή φορέα να χρησιμοποιεί τα προσωπικά σας δεδομένα, μπορείτε, ανά πάσα στιγμή, να επικοινωνήσετε με τον υπεύθυνο επεξεργασίας των δεδομένων (το πρόσωπο ή τον φορέα που διαχειρίζεται τα προσωπικά σας δεδομένα) και να **ανακαλέσετε την άδεια**. Μόλις ανακαλέσετε την άδεια, η επιχείρηση/ο φορέας **δεν μπορεί πλέον να χρησιμοποιεί τα προσωπικά σας δεδομένα**.

Όταν ένας φορέας επεξεργάζεται τα προσωπικά σας δεδομένα στο πλαίσιο των δικών του έννομων συμφερόντων ή του δημόσιου συμφέροντος ή για λογαριασμό μιας επίσημης αρχής, ενδέχεται να έχετε δικαίωμα απαγόρευσης της επεξεργασίας τους. Σε ορισμένες ειδικές περιπτώσεις, μπορεί να προέχει το δημόσιο συμφέρον και να επιτραπεί στην επιχείρηση ή τον φορέα να συνεχίσει να χρησιμοποιεί τα προσωπικά σας δεδομένα. Για παράδειγμα, αυτό θα μπορούσε να συμβεί σε περίπτωση επιστημονικής έρευνας και συγκέντρωσης στατιστικών στοιχείων από δημόσια αρχή στο πλαίσιο των επίσημων καθηκόντων της.

Για την απευθείας αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων που προωθούν συγκεκριμένες μάρκες ή προϊόντα, απαιτείται προηγούμενη συγκατάθεση. Ωστόσο, εάν είστε ήδη πελάτης μιας συγκεκριμένης επιχείρησης, αυτή μπορεί να σας στέλνει απευθείας διαφημιστικά ηλεκτρονικά μηνύματα για τα δικά της παρόμοια προϊόντα ή υπηρεσίες. Έχετε δικαίωμα **να αρνηθείτε ανά πάσα στιγμή** τη λήψη τέτοιων απευθείας διαφημιστικών, οπότε η επιχείρηση **οφείλει να πάψει αμέσως να χρησιμοποιεί τα δεδομένα σας**.

Σε κάθε περίπτωση, την πρώτη φορά που η επιχείρηση ή ο φορέας επικοινωνήσει μαζί σας, πρέπει να σας ενημερώσει σχετικά με το δικαίωμά σας να απαγορεύσετε τη χρησιμοποίηση των προσωπικών σας δεδομένων .

## Πρόσβαση στα προσωπικά σας δεδομένα

Μπορείτε να ζητήσετε πρόσβαση στα προσωπικά σας δεδομένα που διατηρεί μια επιχείρηση ή ένας φορέας, και έχετε το δικαίωμα να λάβετε αντίγραφο των δεδομένων σας, δωρεάν, σε εύχρηστο μορφότυπο. Θα πρέπει να σας **απαντήσουν εντός ενός μηνός** και οφείλουν να σας **δώσουν αντίγραφο των προσωπικών σας δεδομένων** καθώς και κάθε συναφή πληροφορία **σχετικά με το πώς χρησιμοποιήθηκαν ή χρησιμοποιούνται τα δεδομένα αυτά**.

### Μεταφορά των προσωπικών σας δεδομένων (δικαίωμα στη φορητότητα των δεδομένων)

### Σε ορισμένες περιπτώσεις, μπορείτε να ζητήσετε από επιχείρηση ή φορέα **να σας επιστρέψει τα δεδομένα σας ή να τα μεταφέρει απευθείας σε μια άλλη επιχείρηση**, εάν αυτό είναι δυνατό από τεχνική άποψη. Αυτό είναι γνωστό ως «φορητότητα των δεδομένων». Για παράδειγμα, μπορείτε να χρησιμοποιήσετε το δικαίωμα αυτό εάν αποφασίσετε να αντικαταστήσετε μια υπηρεσία με μια άλλη παρόμοια -π.χ. να μετακινηθείτε από έναν ιστότοπο κοινωνικής δικτύωσης σε άλλον- και επιθυμείτε να μεταφερθούν τα προσωπικά σας δεδομένα γρήγορα και εύκολα στη νέα υπηρεσία.

