ΑΚΑΔΗΜΙΑ ΕΜΠΟΡΙΚΟΥ ΝΑΥΤΙΚΟΥ

ΓΙΑΝΝΗΣ ΣΠΥΡΟΥ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΚΑΔΗΜΙΑ ΕΜΠΟΡΙΚΟΥ ΝΑΥΤΙΚΟΥ

Α.Ε.Ν. ΜΑΚΕΔΟΝΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΥΑΚΙΝΘΟΣ ΧΑΡΑΛΑΜΠΟΣ

ΘΕΜΑ :ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΤΟΥ ΣΠΟΥΔΑΣΤΗ: ΓΙΑΝΝΗ ΣΠΥΡΟΥ

Α.Γ.Μ:3129

Ημερομηνία ανάληψης της εργασίας:

Ημερομηνία παράδοσης της εργασίας:

Α/Α	*Ονοματεπώνυμο*	*Ειδικότης*	*Αξιολόγηση*	*Υπογραφή*
1				
2				
3				
ΤΕΛΙΚΗ ΑΞΙΟΛΟΓΗΣΗ				

Ο ΔΙΕΥΘΥΝΤΗΣ ΣΧΟΛΗΣ :

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Το παρόν πόνημα πραγματεύεται το θέμα της ασφάλειας και της ιδιωτικότητας των προσωπικών δεδομένων στο διαδίκτυο. Στο πρώτο κεφάλαιο θα γίνει μια διεξοδική αναφορά στην ηλεκτρονική διακυβέρνηση: ορισμός ηλεκτρονικής διακυβέρνησης, βασικές αρχές ανάπτυξης υπηρεσιών ηλεκτρονικής διακυβέρνησης, αναγκαία χαρακτηριστικά υπηρεσιών ηλεκτρονικής διακυβέρνησης, επίπεδα ολοκλήρωσης υπηρεσιών ηλεκτρονικής διακυβέρνησης. Επιπλέον, θα αναφερθούμε στη διαλειτουργικότητα σε πληροφοριακά συστήματα ηλεκτρονικής διακυβέρνησης, στο ευρωπαϊκό πλαίσιο της διαλειτουργικότητας, καθώς και στην εξέλιξη της ηλεκτρονικής διακυβέρνησης ανά τον κόσμο.

Το δεύτερο κεφάλαιο ασχολείται με τους κινδύνους παραβίασης της ιδιωτικής ζωής μέσω της ηλεκτρονικής διακυβέρνησης και της χρήσης του διαδικτύου. Θα μας απασχολήσει το θέμα της ασφάλειας των προσωπικών δεδομένων, τα διαδικτυακά εγκλήματα που λαμβάνουν χώρα κυρίως μέσω των ιών, ενώ θα κλείσουμε με συμβουλές προς τους χρήστες του διαδικτύου σχετικά με την πιο ορθή και ασφαλή χρήση αυτού.

Στο τελευταίο κεφάλαιο θα γίνει μνεία στις ηλεκτρονικές συναλλαγές ˙ στις ηλεκτρονικές συναλλαγές με τις τράπεζες (Phishing), στην παραπλάνηση σε ψεύτικες ιστοσελίδες (Pharming), στις αγγελίες για την ανεύρεση εργασίας (Scam), στην άμεση συνομιλία των chat, στο διαμοιρασμό αρχείων.

ABSTRACT

This work deals with the issue of security and privacy of our personal data while we use the internet. In the first chapter, we will discuss about the electronic Government (e-Government), definition of the word, basic principles of the development of services of e-Government, necessary features of services of e- Government, online sophistication services of e- Government. Moreover, we will mention the Interoperability in information systems of e- Government, the European frame of the interoperability and the development of e- Government through the world.

In the second chapter, we will talk about the danger of infringement of personal life through the use of internet. Severe subjects are the security of our personal data and the online crimes (mostly through virus) that can be committed. In the end, we will give some advice for safer use of the internet.

In the last chapter, we will discuss about the online transactions, such as Phising, Pharming, Scam and chatrooms.

ΕΙΣΑΓΩΓΗ

Το επίπεδο της πληροφοριακής τεχνολογίας που έχει κατακτηθεί τον 20ό αιώνα έχει προκαλέσει ραγδαίες εξελίξεις στον τρόπο που επικοινωνούμε, συμπεριφερόμαστε, εργαζόμαστε και ζούμε. Όπως συμβαίνει με όλα τα σύγχρονα επιτεύγματα, πάντα υπάρχει και η σκοτεινή τους πλευρά. Με την πληροφορία να είναι η τροφή των νέων τεχνολογιών, η ανάγκη για προστασία και ασφάλεια των δεδομένων είναι πιο αναγκαία από ποτέ.

Η κυβερνο-ασφάλεια είναι ένας τομέας που φαίνεται να χαίρει ιδιαίτερης προσοχής και στην Ελλάδα, το λίκνο της δημοκρατικής κοινωνίας. Το παραπάνω προκύπτει από τη σύσταση φορέων με αντικείμενο την περιφρούρηση και υπεράσπιση των δικαιωμάτων των ιδιωτών και των επιχειρήσεων.

Ωστόσο η μετάβαση στην πληροφοριακή εποχή δημιουργεί πλήθος κινδύνων για τον ιδιώτη, τον δημόσιο και τον ιδιωτικό τομέα, αφενός λόγω της συνεχούς ζήτησης και εμπορευματοποίησης προσωπικών δεδομένων των πολιτών και αφετέρου λόγω της διαρροής ή κλοπής ευαίσθητων δεδομένων των δημόσιων και ιδιωτικών επιχειρήσεων.

Με τις νέες τεχνολογίες να κυριαρχούν τα τελευταία χρόνια καθώς και τη συνεχή άνοδο του διαδικτύου (το Διαδίκτυο των Πραγμάτων), η αξία της πληροφορίας αυξάνεται διαρκώς και ταυτόχρονα η ζήτηση και η απόκτησή της. Σημείο ενδιαφέροντος αποτελεί το γεγονός ότι οι προσωπικές προτιμήσεις και οι συνήθειες του καθενός μπορούν να γίνουν ευκαιρία κέρδους. Με τα ατομικά δεδομένα να διακινούνται και να αποθηκεύονται σε πολλαπλές συσκευές συνδεδεμένες μεταξύ τους, όπως κινητές συσκευές, wearables (υπολογιστές - αξεσουάρ) και sensors (αισθητήρες), η πληροφορία γίνεται ευάλωτη σε πιθανές υποκλοπές και παραβιάσεις.

Οι συνδεδεμένες συσκευές έχουν ξεκινήσει την πορεία τους από τις επιχειρήσεις και τις βιομηχανίες στη μαζική αγορά. Πλέον θα παρατηρούμε συνεχώς περισσότερους αισθητήρες (sensors) και ενεργοποιητές (actuators) στα ηλεκτρονικά αγαθά που χρησιμοποιούμε καθημερινά, στις οικιακές συσκευές και στις υποδομές των πόλεων. Αναμένεται να παρατηρήσουμε μαζική αύξηση των δεδομένων που παράγονται από αυτές τις συσκευές στα δίκτυα και τα συστήματά μας. Ήδη, εκατομμύρια γεγονότα γεννούν τεράστιο αριθμό πληροφοριών κάθε δευτερόλεπτο, που είναι έτοιμες να υποστούν επεξεργασία, να αναλυθούν και να διαμοιραστούν μεταξύ συσκευών και ανθρώπων, ώστε να βελτιώσουν τις ζωές μας.

Οι συσκευές είναι έτοιμες. Τα δίκτυα υπάρχουν και αναπτύσσονται. Και ο χείμαρρος των δεδομένων έχει ήδη ξεκινήσει. Το ερώτημα είναι κατά πόσον οι χρήστες είναι έτοιμοι να αντιμετωπίσουν αυτήν την επιδρομή.

Ο κυριότερος ίσως κίνδυνος για τους ιδιώτες είναι η παραβίαση της ιδιωτικότητάς τους. Οι επιχειρήσεις και οι ιδιωτικοί οργανισμοί κινδυνεύουν από την εκροή πολύτιμων και ευαίσθητων δεδομένων που αφορούν στη λειτουργία τους, τους πελάτες τους και τη στρατηγική τους. Αναφορικά με τον δημόσιο τομέα, η ανάπτυξη του Διαδικτύου και η σημαντικότητα του ρόλου του στη λειτουργία του κράτους, συνοδεύεται από την απειλή διαρροής κρίσιμων κρατικών δεδομένων και πληροφοριών. Τέτοιες ενέργειες μπορεί να προέρχονται από τη δράση αυτόνομων hackers με πολιτικά ή οικονομικά κίνητρα αλλά και από εταιρείες ή άλλα κράτη με σκοπό την κατασκοπεία.

