1ο ΣΧΟΛΕΙΟ ΔΕΥΤΕΡΗΣ ΕΥΚΑΙΡΙΑΣ ΤΡΙΚΑΛΩΝ

Υιοθετώντας Ψηφιακή Συνείδηση

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΣΥΝΤΟΝΙΣΤΕΣ:

ΚΑΤΣΙΚΑΣ ΝΙΚΟΛΑΟΣ
ΔΙΕΥΘΥΝΤΗΣ 1^{ΟΥ} Σ.Δ.Ε. ΤΡΙΚΑΛΩΝ
ΓΟΥΓΑΣ ΒΑΣΙΛΕΙΟΣ
ΕΚΠΑΙΔΕΥΤΗΣ
ΠΛΗΡΟΦΟΡΙΚΟΥ ΓΡΑΜΜΑΤΙΣΜΟΥ

Το παρόν εγχειρίδιο αποτελεί το τελικό προϊόν ενός Project με τίτλο: «Υιοθετώντας Ψηφιακή Συνείδηση», που υλοποιήθηκε κατά το Α΄ Τετράμηνο του σχολικού έτους 2012 – 2013. Η παρουσίαση του εν λόγω Project πραγματοποιήθηκε στην αίθουσα πολλαπλών χρήσεων του σχολείου, στις 05/02/2013, στο πλαίσιο της Ημέρας Ασφαλούς Διαδικτύου.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Η Ημέρα Ασφαλούς Διαδικτύου (Safer Internet Day) εορτάστηκε για πρώτη φορά το 2004 με πρωτοβουλία του έργου SafeBorders και του προγράμματος πλαισίου Safer Internet της Ε.Ε. Έκτοτε διοργανώνεται κάθε 2η ημέρα της 2ης εβδομάδας του 2ου μήνα του έτους από το Πανευρωπαϊκό Δίκτυο Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης INSAFE στο πρόγραμμα Safer Internet της Ε.Ε., εκπρόσωπος του οποίου στην Ελλάδα είναι η Δράση Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου. Θεσμοθετήθηκε για την ευαισθητοποίηση μικρών και μεγάλων στα θέματα που αφορούν την ασφαλή και ηθικά σωστή χρήση του Διαδικτύου, του κινητού τηλεφώνου και όλων των διαδραστικών τεχνολογιών, οι οποίες, πλέον, αποτελούν τμήμα της καθημερινότητάς μας.

Η επικοινωνία με άλλα άτομα στο Διαδίκτυο είναι συναρπαστική, ιδιαίτερα για τους νέους ανθρώπους. Μέσω των δυνατοτήτων που μας παρέχει, ανοίγεται ένας ολόκληρος κόσμος γνωριμίας με άλλες χώρες, άλλες γλώσσες, άλλους πολιτισμούς και άλλες εμπειρίες, τις οποίες μπορούμε να μοιραστούμε. Είναι σημαντικό να έχουμε πάντα υπόψη ότι η δραστηριοποίησή μας στο Διαδίκτυο έχει πολλά κοινά με τη ζωή μας στο φυσικό κόσμο. Και εδώ τίθεται το ζήτημα τόσο της προστασίας των προσωπικών μας δεδομένων, όσο και της ορθής και ηθικής επικοινωνίας με τη βοήθεια της τεχνολογίας, καθώς ότι και αν κάνουμε στο Διαδίκτυο (Internet) αφήνει ίχνη.