### Διαγραφή των προσωπικών σας δεδομένων

Εφόσον τα προσωπικά σας δεδομένα δεν είναι πλέον απαραίτητα ή χρησιμοποιούνται παράνομα, μπορείτε να ζητήσετε τη διαγραφή τους. Αυτό είναι γνωστό ως «δικαίωμα στη λήθη».

Οι **κανόνες αυτοί ισχύουν και για τις μηχανές αναζήτησης**, όπως το Google, καθώς οι εν λόγω μηχανές θεωρούνται ως υπεύθυνοι επεξεργασίας δεδομένων. Μπορείτε να ζητήσετε τη διαγραφή από τα αποτελέσματα μηχανών αναζήτησης των συνδέσμων που οδηγούν σε ιστοσελίδες οι οποίες αναφέρουν το όνομά σας, εάν οι πληροφορίες είναι ανακριβείς, ακατάλληλες, άσχετες ή υπερβολικές.

Εάν μια επιχείρηση διαθέτει τα προσωπικά σας δεδομένα στο διαδίκτυο και της ζητήσετε να τα διαγράψει, η επιχείρηση οφείλει να ενημερώσει σχετικά και **κάθε άλλον ιστότοπο** προς τον οποίον τα έχει κοινοποιήσει.

Για την προστασία άλλων δικαιωμάτων, όπως η ελευθερία της έκφρασης, ορισμένα δεδομένα ενδέχεται να μη διαγραφούν αυτόματα. Για παράδειγμα, αμφιλεγόμενες δηλώσεις δημοσίων προσώπων, δεν μπορούν να διαγραφούν εάν το δημόσιο συμφέρον εξυπηρετείται καλύτερα με τη διατήρησή τους στο διαδίκτυο.

### Πρόσβαση στα δεδομένα σας χωρίς εξουσιοδότηση (παραβίαση δεδομένων)

### Σε περίπτωση κλοπής, απώλειας ή παράνομης πρόσβασης ( **παραβίαση προσωπικών δεδομένων**), ο υπεύθυνος επεξεργασίας δεδομένων (το πρόσωπο ή ο φορέας που διαχειρίζεται τα προσωπικά σας δεδομένα) οφείλει να πραγματοποιήσει σχετική αναφορά στην εθνική αρχή προστασίας δεδομένων. Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει επίσης να σας ενημερώσει αμέσως σε περίπτωση που τίθενται σε σοβαρό κίνδυνο τα προσωπικά σας δεδομένα ή η ιδιωτική σας ζωή εξαιτίας της παραβίασης.

## Υποβολή καταγγελίας

Εάν πιστεύετε ότι δεν τηρούνται τα δικαιώματά σας σχετικά με την προστασία δεδομένων, μπορείτε να υποβάλετε καταγγελία απευθείας στην εθνική σας αρχή προστασίας δεδομένων, η οποία θα διερευνήσει την καταγγελία και θα σας απαντήσει εντός 3 μηνών.

Μπορείτε, επίσης, να προσφύγετε απευθείας στα δικαστήρια κατά της σχετικής επιχείρησης ή του φορέα αντί να απευθυνθείτε πρώτα στην εθνική αρχή προστασίας δεδομένων.

**Μπορεί να δικαιούστε αποζημίωση** εάν έχετε υποστεί υλική ή μη υλική ζημία (π.χ. οικονομικό ή ψυχολογικό πρόβλημα αντίστοιχα), εξαιτίας του γεγονότος ότι μια επιχείρηση ή ένας φορέας δεν τήρησε τους κανόνες της ΕΕ για την προστασία δεδομένων.

