3ο ΓΥΜΝΑΣΙΟ ΥΜΗΤΤΟΥ

ΣΧΟΛΙΚΟ ΕΤΟΣ:2020-2021

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΟΝΟΜΑ	ΔΗΜΗΤΡΗΣ ΠΥΡΣΟΣ
ΤΜΗΜΑ	Α3
ΤΑΞΗ	Α ΓΥΜΝΑΣΙΟΥ
ΟΝΟΜΑ ΚΑΘΗΓΗΤΡΙΑΣ	ΚΑΤΣΙΚΩΣΤΑ ΒΑΣΙΛΙΚΗ

ΗΜΕΡΟΜΗΝΙΑ ΠΑΡΑΔΟΣΗΣ:18/4/2021

ΠΕΡΙΕΧΟΜΕΝΑ

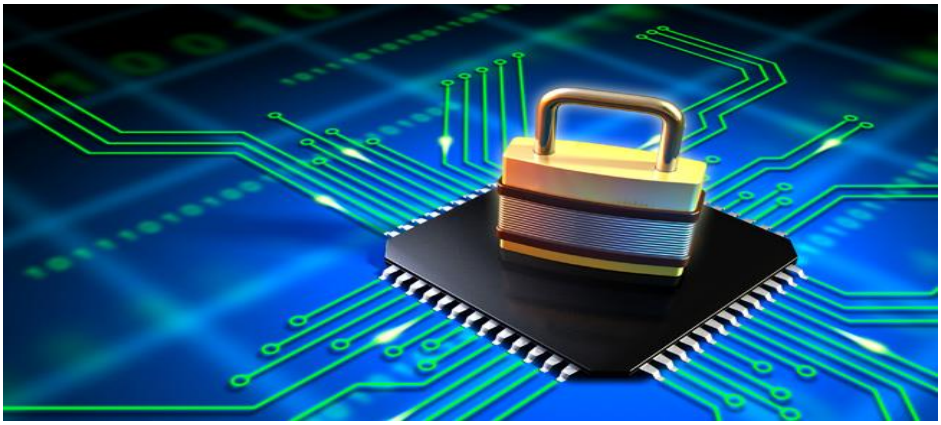
ΕΙΣΑΓΩΓΗ

Όλοι γνωρίζουμε το διαδίκτυο, εκείνο όμως που είναι το πιο σημαντικό είναι το ότι όση ανάγκη έχει το παιδί για ένα ασφαλές διαδίκτυο τόση ανάγκη το έχει κι ένας ενήλικας.

ΚΥΡΙΩΣ ΘΕΜΑ

1.1 **Τι είδους αρχεία μπορούν να μεταδώσουν ιούς**

Ένα άλλου είδους ιός που είναι γνωστός σαν ιός μακροεντολών, μπορεί να επηρεάσει έγγραφα επεξεργασίας κειμένου, λογιστικά φύλλα που χρησιμοποιούν μακροεντολές. Και είναι πιθανόν τα HTML έγγραφα που περιέχουν JavaScript ή ActiveX ή άλλου είδους εκτελέσιμο κώδικα, να μεταδίδουν ιούς ή άλλο μολυσμένο κώδικα.Αφού ο κώδικας του ιού πρέπει να εκτελεστεί για να έχει κάποιο αποτέλεσμα, τα απλά αρχεία δεδομένων είναι ασφαλή. Αυτό περιλαμβάνει γραφικά και αρχεία ήχου, όπως και απλό κείμενο σε .txt αρχεία.Για παράδειγμα, αν απλώς βλέπετε αρχεία εικόνων, δεν μπορεί να μολυνθεί ο υπολογιστής σας με ένα ιό. Ο κώδικας του ιού θα πρέπει να είναι σε μια ειδική μορφή, όπως σε ένα αρχείο .exe ή σε ένα doc αρχείο του Word, που θα πρέπει ο υπολογιστής να το τρέξει.