Χάρη στα δίκτυα εισαγόμαστε σ' ένα είδος παγκοσμίου και πολύμορφου διαλόγου, χωρίς εμφανή όρια ή περιορισμούς, εκτός από αυτούς που εμείς οι ίδιοι επιβάλλουμε στους εαυτούς μας. Ένα μεγάλο μέρος του χρόνου που χρησιμοποιείται στο διαδίκτυο αφορά ομαδικές συσκέψεις, εναλλακτικές συζητήσεις και φόρουμ γύρω από κάθε είδους θέματα. Ωστόσο, είναι αυτή ακριβώς η ανωνυμία και η πρόσβαση παντού που κάνει πολλούς από τους χρήστες του να συμπεριφέρονται όπως οι ραδιοπειρατές στο παρελθόν και να κυκλοφορούν στον κυβερνοχώρο σε αναζήτηση μακρινών και άγνωστων συνομιλητών, που τους προτείνουν από ερωτικά ραντεβού ως δοκιμές κρασιών, περνώντας από την πρόσβαση σε κυβερνητικές βιβλιοθήκες, σε τραγούδια ή σε αρχεία Πανεπιστημίων. Έτσι δημιουργείται η ανατριχιαστική δυνατότητα καταστροφής της προσωπικής ζωής κατά τρόπο ανεπίστρεπτο, που δεν έχει προηγούμενο.

Κατά την πλοήγηση στους χώρους του Διαδικτύου είναι καλό να έχουμε υπόψη μας τα παρακάτω:

- Το Διαδίκτυο είναι κυρίως μια κοινωνία ανθρώπων και κρύβει τους ίδιους κινδύνους που κρύβει κάθε κοινωνία, ιδιαίτερα όταν

διευκολύνεται στο έπακρο ο τρόπος επικοινωνίας των ανθρώπων μεταξύ τους

- Οι πληροφορίες που παρουσιάζονται στο Διαδίκτυο δεν είναι πάντα έγκυρες
- Η κοινοποίηση των προσωπικών στοιχείων του χρήστη (ονοματεπώνυμο, διεύθυνση, τηλέφωνο, φωτογραφία, κωδικοί πρόσβασης, αριθμός πιστωτικών καρτών, e-mail κ.λπ.) είναι καλό να αποφεύγεται
- Η τοποθέτηση του υπολογιστή (εάν είναι δυνατόν) σε κοινόχρηστο χώρο και όχι αποκλειστικά στο παιδικό δωμάτιο ενθαρρύνει τη χρήση του Διαδικτύου σε οικογενειακό περιβάλλον και βοηθά στην επίβλεψη των ιστοσελίδων τις οποίες επισκέπτονται τα παιδιά
- Η καλή επικοινωνία με τα παιδιά είναι απαραίτητη ώστε να ενθαρρύνονται να μιλάνε για αυτούς με τους οποίους επικοινωνούν, ανταλλάσσουν μηνύματα και να ενημερώνουν εάν ποτέ γίνονται θύματα απειλών, εκφοβισμού ή παρενόχλησης οποιασδήποτε μορφής
- Η χρήση του υπολογιστή ως μέσου απασχόλησης του παιδιού χωρίς την παρουσία ενηλίκου είναι καλό να αποφεύγεται. Ο υπολογιστής δεν πρέπει να χρησιμοποιείται ως ηλεκτρονική νταντά (babysitter) !!!
- Η δημιουργία ενός συνόλου από κανόνες χρήσης του Η/Υ αποδεκτών από όλους και η ανάρτηση τους σε εμφανές σημείο δίπλα στον υπολογιστή συντελεί στην προστασία όλων των χρηστών
- Στη διεύθυνση http://www.safeline.gr/ έχουμε ίσως τη μοναδική ελληνική ανοικτή γραμμή για καταγγελία παράνομου περιεχομένου στο διαδίκτυο. Μη διστάσετε να τη χρησιμοποιήσετε

2. ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ

Στο πλαίσιο της ορθής και ηθικής επικοινωνίας με τη βοήθεια της τεχνολογίας, κινούνται οι γνώστες σε όλους μας ιστοσελίδες κοινωνικής δικτύωσης (social media - όπως είναι παράδειγμα το Facebook, Myspace κ.α.) που αποτελούν μέρος της καθημερινής συνήθειας των σημερινών ανθρώπων. Στις ιστοσελίδες αυτές, οι χρήστες μέσα από τα εικονικά τους προφίλ λειτουργούν διαδραστικά με άλλους χρήστες, δημοσιεύουν τις φωτογραφίες και τα βίντεό τους, γίνονται μέλη σε ομάδες κοινών ενδιαφερόντων (groups), δημοσιεύουν και ανταλλάσουν τις καλλιτεχνικές

