ασφάλεια στο διαδίκτυο

Μαθητής Κόνταρης Παναγιώτης

Καθηγήτρια Μήνα Καζά

Σχολικό έτος : 2020-2021

Οινούσσες

Περιεχόμενα

1. Τι είναι διαδίκτυο

Το διαδίκτυο είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών το οποίο περιέχει αμέτρητες πληροφορίες. Μαζί με την ανακάλυψη του σπασίματος της αλυσίδας του DNA, το διαδίκτυο θεωρούνται οι μεγαλύτερες ανακαλύψεις του 21αιώνα. Το διαδίκτυο ειδικά ανοίγει δρόμους για την ΄΄humancy bor΄΄ εποχή όπου τεχνική νοημοσύνη θα γίνουν ένα καινούριο είδος. Αυτό θα προσφέρει πολλές εξελικτικές ευκαιρίες στο είδος μας, σε τομείς όπως η ιατρική, το περιβάλλον, τρόφιμα μεταφορές και άλλα.

2. Ασφαλής πλοήγηση – προστασία από τους ιούς

Βέβαια μαζί του φέρνει και κινδύνους. Επομένως η γνώση για ασφαλή προήγηση στο διαδίκτυο θεωρείται προσόν και για τις μελλοντικές εφαρμογές στους τομείς της ΄΄Antiliciul lntelligense΄΄ δηλαδή τεχνικής νοημοσύνης. Το να χρησιμοποιούμε τα οφέλη του διαδικτύου, δηλαδή πληροφόρηση από πολλές και αξιόπιστες πηγές είναι ότι πιο καλό έχει να μας φωτίζει το παγκόσμιο σύστημα δικτύων. Όταν βγούμε από αυτό το πλαίσιο δυστυχώς τα πράγματα γίνονται αρκετά επικίνδυνα γιατί όπως όλοι έχουν πρόσβαση στο διαδίκτυο, έτσι και ο άνθρωπος με κακές προθέσεις έχουν και αυτοί την ίδια δυνατότητα να μπουν στο διαδίκτυο. Αυτοί θέλουν να εκμεταλλευτούν με την σιγουριά της ανωνυμίας άλλους. Όταν δεν εμφανίζεται μπορείς πολύ εύκολα να δείξεις τον κακό σου χαρακτήρα. Η εκμετάλλευση σε τομείς όπως βιντεοπαιχνίδια με πληρωμή, πλατφόρμα κοινωνικής διασύνδεσης όπου άνθρωποι κακολογούν άλλους, πολλές φορές με σκληρό και άδικο τρόπο. Site με κακόβουλο λογισμικό που εγκαθίσταται στο κομπιούτερ των ανυποψίαστων χρηστών και τους κλέβουν πληροφορίες για την ζωή τους, καθώς και λεφτά από τράπεζες, κάρτες πληρωμής. Και τέλος το πιο άσχημο παιδικής εκμετάλλευσης-αποπλάνησης. Είναι λίγα από τα πράγματα που κάποιοι με εκπαιδευμένα στην ασφαλή πλοήγηση μπορεί να πάθει στο διαδίκτυο.

Πρέπει λοιπόν να προσέχω στο διαδίκτυο από:

Α) Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψίαστου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση

γίνεται όταν ο χρήστης καλείτε να λάβει κάποια-φαινομενικά αθώο-αρχείο όπως ένα κείμενο ή μια φωτογραφία και, όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα. Μπορεί να καταστρέψει αρχεία ή και ολόκληρο τον σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστοτόπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφάλειας στο λογισμικό του χρήστη (φυλλομετρητή ή Λειτουργικό σύστημα).Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται worm (=σκουλήκι). Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την ¨προσκόλληση¨ του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης, επειδή καταναλώνει σημαντικό εύρος ζώνης (bandwidth). Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά τον χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων πραγμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία. Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι που προαναφέρθηκαν, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό όχι μόνων είναι δυνατό να υφαρπαγούν προσωπικά δεδομένα κάποιου χρήστη, όπως ο αριθμός ταυτότητας του ή το ΑΦΜ του όσο και, πιο σημαντικό, αριθμοί πιστωτικών καρτών, λογαριασμών τραπέζης κτλ. Ανάλογη μέγεθος ακολουθείται και από ορισμένους ιστοτόπους, στους οποίους ο ανύποπτος χρήστης καταχωρεί παρόμοια στοιχεία παραγγέλλοντας ένα προϊόν, το οποίο όχι μόνο δεν θα λάβει ποτέ, αλλά τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους δημιουργούς του ιστότοπου για να πραγματοποιήσουν οι ίδιοι αγορές, χρεώνοντας τον ¨πελάτη¨ τους. Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείτε

¨Phishing¨ (παραφθορά της λέξης fishing=ψάρεμα). Αρκετά προγράμματα περιήγησης (browsers) αναγνωρίζουν τους ιστότοπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα, ωστόσο αυτό δεν συμβαίνει σε ποσοστό 100%. Οι χρήστες είναι καλό να γνωρίζουν ότι κανείς χρηματοπιστωτικός φορέας δεν χρησιμοποιεί το διαδίκτυο για να ανανεώσει προσωπικές πληροφορίες, ενώ ένας προστατευμένος ιστότοπο αρχίζει πάντα με το πρόθεμα https (secure, ασφαλείς). Αρκετές φορές οι χρήστες του διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν πληροφορίες που χρειάζονται. Μερικοί ιστότοποι εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές. Το κίνητρο για τέτοιες πράξεις μπορεί να είναι είτε η αποκοδιμή ιδίου οφέλους είτε, απλά, η χαρά της παραπλάνησης των (αγνώστων) χρηστών. Ο όρος που περιγράφει αυτού του τύπου την παραπλάνηση είναι ¨Hoax¨.

3. Πως μπορώ να αντιμετωπίσω τους κίνδυνους στο διαδίκτυο –κανόνες ασφαλούς πλοήγησης

Ας είμαστε προσεκτικοί ποιους αποδεχόμαστε να γίνουν <<φίλοι>> μας και με ποιους μιλάμε στο διαδίκτυο. Δυστυχώς, υπάρχουν ενήλικοι με κακές προθέσεις που χρησιμοποιούν το διαδίκτυο προκειμένου να πλησιάσουν τα παιδιά. Άρα, λοιπόν, είμαστε περισσότερο ασφαλείς όταν μιλάμε στο διαδίκτυο με ανθρώπους που γνωρίζουμε και στον πραγματικό κόσμο.

4. Πού μπορώ να απευθυνθώ για βοήθεια

- Στην αστυνομία
- Στους γονείς μας
- Στους εκπαιδευτικούς του σχολείου
- Στα κέντρα ασφαλής πλοήγησης