

Διδασκαλία της ασφάλειας στο διαδίκτυο και την προστασία κωδικών από κακόβουλους, αλλά και την τεχνολογική εξέλιξη/άνθιση

Λέξεις κλειδιά

1. Θα δίνετε τον κωδικό σας?

2. Εν συνεχεία εξηγούμε τον όρο phishing

3. Επειτα προβάλλουμε κάποια (η όλες) από τις παρακάτω εικόνες με τους πιο συχνά χρησιμοποιούμενος κωδικούς στον κόσμο.

4. Have I been Pwned?

5.1 How secure is my password?

5.2 Επιθέσεις DDOS

6. Νόμος του Moore

7. Ανωνυμία στο διαδίκτυο

7.1 Εισαγωγή στην Κρυπτογραφία

7.2 Ασφάλεια και προσωπικά δεδομένα

**Απευθύνεται σε μαθητές Α Λυκείου. Απαιτείται η κατανόηση αγγλικών
Διάρκεια: 4-5 διδακτικές ώρες**

Λέξεις κλειδιά:

Νόμος του Moore, Προστασία κωδικών από hacking, Τι είναι hacking, και τι είναι οι DDOS επιθέσεις, Phishing, Ισχύς κωδικών, cookies, ανωνυμία στο διαδίκτυο

1. Θα δίνετε τον κωδικό σας?

Το εκπαιδευτικό σενάριο ξεκινάει ρωτώντας τους μαθητές αν κάποιος είναι διατεθειμένος για τις ανάγκες του μαθήματος να μας πει (εκφωνώντας τον) τον κωδικό του από κάποιο email ή κάποιο social media. Αναμενόμενα, δύσκολα κάποιος μαθητής θα δεχτεί, και έτσι ακολουθεί η ερώτηση “Κατά πόσο πιστεύετε ότι είναι εφικτό κάποιος να σας κλέψει τον κωδικό σας, χωρίς να του τον πείτε?”.

Θα απαντήσουμε δείχνοντας το συγκεκριμένο βίντεο:

- https://www.youtube.com/watch?v=opRMrEfAlil&ab_channel=JimmyKimmelLive
- https://www.youtube.com/watch?v=UzvPP6_LRHc&ab_channel=JimmyKimmelLive

Σκοπός είναι να θέσουμε αμφιβολίες για την ικανότητα διαφύλαξης σημαντικών στοιχείων, που μπορούν να οδηγήσουν στην αλίευση των κωδικών μας.

2. Εν συνεχεία εξηγούμε τον όρο **phishing**

Μπορούμε να προβάσουμε κάποιο από τα βίντεο:

1. https://www.youtube.com/watch?v=Y7zNIEMDml4&ab_channel=IDGTECHtalk
2. https://www.youtube.com/watch?v=9TRR6IHviQc&ab_channel=SafetyinCanada (3 λεπτά, αγγλικά)
3. https://www.youtube.com/watch?v=BnmneAjVrM4&ab_channel=Kaspersky (2 λεπτά, αγγλικά)

Μπορούμε επίσης να προβάσουμε και τα βίντεο των παρακάτω διαδικτυακών φαρσέρ, που στοχεύουν στην ενίσχυση της προστασίας προσωπικών δεδομένων:

- https://www.youtube.com/watch?v=6RPRtekUA3I&ab_channel=JackValeFilms
- https://www.youtube.com/watch?v=F7pYHN9iC9I&ab_channel=DuvalGuillaume
- https://www.youtube.com/watch?v=YLWmjpPoJHk&ab_channel=BuzzFeedVideo

3. Έπειτα προβάσουμε κάποια (η όλες) από τις παρακάτω εικόνες με τους πιο συχνά χρησιμοποιούμενος κωδικούς στον κόσμο.

