

3ο ΓΥΜΝΑΣΙΟ ΥΜΗΤΤΟΥ

ΣΧ. ΕΤΟΣ: 2020-21

## Ασφάλεια στο Διαδίκτυο



Φοίβος Τσακίρακης Δρακωτός

Τμήμα Α3

21/ 04 /2021

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ: κ.Κατσικώστα

## **ΠΕΡΙΕΧΟΜΕΝΑ**

<b>ΠΡΟΛΟΓΟΣ – ΕΙΣΑΓΩΓΗ .....</b>	<b>3</b>
<b>ΚΕΦΑΛΑΙΟ 1. Ορισμός της ασφάλειας</b>	
1.1. Ορισμός Ασφάλειας διαδικτύου .....	3
<b>ΚΕΦΑΛΑΙΟ 2. Ασφάλεια λογισμικού υπολογιστή</b>	
2.1. Τι είναι ένας υπολογιστικός ιός .....	4
2.2. Τρόπος διάδοσης ιών.....	5
2.3. Αντιμετώπιση ιών .....	8
<b>ΚΕΦΑΛΑΙΟ 3. Ασφάλεια προσωπικών δεδομένων</b>	
3.1. Ασφάλεια πληροφοριών στο διαδίκτυο .....	10
3.2. Βασικοί κανόνες .....	11
<b>ΣΥΜΠΕΡΑΣΜΑΤΑ-ΠΡΟΤΑΣΕΙΣ .....</b>	<b>12</b>
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ ΚΑΙ ΠΗΓΕΣ.....</b>	<b>13</b>

## ΠΡΟΛΟΓΟΣ – ΕΙΣΑΓΩΓΗ

«Η εργασία αυτή πραγματοποιήθηκε στα πλαίσια του μαθήματος Πληροφορικής Α Γυμνασίου για το β τετράμηνο. Αφορά μόνο την ασφάλεια λογισμικού και τον πληροφοριών μέσα στο διαδίκτυο. Αναφέρεται στους τρόπους αντιμετώπισης των ιών και κανόνες για την ασφάλεια των πληροφοριών ».

### ΚΕΦΑΛΑΙΟ 1. Ορισμός της ασφάλειας

#### 1.1.Ορισμός Ασφάλειας διαδικτύου

**Η ασφάλεια στο Διαδίκτυο ή η διαδικτυακή ασφάλεια** είναι η γνώση των κινδύνων προσωπικής ασφάλειας και ασφάλειας του χρήστη σε ιδιωτικές πληροφορίες και περιουσίες που σχετίζονται με τη χρήση του Διαδικτύου και την προστασία από το ηλεκτρονικό έγκλημα.



**Η ασφάλεια είναι σημαντική για την καλύτερη λειτουργία του υπολογιστή και την προστασία των προσωπικών δεδομένων και πληροφοριών μας.**

## ΚΕΦΑΛΑΙΟ 2. Ασφάλεια λογισμικού υπολογιστή

### 2.1 Τι είναι ένας υπολογιστικός ιός

Ένας υπολογιστικός ιός είναι ένα πρόγραμμα που έχει σχεδιαστεί ώστε να δημιουργεί αντίγραφα του εαυτού του. Η λειτουργία αυτή μάλιστα γίνεται κατά κανόνα χωρίς την επίγνωση του χρήστη. Πέραν αυτής της λειτουργίας οι περισσότεροι ιοί έχουν περαιτέρω παρενέργειες, οι οποίες ποικίλουν από την εμφάνιση ενοχλητικών αλλά άκακων μηνυμάτων μέχρι καταστρεπτικές ενέργειες για τα δεδομένα του χρήστη.



Οι ιοί μπορεί να είναι κρυμμένοι σε προγράμματα διαθέσιμα σε δισκέτες ή CDs, ενσωματωμένοι σε επισυνάψεις ηλεκτρονικού ταχυδρομείου ή σε υλικό διαθέσιμο στο Διαδίκτυο.

Οποιοδήποτε υπολογιστικό σύστημα με ένα ενεργό αντίγραφο ενός ιού καλείται μολυσμένο.

Για να μολυνθεί ένα υπολογιστικό σύστημα ο ιός πρέπει όπως κάθε άλλο πρόγραμμα να εκτελεστεί. Ο τρόπος εκτέλεσης ποικίλλει από ιό σε ιό.



## 2.2 Τρόπος διάδοσης ιών

Μόλις ένα υπολογιστικό σύστημα μολυνθεί από ιό, αυτός έχει τη δυνατότητα να αντιγράψει τον εαυτό του, να μολύνει, άλλα αρχεία που χρησιμοποιεί ο χρήστης.



Οι μακρο-ιοί όχι μόνο μολύνουν αρχεία στον υπολογιστή του χρήστη, αλλά συχνά διαδίδονται και μέσω του τοπικού δικτύου ή και του Διαδικτύου.

### **Παρασιτικοί ιοί**

Οι παρασιτικοί ιοί προσκολλώνται σε άλλα εκτελέσιμα προγράμματα. Όταν αυτά εκτελούνται φορτώνεται ο ιός στη μνήμη, ο οποίος στη συνέχεια καλεί το αρχικό πρόγραμμα ώστε να κρύψει την παρουσία του.



Ο ιός γενικά γίνεται αντιληπτός μόνο από τις παρενέργειές του, αν ένας ιός δεν έχει κάποιες παρενέργειες μπορεί να αντιγράψει τον εαυτό του επί σημαντικό χρονικό διάστημα χωρίς να γίνει αντιληπτός από το χρήστη.