τους δημιουργίες (μουσική, εικαστικά έργα κ.λπ.), επισκέπτονται σελίδες άλλων χρηστών και χρησιμοποιούν πλήθος εφαρμογών (κουίζ, παιχνίδια, κ.λπ.). Επιπλέον επιτρέπει στους χρήστες να δημιουργούν οι ίδιοι περιεχόμενο στο Διαδίκτυο και να το μοιράζονται με άλλους χρήστες, δίχως να έχουν εξειδικευμένες τεχνικές γνώσεις.

Όπως ισχύει σε κάθε μορφή ηλεκτρονικής επικοινωνίας, έτσι και στους ιστοχώρους (κοινωνικής δικτύωσης αλλά και όχι μόνο – π.χ. ενημερωτικοί), **η γνώση θεμελιωδών κανόνων** ασφάλειας και **η ανάπτυξη κριτικής σκέψης** είναι καθοριστικοί παράγοντες στην προστασία από κακόβουλους ανθρώπους, απατεώνες ή ακόμα και από ασυνείδητους επιχειρηματίες, ώστε η απόλαυση των άπειρων παρεχόμενων δυνατοτήτων ψυχαγωγίας, επικοινωνίας και διασκέδασης να είναι αδιάλειπτη. Μέσω των ιστοσελίδων κοινωνικής δικτύωσης εύκολα και απλά μπορούν να δημιουργηθούν τεράστιες βάσεις προσωπικών δεδομένων και προτιμήσεων από τις πληροφορίες που δημοσιεύονται στα προφίλ των χρηστών αλλά και από τη γενικότερη δραστηριότητά τους στην ιστοσελίδα. Τα στοιχεία αυτά είναι δυνατό να χρησιμοποιηθούν με πολλούς τρόπους. Επομένως ο χρήστης με κριτική σκέψη θα πρέπει να προβεί στην δημοσιοποίηση των πληροφοριών που επιθυμεί.

3. ΕΜΦΑΝΙΖΟΜΕΝΟΙ ΚΙΝΔΥΝΟΙ

Οι κίνδυνοι που μπορεί να συναντήσει ο χρήστης από την χρήση των social media, του ηλεκτρονικού ταχυδρομείου και γενικότερα του Παγκόσμιου Ιστού (www) είναι οι ακόλουθοι:

- Αποπλάνηση (grooming): Είναι η διαδικασία κατά την οποία, παιδόφιλοι, προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν τα δωμάτια ανοιχτής επικοινωνίας (chat-rooms), τις ιστοσελίδες κοινωνικής δικτύωσης και άλλους χώρους διαδικτυακής επικοινωνίας για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Συχνά τέτοιου είδους ιστοχώροι **θεωρούνται από τα παιδιά ασφαλείς τόποι** συνομιλίας στο Διαδίκτυο, τόσο **εξαιτίας της δημόσιας φύσης της συζήτησης**, αλλά και της **λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους**. Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες. Οι συζητήσεις μπορεί να διαρκέσουν ημέρες, εβδομάδες, ακόμη και μήνες, μέχρι ο παιδόφιλος να αποκτήσει την εμπιστοσύνη του παιδιού.