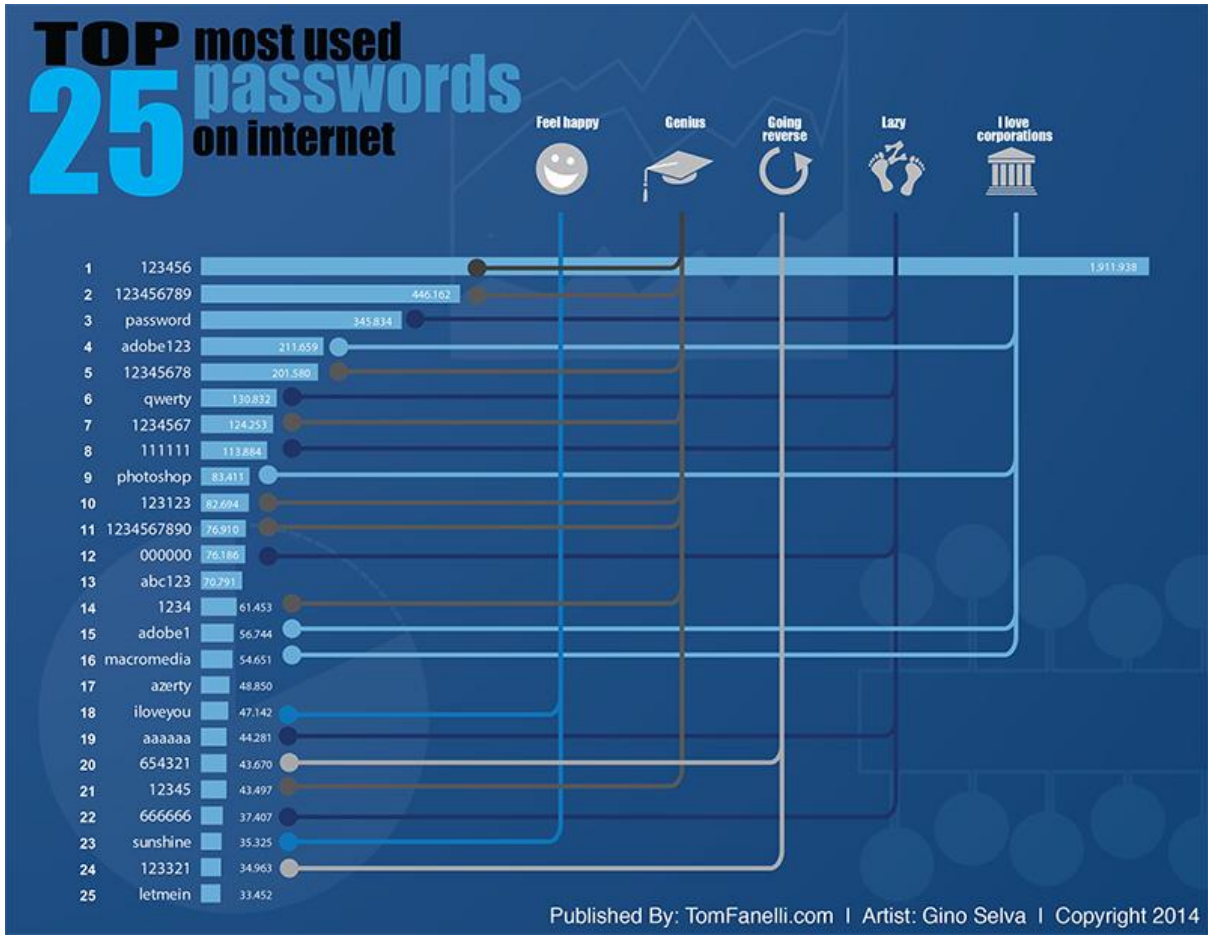
Top 30 Most Used Passwords in the World




1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

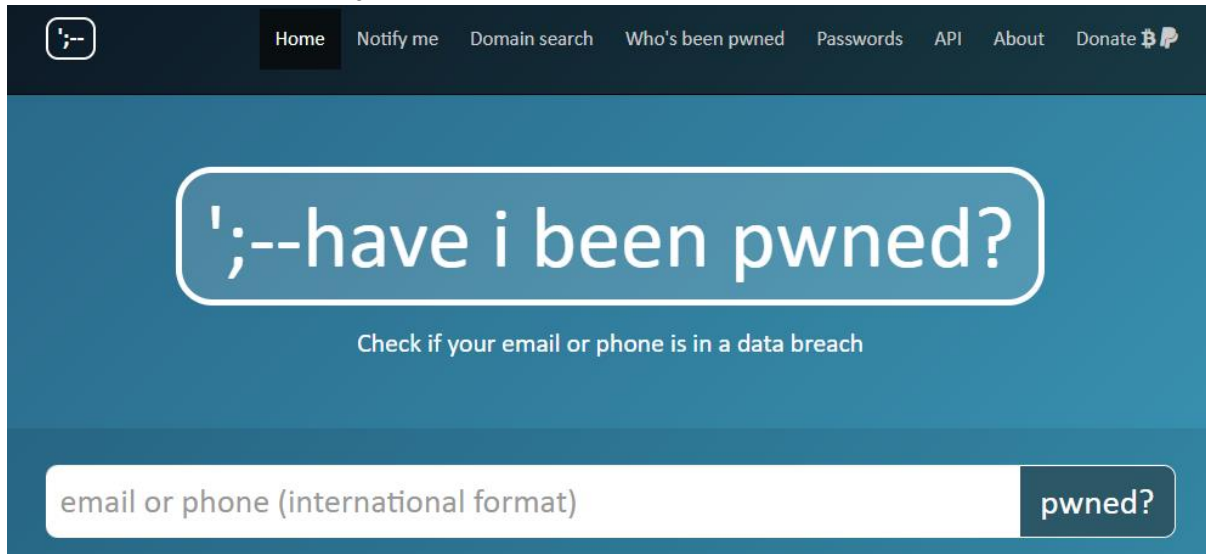
The 50 Most Used Passwords

1. 123456	11. 123123	21. mustang	31. 7777777	41. harley
2. password	12. baseball	22. 666666	32. f*cky*u	42. zxcvbnm
3. 12345678	13. abc123	23. qwertyuiop	33. qazwsx	43. asdfgh
4. qwerty	14. football	24. 123321	34. jordan	44. buster
5. 123456789	15. monkey	25. 1234...890	35. jennifer	45. andrew
6. 12345	16. letmein	26. p*s*y	36. 123qwe	46. batman
7. 1234	17. shadow	27. super man	37. 121212	47. soccer
8. 111111	18. master	28. 270	38. killer	48. tigger
9. 1234567	19. 696969	29. 654321	39. trustno1	49. charlie
10. dragon	20. michael	30. 1qaz2wsx	40. hunter	50. robert



4. Have I been Pwned?