Η στρατηγική ασφάλειας έχει δύο βασικές κατευθύνσεις, τις αμυντικές και τις επιθετικές. Με βάση πρόσφατη μελέτη της McKinsey, οι οργανισμοί θα πρέπει να επενδύσουν στο χτίσιμο της ψηφιακής τους ανθεκτικότητας (digital resilience) ώστε να προστατεύσουν τις πιο πολύτιμες και ευαίσθητες πληροφορίες τους.

Ένας σύντομος οδηγός προστασίας και ασφάλειας των δεδομένων και της ιδιωτικότητας θα μπορούσε να περιλαμβάνει τα παρακάτω:

•Λεπτομερής ενημέρωση των χρηστών για τα θέματα ασφαλείας του Διαδικτύου αλλά και γενικά της τεχνολογίας, σε όποιο περιβάλλον και αν βρίσκονται και λειτουργούν (ιδιωτικό, εταιρικό, δημόσιο)

•Η σωστή χρήση κατάλληλων anti-virus μπορεί να είναι σωτήρια για τους υπολογιστές και τα δεδομένα των χρηστών.

•Ενδυνάμωση της ασφάλειας του wi-fi router (WPA2 με strong encryption και firewall).

•Χρήση ειδικών βιομετρικών χαρακτηριστικών για τη σύνδεση σε βάσεις δεδομένων και άλλες ανάλογες εργασίες.

•Εντατική χρήση ανοιχτού λογισμικού.

•Χρήση πολύ ισχυρών κωδικών.

•Χρήση διαφορετικών λογαριασμών ηλεκτρονικού ταχυδρομείου για διαφορετικές εργασίες.

•Ταυτοποίηση του χρήστη σε δύο επίπεδα.

•Αποφυγή αποθήκευσης μεγάλου ιστορικού δεδομένων καθώς και πολλών δεδομένων στις υπηρεσίες cloud.

•Μείωση του αριθμού των administrators σε κάθε εταιρεία/φορέα/ ιδιωτικό υπολογιστή και παροχή σχετικής άδειας μόνο σε έκτακτες περιπτώσεις.

•Παρακολούθηση χρήσης και κυκλοφορίας των ατομικών πληροφοριών.

•Καλές και σωστές υποδομές ασφαλείας, σε όλα τα επίπεδα χρήσης και ύπαρξη σχεδίου δράσης (cyber-insurance).

• Θέσπιση αυστηρού νομοθετικού πλαισίου.

ΚΕΦΑΛΑΙΟ 1: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Στο παρόν κεφάλαιο μελετάται και αποτυπώνεται συνοπτικά η έννοια της Ηλεκτρονικής Διακυβέρνησης, με την παράθεση των σημαντικότερων ορισμών. Στη συνέχεια παρουσιάζονται οι βασικές αρχές, οι τομείς, καθώς και τα διαφορετικά επίπεδα στα οποία μπορεί να ενταχθεί μία ηλεκτρονική υπηρεσία. Ακόμη παρουσιάζεται η εξέλιξη των ηλεκτρονικά παρεχόμενων υπηρεσιών σε παγκόσμιο επίπεδο, καθώς και η υπάρχουσα κατάσταση στην Ελλάδα.

1.1 Ηλεκτρονική Διακυβέρνηση

Ο όρος «Ηλεκτρονική Διακυβέρνηση» (ΗΔ) (*electronic Government – e-Government*) χρησιμοποιείται για να περιγράψει τη χρήση και εφαρμογή Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) σε διαδικασίες και υπηρεσίες της Δημόσιας Διοίκησης. Η χρήση τους δεν μπορεί να θεωρηθεί ως κάτι καινούργιο ή καινοτόμο, καθώς εφαρμόζεται αρκετές δεκαετίες τώρα σε διάφορους επιμέρους τομείς ή διαδικασίες της Δημόσιας Διοίκησης. Ο συγκεκριμένος όρος μπορεί να εμφανίστηκε στα τέλη της δεκαετίας του 1990, αλλά η αλληλεπίδραση προϋπήρχε, σχεδόν από την εμφάνιση των πρώτων Πληροφοριακών Συστημάτων (Grönlund & Horan, 2005) & (Danziger & Andersen, 2002)

Μια τυπική υπηρεσία Ηλεκτρονικής Διακυβέρνησης έχει τα ακόλουθα χαρακτηριστικά, τα οποία τη διαφοροποιούν από μία διαδικασία ή απλή διεργασία ενός φορέα (Διακονικολάου & Μυλωνόπουλος, 2004), (ΚτΠ, 2008).

- *Έχει τελικό χρήστη*: Ο χρήστης μπορεί να είναι πολίτης, επιχείρηση ή άλλος φορέας της Δημόσιας Διοίκησης.
- *Έχει τελικό παραδοτέο*: Το τελικό παραδοτέο πρέπει να είναι αυτοτελές και ο τελικός χρήστης που το παραλαμβάνει να είναι σε θέση να το αξιοποιήσει χωρίς να απαιτούνται επιπλέον διεργασίες ή συναλλαγές.
- *Έχει πάροχο*

- *Έχει ρυθμιστή*: Ο ρυθμιστής της υπηρεσίας είναι μία, κατ' ελάχιστον, μονάδα της Δημόσιας Διοίκησης, αρμόδια για το ρυθμιστικό πλαίσιο της ηλεκτρονικής υπηρεσίας.

Αντίστοιχα, στο άρθρο 4 της Οδηγίας 2006/123/ΕΚ "Σχετικά με τις υπηρεσίες στην Εσωτερική Αγορά" δίνονται οι εξής ορισμοί:

- Ο όρος Υπηρεσία αναφέρεται στην παροχή ενός συγκεκριμένου αποτελέσματος που επιθυμεί να λάβει ένας πολίτης ή μια επιχείρηση από έναν οργανισμό του Δημόσιου Τομέα.

- Η ολοκλήρωση μιας Υπηρεσίας συνίσταται στην εκτέλεση των διαδικασιών που απαιτούνται.

- Οι Αιτούντες – Αποδέκτες μπορεί να είναι είτε φυσικά είτε νομικά πρόσωπα Οι Φορείς της Δημόσιας Διοίκησης παρέχουν υπηρεσίες προς τους Αιτούντες - Αποδέκτες.

- Ο Αρμόδιος Φορέας για την εκτέλεση μιας υπηρεσίας μπορεί να ορίζεται μονοσήμαντα από τη φύση και τα στοιχεία μιας υπηρεσίας.

1.1.1 Ορισμός Ηλεκτρονικής Διακυβέρνησης

Εξαιτίας της πληθώρας και ποικιλομορφίας των προσεγγίσεων της Ηλεκτρονικής Διακυβέρνησης ανά τον κόσμο, η καθιέρωση ενός ενιαίου, καθολικού και λειτουργικού ορισμού, αποδεικνύεται εξαιρετικά δύσκολη. Τα τελευταία χρόνια έχουν διατυπωθεί διάφοροι ορισμοί για τον συγκεκριμένο όρο· κάποιοι εστιάζουν περισσότερο στη χρήση και αξιοποίηση των ΤΠΕ, ενώ κάποιοι το αντιμετωπίζουν υπό την ευρύτερη έννοια του μετασχηματισμού της παραδοσιακής διακυβέρνησης. Οι πλέον ευρέως αποδεκτοί ορισμοί που έχουν διατυπωθεί μέχρι σήμερα, παρατίθενται στη συνέχεια.

- Ευρωπαϊκή Επιτροπή: ΗΔ είναι "Η χρήση των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών στη Δημόσια Διοίκηση, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, με σκοπό την βελτίωση της εξυπηρέτησης του κοινού, την ενδυνάμωση της δημοκρατίας και την υποστήριξη των δημόσιων πολιτικών".

- ❖ Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ): ΗΔ είναι "Η χρήση από την κυβέρνηση εφαρμογών Διαδικτύου και άλλων τεχνολογιών, σε συνδυασμό με διαδικασίες που ενσωματώνουν αυτές τις τεχνολογίες για την ενίσχυση της πρόσβασης στην κρατική πληροφορία και υπηρεσία προς το κοινό, άλλες υπηρεσίες και κρατικές οντότητες, ή την βελτίωση σε κυβερνητικές λειτουργίες ως προς την αποτελεσματικότητα, την ποιότητα των υπηρεσιών και τον μετασχηματισμό τους".

- ❖ Ευρωπαϊκό Παρατηρητήριο για την Τεχνολογία Πληροφορίας: "Η Ηλεκτρονική Διακυβέρνηση ορίζεται ως η χρήση των τεχνολογιών Διαδικτύου στη διεξαγωγή, ενίσχυση και υποστήριξη των σχέσεων μεταξύ κυβερνητικών φορέων, πολιτών και επιχειρήσεων".

- ❖ Ηνωμένα Έθνη: "Η Ηλεκτρονική Διακυβέρνηση ορίζεται ως η αξιοποίηση του Διαδικτύου και του Παγκόσμιου Ιστού για την ηλεκτρονική παροχή πληροφοριών και υπηρεσιών στους πολίτες".