- Παρενόχληση (***cyberbullying***): Είναι η επιθετική συμπεριφορά από πρόθεση με τη χρήση ηλεκτρονικών μέσων. Τέτοιου είδους συμπεριφορές μπορεί να κάνουν τα νέα άτομα να νιώθουν μοναχικά, δυστυχή και φοβισμένα, να αισθάνονται ανασφαλή και να πιστεύουν ότι κάτι δεν πάει καλά. Χάνουν την εμπιστοσύνη στον εαυτό τους και μπορεί να μην θέλουν να ξαναπάνε στο σχολείο ή να θέλουν να απομονωθούν από τις παρέες τους. Επιπλέον, σε ακραίες περιπτώσεις η συνεχής, επίμονη και έντονη παρενόχληση έχει οδηγήσει σε τρομερές συνέπειες όπως η πρόθεση για αυτοκτονία. Περιστατικά παρενόχλησης μεταξύ παιδιών και εφήβων μπορούν να συμβούν με πολύ διαφορετικές μορφές. Δεν εκδηλώνονται μόνο μέσω καυγάδων και επιθετικότητας, αλλά και μέσω διαφορετικών τύπων εκφοβισμού που αφήνουν το θύμα εκτεθειμένο.
- Κλοπή Ταυτότητας (Ηλεκτρονικής): Κλοπή ταυτότητας στο Διαδίκτυο ονομάζεται η πρακτική του να χρησιμοποιεί κανείς την εικονική ταυτότητα ενός άλλου ατόμου, δηλαδή να χρησιμοποιεί το όνομα χρήσης (username) και τον κωδικό πρόσβασης (password) του ατόμου αυτού σε διάφορες διαδικτυακές υπηρεσίες, υποδύοντας έτσι το άτομο αυτό. Σκοπός όσων επιχειρούν κλοπή ταυτότητας μπορεί να είναι η **οικονομική εξαπάτηση** αλλά και ο **εξευτελισμός ή η διάδοση φημών** για ένα άτομο στο διαδικτυακό του περιβάλλον. Οι συνέπειες και φυσικά οι εκπλήξεις, με τις οποίες μπορεί κανείς να έρθει αντιμέτωπος, είναι πολλαπλές. Μπορεί κανείς να συναντήσει άπρεπα ή προσβλητικά μηνύματα που στέλνονται εξ ονόματός του, σχόλια σε blogs και fora. Η κλοπή ταυτότητας τις περισσότερες φορές πραγματοποιείται κατά κύριο λόγο στις **υπηρεσίες κοινωνικής δικτύωση**ς και γενικά στις εφαρμογές και τα εικονικά περιβάλλοντα στα οποία επικοινωνούν με τους ηλεκτρονικούς τους φίλους. Μπορεί, λοιπόν, κανείς να σφετεριστεί την ταυτότητα ενός ατόμου, είτε **υποκλέπτοντας τους κωδικούς πρόσβασης** όπως αναφέραμε παραπάνω, είτε **ανοίγοντας ένα ψευτικό προφίλ / λογαριασμό** με το όνομα του άλλου ατόμου. Έτσι, πίσω από την κλεμμένη αυτή ταυτότητα, μπορεί να επικοινωνήσει με φίλους του ατόμου αυτού και να αναρτήσει φωτογραφίες και άλλο οπτικοακουστικό υλικό με σκοπό τον εξευτελισμό του ατόμου αυτού ή και τρίτων στο περιβάλλον του.
- Επεξεργασία Φωτογραφιών: Όταν δημοσιεύετε υλικό ή πληροφορία με τη ρύθμιση ορατό σε όλους σημαίνει ότι επιτρέπεται στον καθένα

συμπεριλαμβανομένων και χρηστών ΕΚΤΟΣ της πλατφόρμας να έχει πρόσβαση και να χρησιμοποιεί τις πληροφορίες αυτές και να τις συνδέουν με το όνομα και την εικόνα προφίλ του χρήστη που τις δημοσιεύει. Επίσης υπάρχει η δυνατότητα της επεξεργασίας των εικόνων καθώς και η δημιουργία φωτομοντάζ.