Επειτά, κάνουμε επίδειξη του website <https://haveibeenpwned.com/> το οποίο στοχεύει να μας ενημερώσει αν κάποια διεύθυνση email μας έχει παραβιαστεί. Μπορούμε να προτείνουμε είτε να δοκιμάσουν να βάλουν το email τους, είτε εκείνη την στιγμή είτε όταν επιστρέψουν στο σπίτι τους.

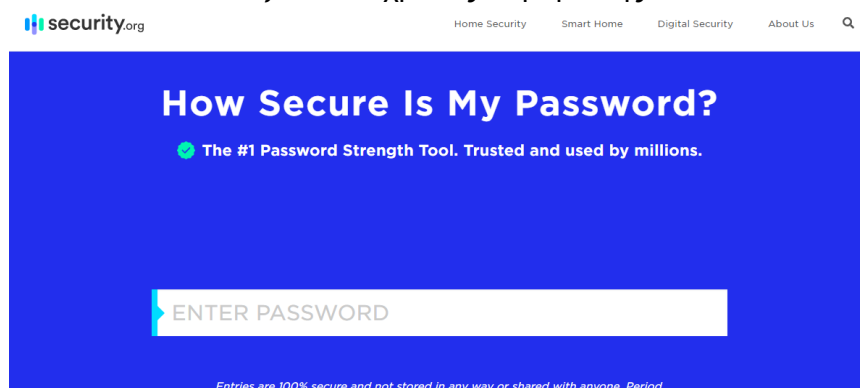


Προαιρετικά μπορούμε να παραθέσουμε τα παρακάτω άρθρα σχετικά με την ασφάλεια των κωδικών:

- <https://www.pcmag.com/how-to/simple-tricks-to-remember-seriously-secure-passwords>
- <https://www.pcmag.com/picks/the-best-password-managers>
- <https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up>

5.1 How secure is my password?

Επειτα τους παρακινούμε να δούνε το website <https://www.security.org/how-secure-is-my-password/> που μας ενημερώνει πόσο χρόνο χρειάζεται κάποιος αυτοματοποιημένος αλγόριθμος να παραβιάσει κάποιον κωδικό. Η επίδειξη γίνεται βάζοντας έναν απλο κωδικό, και στη συνέχεια τον εμπλουτίζουμε βήμα βήμα (με κάποιο σημείο στίξης για παράδειγμα) βλέποντας σε real time πόσο αυξάνεται ο χρόνος παραβίασης.