Συνολικά, τα κοινά τους σημεία μπορούν να συνοψιστούν στα παρακάτω χαρακτηριστικά:

- Παροχή υπηρεσιών που βασίζονται στις τεχνολογίες Διαδικτύου
- Αξιοποίηση των ΤΠΕ σε όλες τις δραστηριότητες της Δημόσιας Διοίκησης
- Μετασχηματισμός διαδικασιών της Δημόσιας Διοίκησης

1.1.2 Βασικές Αρχές Ανάπτυξης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με την αναφορά των Ηνωμένων Εθνών (United Nations, 2003), οι βασικές αρχές (*Principles*) για την ανάπτυξη ενός ολοκληρωμένου και επιτυχημένου περιβάλλοντος Ηλεκτρονικής Διακυβέρνησης είναι:

- ➢ υποστήριξη, δέσμευση και συμμετοχή της κεντρικής κυβέρνησης στον στρατηγικό σχεδιασμό και την υλοποίηση των στόχων,

- ➢ αποτελεσματικότητα και αποδοτικότητα της κεντρικής κυβέρνησης στην υλοποίηση των απαιτούμενων αλλαγών,

- ➢ διασφάλιση απαιτούμενης και επαρκούς χρηματοδότησης,

- ➢ καλλιέργεια και ανάπτυξη της απαραίτητης κουλτούρας στη Δημόσια Διοίκηση,

- προγραμματισμός και συντονισμός των απαιτούμενων δράσεων,
- διαμόρφωση κατάλληλου νομικού και κανονιστικού πλαισίου,
- συνεχής παρακολούθηση και αξιολόγηση,
- προώθηση και ανάδειξη των πλεονεκτημάτων στο ευρύ κοινό και
- εγκαθίδρυση του απαιτούμενο επιπέδου εμπιστοσύνης.

1.1.3 Αναγκαία Χαρακτηριστικά Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με την έκθεση της Ομάδας Εργασίας ΣΤ-5 (Διακονικολάου & Μυλωνόπουλος, 2004), ο τελικός χρήστης μίας υπηρεσίας Ηλεκτρονικής Διακυβέρνησης:

- Δεν απαιτείται να γνωρίζει ή να είναι εξοικειωμένος με τον τρόπο λειτουργίας, τη δομή και τις αρμοδιότητες των οργανωτικών μονάδων της Δημόσιας Διοίκησης που εμπλέκονται για την εξυπηρέτησή του.
- Πρέπει να έρχεται σε επαφή αποκλειστικά με το σημείο εκκίνησης της υπηρεσίας (κέντρο εξυπηρέτησης, δημόσιο πληροφοριακό σύστημα) και να παραλαμβάνει το αποτέλεσμα της υπηρεσίας από ένα σημείο εξόδου, χωρίς να εμπλέκεται σε ενδιάμεσα στάδια εξυπηρέτησης (*One Stop Shop*).
- Πρέπει να έχει συνεχή ενημέρωση για τη ροή της πληροφορίας και τη λήψη των αποφάσεων που αφορούν την υπόθεση που διεκπεραιώνει ηλεκτρονικά.

Για να ικανοποιηθούν οι συγκεκριμένες απαιτήσεις, θα πρέπει οι ηλεκτρονικές υπηρεσίες να παρέχονται από ένα Π.Σ. που υπερβαίνει τα όρια ενός φορέα, καθώς και να συνδυάζει περιεχόμενο και λειτουργίες από τις επιμέρους διαδικτυακές υπηρεσίες των εμπλεκόμενων φορέων, με τρόπο διαφανή για τον τελικό χρήστη κάθε υπηρεσίας. Προς την κατεύθυνση αυτή κινούνται οι προσπάθειες για την κατασκευή διαδικτυακών πυλών ενημέρωσης και εξυπηρέτησης, που καλύπτουν ένα ευρύ φάσμα φορέων της Δημόσιας Διοίκησης (π.χ. Οικονομικές Υπηρεσίες) ή, στη βέλτιστη περίπτωση

1.1.4 Βασικοί Τομείς Ηλεκτρονικής Διακυβέρνησης

Η Ηλεκτρονική Διακυβέρνηση αποτελείται από διαδικασίες που σχετίζονται όχι μόνο με το εξωτερικό, αλλά και με το εσωτερικό περιβάλλον της Δημόσια Διοίκησης. Προκειμένου να επιτευχθεί η πλήρης δυναμική της, είναι αναγκαίος ο ανασχεδιασμός των διαδικασιών, αφού ληφθούν υπ' όψιν απαιτήσεις και προοπτικές για όλους τους τομείς που περιλαμβάνει. Οι βασικότεροι τομείς (*Domains*) ενός περιβάλλοντος Ηλεκτρονικής Διακυβέρνησης προκύπτουν από την αναγνώριση των εμπλεκόμενων μελών (*Actors*) στις αλληλεπιδράσεις με τη Δημόσια Διοίκηση. Οι πιο συνήθεις εμπλεκόμενοι είναι i) οι πολίτες, ii) οι επιχειρήσεις και iii) η ίδια η Δημόσια Διοίκηση. Βάσει αυτών των εμπλεκομένων προκύπτουν οι ακόλουθοι τομείς:

***Government to Citizen (G2C)*:**

- περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ μεμονωμένων πολιτών και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική υποβολή φορολογίας εισοδήματος φυσικών προσώπων)
- περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ επιχειρήσεων και οργανισμών του ιδιωτικού τομέα και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική προμήθεια για δημόσιους φορείς)
- περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ φορέων και οργανισμών που εμπίπτουν στη δικαιοδοσία της Δημόσιας

Οι τομείς του G2B και G2C χαρακτηρίζονται ως "Εξωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης" (*external e-Government*) ενώ ο τομέας G2G χαρακτηρίζεται ως "Εσωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης" (*internal e-Government*). Σε αρκετές περιπτώσεις πραγματοποιείται και ένας επιπλέον διαχωρισμός στο εσωτερικό περιβάλλον, προκειμένου να περιγραφούν οι αλληλεπιδράσεις της Δημόσιας Διοίκησης με Δημόσιους Φορείς άλλων κρατών.

1.1.5 Επίπεδα Ολοκλήρωσης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Οι ηλεκτρονικές υπηρεσίες κατατάσσονται, γενικά, στις ακόλουθες κατηγορίες-επίπεδα, ανάλογα με το βαθμό ολοκλήρωσης (*Online Sophistication*) της υπηρεσίας που μπορεί να επιτευχθεί ηλεκτρονικά:

- *Επίπεδο 1: Πληροφοριακές Υπηρεσίες (Information):* Παροχή πληροφοριακού υλικού σχετικά με τον τρόπο διεκπεραίωσης της υπηρεσίας. Το υλικό αυτό αφορά: στα δικαιολογητικά που πρέπει να προσκομιστούν, στους φορείς που εμπλέκονται για την ολοκλήρωση της υπηρεσίας, στη διαδοχή εκτέλεσης των συναλλαγών που περιλαμβάνει η υπηρεσία, κλπ.

- *Επίπεδο 2: Επικοινωνιακές Υπηρεσίες (Interaction):* Παροχή πληροφοριακού υλικού για τον τρόπο διεκπεραίωσης της υπηρεσίας, καθώς και επίσημο υλικό (πρότυπα αιτήσεων, βεβαιώσεων, κλπ), το οποίο οι χρήστες μπορούν να εξασφαλίσουν με αξιοποίηση του Διαδικτύου, να το εκτυπώσουν και να το χρησιμοποιήσουν κατά τη συναλλαγή τους με το φορέα σε φυσικό επίπεδο.

- *Επίπεδο 3: Διαδραστικές Υπηρεσίες (Two-way interaction):* Πέραν του πληροφοριακού υλικού που παρέχεται σε αυτό το επίπεδο, προσφέρονται on-line φόρμες για συμπλήρωση και ηλεκτρονική αποστολή στην αρμόδια υπηρεσία- φορέα.

- *Επίπεδο 4: Συναλλακτικές Υπηρεσίες (Transactions):* Επιπλέον των φορμών αποστολής στοιχείων, οι ηλεκτρονικές υπηρεσίες που εντάσσονται σε αυτό το επίπεδο υποστηρίζουν λειτουργίες, όπου ο χρήστης ολοκληρώνει τις συναλλαγές που περιλαμβάνει η υπηρεσία.

