Ενδεικτικές σελίδες:

- https://techguru.gr/blog/h-mikri-egkyklopedia-ton-ion-ypologiston/
- https://ioi-viruses.webnode.gr/τύποι-ιών/

ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ, ΟΜΑΔΑΣ Α

Απαντήστε στις παρακάτω ερωτήσεις σχετικά με ιούς:

1. Τι είναι οι Ιοί των υπολογιστών;

Οι ϊοί υπολογιστών είναι προγράμματα τα οποία έχουν δημιουργήσει προγραμματιστές ή Hacker, όπως πολλά άλλα **προγράμματα, τα οποία όμως είναι κακόβουλα και όχι χρηστικά**. Αυτά τα προγράμματα εκτελούνται στον υπολογιστή μας και εκτελεί συγκεκριμένες ενέργειες **κλοπής, παρακολούθησης, καταστροφής αρχείων** κτλ.

2. Ποιοι υπολογιστές κολλάνε ιούς;

Όλοι οι υπολογιστές οι οποίοι έχουν λειτουργικό σύστημα **Windows**. Αυτό συμβαίνει διότι τα Windows ανέκαθεν είχαν πολλές "**προγραμματιστικές τρύπες**" οι οποίες είναι εύκολα εκμεταλλεύσιμες από τους προγραμματιστές που γνωρίζουν τα προβλήματα που υπάρχουν στην ασφάλεια των Windows. Εξού και τα δεκάδες updates και patches που δημοσιεύει η Microsoft. Έπειτα τα Windows είναι τα πιο δημοφιλή προς χρήση παγκοσμίως, οπότε τα "θύματα" θα είναι πάρα πολλά.

3. Ποιοι είναι οι τύποι των ιών;

Ας αναλύσουμε ορολογίες που ακούγονται συχνά και δεν είναι κατανοητή η διαφορά μεταξύ τους. Τα παρακάτω είναι τύποι ϊών/κακόβουλων λογισμικών ή αλλιώς "**Malware**":

- Worm: αναφέρεται σε έναν τύπο κακόβουλου λογισμικού που αναπαράγεται και εξαπλώνεται αυτόματα σε άλλους υπολογιστές, συνήθως μέσω δικτύων. Τα σκουλήκια διαφέρουν από τα ιούς στο ότι δεν χρειάζονται να συνδεθούν με κάποιο εκτελέσιμο αρχείο ή πρόγραμμα για να εξαπλωθούν.

  Ένα σκουλήκι συνήθως εκμεταλλεύεται ευπάθειες στο λογισμικό ή το δίκτυο για να εισβάλει σε έναν υπολογιστή και να εξαπλώσει αντίγραφά του σε άλλους υπολογιστές μέσω δικτύων. Σκουλήκια μπορεί να προκαλέσουν ζημιές στο δίκτυο, να καταστρέψουν ή να κλέψουν δεδομένα, και γενικά να προκαλέσουν προβλήματα στη λειτουργία των υπολογιστών που επηρεάζουν

  - **Trojan:** "Μεταμφιεσμένος" ϊός σε μορφή καλόβουλου λογισμικού (όπως ψεύτικο λογισμικό προστασίας από ϊούς και επιδιόρθωση εικονικών προβλημάτων του συστήματος) με σκοπό να ξεγελάσει τον χρήστη και να πέσει στη παγίδα του ϊού (άντληση χρήματος, τραπεζικών στοιχείων κ.α.)
  - **Ransomware:** Εξαπλώνεται όλο και περισσότερο. Κλειδώνουν την χρήση του υπολογιστή με σκοπό να λάβουν "λύτρα" από το χρήστη προκειμένου να ανακτηθεί το σύστημα και τα αρχεία.

- **Spyware:** Κρυφά προγράμματα τα οποία έχουν σκοπό την συλλογή πληροφοριών ενός υπολογιστή και του δικτύου του, των προσωπικών στοιχείων του χρήστη, των αρχείων του και γενικά παρακολουθεί τι είδους χρήση κάνει. Βαραίνει το σύστημα, τη ταχύτητα και τη λειτουργικότητα του υπολογιστή.
- **Adware:** Προγράμματα τα οποία συνήθως εγκαθίστανται στους περιηγητές Internet/browsers (Chrome, Firefox, Internet Explorer κτλ) με σκοπό να κατευθύνουν τον χρήστη προς συγκεκριμένα διαφημιστικά site, με άσχετα αποτελέσματα στις αναζητήσεις. Επίσης, "πετάγονται" διαφημίσεις σε παράθυρα και σελίδες που δεν έχει ξαναδεί ο χρήστης. Και αυτό βαραίνει το σύστημα και τη λειτουργικότητα του υπολογιστή, σαν τα spyware.

4. Μπορείτε να αναφέρετε κάποιους επικίνδυνους ιούς από το παρελθόν;

1. ***ILOVEYOU***

   Αυτός ήταν ίσως ο πιο επικίνδυνος ιός υπολογιστή που δημιουργήθηκε ποτέ που με τη μορφή ενός ατέρμονου worm – ήταν ένα αυτόνομο πρόγραμμα ικανό να αντιγράφεται μόνο του. Γνωστός ως ILOVEYOU, αυτός ο ιός ταξίδεψε αρχικά το Διαδίκτυο μέσω e-mail και κατάφερε να συντρίψει υπολογιστές σε ολόκληρο τον κόσμο

2. ***Melissa***

   Ο Melissa ήταν ο πρώτος μαζικός ταχυδρομικός ιός μακροεντολών στη νέα εποχή της ηλεκτρονικής αλληλογραφίας που έγινε η έκτακτη είδηση σε όλο τον κόσμο στις 26 Μαρτίου 1999

   Όταν κάποιος έκανε κλικ επάνω του, ο ιός αναπαραγόταν και επιδίωκε να αποσταλεί μέσω e-mail στα πρώτα 50 ονόματα στον κατάλογο με το μήνυμα, “Εδώ είναι το έγγραφο που ζήτησες … μην το δείξεις σε κανέναν άλλο. ☺ ”

3. ***My Doom***

   Ο My Doom εμφανίστηκε στις 26 Ιανουαρίου 2004 και συγκλόνισε όλο τον κόσμο, καθώς εξαπλωνόταν μέσω e-mail μέσω του ηλεκτρονικού ταχυδρομείου σε τυχαίες διευθύνσεις αποστολέων και γραμμές θέματος. Αλλά, μόλις το μήνυμα άνοιγε, το συνημμένο εκτελούνταν και το worm μεταφερόταν σε διευθύνσεις email στο βιβλίο διευθύνσεων του χρήστη. Η ζημία που προκλήθηκε από αυτό το ταχύτατο mailer worm ήταν 38 δισεκατομμύρια $.