Στην συνέχεια θέτουμε την ερώτηση “Και πόσο καλά γνωρίζουμε ότι δεν θα μας κλέψει αυτό το website τον κωδικό μας?”. Σκοπός είναι να εξηγήσουμε το πρωτόκολλο https



5.2 Επιθέσεις DDOS

Προαιρετικά μπορούμε να επιδείξουμε το παρακάτω βίντεο στα ελληνικά για τις επιθέσεις DDOs. https://www.youtube.com/watch?v=7JYVv9bZzVM&ab_channel=PhoenixGR (ελληνικά).

6. Νόμος του Moore

Καταλήγουμε στο συμπέρασμα ότι μπορεί σήμερα οι κωδικοί μας να θέλουν Χιλιάδες χρόνια για να παραβιαστούν από κάποιο κακόβουλο πρόγραμμα, αλλά όσο εξελίσσονται οι ταχύτητες των δικτύων και η επεξεργαστική ισχύς των υπολογιστών, αυτός ο χρόνος θα μειώνεται κάθε χρόνο.

Με αφορμή το παραπάνω, κάνουμε μία εισαγωγή **στον νόμο του Moore**, προβάλλοντας κάποιο από τα βίντεο:

1. <https://youtu.be/d7DENvGDdds> (Στα ελληνικά, διάρκεια 4 λεπτά)
2. https://www.youtube.com/watch?v=aWLBmapcJRU&ab_channel=QUTIFB101 (στα αγγλικά, διάρκεια 2 λεπτά με cartoon animations)
3. https://www.youtube.com/watch?v=CUnQNTwmHHo&t=10s&ab_channel=CuriousReason (στα αγγλικά, διάρκεια 11 λεπτά)
4. Μπορεί να ακολουθήσει μία συζήτηση για το πόσο άλλες επιστήμες (όπως η χημεία, η τεχνολογία υλικών, φυσική, μαθηματικά κλπ) επηρεάζουν και προβλέπουν τις τεχνολογικές εξελίξεις, και να τεθεί το ερώτημα για το αν ο νόμος του Moore ακόμα επαληθεύεται, και μέχρι πότε. Συνοδευτικά, μπορεί να προβληθεί το παρακάτω timelapse γράφημα, που δείχνει την έκρηξη της τεχνολογίας, και την πρόβλεψη για το μέλλον. https://www.youtube.com/watch?v=7uvUiq_jTLM&ab_channel=DataGrapha

7. Ανωνυμία στο διαδίκτυο

Επειτα από τα παραπάνω, δίνεται μία καλή ευκαιρία για μία εισαγωγή για την ανωνυμία στο διαδίκτυο και την επεξήγηση των ψηφιακών “ιχνών”. Για παράδειγμα θα μπορούσε να γίνει επίδειξη του **TOR Browser**, και του **Signal App**



Signal - Ιδιωτικές συνομιλίες

🔒 Επιλογή συντακτών

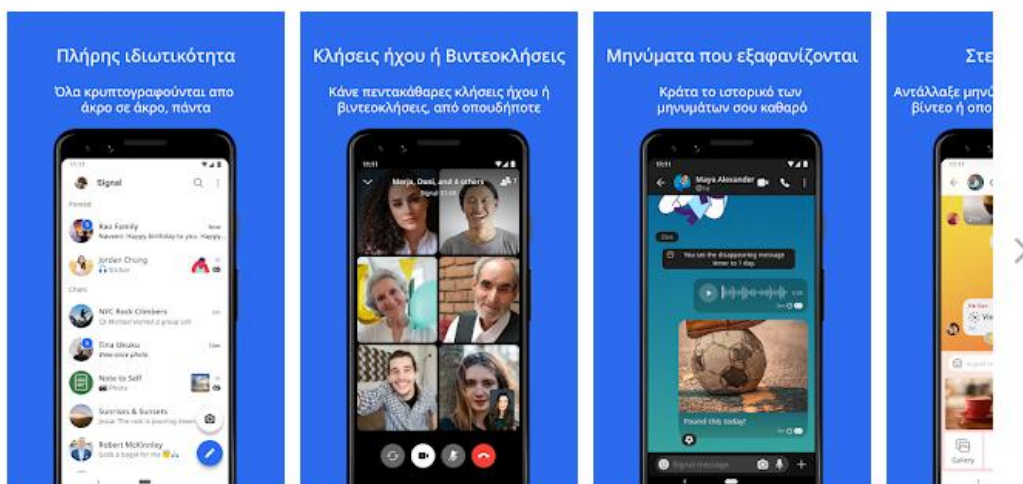
Signal Foundation Επικοινωνία


★★★★★ 1.872.718 👤

📱 Κατάλληλο για όλους

📌 Αυτή η εφαρμογή είναι διαθέσιμη για ορισμένες από τις συσκευές σας.