ΚΕΦΑΛΑΙΟ 6

Έλλειψη προφύλαξης των προσωπικών δεδομένων των ανηλίκων

Ανυποψίαστοι και αδύναμοι είναι το 57% των ανηλίκων όσον αφορά την προστασία των προσωπικών τους δεδομένων μέσα από το Διαδίκτυο. Αυτό έδειξε έρευνα του Πανευρωπαϊκού Δικτύου Ασφαλούς Διαδικτύου «Insafe» (τελεί υπό την αιγίδα της Κομισιόν) που έγινε (6-7/2/07) σε 37 χώρες με συμμετοχή 21.825 παιδιών και εφήβων - τα 322 ήταν Ελληνόπουλα. Ειδικότερα, τα παιδιά κάτω των 10 ετών δεν γνωρίζουν τους κινδύνους που εγκυμονούν οι συναντήσεις με άτομα που γνώρισαν μέσα από τα chat rooms, αφού περισσότερα από το 1/3 δήλωσαν ότι θα συναντούσαν τους άγνωστους αυτούς χωρίς να ενημερώσουν τους γονείς τους, ενώ τα Ελληνόπουλα είναι πιο υποψιασμένα. Στις ηλικίες μεταξύ 14-17 χρόνων η έκθεση στους κινδύνους του Διαδικτύου είναι μεγαλύτερη με το 22% των 17χρονων να δηλώνει ότι θα ξεχνούσαν να αναφέρουν μια συνάντηση με αγνώστους στους γονείς τους και το 24% των 18χρονων ότι θα πήγαιναν μόνοι τους. Από τα 322 Ελληνόπουλα, 8 στα 10 δηλώνουν ότι έχουν δικό τους υπολογιστή (82,30%). 6 στα 10 (62,73%) ότι «σερφάρουν» έως 5 ώρες εβδομαδιαίως, 2 στα 10 πως είναι online πάνω από 10 ώρες (22,98%) και 7 στα 10 ότι δεν συνομιλούν με αγνώστους στο Διαδίκτυο και δεν θα τους συναντούσαν. Επίσης 1 στα 2 δηλώνουν ότι δίνουν πολλές προσωπικές πληροφορίες και για τη ζωή τους μέσα από τους ιστοχώρους κοινωνικής δικτύωσης, τα social networking sites, όπως το MySpace ή το Bebo. Ωστόσο, 1 στα 4 παιδιά θα έδινε τα στοιχεία του τραπεζικού λογαριασμού του πατέρα του μέσα από το Διαδίκτυο, ενώ 4,5 στα 10 θα συμπλήρωναν μόνο βασικά στοιχεία (τηλέφωνο, διεύθυνση κ.λπ.) σε φόρμες ιστοχώρων. Στα δύο μόνο το ένα θα έλεγε στους γονείς ή στον δάσκαλο ότι έλαβε διαδικτυακά από φίλο φωτογραφία πορνογραφικού περιεχομένου, 8 στα 10 παιδιά (80,43%) θα ζητούσαν από τη μητέρα τους να τους αγοράσει με πιστωτική κάρτα κάτι από το Διαδίκτυο, δύο (6,52%) θα «δανείζονταν» την πιστωτική κάρτα του γονιού τους ή θα χρησιμοποιούσαν στοιχεία κάρτας που θα τους έδινε φίλος τους (13,04%). Τέλος, 8 στα 10 Ελληνόπουλα ότι θα άκουγαν προσεκτικά τις συμβουλές των δασκάλων τους για ασφαλή χρήση του Διαδικτύου. Τέλος, η περιφρούρηση του Διαδικτύου είναι πολύ σημαντική αν σκεφτεί κανείς πως 1 στους 5 ανηλίκους δέχεται σεξουαλική προσέγγιση ή παρενόχληση στο Διαδίκτυο, μόνο το 17% το αναφέρει στους γονείς του, ενώ Εθνικών Κόμβων ελάχιστες απ' αυτές τις περιπτώσεις έκθεσης σε σεξουαλικού περιεχομένου ιστοσελίδες (περίπου το 3%) έχει αναφερθεί στις Αρχές. Η ΕΛ.ΑΣ έχει εξαπολύσει από το 2001 σαρωτικές επιχειρήσεις και έχει ασχοληθεί με 50 υποθέσεις στις οποίες σχηματίστηκαν δικογραφίες εις βάρος 120 δραστών. Αξιοσημείωτο είναι πως αν πληκτρολογήσει κάποιος τη λέξη «σεξ» σε μια μηχανή αναζήτησης μέσα σε λίγα δευτερόλεπτα εμφανίζονται πάνω από 2,764,667 sites.