Από το 2007 και έπειτα, έχει υιοθετηθεί και ένα 5ο επίπεδο ολοκλήρωσης, το οποίο αφορά στην προληπτική και στοχευμένη παροχή υπηρεσιών (*Pro-active Personalization*) (Gapgemini, 2007). Το συγκεκριμένο επίπεδο περιλαμβάνει την αυτοματοποιημένη παροχή ηλεκτρονικών υπηρεσιών, κατά την οποία ο δημόσιος φορέας προβαίνει προληπτικά σε δράσεις με στόχο να βελτιώσει την ποιότητα της παρεχόμενης υπηρεσίας και το βαθμό φιλικότητάς της προς το χρήστη. Επιπρόσθετα, περιλαμβάνει και την αυτόματη εκτέλεση συγκεκριμένων ηλεκτρονικών υπηρεσιών, απαλλάσσοντας από τις αντίστοιχες ενέργειες τον πολίτη ή την επιχείρηση. Το $5^{ο}$ στάδιο ψηφιακής ολοκλήρωσης μιας υπηρεσίας υφίσταται μόνον για ορισμένες ηλεκτρονικές υπηρεσίες και εκφράζει τις ακόλουθες δύο διαστάσεις:

- Την προληπτική παροχή υπηρεσιών *(proactive automated service delivery)*, όπου η Δημόσια Διοίκηση προχωρά προληπτικά σε δράσεις για να αναβαθμίσει την παροχή μιας ηλεκτρονικής υπηρεσίας και τη φιλικότητά της προς το χρήστη. Παραδείγματα τέτοιων δράσεων αποτελούν η έγκαιρη ειδοποίηση του πολίτη / χρήστη σε περίπτωση που πρέπει να προβεί σε κάποια ενέργεια, η προσυμπλήρωση δεδομένων σε αιτήσεις του χρήστη προς το Δημόσιο, κ.α.

- Την αυτοματοποιημένη παροχή υπηρεσιών *(automated service provision)*, όπου η Δημόσια Διοίκηση παρέχει αυτόματα συγκεκριμένες υπηρεσίες χωρίς να απαιτείται αντίστοιχη αίτηση από τον πολίτη ή τις επιχειρήσεις.

1.2 Διαλειτουργικότητα σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης

Η έννοια της διαλειτουργικότητας (*Interoperability*) αφορά στα Πληροφοριακά Συστήματα που αξιοποιούνται για την ολοκλήρωση διαδικασιών της Δημόσιας Διοίκησης, και συνδέεται άμεσα με την Ηλεκτρονική Διακυβέρνηση, επιτρέποντας τη μεταφορά και χρήση πληροφορίας με ενιαίο και αποτελεσματικό τρόπο από και προς διαφορετικά Πληροφοριακά Συστήματα. Η διαλειτουργικότητα σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης διακρίνεται σε οργανωσιακή, σημασιολογική και τεχνική, ανάλογα με το αντικείμενο στο οποίο αναφέρεται (ΚΤΠ, 2008):

- *Οργανωσιακή διαλειτουργικότητα (Organisational Interoperability)*: σχετίζεται με τον καθορισμό κοινών στόχων, τη διαμόρφωση διαδικασιών και στην δημιουργία διαύλων συνεργασίας μεταξύ των τμημάτων της Δημόσιας Διοίκησης, με διαφορετικές δομές και διαδικασίες, που επιζητούν την αμοιβαία ανταλλαγή πληροφορίας

- *Σημασιολογική διαλειτουργικότητα (Semantic Interoperability)*: σχετίζεται με τον ορισμό μιας σαφώς προσδιορισμένης και κοινά αποδεκτής περιγραφής της ανταλλασσόμενης πληροφορίας ώστε να είναι κατανοητή και αξιοποιήσιμη από οποιαδήποτε εφαρμογή. Μέσω της δημιουργίας προτύπων διασφαλίζεται κοινή ορολογία και λεξιλόγιο, επιτρέποντας στα Π.Σ. να συνδυάζουν και να επεξεργάζονται πληροφορίες από άλλα Π.Σ.

- *Τεχνική διαλειτουργικότητα (Technical Interoperability)*: σχετίζεται με τη μεταφορά και αξιοποίηση της πληροφορίας σε πραγματικό χρόνο μέσω κατάλληλων φυσικών *(Physical)* και δικτυακών *(Network)* διασυνδέσεων.

1.2.1 Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας

Στο πλαίσιο υποστήριξης της στρατηγικής της Ευρωπαϊκής Ένωσης, έχει θεσπιστεί το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (*European Interoperability Framework, EIF*) (EC, 2010), με στόχο την παροχή φιλικών, προς τον πολίτη, υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, διασφαλίζοντας παράλληλα τη διαλειτουργικότητα των συστημάτων και των υπηρεσιών σε πανευρωπαϊκό επίπεδο. Οι βασικές αρχές που διέπουν το Ευρωπαϊκό Πλαίσιο είναι:

- *Επικουρικότητα (Subsidiarity) και Αναλογικότητα (Proportionality)*: Όλες οι αποφάσεις θα πρέπει να λαμβάνονται με επίκεντρο το συμφέρον του πολίτη, 21 και μόνο εάν είναι πιο αποτελεσματικές από αυτές που ισχύουν σε εθνικό, περιφερειακό ή τοπικό επίπεδο. Επιπρόσθετα, θα παρέχουν τη μεγαλύτερη δυνατή ελευθερία στα Κράτη-Μέλη.

- *Επικέντρωση στο χρήστη (User Centric)*: Οι παρεχόμενες ηλεκτρονικές υπηρεσίες προορίζονται για την εξυπηρέτηση των αναγκών των πολιτών και των επιχειρήσεων και με βάση τις ανάγκες τους θα πρέπει να προσδιοριστεί ποιες υπηρεσίες θα παρέχονται στους πολίτες και με ποιο τρόπο.

- *Ένταξη (Inclusion) και Προσβασιμότητα (Accessibility)*: Οι παρεχόμενες ηλεκτρονικές υπηρεσίες θα πρέπει να είναι προσβάσιμες και προσπελάσιμες από όλες τις κοινωνικές ομάδες, χωρίς αποκλεισμούς σε μειονότητες ή άτομα με ειδικές ανάγκες.

- *Ασφάλεια (Security) και Ιδιωτικότητα (Privacy)*: Όλες οι οντότητες που αλληλεπιδρούν με τη Δημόσια Διοίκηση θα πρέπει να είναι σίγουρες για την ύπαρξη ενός επιπέδου εμπιστοσύνης που συμμορφώνεται πλήρως με τις σχετικές οδηγίες και κανονισμούς.

- *Πολυγλωσσία (Multilingualism)*: Οι παρεχόμενες ηλεκτρονικές υπηρεσίες θα πρέπει να είναι διαθέσιμες σε παραπάνω από μία γλώσσες, χωρίς όμως αυτό να επηρεάζει αρνητικά το επίπεδο των προσφερομένων υπηρεσιών.

- *Διοικητική Απλοποίηση (Administrative simplification)*: Οι Δημόσιοι Φορείς θα πρέπει να συνεργάζονται ώστε να δημιουργήσουν κοινά αξιοποιήσιμες ηλεκτρονικές υπηρεσίες, μειώνοντας και διαμοιράζοντας το φόρτο διαχείρισής τους.

- *Διαφάνεια (Transparency)*: Οι πολίτες και οι επιχειρήσεις θα πρέπει να μπορούν να παρακολουθούν όλες τις διεργασίες της Δημόσιας Διοίκησης, να έχουν εικόνα για το σκεπτικό των αποφάσεων και να μπορούν να ανατροφοδοτήσουν με σχόλια, συμβάλλοντας στη βελτίωση των παρεχόμενων υπηρεσιών.

- *Διατήρηση Πληροφορίας (Preservation of Information)*: Όλες οι διαθέσιμες πληροφορίες και εγγραφές θα πρέπει να διατηρούνται με τέτοιο τρόπο ώστε να εξασφαλίζεται η αναγνωσιμότητα, η αξιοπιστία και η ακεραιότητά τους.

- *Ανοιχτότητα (Openness)*: Όλες οι εμπλεκόμενες οντότητες θα πρέπει να μοιραστούν και να ανταλλάσσουν γνώσεις και πληροφορίες για την αναβάθμιση του επιπέδου των παρεχόμενων υπηρεσιών.

- *Επαναχρησιμοποίηση (Reusability)*: Οι Δημόσιοι Φορείς θα πρέπει να ανταλλάσσουν μεταξύ τους λύσεις, προδιαγραφές και προτυποποιήσεις ώστε να αξιοποιούνται στο έπακρο επιτυχημένες υλοποιήσεις και βέλτιστες πρακτικές.

- *Τεχνολογική Ουδετερότητα (Technological Neutrality) και Προσαρμοστικότητα (Adaptability)*: Ο σχεδιασμός, η υλοποίηση και η παροχή των ηλεκτρονικών υπηρεσιών θα πρέπει να επικεντρώνονται σε πραγματικές λειτουργικές ανάγκες παρά στην επιβολή και αξιοποίηση συγκεκριμένων τεχνολογιών.

- *Αποτελεσματικότητα (Effectiveness) και Αποδοτικότητα (Efficiency)*: Η Δημόσια Διοίκηση θα πρέπει να διασφαλίζει ότι οι παρεχόμενες υπηρεσίες εξυπηρετούν τους πολίτες και τις επιχειρήσεις με τον αποτελεσματικό και αποδοτικό τρόπο.