Εγκαταστήθηκε




 [Donate Now](#)

Defend yourself.


Protect yourself against tracking, surveillance, and censorship.




Download for Windows
Signature



Download for macOS
Signature



Download for Linux
Signature

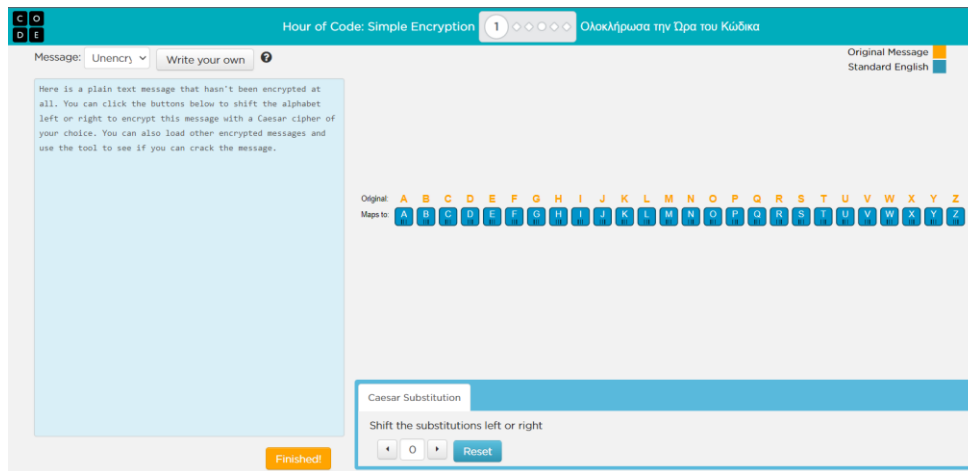


Download for Android

<https://www.torproject.org/download/>

7.1 Εισαγωγή στην Κρυπτογράφηση

Μπορούμε να προβάσουμε ένα παράδειγμα μίας μεθόδου κρυπτογράφησης από το studio.code.org/s/hoc-encryption/lessons/1/levels/1



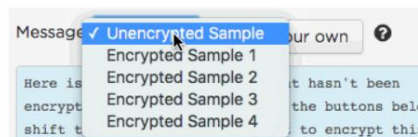
Παζλ 1 από 6

Crack a Caesar cipher!

This tool lets you play with text and do Caesar ciphers. You can use this to either encrypt a message or decrypt it.

Do this

- Load a **Sample message** from the message dropdown. This will load a message that has been encrypted with a Caesar cipher.



- Using the buttons in the Caesar substitution tab, you can shift the alphabet forwards or backwards to try to unscramble the message.



See how long it takes you to crack the cipher! Is this a good method?

OK

7.2 Ασφάλεια και προσωπικά δεδομένα

Σε αυτό το σημείο μπορεί να γίνει επίδειξη για το τι είναι τα cookies, και πως μπορούμε να τα “καθαρίζουμε”. Αν χρησιμοποιούμε τον chrome ως browser, η διεύθυνση `chrome://settings/siteData` είναι μία καλή έναρξη για να δείξουμε τι “αποθηκεύει” ο κάθε υπολογιστής για εμάς.

Διαγραφή δεδομένων περιήγησης

Βασικά

Σύνθετες

Χρονικό εύρος Τελευταία ώρα

- Ιστορικό περιήγησης**
Διαγράφει το ιστορικό από όλες τις συγχρονισμένες συσκευές
- Εμφάνιση cookie και άλλων δεδομένων ιστότοπου**
Θα αποσυνδεθείτε από τους περισσότερους ιστότοπους. Θα παραμείνετε συνδεδεμένοι στον Λογαριασμό σας Google, για να μπορείτε να διαγράψετε τα συγχρονισμένα δεδομένα σας.
- Εικόνες και αρχεία στην κρυφή μνήμη**
Απελευθερώνει λιγότερο από 198 MB. Ορισμένοι ιστότοποι μπορεί να φορτωθούν πιο αργά κατά την επόμενη επίσκεψή σας.