Τέλος εξίσου σημαντικό είναι οι ίδιοι οι γονείς να μάθουν στα παιδιά τους να σερφάρουν με ασφάλεια στον καταπληκτικό αλλά αχανή κόσμο του διαδικτύου, να χρησιμοποιούν την πλειάδα των πληροφοριών που παρέχει σωστά, και να αποφεύγουν τους πιθανούς κινδύνους. Σύμφωνα με την τελευταία έρευνα του Ευρωβαρόμετρου “Safer Internet”, Μάιος 2006 γύρω από την Ασφάλεια του Διαδικτύου:

Η νομοθεσία από την Ευρωπαϊκή Ένωση για ασφαλή πλοήγηση των νέων

Στις 25 Ιανουαρίου 1999, η Επιτροπή υιοθέτησε ένα πολυετές κοινοτικό πρόγραμμα δράσης που αποσκοπεί στην προώθηση της ασφαλέστερης χρήσης του Διαδικτύου για την καταπολέμηση του παράνομου και επιβλαβούς περιεχομένου στα παγκόσμια δίκτυα. Το πρόγραμμα δράσης για ένα ασφαλέστερο Διαδίκτυο διαρθρώνεται γύρω από τους παρακάτω τομείς δράσης : 1.Δημιουργία ενός ασφαλέστερου περιβάλλοντος. 2. Δημιουργία ενός ευρωπαϊκού δικτύου «θερμών γραμμών» για να αναφέρουν οι καταναλωτές τις υποψίες τους για παιδική πορνογραφία. 3.Ενθάρρυνση της αυτορρύθμισης και των κωδίκων συμπεριφοράς. 4.Ανάπτυξη συστημάτων φιλτραρίσματος και κατάταξης. 5.Επίδειξη των οφελών των εθελοντικών συστημάτων φιλτραρίσματος και κατάταξης όπως, π.χ., το ICRA. 6.Διευκόλυνση της διεθνούς συμφωνίας για τα συστήματα κατάταξης. 7.Ενθάρρυνση δράσεων ευαισθητοποίησης. 8.Προετοιμασία του πεδίου για δράσεις ευαισθητοποίησης. 9. Ενθάρρυνση της εκτέλεσης δράσεων ευαισθητοποίησης ευρείας κλίμακας. 10.Δράσεις στήριξης. 11.Εκτίμηση των νομικών συνεπειών. 12.Συντονισμός με συναφείς διεθνείς δράσεις. 13.Αξιολόγηση του αντίκτυπου των κοινοτικών μέτρων. Το 2005, η Ευρωπαϊκή Επιτροπή καθιέρωσε το Πρόγραμμα «Safer Internet Plus», ένα 4ετές πρόγραμμα που έχει σκοπό να καταστήσει ασφαλέστερο το Διαδίκτυο για τα παιδιά της Ευρώπης. Το πρόγραμμα αποτελεί συνέχεια των δράσεων που αναλαμβάνει η Ευρωπαϊκή Ένωση για την προαγωγή της ασφαλέστερης χρήσης του Διαδικτύου και την καταπολέμηση του παράνομου και επιβλαβούς περιεχομένου από το 1996. Καλύπτει τις νέες επιγραμμικές τεχνολογίες συμπεριλαμβανομένων του κινητού και ευρυζωνικού περιεχομένου, των επιγραμμικών παιχνιδιών, και κάθε μορφής επικοινωνίας πραγματικού χρόνου όπως δικτυακοί χώροι συζήτησης (chat rooms) και άμεσα μηνύματα (instant messages), με βασικό στόχο τη βελτίωση της προστασίας των παιδιών και των ανηλίκων