1.3 Εξέλιξη Ηλεκτρονικής Διακυβέρνησης ανά τον Κόσμο

Η έκθεση των Ηνωμένων Εθνών για το 2012 για την ανάπτυξη της Ηλεκτρονικής Δια κυβέρνηση σε παγκόσμιο επίπεδο (United Nations, 2012), επικεντρώνεται στην έννοια των ενοποιημένων ολοκληρωμένων υπηρεσιών που αξιοποιούν διασυνδέσεις μεταξύ διαφόρων δημόσιων υπηρεσιών και θεματικά παρόμοιων διαδικτυακών πυλών μίας στάσης, που μπορούν να αναμορφώσουν την ηλεκτρονική παροχή δημόσιων υπηρεσιών τόσο στο εμπρόσθιο τμήμα (*Frontend*) όσο και στο οπίσθιο (*Back-end*), να αυξήσουν την λειτουργική παραγωγικότητα, καθώς και τη βελτίωση των διαδικασιών και μηχανισμών διακυβέρνησης σε διάφορους τομείς της Δημόσιας Διοίκησης. Και οι 20 χώρες που σημειώνουν τους υψηλότερους δείκτες ανάπτυξης, συμπεριλαμβάνονται στις υψηλά ανεπτυγμένες οικονομίες. Από αυτές, οι 14 είναι στη Βόρεια Αμερική και την Ευρώπη, 3 στην Ανατολική Ασία (Δημοκρατία της Κορέας, Σιγκαπούρη και Ιαπωνία), 2 στην Ωκεανία (Αυστραλία και Νέα Ζηλανδία και 1 στη Δυτική Ασία (Ισραήλ).

ΚΕΦΑΛΑΙΟ 2: ΚΙΝΔΥΝΟΙ ΠΑΡΑΒΙΑΣΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ

2.1 Εισαγωγή

Σε κάθε βήμα της περιδιάβασής μας στο Διαδίκτυο "προσφέρουμε" προσωπικές πληροφορίες. Αυτές οι πληροφορίες είναι σαν ένα γρίφος που πρέπει να συμπληρωθεί για να αποκαλυφθεί η εικόνα μας. Η περιήγηση μας στο Διαδίκτυο έχει πολλά κοινά με τη ζωή μας στο φυσικό κόσμο. Έτσι τίθενται κάποια πολύ σοβαρά ζητήματα: της προστασίας των προσωπικών μας δεδομένων, της ορθής και ηθικής επικοινωνίας με τη βοήθεια της τεχνολογίας και το γεγονός πως ότι και αν κάνουμε στο Διαδίκτυο αφήνει ίχνη.

Όταν στέλνουμε ηλεκτρονικά μηνύματα σίγουρα δίνουμε πληροφορίες στο άτομο με το οποίο επικοινωνούμε. Εάν δεν είμαστε προσεχτικοί, μπορεί επίσης να δώσουμε πληροφορίες σε ένα μεγάλο αριθμό ατόμων, συμπεριλαμβανομένου του εργοδότη μας, της κυβέρνησης, του παροχέα ηλεκτρονικού ταχυδρομείου και οποιουδήποτε βρίσκεται στη διαδρομή του μηνύματός μας προς τον παραλήπτη.

Προσεχτικοί πρέπει να είμαστε και όταν συμμετέχουμε σε ομάδες συζητήσεων (groups ή listserves) του Διαδικτύου όπου είμαστε μέλη και δίνουμε προσωπικές πληροφορίες σε όλα τα μέλη της ομάδας (π.χ. διεύθυνση του ηλεκτρονικού μας ταχυδρομείου). Δεν απαγορεύεται σε μέλος να πάρει και να διανέμει τη διεύθυνσή μας.

Σημαντικό είναι να γνωρίζουμε ότι κατά την πλοήγησή μας στο Διαδίκτυο με χρήση οποιουδήποτε φυλλομετρητή αφήνουμε ίχνη. Όταν απλά κοιτάζουμε πληροφορίες στο Διαδίκτυο πολύ πιθανόν ο φυλλομετρητής μας να δίνει τον αριθμό του υπολογιστή και τις σελίδες που επισκεφθήκαμε στον παροχέα Διαδικτύου. Αν ο φυλλομετρητής χειρίζεται και το ηλεκτρονικό μας ταχυδρομείο, τότε πολύ πιθανόν να παρέχει την ηλεκτρονική διεύθυνση και το τηλέφωνό μας.

Επίσης πολλές από τις ιστοσελίδες που επισκεπτόμαστε, φυλάνε στον υπολογιστή μας δεδομένα για την επίσκεψη μας, τα λεγόμενα "Cookies". Τα Cookies είναι μικρά κομμάτια από πληροφορίες όπως το όνομα χρήστη, πληροφορίες της εγγραφής μας σε μια σελίδα, προτιμήσεις, διαδικτυακά «καλάθια με ψώνια» και λοιπά. Οι νόμιμες εταιρείες

χρησιμοποιούν τα Cookies για να κάνουν προσφορές σε χρήστες που τους επισκέπτονται ξανά. Παράνομες εταιρείες χρησιμοποιούν Cookies για να πάρουν πληροφορίες για τους χρήστες και να τις πουλήσουν σε εταιρείες Marketing.

Προσεχτικοί πρέπει να είμαστε και όταν στέλνουμε Μηνύματα της Στιγμής (Instant Messages) π.χ. με Google Talk ή με Microsoft Live Messenger. Πρέπει να γνωρίζουμε ότι πολλές από αυτές τις εταιρείες αυτόματα αποθηκεύουν τα μηνύματά μας, εκτός και εάν έχουμε κάνει τις ανάλογες ρυθμίσεις.
Κοινωνικά Δίκτυα όπως το Facebook και MySpace επιτρέπουν την αποστολή φωτογραφιών και την αποθήκευση προσωπικών σημειώσεων. Προσωπικές πληροφορίες που ανταλλάσσονται σε τέτοια δίκτυα μπορεί να προκαλέσουν προβλήματα του χρήστη με το σχολείο, τον εργοδότη του και όχι μόνο. Τέτοιες ιστοσελίδες δέχονται συχνά και με ευκολία επισκέψεις από παιδοφίλους που ενδιαφέρονται είτε να παραπλανήσουν ανήλικους σε πραγματικές συναντήσεις ή να κλέψουν φωτογραφίες και πληροφορίες που ανταλλάσσονται από άτομα που χρησιμοποιούν αυτά τα δίκτυα.

Ίχνη στο Διαδίκτυο είναι δυνατό να αφήσουμε και κατά τη χρήση ιστολογίων (Blog). Πολλοί νεαροί που χρησιμοποιούν το Διαδίκτυο, έχουν δημιουργήσει το δικό τους ιστολόγιο (Blog), κάτι σαν ενημερωτικό φυλλάδιο ή εφημερίδα, το οποίο ανανεώνεται συχνά και είναι για ελεύθερη πρόσβαση. Οι χρήστες των ιστολογίων μπορούν να καταθέσουν σχόλια. Σε κάποια από τα ιστολόγια χρειάζεται να κάνει κάποιος εγγραφή για να μπορεί να σχολιάσει, δίνοντας έτσι πληροφορίες όπως ηλεκτρονική διεύθυνση, όνομα κ.λπ.

2.2 Προσωπικά δεδομένα

Συναντάμε συχνά διάφορους ορισμούς σχετικά με το τι είναι τα «Προσωπικά δεδομένα». Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα προτείνει τον παρακάτω ορισμό: «Προσωπικά δεδομένα είναι κάθε πληροφορία που σε χαρακτηρίζει, όπως για παράδειγμα το όνομά σου, η διεύθυνσή σου, το τηλέφωνό σου, τα ενδιαφέροντά σου, οι επιδόσεις σου στο σχολείο, οι φωτογραφίες σου, οι απόψεις σου, κ.α. [...]. Μερικές φορές τα προσωπικά σου δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις, στην κατάσταση της υγείας σου ή στην ερωτική σου ζωή».

Η ανάγκη για την προστασία των προσωπικών μας δεδομένων ίσως δεν έχει γίνει κατανοητή από όλους μας. Αυτό συμβαίνει γιατί δεν έχουμε αντιληφθεί τους κινδύνους που δημιουργούνται για τα προσωπικά μας δεδομένα. Αυτοί οι κίνδυνοι μπορεί να προέλθουν είτε από λάθος χρήση, είτε από κακή πρόθεση κάποιου τρίτου, είτε και τα δύο μαζί.