1.2 **Πως μεταδίδονται οι ιοί;**

Όταν εκτελείτε τον κώδικα που είναι μολυσμένος από έναν ιό, ο κώδικας του ιού τρέχει και προσπαθεί να μολύνει άλλα προγράμματα στον ίδιο υπολογιστή ή σε άλλους συνδεδεμένους με αυτόν μέσω δικτύου. Όταν μοιράζεστε ένα μολυσμένο αρχείο με άλλους χρήστες, η εκτέλεση του αρχείου μπορεί επίσης να επηρεάσει τους υπολογιστές του και τα αρχεία αυτών των υπολογιστών μπορούν να μολύνουν ακόμα περισσότερους υπολογιστές. Αν ο υπολογιστής είναι μολυσμένος με έναν ιό του τομέα εκκίνησης, ο ιός θα προσπαθήσει να κάνει αντίγραφα του εαυτού του στις περιοχές του συστήματος των δισκετών και των σκληρών δίσκων. Μετά οι μολυσμένες δισκέτες και ο ιός του σκληρού δίσκου θα προσπαθήσει να μολύνει περισσότερες δισκέτες. Μερικοί ιοί που είναι γνωστοί σαν ιοί multiparite (πολυμερείς) μπορούν να διανεμηθούν μολύνοντας αρχεία και να μολύνουν τις περιοχές εκκίνησης των δισκετών.

1.3 **Τι κάνουν οι ιοί στους υπολογιστές;**

Οι ιοί είναι προγράμματα και μπορούν να κάνουν τα ίδια πράγματα όπως και τα άλλα προγράμματα που τρέχουν σε έναν υπολογιστή. Το πραγματικό αποτέλεσμα ενός ιού εξαρτάται από τον τρόπο που είναι προγραμματισμένος από αυτόν που τον έγραψε. Μερικοί ιοί είναι σκόπιμα σχεδιασμένοι να χαλάνε αρχεία ή με άλλο τρόπο να επηρεάζουν τη λειτουργία του υπολογιστή σας, ενώ άλλοι δεν κάνουν τίποτα άλλο παρά να μεταδίδονται. Αλλά και αυτοί που απλώς μεταδίδονται μπορούν να κάνουν κακό, αφού χαλούν αρχεία και μπορούν να προκαλέσουν άλλα προβλήματα κατά τη διαδικασία της μετάδοσης τους.

1.4 **Τι μπορώ να κάνω για να περιορίσω την πιθανότητα να λάβω ιούς μέσω ηλεκτρονικού ταχυδρομείου:**

Να χειρίζεστε πολύ προσεκτικά οποιαδήποτε συνημμένα μπορεί να περιέχουν εκτελέσιμο κώδικα, όπως θα κάνετε με οποιαδήποτε νέα αρχεία: αποθηκεύστε το συνημμένο στο δίσκο και μετά ελέγξτε τα αρχεία με ένα ενημερωμένο αντιβιοτικό πρόγραμμα, πριν τα ανοίξετε. Αν το ηλεκτρονικό ταχυδρομείο ή το νέο πρόγραμμα έχει τη δυνατότητα να εκτελεί αυτόματα JavaScript, Word μακροεντολές ή άλλο εκτελέσιμο κώδικα που περιέχεται σε αυτό ή είναι συνημμένο σε ένα μήνυμα, σας προτείνουμε να απενεργοποιήσετε αυτή τη λειτουργία.

2.1 **Απάτη στο Internet**

Μπορεί να συμβεί όπως συμβαίνει και στην εκτός Internet ζωή μας. Πρέπει να εμπιστευόμαστε γνωστές εταιρίες και γενικότερα εταιρίες που έχουν Ψηφιακά Πιστοποιητικά.

2.2 **Κρυπτογράφηση Δεδομένων**

Τα θέματα ασφάλειας σχετικά με το Διαδίκτυο, τις περισσότερες φορές αφορούν την προστασία των δεδομένων που μεταδίδονται. Πιο συγκεκριμένα,