- Spam: Το λεγόμενο spam ή junk mail είναι μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ. ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων. Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα 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, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.
- Phishing: Πρόκειται για ιδιαίτερα διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» προσωπικών δεδομένων και ειδικότερα στοιχείων που αφορούν οικονομικές συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας κ.λπ.). Κάποια γνωστή τράπεζα, οργανισμός, τηλεπικοινωνιακός πάροχος ή άλλη νόμιμη εταιρεία εμφανίζεται ως αποστολέας ηλεκτρονικού μηνύματος που ενημερώνει τους παραλήπτες του για την ύπαρξη κενών ασφαλείας σε κάποιο λογαριασμό ή συνδρομή. Μέσα στο κείμενο παρατίθεται και ένας σύνδεσμος προς πλαστή ιστοσελίδα, η οποία πλασάρεται ως η επίσημη ιστοσελίδα του αποστολέα. Πηγαίνοντας στην ιστοσελίδα αυτή, το θύμα καλείται να συμπληρώσει τα στοιχεία του π.χ. για να μην κλειστεί ο λογαριασμός του. Την ίδια ώρα αυτοί που κρύβονται πίσω από το ψεύτικο μήνυμα αποκτούν πρόσβαση στα στοιχεία αυτά και στη συνέχεια μπορούν να κάνουν ηλεκτρονικές απάτες εις βάρος του πραγματικού ιδιοκτήτη αυτών των στοιχείων.
- Ιοί (virus): Είναι ένα κακόβουλο πρόγραμμα το οποίο γραμμένο αποκλειστικά για να αλλάζει τον τρόπο με τον οποίο λειτουργεί ο

υπολογιστής, δίχως την άδεια του χρήστη και φυσικά δίχως να το γνωρίζει. Μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν **μεταμορφικό ιό**. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω διδκτύου (τοπικού) ή του διδαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του.

4. ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ

Πώς μπορεί ο μέσος χρήστης να προστατευτεί; Χρησιμοποιώντας τους ακόλουθους κανόνες:

- Δημιουργία ευφάνταστων κωδικών πρόσβασης οι οποίοι τουλάχιστον να περιέχουν οκτώ χαρακτήρες. Ημερομηνίες γέννησης, πινακίδες κυκλοφορίας οχημάτων κ.α. πρέπει να αποφεύγονται. Οι κωδικοί πρόσβασης να αλλάζουν ανά τακτά χρονικά διαστήματα και φυσικά να μην είναι γνωστοί σε άλλα άτομα.
- Google Yourself. Δηλαδή ο χρήστης να ψάχνει στο Διαδίκτυο με την βοήθεια μηχανής αναζήτησης, στοιχεία για το πρόσωπό του, έτσι ώστε να διαπιστώσει εάν πιθανόν έχει πέσει θύμα κλοπής ταυτότητας αλλά και διασποράς αρνητικών φημών για το πρόσωπό του (παρενόχληση).
- Αποφυγή αποστολής φωτογραφιών σε αγνώστους. Ιδιαίτερη προσοχή με το αναρτώμενο φωτογραφικό υλικό αφού ο οποιοσδήποτε μπορεί να το αντιγράψει και να το χρησιμοποιήσει με οποιοδήποτε τρόπο επιθυμεί.
- Ανάπτυξη κριτικής διάθεσης στην πληροφορία που είναι προσβάσιμη στο Διαδίκτυο. Δεν θα πρέπει να γίνεται οτιδήποτε πιστευτό, δίχως προηγουμένως να φιλτραριστεί.