Χαρακτηριστικό της ανάγκης προστασίας των προσωπικών δεδομένων είναι ότι η πολιτεία έχει δημιουργήσει ένα ξεχωριστό νομοθετικό πλαίσιο, που περιγράφει με σαφήνεια ποιες πληροφορίες και ποια δεδομένα προσωπικού χαρακτήρα μπορούν να χρησιμοποιηθούν από τρίτους. Πρόκειται για το Νόμο 2472/1997, με τίτλο «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Η ιδιωτικότητα της προσωπικής μας ζωής, στην καθημερινότητά μας, δεν συμπεριλαμβάνει μόνο τι κάνουμε στον πραγματικό κόσμο, αλλά και τι κάνουμε και πως φερόμαστε και στον κόσμο του διαδικτύου, όπου πλέον όλοι μας έχουμε ένα ψηφιακό αποτύπωμα.

Με τον όρο ψηφιακό αποτύπωμα αναφερόμαστε στο σύνολο των πληροφοριών που μπορεί να βρει κάποιος στο Διαδίκτυο για τον εαυτό μας:

- προσωπικές πληροφορίες (όνομα, επίθετο, περιοχή κατοικίας, ηλικία κ.α.)
- προτιμήσεις (π.χ. αγαπημένος τραγουδιστής)
- φωτογραφίες, βίντεο και
- πολλά άλλα δεδομένα που έχουμε μοιραστεί στα social media και διάφορες άλλες ιστοσελίδες.

Αυτό δεν το καταλαβαίνουμε εύκολα, ιδιαίτερα όταν είμαστε σε νεαρή ηλικία γιατί όταν καθόμαστε στον υπολογιστή μας (στο δωμάτιο μας) έχουμε την αίσθηση ότι είμαστε μόνοι μας. ΛΑΘΟΣ. Είμαστε μαζί με όλους εκείνους στους οποίους έχουμε επιτρέψει να παρακολουθούν (και να καταγράφουν) τις κινήσεις μας στο διαδίκτυο. Μη γνωρίζοντας αυτό, όταν είμαστε συνδεδεμένοι στο διαδίκτυο νιώθουμε μεγαλύτερη ασφάλεια και κάνουμε πράξεις όπως το να αποκαλύψουμε στοιχεία που στον πραγματικό κόσμο ποτέ δεν θα το κάναμε.

Στη συνέχεια για την καλύτερη κατανόηση, μπορούμε να δούμε δέκα ερωτήσεις με τις αντίστοιχες απαντήσεις σχετικά με την προστασία των προσωπικών δεδομένων, από τον ιστότοπο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

2.3 Διαδικτυακά εγκλήματα - Ιοί

Στην ηλεκτρονική αλληλογραφία (E-mail) το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του διαδικτύου παρέχει το πλεονέκτημα της οικονομικής και ταχύτατης επικοινωνίας με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο ενώ παράλληλα αποτελεί το συνηθέστερο τρόπο για τη μετάδοση ιών στα αρχεία και στα λογισμικά των υπολογιστών. Οι ιοί των υπολογιστών ξεκίνησαν αρχικά με σκοπό τη "φάρσα" μεταξύ των προγραμματιστών και τον έλεγχο της πειρατείας των προγραμμάτων. Σήμερα οι ιοί έχουν αλλάξει χρήση. Οι νέοι ιοί έχουν ως αντικείμενο την υποκλοπή, την κατασκοπεία, με σκοπό την αξιοποίηση στοιχείων και πληροφοριών για στρατιωτικούς ή και εγκληματικούς λόγους. Συνήθως υποκλέπτονται αριθμοί πιστωτικών καρτών και κωδικοί λογαριασμών (password).

Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο του αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής html) που ενεργοποιείται αυτόματα με την ανάγνωση του e-mail. Οι χρήστες θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς. Ενοχλητική αλληλογραφία (spam mail) Από τα πρώτα δυσάρεστα εμπόδια που κλήθηκαν (και καλούνται) να αντιμετωπίσουν οι χρήστες του Internet ήταν και είναι το spam mail. Τα τελευταία χρόνια, μάλιστα, έχει αποκτήσει και παρέα: τα διαδοχικά pop-up windows με διαφημιστικά banners, που αφαιρούν από το web τη βασική του γοητεία: την πλοήγηση.

Το λεγόμενο spam ή junk mail μπορεί να περιλαμβάνει: Ενοχλητικό ή και δυσάρεστο περιεχόμενο για τον παραλήπτη.

- Διαφημίσεις ιστοχώρων ή ενημερωτικά δελτία προώθησης προϊόντων ή
- υπηρεσιών.

Προειδοποιητικά μηνύματα: είτε ειδοποιούν το χρήστη για την ύπαρξη ιού ή

- άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες.

Περιεχόμενο συμπαράστασης: παρουσιάζουν κάποια υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται. Περιεχόμενο εκφοβισμού: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες. Συμβουλές προστασίας από τα spam mails στην ηλεκτρονική αλληλογραφία.

Ο χρήστης θα πρέπει να μην απαντάει σε μηνύματα τέτοιου είδους ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται μόνιμα, συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα. Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το Outlook Express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος. Επίσης, στο διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα e-mails προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Πρέπει να αλλάζει τακτικά ο κωδικός πρόσβασης στο λογαριασμό e-mail. Η "Απομνημόνευση του ID μου στον υπολογιστή" έτσι ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή. Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

2.4 Συμβουλές

Προσπάθησε να διατηρείς τον έλεγχο των προσωπικών σου δεδομένων:

- Ρώτα γιατί είναι απαραίτητα τα δεδομένα σου – Σκέψου ποιος είναι αυτός που τα ζητάει. Είναι κάποιος που εμπιστεύεσαι; Πώς πρόκειται να τα χρησιμοποιήσει; Θα τα αποστείλει σε άλλους και, αν ναι, σε ποιους; Αν δεν είσαι σίγουρος για κάτι από όλα αυτά, ρώτα και μάθε πριν διαθέσεις πληροφορίες που σε αφορούν.
- Σκέψου πριν αποκαλύψεις δεδομένα – Αν λαμβάνεις γράμματα, e-mails, μηνύματα στο κινητό ή στο Facebook που σου ζητούν πληροφορίες, μην απαντήσεις αν δεν είσαι σίγουρος από ποιον προέρχονται.
- Διάβαζε προσεκτικά τα «ψιλά γράμματα» - Κάποιες εταιρείες μπορεί να γράφουν εκεί όρους για την χρησιμοποίηση των δεδομένων σου, π.χ. για διαφημιστικούς σκοπούς. Θυμήσου ότι πρέπει πάντα να δίνεις τη συγκατάθεσή σου γι' αυτό.
- Διάβαζε την πολιτική ιδιωτικότητας στις ιστοσελίδες που επισκέπτεσαι – μάθε πώς χρησιμοποιούν τα δεδομένα σου, π.χ. αν εγκαθιστούν αρχεία cookies και αν προωθούν τις πληροφορίες που σε αφορούν σε διαφημιστικές εταιρείες.
- Εμπιστεύσου το ένστικτό σου – Αν δεν είσαι σίγουρος για την ασφάλεια μιας ιστοσελίδας ή δεν νιώθεις άνετα με τον τρόπο που πρόκειται να χρησιμοποιηθούν τα προσωπικά σου δεδομένα, προτίμησε κάποια άλλη.
- Δυσκόλεψε τους**…** «κακούς» – Χρησιμοποίησε διαφορετικά συνθηματικά στους λογαριασμούς σου (π.χ. e-mail, Facebook, Twitter). Διάλεξε συνθηματικά που είναι εύκολο για σένα να θυμάσαι, αλλά δύσκολο για τους άλλους να μαντέψουν.
- Σκέψου ποιος μπορεί να βλέπει τα δεδομένα σου – Μην επισκέπτεσαι ιστοσελίδες που δεν θα ήθελες οι άλλοι να γνωρίζουν όταν μοιράζεσαι τον υπολογιστή σου με άλλους.
- Σκέψου πριν αγοράσεις στο διαδίκτυο – Χρησιμοποίησε ασφαλείς ιστοσελίδες, στις οποίες φαίνονται καθαρά τα στοιχεία επικοινωνίας της εταιρείας και οι οποίες διαθέτουν πολιτική ιδιωτικότητας. Έλεγχε αν είναι ασφαλές το κανάλι επικοινωνίας (π.χ. θα πρέπει η διεύθυνση της σελίδας να ξεκινάει με https και στο πρόγραμμα πλοήγησης στο διαδίκτυο να εμφανίζεται ένα λουκέτο ως εικονίδιο).
- Θυμήσου να αποσυνδέεσαι από τις ιστοσελίδες, στις οποίες έχεις εισέλθει/συνδεθεί με χρήση συνθηματικών (π.χ. όταν κάνεις αγορές από το διαδίκτυο ή την ιστοσελίδα κοινωνικής δικτύωσης).