θέματα ασφαλείας δεδομένων προκύπτουν στις περιπτώσεις μετάδοσης δεδομένων όπως αριθμούς πιστωτικών καρτών, αριθμούς ταυτότητας, προσωπικά δεδομένα, τραπεζικούς λογαριασμούς καθώς και προσωπική αλληλογραφία. Η πιο διαδεδομένη μέθοδος ασφάλειας μεταφοράς δεδομένων είναι η κρυπτογράφηση, που ορίζεται ως η διαδικασία κατά την οποία χρησιμοποιείται ένα πρόγραμμα λογισμικού προκειμένου να κρυπτογραφηθούν οι πληροφορίες ενώ διαβιβάζονται. Η κρυπτογράφηση βασίζεται σε ένα κλειδί το οποίο αποτελείται από δύο κομμάτια. Η πιο διαδεδομένη μέθοδος ασφάλειας μεταφοράς δεδομένων είναι η **κρυπτογράφηση**, που ορίζεται ως η διαδικασία κατά την οποία χρησιμοποιείται ένα πρόγραμμα λογισμικού προκειμένου να κρυπτογραφηθούν οι πληροφορίες ενώ διαβιβάζονται. Η κρυπτογράφηση βασίζεται σε ένα κλειδί το οποίο αποτελείται από δύο κομμάτια.

♣ Το **δημόσιο κομμάτι**: που διανέμεται σε εκείνους με τους οποίους επιθυμείται να επικοινωνείτε.

♣ Το **ιδιωτικό κομμάτι**: που προορίζεται μόνο για τη χρήση από το παραλήπτη. Όταν στέλνετε προσωπικές πληροφορίες, χρησιμοποιείται το δημόσιο κλειδί για να κρυπτογραφηθούν οι προσωπικές πληροφορίες. Αυτό σημαίνει ότι αν σε οποιαδήποτε στιγμή κατά την διαβίβαση οι πληροφορίες σας παραβιασθούν ή υποκλαπούν, τότε αυτές «ανακατεύονται» και γίνεται πολύ δύσκολο να αποκρυπτογραφηθούν. Μόλις ο παραλήπτης λάβει τις κρυπτογραφημένες προσωπικές πληροφορίες, χρησιμοποιείται το ιδιωτικό κομμάτι του κλειδιού για να αποκωδικοποιηθούν.

2.3 **Ψηφιακά Πιστοποιητικά**

Ένα ψηφιακό πιστοποιητικό είναι μια δήλωση που επιβεβαιώνει την ταυτότητα ενός προσώπου ή την ασφάλεια μιας τοποθεσίας Web. Μπορείτε να τα χρησιμοποιήσετε για να προστατεύσετε τα προσωπικά σε στοιχεία στο Internet και τον υπολογιστή σας από μη ασφαλές λογισμικό.

Ο Internet Explorer χρησιμοποιεί **δύο τύπους πιστοποιητικών**:

♣ **Τα προσωπικά πιστοποιητικά**: που χρησιμοποιούντα ως είδος εγγύησης ότι είστε αυτοί που ισχυρίζεστε. Οι πληροφορίες αυτές χρησιμοποιούνται όταν αποστέλλετε προσωπικές πληροφορίες, μέσω του Intenet, σε μια τοποθεσία Web, η οποία απαιτεί πιστοποιητικό που να επιβεβαιώνει την ταυτότητά σας. Μπορείτε να ελέγξετε τη χρήση της ταυτότητας σας με το ιδιωτικό κλειδί που έχετε στον υπολογιστή σας και γνωρίζετε μόνο εσείς.

♣ **Τα πιστοποιητικά τοποθεσιών Web**: περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη τοποθεσία είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι καμιά άλλη τοποθεσία Web δεν είναι δυνατό να παρουσιαστεί με την ταυτότητα της αρχικής ασφαλούς τοποθεσίας. Όταν αποστέλλετε προσωπικές πληροφορίες μέσω Internet, ενδείκνυται να ελέγχετε το πιστοποιητικό της τοποθεσίας Web την οποία χρησιμοποιείτε, για να βεβαιωθείτε ότι θα προστατεύσει τις προσωπικές σας πληροφορίες. Όταν κάνετε λήψη λογισμικού από μια τοποθεσία Web, μπορείτε να χρησιμοποιήσετε ψηφιακά πιστοποιητικά για να βεβαιωθείτε ότι το λογισμικό προέρχεται από γνωστή, αξιόπιστη πηγή.