- Σκέψη πριν την επίσκεψη κάθε link (υπερσύνδεσμο). Πολλά από τα links που συναντιούνται κατά την περιήγησή στα social media δεν είναι αυτά που φαίνονται με την πρώτη ματιά, καθώς ενδέχεται να κρύβουν απάτες, ψεύτικες ειδήσεις ή ακατάλληλο περιεχόμενο. Για το λόγο αυτό, η χρήση μιας μηχανής αναζήτησης (π.χ. της Google) για τον έλεγχο της ακεραιότητας του συνδέσμου πριν την ενεργοποίηση, είναι απαραίτητη.
- Δεν αποκαλύπτει προσωπικά του στοιχεία.
- Αποδοχή με προσοχή τα αιτήματα φιλίας «friend requests».
- Έλεγχος των posts (αναρτήσεων) πριν κοινοποιηθούν.
- Σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά στοιχεία, δε θα πρέπει να απαντιούνται. Επίσης, προσωπικά στοιχεία ή στοιχεία των συναλλαγών μέσω μίας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail) δε θα πρέπει ποτέ να αποστέλλονται. Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα. Ποτέ μια τράπεζα δε θα στείλει mail ζητώντας κάποια στοιχεία της χρεωστικής/πιστωτικής κάρτας (Phising).
- Τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν υπάρχει βεβαιότητα, δε θα πρέπει να ανοίγονται. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό.
- Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail (λογαριασμών ηλεκτρονικού ταχυδρομείου που είναι προσβάσιμοι μέσω ενός φυλλομετρητή - browser), οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.
- Ανανέωση των φυλλομετρητών (browsers – όπως π.χ. Mozilla Firefox, Google Chrome) με αναβαθμίσεις ασφαλείας (security updates), ώστε οι τρόποι προστασίας να γίνονται συστηματικά καλύτεροι.

- Εγκατάσταση αντιβιοτικού προγράμματος (antivirus), το οποίο θα πρέπει να ενημερώνεται συχνά και ανά τακτά χρονικά διαστήματα να πραγματοποιεί έλεγχο του συστήματος και προστατεύει από τους ιούς. Πριν από τα «κατέβασμα» ενός αρχείο από το Διαδίκτυο, πρέπει να γίνεται ο έλεγχος πρώτα με το antivirus.

- Σε περίπτωση που το αντιβιοτικό σας αδυνατεί να αποκαταστήσει τη ζημιά, μη διαγράψετε κανένα μολυσμένο αρχείο. Επανελέγξτε τα μολυσμένα αρχεία με κάποιο άλλο πρόγραμμα, ίσως αυτό να έχει δυνατότητα αποκατάστασης που δεν έχει το πρώτο πρόγραμμα.

- Προσπαθήστε να βρείτε από το Διαδίκτυο το πρόγραμμα απομάκρυνσης του ιού (virus removal tool) επισκεπτόμενοι τις κατάλληλες διευθύνσεις (εδώ πρέπει να γνωρίζετε την ακριβή ονομασία του ιού, προκειμένου να βρείτε το κατάλληλο για αυτόν πρόγραμμα) και, αφού το κατεβάσετε σε μια «καθαρή» δισκέτα, τρέξτε το στον υπολογιστή σας πάνω από μία φορά. Σε περίπτωση που ούτε το αντιβιοτικό σας, ούτε το ειδικό πρόγραμμα απομάκρυνσης μπορεί να «καθαρίσει» τον υπολογιστή σας, μπορεί να χρειαστεί να κάνετε format. Σε αυτήν την περίπτωση είναι καλό να έχετε κρατήσει αντίγραφα όλων των προγραμμάτων που υπάρχουν στον υπολογιστή σας, για να μπορέσετε μετά το format να τα ξαναπεράσετε.

- Εγκατάσταση ενός firewall (τείχος προστασίας) ή ενεργοποίηση αυτό που παρέχει το λειτουργικό σύστημα. Το τοίχος προστασίας θα ελέγχει όλα τα αρχεία που εισέρχονται ή εξέρχονται από τον υπολογιστή κατά τη σύνδεση στο Διαδίκτυο. Το τοίχος προστασίας εκτός από λογισμικό μπορεί να είναι και υλικό (δηλαδή συσκευή).

- Στην περίπτωση χρήσης ασύρματου οικιακού διδτύου (Wi-Fi), ενεργοποίηση των παραμέτρων ασφάλειας του δρομολογητή (router). Λεπτομέρειες θα βρείτε στις οδηγίες του κατασκευαστή. Ακόμη και στην περίπτωση που είναι ενεργοποιημένες οι παράμετροι ασφάλειας σε ένα ασύρματο δίκτυο, είναι προτιμότερο να χρησιμοποιείται ενσύρματη πρόσβαση για την μεγιστοποίηση του επιπέδου ασφαλείας.