- Όταν δημοσιεύεις πληροφορίες που σε αφορούν στο διαδίκτυο προσπάθησε να προστατεύεις τα προσωπικά σου δεδομένα και να μην ανακοινώνεις σε όλο τον κόσμο αυτά που δεν θα έλεγες σε κάποιον αν τον είχες πρόσωπο με πρόσωπο! Να θέτεις στον εαυτό σου τις ίδιες ερωτήσεις όπως αυτές που θέτεις στον «πραγματικό κόσμο»: θα ήθελες αυτές τις πληροφορίες να τις μάθουν όλοι οι φίλοι σου, οι καθηγητές σου, οι γονείς σου;
- Να συνειδητοποιήσεις ότι δεν είσαι ο κυρίαρχος των πληροφοριών που δημοσιεύεις στο διαδίκτυο. Οπότε ο καλύτερος τρόπος να προστατευτείς είναι να προσέχεις τι δημοσιεύεις.
- Να διαβάζεις προσεχτικά τους «όρους χρήσης» πριν εγγραφείς ή πριν «ανεβάσεις» πληροφορίες σε ιστοσελίδες, ηλεκτρονικά φόρα, ιστολόγια, ή υπηρεσίες κοινωνικής δικτύωσης. Μπορεί να σου φαίνεται «βαρετό», αλλά είναι πολύ σημαντικό!
- Να «μετράς τα λόγια σου» σε ιστολόγια, ηλεκτρονικά φόρα, κοινωνικά δίκτυα, κτλ. Φρόντισε να διατυπώνεις τα μηνύματά σου με τρόπο που να γίνονται κατανοητά και εκτός του πλαισίου συζήτησης (π.χ αν αστειεύεσαι για κάτι, να το λες καθαρά!). Προσπάθησε να διατηρείς ένα σωστό επίπεδο στη γλώσσα που χρησιμοποιείς χωρίς υβριστικά σχόλια για τους υπόλοιπους χρήστες. Αν είσαι διαχειριστής μιας τέτοιας ιστοσελίδας, ενημέρωσε σχετικά τους «συντάκτες» σου.
- Να αποφεύγεις να δημοσιεύεις φωτογραφίες σου ή βίντεο που θα μπορούσαν να γίνουν «ενοχλητικά».
- Να μην δημοσιεύεις περιεχόμενα που μπορεί να ενοχλήσουν κάποιον, ούτε φωτογραφίες και βίντεο χωρίς έγκριση. Σε περίπτωση αμφιβολίας, προσπάθησε να μπεις στη θέση αυτού του προσώπου και να φανταστείς τις συνέπειες... Σκέψου πόσο εύκολο είναι να γίνεις από «θύτης» «θύμα»...
- Να επαληθεύεις τακτικά τι είναι δημοσιευμένο στο διαδίκτυο σχετικά με εσένα (π.χ. βάλε το ονοματεπώνυμο σου σε μια μηχανή αναζήτησης για να δεις τι πληροφορίες θα «φέρειγια εσένα).
- Να χρησιμοποιείς εάν είναι δυνατόν ένα ψευδώνυμο κατά την εγγραφή σου σε ιστοσελίδες και ηλεκτρονικά φόρα που θα το επικοινωνείς μόνο σε κοντινούς σου ανθρώπους.

ΚΕΦΑΛΑΙΟ 3 : Ηλεκτρονικές συναλλαγές

3.1 Στις ηλεκτρονικές συναλλαγές με τις τράπεζες (Phishing)

Το ηλεκτρονικό "ψάρεμα" είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά ηλεκτρονικά μηνύματα. Μπορούν να οδηγήσουν στην κλοπή των αριθμών πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών λογαριασμών ή άλλων προσωπικών δεδομένων. Ο εγκληματίας κλέβει τα προσωπικά σας στοιχεία, αναλαμβάνει την ταυτότητά σας και μπορεί να εκδώσει: Να κάνει αίτηση και να εκδώσει πιστωτικές κάρτες στο όνομά σας.

Να αδειάσει τον τραπεζικό σας λογαριασμό και να χρησιμοποιήσει τις πιστωτικές σας κάρτες στο μέγιστο όριο. Να μεταφέρει χρήματα από το λογαριασμό όψεως στο λογαριασμό ταμιευτηρίου και να χρησιμοποιήσει αντίγραφο της κάρτας αναλήψεων για να βγάλει χρήματα από το λογαριασμό σας σε μηχανήματα ATM σε όλο τον κόσμο.

Συμβουλές προστασίας από το ηλεκτρονικό ψάρεμα (Phishing):

Σε κάθε εισαγωγή του χρήστη στο πληροφοριακό σύστημα της τράπεζας με την οποία συναλλάσσεται, ο ενδιαφερόμενος πρέπει να βεβαιώνεται ότι έχει συνδεθεί με τον πραγματικό δικτυακό τόπο (site) της τράπεζας. Αυτό γίνεται με το ψηφιακό πιστοποιητικό ασφαλείας που έχει προμηθευτεί η τράπεζα και το οποίο πιστοποιεί ότι τα προγράμματα που μεταφέρονται στο σταθμό του χρήστη είναι τα γνήσια που έχουν εκπονηθεί από την τράπεζα, γεγονός που επιβεβαιώνεται με την ύπαρξη των παραπάνω ψηφιακών πιστοποιητικών. Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο στο κάτω μέρος της οθόνης για όσο χρονικό διάστημα ο χρήστης χρησιμοποιεί την εφαρμογή υποδεικνύει πως η τοποθεσία web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών του. Όμως, το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο. Για να διασφαλίσετε τη γνησιότητά του, κάντε διπλό κλικ, ώστε να διαπιστώσετε αν υπάρχει το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το "Issued to" (εκδόθηκε για) θα πρέπει να αντιστοιχεί στο όνομα της τοποθεσίας. Εάν το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως "spoofed" (πλαστή). Σε περίπτωση που δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο, μην εισαγάγετε προσωπικά δεδομένα.

3.2 Στην παραπλάνηση σε ψεύτικες ιστοσελίδες (Pharming)

Απάτη με pharming (παραπλάνηση): ανακατεύθυνση του browser σε ψεύτικες ιστοσελίδες. Η κίνηση του διαδικτύου ανακατευθύνεται από μία τοποθεσία σε μία άλλη πανομοιότυπη, "Pharming" σημαίνει ότι εγκληματίες χάκερ ανακατευθύνουν την κίνηση του διαδικτύου από μία ιστοσελίδα σε μια άλλη, πανομοιότυπη, έτσι ώστε να σας ξεγελάσουν και να καταχωρίσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής ιστοσελίδας. Ιστοσελίδες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να αποκτήσουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας. Αυτό επιτυγχάνεται με τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS", κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση.

Συμβουλές προστασίας από το Pharming:

Με τη χρήση του λογισμικού firewall (τείχος προστασίας), που με κατάλληλες ρυθμίσεις επιτρέπει ή απορρίπτει πακέτα δεδομένων. Τα firewall τελευταίας γενιάς έχουν ενσωματωθεί στα λειτουργικά συστήματα. Με την αναζήτηση ψηφιακού πιστοποιητικού ασφαλείας. Καλύτερα να πληκτρολογούμε την ηλεκτρονική διεύθυνση στον browser παρά να οδηγούμαστε σε αυτή με χρήση βοηθητικών links.

Ο χρήστης πρέπει αν ελέγχει το αν το κυρίως μήνυμα είναι εικόνα, με σκοπό να αποφευχθεί ο εντοπισμός τους από τα φίλτρα ανεπιθύμητης αλληλογραφίας. Αυτό μπορείτε να το καταλάβετε εύκολα αν τοποθετήσετε το δείκτη του ποντικιού στο κυρίως μήνυμα, ο δείκτης θα μετατραπεί σε χεράκι.

3.3 Στις αγγελίες για την ανεύρεση εργασίας (Scam)

Αυτές οι ψεύτικες αγγελίες για την εύρεση εργασίας γίνονται όλο και πιο κομψές και συχνά χρησιμοποιούν συνηθισμένη εικόνα ή πειστικά εταιρικά λογότυπα και φρασεολογία. Πολλές φορές διαθέτουν και συνδέσμους προς πλαστές ιστοσελίδες, που εμφανίζονται ως τοποθεσίες

πραγματικών εταιρειών. Επιπλέον κάποιες φορές ακόμα χρεώνουν για υπηρεσίες που δε θα παράσχουν ποτέ. Έπειτα από μερικές μέρες, οι κλέφτες κλείνουν το scam και εξαφανίζονται.