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

3.1Οδηγίες καλής χρήσης του Διαδικτύου

- Τα μηνύματα Ηλεκτρονικού Ταχυδρομείου και οι πληροφορίες που αποστέλλετε με οποιοδήποτε τρόπο σε άλλους χρήστες του Διαδικτύου δεν πρέπει:
    - να προσβάλλουν τα ανθρώπινα δικαιώματα και τις διάφορες μειονότητες
    - να σχετίζονται με παράνομες πράξεις
    - να έχουν υβριστικό χαρακτήρα ή διαφημιστική χροιά
    - να τους προσβάλλουν, αλλά να ακολουθούν τους νόμους, τα χρηστά ήθη και τα ήθη χρήσης του Διαδικτύο
- Μην διακινείτε δικτυακούς τόπους και γενικότερα πληροφορίες που:
    - προπαγανδίζουν την επιθετική συμπεριφορά, το μίσος και το ρατσισμό
    - προωθούν τα ναρκωτικά, το αλκοόλ και τα τυχερά παιχνίδι
    - περιέχουν πορνογραφικό περιεχόμενο
    - αναφέρονται σε παραβιάσεις ασφάλειας διαφόρων συστημάτων
    - αφορούν στην παράνομη διανομή προγραμμάτων
    - περιέχουν οπτικοακουστικό υλικό - προϊόν πνευματικής δημιουργίας που προστατεύεται
    - αφορούν σε υλικό με διαφημιστικά banners
- Ελέγχετε προσεκτικά το περιεχόμενο των μηνυμάτων σας για την απομάκρυνση ιών ή άλλων στοιχείων που μπορεί να βλάψουν άλλους χρήστες του Διαδικτύου.
- Χρησιμοποιείτε υπολογιστή με λογισμικό προστασίας από τους ιούς (antivirus), το οποίο να είναι ενεργό και ανανεώνεται αυτόματα με τους νέους ιούς από τον κατασκευαστή του.

3.2 Ασφαλής παρουσία στο Διαδίκτυο

- Τα άτομα που γνωρίζετε στο Διαδίκτυο δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι. Μπορεί να σας λένε ψέματα για να κερδίσουν την εμπιστοσύνη σας.
- Μην δίνετε ποτέ τα προσωπικά σας στοιχεία, ούτε να αποκαλύπτετε σε άλλους χρήστες του Διαδικτύου πληροφορίες που αφορούν τους φίλους σας, την οικογένειά σας ή το σχολείο σας.
- Μην αποκαλύπτετε τους κωδικούς πρόσβασης (password) που χρησιμοποιείτε.

- Μην επιχειρείτε συναλλαγές μέσω του Διαδικτύου για την αγορά προϊόντων και μην δίνετε στοιχεία που αφορούν πιστωτικές κάρτες.
- Να είστε επιφυλακτικός/ή ως προς την αποδοχή όσων διαβάζετε στο Διαδίκτυο ή αυτών που σας λένε οι άλλοι χρήστες του, πριν το υποβάλετε στην κρίση σας.

- Συζητήστε με τους δασκάλους σας, τους γονείς σας και με πρόσωπα που εμπιστεύεστε για τις δραστηριότητες σας στο Διαδίκτυο, ιδιαίτερα αν αντιμετωπίσετε οτιδήποτε περίεργο ή ασυνήθιστο.
- Να έχετε πάντα υπόψη σας ότι τα προϊόντα της πνευματικής δημιουργίας (μουσική, λογοτεχνία, κινηματογράφος, video κτλ.) προστατεύονται από τους νόμους και η διανομή τους μέσω του Διαδικτύου είναι παράνομη πράξη.
- Το ίδιο παράνομη πράξη θεωρείται και η διακίνηση προγραμμάτων υπολογιστών (Software), εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (Open source software).
- Μην ανοίγετε μηνύματα e-mail και επισυναπτόμενα αρχεία από άγνωστους αποστολείς με περίεργα θέματα (subject) ή χωρίς θέμα. Είναι πολύ πιθανό να περιέχουν ιούς και να προκαλέσουν σοβαρά προβλήματα στον υπολογιστή σας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

FACE TO FACE ΕΚΠΑΙΔΕΥΤΙΚΟΣ ΚΑΙ ΕΞΕΤΑΣΤΙΚΟΣ ΦΟΡΕΑΣ

https://eclass31.weebly.com/alphasigmaphi940lambdaepsiloniotaalpha-sigmatauomicron-deltaiotaalphadelta943kappatauupsilonomicron.html