ΟΔΗΓΙΕΣ ΓΙΑ ΠΑΙΔΙΑ

• Μη συνδέεστε για πολύ ώρα στο διαδίκτυο. • Μη δίνετε το όνομά σας, το πού μένετε ή το σχολείο στο οποίο πηγαίνετε σε ιστοσελίδες ή σε άτομα που γνωρίζετε στο διαδίκτυο. • Σε περίπτωση που νιώσετε άβολα είτε διαβάζοντας κάποιο μήνυμα είτε συνομιλώντας στο διαδίκτυο, κλείστε τη σύνδεση και αμέσως ενημερώστε τους γονείς σας για ό,τι είδατε ή διαβάσατε. 187 • Μην ανοίγετε τα παράθυρα με διαφημίσεις παιχνιδιών ή νέων ταινιών που εμφανίζονται στην οθόνη του Η/Υ σας. Πολλές φορές επιλέγοντάς τα, συνδέεστε χωρίς να το γνωρίζετε με σελίδες που έχουν βλαβερό για εσάς περιεχόμενο. • Να είστε πολύ προσεκτικοί όταν κάποιος «φίλος» που γνωρίσατε μέσω διαδικτύου σας ζητήσει να συναντηθείτε. Ενημερώστε τους γονείς σας ή κάποιον μεγαλύτερό σας ώστε να είναι μαζί σας στη συνάντηση. • Μην πιστεύετε εύκολα αυτά που σας λένε ή διαβάζετε στο διαδίκτυο. Δεν είναι πάντα αλήθεια. •

Αποφεύγετε να διαχέετε τα προσωπικά σας στοιχεία (όνομα, διεύθυνση, αριθμό ταυτότητας, διαβατηρίου κτλ) στο διαδίκτυο. • Κρατήστε μυστικό τον κωδικό σύνδεσής σας στο διαδίκτυο • Διαβάστε προσεκτικά κάθε μήνυμα και παράθυρο που εμφανίζεται στην οθόνη του υπολογιστή σας. • Μην ανοίγετε τα παράθυρα που εμφανίζονται στην οθόνη του Η/Υ (pop-up windows)σας μιας και μπορεί να κρύβουν κινδύνους τόσο για τη λειτουργία του Η/Υ σας όσο και για τα προσωπικά σας στοιχεία, αφού έχουν αναπτυχθεί τρόποι για την καταστρατήγησή τους. • Δώστε προσοχή στα δωμάτια άμεσης συνομιλίας (chatrooms). Να διαβάζετε πάντα την πολιτική που εφαρμόζουν όσον αφορά την ασφάλεια των προσωπικών σας δεδομένων. • Μην αποκαλύπτετε τα πραγματικά σας στοιχεία και μην είστε ευκολόπιστοι σε όσα σας λένε. • Να διατηρείτε πάντα μία κριτική άποψη και συμπεριφορά απέναντι σε αυτά που βλέπετε, ακούτε και διαβάζετε στο διαδίκτυο και πολύ περισσότερο σε αυτά που ενδεχομένως κάποιοι να σας περιγράφουν . • Σε περίπτωση που το άτομο με το οποίο συνομιλείτε σας κάνει να νιώσετε άβολα, διακόψτε τη συνομιλία και αναφέρετε το συμβάν σε κάποιον που εμπιστεύεστε (π.χ. γονείς, κηδεμόνας, φίλοι) • Σε περίπτωση που θα συναντήσετε το άτομο με το οποίο συνομιλείτε μέσω διαδικτύου, ενημερώστε κάποιον για τη συνάντηση αυτή και πηγαίνετε συνοδευόμενοι από τους φίλους σας. Προτιμήστε η συνάντηση να γίνει σε κάποιο δημόσιο χώρο όπου θα υπάρχει κόσμος.