Συμβουλές προστασίας από το Scam:

Ποτέ μη δίνετε κανένα προσωπικό στοιχείο που δε σχετίζεται με τη δουλειά (όπως στοιχεία ταυτότητας, τον αριθμό φορολογικού μητρώου, τον αριθμό της πιστωτικής σας κάρτας, την ημερομηνία γέννησης και την οικογενειακή σας κατάσταση)στο διαδίκτυο, μέσω e-mail. Να δημοσιεύσετε το βιογραφικό σας μόνο σε ιστοσελίδα εύρεσης εργασίας που εφαρμόζει πολιτική προστασίας προσωπικών δεδομένων και επιτρέπει την πρόσβαση από τον εξωτερικό κόσμο στα βιογραφικά αποκλειστικά σε πιστοποιημένα γραφεία εύρεσης εργασίας. Να διασταυρώνετε τα στοιχεία κάθε ενδεχόμενου εργοδότη, επαγγελματία ή γραφείου εύρεσης εργασίας. Ο καλύτερος τρόπος για να εξακριβώσετε τα στοιχεία ενός ενδεχόμενου εργοδότη είναι να επισκεφθείτε τα γραφεία της αντίστοιχης εταιρείας, σε ώρες εργασίας. Να μην εμπιστεύεστε όσους σας ζητούν χρήματα εκ των προτέρων για να σας βρουν δουλειά. Ποτέ μη δεχθείτε να πληρώσετε για "αποκλειστικές" πληροφορίες σχετικά με θέσεις εργασίας ή για να πάρετε κάποια συγκεκριμένη θέση. Στην περίπτωση όμως που πληρώσετε για υπηρεσίες εύρεσης εργασίας, μη δώσετε τα στοιχεία της πιστωτικής σας κάρτας ή του τραπεζικού σας λογαριασμού. Να αξιολογείτε προσεκτικά τα στοιχεία επαφής που δίνονται σε αγγελίες εργασίας ή σε σχετικά e-mail και να προσέχετε εάν υπάρχουν ανορθογραφίες, κάποια διεύθυνση e-mail που δεν αναφέρει το όνομα της εταιρείας ή εάν η περιοχή ή ο ταχυδρομικός κώδικας δεν είναι παντού τα ίδια. Να πληκτρολογείτε τις διευθύνσεις των ιστοσελίδων (URL) στο browser αντί να χρησιμοποιείτε links. Να δημιουργήσετε διεύθυνση ηλεκτρονικού ταχυδρομείου και έναν ξεχωριστό λογαριασμό για όλες τις μη προσωπικές επικοινωνίες. Εάν κάποια ευκαιρία υπόσχεται υπερβολικά πολλά ή κάτι άλλο δε φαίνεται σωστό, μάλλον πρόκειται για παραπλανητικό μήνυμα.

3.4 Στα ηλεκτρονικά ημερολόγια (Blogs)

Η πρακτική του blogging, η τήρηση προσωπικού ημερολογίου στο Διαδίκτυο, μεγαλώνει δραματικά, ειδικά ανάμεσα στους εφήβους, οι οποίοι ορισμένες φορές διατηρούν ημερολόγια blog χωρίς να το γνωρίζουν οι γονείς ή οι κηδεμόνες τους. Σύμφωνα με κάποιες πρόσφατες μελέτες, τα μισά από τα ημερολόγια blog σήμερα δημιουργούνται από εφήβους από τους οποίους δύο στους τρεις δημοσιοποιούν την ηλικία τους, τρεις στους πέντε αποκαλύπτουν την τοποθεσία όπου κατοικούν και έναν στους πέντε να αποκαλύπτει το πλήρες όνομά του. Αυτό

συμβαίνει χωρίς να λέγεται ότι υπάρχουν πιθανοί κίνδυνοι από τη δημοσιοποίηση αυτού του τύπου προσωπικών λεπτομερειών. Και καθώς πολλά νεαρά άτομα δημιουργούν όλο και περισσότερα ημερολόγια blog, οδηγούνται σε έναν αυξανόμενο ανταγωνισμό μεταξύ τους για να τραβήξουν την προσοχή. Μερικές φορές αυτό μπορεί να τα οδηγήσει να δημοσιεύσουν ακατάλληλο υλικό, όπως προκλητικές εικόνες των εαυτών τους ή των φίλων τους.

Συμβουλές προστασίας για τα Blogs:

Καθιερώστε κανόνες για τη χρήση του διαδικτύου, αν η χρήση γίνεται κυρίως από νεαρά άτομα. Σχολαστικός έλεγχος και επιμέλεια για το περιεχόμενο πριν το δημοσιεύσουμε. Πληροφορίες που πιθανόν φαίνονται ακίνδυνες, όπως το σήμα ή το όνομα του σχολείου ή οι φωτογραφίες της πόλης, μπορούν, με κατάλληλους συνδυασμούς, να φανούν χρήσιμες σε επιτήδειους. Δοκιμάστε την υπηρεσία δημιουργίας ημερολόγιων blog και βρείτε εάν προσφέρει ιδιωτικά ημερολόγια με προστασία κωδικού πρόσβασης. Επισκεφθείτε το ημερολόγιο του παιδιού σας συχνά και επιθεωρήστε το. Επισκεφθείτε άλλα ημερολόγια για να βρείτε καλά παραδείγματα ώστε να τα υιοθετήσουν τα παιδιά σας. Μην παρέχετε ποτέ προσωπικές πληροφορίες, όπως επώνυμο, πληροφορίες επικοινωνίας, διεύθυνση κατοικίας, αριθμούς τηλεφώνων, όνομα σχολείου, ηλεκτρονική διεύθυνση, επώνυμο φίλων ή συγγενών, όνομα άμεσης επικοινωνίας, ηλικία ή ημερομηνία γέννησης. Μη δημοσιεύετε ποτέ προκλητικές φωτογραφίες του εαυτού σας ή κάποιων άλλων και βεβαιωθείτε πως όποια φωτογραφία δημοσιεύεται δεν αποκαλύπτει κάποιες προσωπικές πληροφορίες. Θεωρήστε πως ό,τι δημοσιεύεται στο διαδίκτυο είναι μόνιμο. Οποιοσδήποτε μπορεί να εκτυπώσει ένα ημερολόγιο ή να το αποθηκεύσει στον υπολογιστή του. Χρησιμοποιήστε τοποθεσίες παροχής ημερολογίων blog με ξεκάθαρους όρους χρήσης και βεβαιωθείτε πως μπορείτε να προστατέψετε με κωδικό πρόσβασης και τα ενεργά ημερολόγια blog και όχι μόνο τους λογαριασμούς. (Εάν όχι, είναι καλύτερο να θεωρήσετε πως οποιοσδήποτε μπορεί να το δει.)

Αποφεύγετε να υπερβάλλετε ή να ανταγωνίζεστε με άλλους δημιουργούς ημερολογίων (bloggers). Διατηρήστε τα ημερολόγια blog θετικά και μην τα χρησιμοποιείτε για να δυσφημήσετε ή να επιτεθείτε σε άλλους.

3.5 Στην άμεση συνομιλία των chat

Το chat στο διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται "δωμάτιο επικοινωνίας" (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές επειδή βρίσκεται στον φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός internet cafe, μπορεί να μετατρέψει αυτό τον τρόπο της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν επισημανθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίστηκαν, έπεσαν θύματα παιδόφιλων ή κυκλωμάτων παιδικής πορνογραφίας ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας.

Προέχει σωστή ενημέρωση για αυτό τον τρόπο επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι η έλλειψη γνώσεων σχετικά τόσο από τους γονείς όσο και από τους εκπαιδευτικούς.

3.6 Στο διαμοιρασμό αρχείων.

Είναι η δυνατότητα που προσφέρει το διαδίκτυο στους χρήστες του να διαμοιράζονται αρχεία κάθε είδους. Πραγματοποιείται με προγράμματα (ελεύθερα ή με πληρωμή) όπως τα εξής: Προγράμματα για Windows: KaZaa, Limewire, Morpheus, SwapNut,WinMX. Καθένα από τα ανωτέρω προγράμματα λειτουργεί έτσι ώστε να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή σε όλους χρήστες, οι οποίοι είναι συνδεδεμένοι στο διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα. Επομένως κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία στον δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας σύγχρονη επικοινωνία μεταξύ υπολογιστών, γι’

αυτό τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης (peer-to-peer). Η ευρύτατη χρήση της δυνατότητας αυτής του διαδικτύου οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείου (μουσικής, εικόνων, προγραμμάτων), με μηδαμινό κόστος για το χρήστη. Η συγκέντρωση των ταυτόχρονα διασυνδεδεμένων χρηστών σε κάθε τέτοιο πρόγραμμα διαμοιρασμού αρχείων ανέρχεται σε μερικά εκατομμύρια. Δημιουργούνται έτσι μερικές από τις μεγαλύτερες διαδικτυακά πληθυσμιακές κοινότητες, μέσα στις οποίες διακινείται σχεδόν ανεξέλεγκτα κάθε είδους υλικό.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- http://docplayer.gr/10945204-Asfaleia-dedomenon-stin-koinonia-tis-pliroforias-idiotikotita.html
- http://internet-safety.sch.gr/index.php/component/k2/item/256-kdks
- Πηγή: Νορβηγική Αρχή Προστασίας Δεδομένων
- http://www.ekped.gr/praktika10/web/169.pdf
- Πηγή: http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL
- http://www.kathimerini.gr/836171/article/oikonomia/ellhnikh-oikonomia/apoyh-prostasia-dedomenwn-idiwtikothta-kai-asfaleia-sto-diadiktyo