### **Συνδυαστικοί ιοί**

Οι συνδυαστικοί ιοί χρησιμοποιούν μια πληθώρα τεχνικών με σκοπό την διάδοσή τους. Μεταξύ άλλων στέλνουν αυτόματα τον εαυτό τους μέσω ηλεκτρονικού ταχυδρομείου,

εκμεταλλεύονται προβλήματα ασφαλείας του λειτουργικού συστήματος για να μολύνουν αυτόματα μεγάλα σύνολα υπολογιστικών συστημάτων.



### 2.3 Αντιμετώπιση ιών

Το αντικό λογισμικό επιτρέπει την προστασία του χρήστη από το σύνολο σχεδόν των ιών.

Ωστόσο, δεν αποτελεί πανάκεια στο πρόβλημα.

Για να λειτουργεί το πρόγραμμα σωστά θα πρέπει να ακολουθούμε αυτές τις

διαδικασίες συχνά.





#### **Τακτική ενημέρωση του λογισμικού**

Καινούριοι ιοί εμφανίζονται επί καθημερινής βάσεως. Το αντικό λογισμικό γενικά μπορεί να προστατεύσει το χρήστη μόνο από τους ιούς που περιέχονται στη βάση δεδομένων του.

Τα περισσότερα σύγχρονα αντικα λογισμικά ενσωματώνουν για το σκοπό αυτό μηχανισμούς αναβάθμισης της βάσης αυτής, ώστε να έχουν τη δυνατότητα να

αντιμετωπίσουν το σύνολο των υπαρχόντων ιών.**Συνεχής εκτέλεση του λογισμικού**

Τα περισσότερα σύγχρονα αντικα λογισμικά ενσωματώνουν προγράμματα τα οποία συνεχώς ελέγχουν κάθε αρχείο ή μήνυμα ηλεκτρονικής αλληλογραφίας που ανακτά ο χρήστης, ώστε να εντοπίζουν τον ιό πριν αυτός εκτελεστεί και προσβάλλει το υπολογιστικό σύστημα. Είναι σημαντικό ο χρήστης να μην κλείνει τα προγράμματα αυτά, για οποιοδήποτε λόγο.

## ΚΕΦΑΛΑΙΟ 3. Ασφάλεια προσωπικών δεδομένων

### 3.1 Ασφάλεια πληροφοριών στο διαδίκτυο

Οι ευαίσθητες πληροφορίες όπως οι προσωπικές και η ταυτότητα του χρήστη , οι κωδικοί πρόσβασης συνδέονται συχνά με προσωπικά είδη (π.χ. τραπεζικοί λογαριασμοί) και με την ιδιωτική τους ζωή και ενδέχεται να παρουσιάσουν ανησυχία σχετικά με την ασφάλεια των χρηστών εάν διαρρεύσουν.



Η μη εξουσιοδοτημένη πρόσβαση και η χρήση ιδιωτικών πληροφοριών μπορεί να έχει ως συνέπεια την κλοπή ταυτότητας , καθώς και την κλοπή ιδιοκτησίας

### 3.2. Βασικοί κανόνες

Υπάρχουν βασικοί κανόνες που μας προστατεύουν από τους κινδύνους του διαδικτύου που απειλούν τα προσωπικά μας δεδομένα. Αν τους ακολουθήσουμε προστατεύουμε τις πληροφορίες μας.

1. Να έχουμε στο μυαλό μας ότι το Διαδίκτυο είναι κυρίως μια κοινωνία ανθρώπων και κρύβει τους ίδιους κινδύνους που κρύβει κάθε κοινωνία.
2. Οι πληροφορίες που παρουσιάζονται στο Διαδίκτυο δεν είναι πάντα έγκυρες.
3. Η κοινοποίηση των προσωπικών στοιχείων, όπως ονοματεπώνυμο, διεύθυνση, τηλέφωνο, φωτογραφία, κωδικοί πρόσβασης, αριθμός πιστωτικών καρτών, e-mail κ.λπ., είναι καλό να αποφεύγεται.
4. 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 από τους μεγάλους.
5. Η χρήση του υπολογιστή ως μέσου απασχόλησης του παιδιού χωρίς την παρουσία ενηλίκου είναι καλό να αποφεύγεται. Ο υπολογιστής δεν πρέπει να χρησιμοποιείται έτσι.
6. Η δημιουργία ενός συνόλου από κανόνες χρήσης του Η/Υ αποδεκτών από όλους και η ανάρτηση τους σε εμφανές σημείο δίπλα στον υπολογιστή βοηθά στην προστασία όλων των χρηστών.

Οι κανόνες είναι απλοί και αν τους ακολουθούμε έχουμε ασφάλεια.

## ΣΥΜΠΕΡΑΣΜΑΤΑ-ΠΡΟΤΑΣΕΙΣ

Το συμπέρασμα είναι ότι η ασφάλεια του υπολογιστή μας και των προσωπικών μας πληροφοριών και για να έχουμε αυτή την ασφάλεια πρέπει να τηρούμε τους κανόνες που ανέφερα.



## ΒΙΒΛΙΟΓΡΑΦΙΑ ΚΑΙ ΠΗΓΕΣ

1. <https://www.sch.gr/assist/odigies/asfaleia-kai-prostasia/odigies-asfaleias-kai-prostasias-apo/>
2. [https://el.wikipedia.org/wiki/Ασφάλεια\\_στο\\_διαδίκτυο](https://el.wikipedia.org/wiki/Ασφάλεια_στο_διαδίκτυο)
3. <https://www.sch.gr/category/safeweb/>
4. [http://edu-gate.minedu.gov.gr/index.php?option=com\\_sppagebuilder&view=page&id=23&Itemid=126](http://edu-gate.minedu.gov.gr/index.php?option=com_sppagebuilder&view=page&id=23&Itemid=126)