- Pop up windows: Πολλές φορές κατά την πλοήγηση ανοίγουν, χωρίς να το προκαλέσει ο χρήστης, παράθυρα (pop up windows) των οποίων το περιεχόμενο ποικίλει. Αυτό μπορεί να είναι:

  1) Διαφημίσεις.

2) Προειδοποιητικά μηνύματα που καλούν τον χρήστη να προβεί σε ενέργειες (αποδεχόμενος συγκεκριμένες προσφορές) με άγνωστες ή επικίνδυνες για αυτόν συνέπειες.

3) Κάλεσμα για παιγνίδια είτε κανονικά είτε τυχερά.

4) Δωρεές.

5) Δεσμοί σε σελίδες πορνογραφικού περιεχομένου και γενικά ποικιλία δελεαστικών προτάσεων. Η ενδεδειγμένη ενέργεια είναι να κλείνουν άμεσα αυτά τα παράθυρα. Σε περίπτωση που αυτό δεν είναι δυνατόν από το Χ στο πάνω δεξιά μέρος του παραθύρου, εναλλακτικοί τρόποι είναι : α) Δεξί κλικ στην γραμμή κατάστασης, στο αντίστοιχο εικονίδιο και επιλογή «κλείσιμο», β)Πατώντας ταυτόχρονα Alt + F4 (επιλογή από το πληκτρολόγιο που κλείνει το ενεργό παράθυρο). Η εμφάνιση τέτοιων παραθύρων μπορεί να αποφευχθεί χρησιμοποιώντας κατάλληλα προγράμματα (pop up blockers/ killers), τα οποία προσφέρονται στο διαδίκτυο. Επισημαίνεται ότι η χρήση τέτοιων προγραμμάτων μπορεί να εμποδίσει την πρόσβαση σε κάποιες, χρήσιμες κατά τα άλλα, ιστοσελίδες. Μία τέτοια περίπτωση είναι αυτή κατά την οποία έγκυρες εταιρείες προσφέρουν μέσω pop up παραθύρων προγράμματα εφαρμογών απαραίτητα για τη σωστή εμφάνιση ενός πλήθους ιστοσελίδων (π.χ. Flash Player από την Macromedia). Σε αυτή την περίπτωση μπορούμε προσωρινά να απενεργοποιήσουμε τον blocker.

5. ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Στις μέρες μας ολοένα και μεγαλύτερο ποσοστό ενηλίκων (ιδιαίτερα των νέων) χρησιμοποιεί το διαδίκτυο για τις αγορές του. Η αγορά μέσω διαδικτύου είναι μια ευχάριστη εμπειρία η οποία από την μια μπορεί να ελαττώσει τον κόπο αλλά και από την άλλη είναι δυνατό να βρεθεί κάποιο προϊόν πιθανόν σε πιο ανταγωνιστική τιμή από την προσδοκώμενη. Όταν γίνεται μια ηλεκτρονική συναλλαγή ο χρήστης εμπιστεύεται την εταιρεία (έμπορο) που διεκπεραιώνει την συναλλαγή ως φυσικό πρόσωπο αλλά και τις διαδικασίες ασφαλείας που ακολουθεί για την πραγματοποίηση των ηλεκτρονικών συναλλαγών. Για την ασφαλή διεξαγωγή των συναλλαγών ο καταναλωτής πρέπει να ακολουθεί ορισμένους βασικούς κανόνες:

- Έλεγχος αν η διεύθυνση αρχίζει με το https (αντί του http) και υπάρχει εικονίδιο με λουκέτο πριν δοθεί οποιοδήποτε στοιχείο. Με διπλό κλικ στο λουκέτο, θα εμφανιστούν πληροφορίες που θα βοηθήσουν την επιβεβαίωση ότι η ιστοσελίδα είναι γνήσια.