ΟΔΗΓΙΕΣ ΓΙΑ ΕΝΗΛΙΚΕΣ/ΓΟΝΕΙΣ

• Να είστε ιδιαίτερα προσεκτικοί στις συναλλαγές μέσω διαδικτύου, όταν αυτές θα γίνουν με την πιστωτική σας κάρτα. • Μην παρασύρεστε από παράθυρα διαφημίσεων που σχετίζονται με τυχερά παιχνίδια τζόγου. • Μη γνωστοποιείτε τα προσωπικά σας στοιχεία στο διαδίκτυο, π.χ. το όνομα σας, τη διεύθυνσή σας, τον αριθμό της ταυτότητάς σας ή της πιστωτικής σας κάρτας. • Στην περίπτωση που είστε γονείς και έχετε παιδιά που χρησιμοποιούν το διαδίκτυο, τοποθετήστε τον υπολογιστή σε έναν κεντρικό κοινόχρηστο χώρο του σπιτιού σας ώστε να τα επιβλέπετε. • Εγκαταστήστε ειδικά λογισμικά φίλτρα τα οποία «μπλοκάρουν» την πρόσβαση σε σελίδες απαγορευμένου και βλαβερού περιεχομένου για τα παιδιά και παράλληλα φτιάξτε μία λίστα με ιστοσελίδες που εσείς εγκρίνετε για τα παιδιά σας. • Συμβουλέψτε τα παιδιά σας να μην είναι ευκολόπιστα και να μην δίνουν σε αγνώστους τα προσωπικά τους στοιχεία. Μιλήστε τους για τους κινδύνους που μία τέτοια πράξη συνεπάγεται.

* Ευγενία Αλεξανδροπούλου- Αιγυπτιάδου, «Προσωπικά δεδομένα» εκδόσεις Σάκκουλα Αθήνα-Κομοτηνή, 2007
* Ειρήνη Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω
* Ηλεκτρονικών Υπολογιστών, εκδόσεις Αντ.Ν. Σάκκουλα, ΑθήναΚομοτηνή, 1993
* Αποστόλης Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδ. Αντ. Ν Σάκκουλας, ΑθήναΚομοτηνή, 2002
* Αποστόλης Γέροντας, Πληροφορική και δίκαιο, εκδόσεις Αντ.Ν.
* Σάκκουλα, Αθήνα-Κομοτηνή, 1990
* Ιωάννης Δ. Ιγγλεζάκης, Εισαγωγή στο δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2006
* Γρηγόρης Λάζος, Πληροφορική και έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2001
* Τάσος Ν.Μαρίνου, Οι ηλεκτρονικοί υπολογιστές και το δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Κομοτηνή, 1991
* Λίλιαν Μήτρου, Το δίκαιο στην κοινωνία της πληροφορίας, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2002
* Γεώργιος Νούσκαλης, Ψηφιακή Τεχνολογία και Δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2004, Η ποινική προστασία της ψηφιακής τεχνολογίας
* Ευάγγελος Παπακωνσταντίνου, Νομικά θέματα πληροφορικής, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2006 Διαδίκτυο και προστασία δεδομένων προσωπικού χαρακτήρα 88
* Θεόδωρος Σιδηρόπουλος, Το δίκαιο του Διαδικτύου, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2003
* Τατιάνα-Ελένη Συνοδινού, Η Νομική Προστασία των Βάσεων Δεδομένων, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη, 2004
* ¾Α.Φραγκούλη, Προστασία Δεδομένων στο Διαδίκτυο, εις συλλογικόν έργον Εφαρμογές Εμπορικού Δικαίου, Επιμέλειας Γ Τριανταφυλλάκη,