- Αποφυγή πραγματοποίησης οικονομικών συναλλαγών μέσω Διαδικτύου από Internet café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές . Ο προσωπικός υπολογιστής ή κάποιος υπολογιστής για τον οποίο υπάρχει βεβαιότητα για το επίπεδο ασφάλειας, θα πρέπει να προτιμάται..
- Οι αγορές να πραγματοποιούνται μόνο από γνωστές εταιρείες που παρέχουν εγγυήσεις ασφάλειας. Μια πολύ συνετή κίνηση είναι η μιας κάρτας, αποκλειστικά για πραγματοποίηση οικονομικών συναλλαγών μέσω διαδικτύου. Επομένως σε περίπτωση θα ακυρωθεί μόνο η συγκεκριμένη κάρτα.
- Κατά την πρώτη χρήση μιας ιστοσελίδας για αγορές, έλεγχος για ύπαρξη διεύθυνσης, τηλεφώνου και γενικότερα στοιχείων επικοινωνίας. Κλήση του αριθμού, για την επιβεβαίωση ύπαρξης. Επίσης στην ιστοσελίδα, θα πρέπει να βρίσκονται σε εμφανή σημεία οι όροι και οι προϋποθέσεις καθώς επίσης και τρόποι πληρωμής αλλά και αποστολής των προϊόντων.
- Εάν είναι δυνατόν χρήση της δυνατότητας της πληρωμής με αντικαταβολή.
- Έμπιστος Τρίτος (Trusted Third Party – PayPal), όπου η καταβολή του αντιτίμου γίνεται στην συγκεκριμένη εταιρεία και κατόπιν συνεννόησης με τον παραλήπτη του αντικειμένου αγοράς (δηλαδή εάν πληρεί τις προδιαγραφές, δεν έχει καταστραφεί και γενικότερα εάν ο αποστολέας είναι συνεπής στις υποχρεώσεις του), αποστολή του ποσού στο ηλεκτρονικό μαγαζί.
- Σίγουρα ο χρήστης θα πρέπει να εφαρμόζει τις ενέργειες που αναφέρθηκαν στην παράγραφο με ονομασία Τρόποι Προστασίας.

6. ΕΠΙΛΟΓΟΣ

Ένα μεγάλο πλεονέκτημα του Διαδικτύου είναι η ανεύρεση μεγάλου όγκου πληροφοριών που πριν χρειαζόμασταν μήνες, ίσως και χρόνια, για να συλλέξουμε. Πλέον, μέσα σε λίγα μόνο λεπτά, με μερικά κλικ, με τη βοήθεια του υπολογιστή έχουμε τη δυνατότητα να μελετήσουμε βιβλία, άρθρα, να περιηγηθούμε εικονικά στα μεγαλύτερα μουσεία του κόσμου, να παρακολουθήσουμε ιστορικά οπτικοακουστικά αρχεία. Η χρήση του Διαδικτύου είναι μια ευχάριστη εμπειρία η οποία με την υιοθέτηση ορισμένων βασικών και απλών κανόνων ασφαλείας καθώς και τρόπου χρήσης, μπορεί να γίνει ακόμη συναρπαστικότερη. **Καλό σερφάρισμα λοιπόν σε όλους!**

7. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Συμπεράσματα συνεδριάσεων εμπειρογνωμόνων σε θέματα Πληροφορικής Τεχνολογίας στα πλαίσια της Europol

[2] http://www.saferinternet.gr/

[3] Ανεξάρτητη Αρχή, Συνήγορος του Πολίτη / Συνήγορος του Παιδιού

[4] http://e-yliko.gr

SAFER INTERNET DAY 2013

5 ΦΕΒΡΟΥΑΡΙΟΥ

10 Χρόνια Ημέρας Ασφαλούς Διαδικτύου

s@ferinternet.gr
για ένα ασφαλέστερο διαδίκτυο

ins@fe

INHOPE

www.saferinternetday.org