Ενδέχεται να αποθηκεύονται στον Λογαριασμό σας Google [άλλες](#)

Ακύρωση

Διαγραφή δεδομένων

Γενικές ρυθμίσεις

- Επιτρέπονται όλα τα cookie
- Αποκλεισμός cookie τρίτων μερών στην Ανώνυμη περιήγηση**
Οι ιστότοποι μπορούν να χρησιμοποιούν cookie για να βελτιώσουν την εμπειρία περιήγησής σας, για παράδειγμα, για να παραμείνετε συνδεδεμένοι ή να διατηρηθούν τα προϊόντα στο καλάθι αγορών σας.
Ενώ βρίσκεστε σε κατάσταση ανώνυμης περιήγησης, οι ιστότοποι δεν μπορούν να χρησιμοποιήσουν τα cookie σας για να βλέπουν τη δραστηριότητα περιήγησής σας σε διαφορετικούς ιστότοπους, για παράδειγμα, για την εξατομίκευση των διαφημίσεων. Ορισμένες λειτουργίες κάποιων ιστότοπων μπορεί να μην είναι διαθέσιμες.
- Αποκλεισμός cookie τρίτων
- Αποκλεισμός όλων των cookie (δεν συνιστάται)
- Διαγραφή cookie και δεδομένων ιστότοπου κατά το κλείσιμο όλων των παραθύρων
- Να αποστέλλεται ένα αίτημα "Να μην γίνεται εντοπισμός" με την επισκευμότητα της περιήγησής σας

HTTP cookies

Από τη Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια

Τα **cookies** είναι μικρά αρχεία κειμένου τα οποία αποθηκεύονται στον **φωλομετρητή** μας κατά την πλοήγησή μας στο **διαδίκτυο**. Σκοπός τους είναι να εδωποιούν τον ιστότοπο που επισκέπτεται ο χρήστης, για την προηγούμενη δραστηριότητά του^[1] Συνήθως περιγράφουν στοιχεία μας όπως όνομα χρήστη (user name) και συνθηματικό πρόσβασης (password) με σκοπό κατά την επίσκεψή μας στον ίδιο ιστότοπο αργότερα, να μας "θυμάται" και να μην χρειάζεται να κάνουμε login.

Τα cookies μπορεί να προέρχονται από τον ιστότοπο τον οποίο έχουμε επισκεφθεί ή από κάποιον άλλον (third-party cookies), για παράδειγμα μέσω διαφημίσεων. Έχει όμως αποδειχθεί ότι τα third-party cookies συλλέγουν πληροφορίες για τη συμπεριφορά του κάθε χρήστη στο διαδίκτυο, κάτι που εγείρει σημαντικά ερωτήματα για την ιδιωτικότητα. Αυτό ώθησε την **Ε.Ε.**^[2] και τις **Η.Π.Α.**^[3] να εκδώσουν οδηγίες για τη χρήση τους και την ενημέρωσή του χρήστη, για κάθε ιστότοπο που τα χρησιμοποιεί.^[4] Υπάρχουν προγράμματα που καθαρίζουν τα κακόβουλα cookies, ενώ αν ο χρήστης επιθυμεί να τα διαγράψει δίνεται αυτή η δυνατότητα μέσα από το **φωλομετρητή** ιστοσελίδων.

Εξατομίκευση^[5]

Οι δικτυακοί τόποι με την χρήση των συγκεκριμένων πληροφοριών (cookies) έχουν την δυνατότητα να προσφέρουν προσωποποιημένες υπηρεσίες που καλύπτουν τις εξατομικευμένες ανάγκες του συγκεκριμένου χρήστη, αποσκοπώντας τελικά στην αύξηση της επισκεψιμότητας/ κέρδους τους. Τα cookies διαδραματίζουν καθοριστικό ρόλο στην λειτουργία του διαδικτυακού τόπου αλλά και των ψηφιακών εφαρμογών. Καθορίζουν τον τρόπο λειτουργίας, εμφάνισης και χρήσης της παρουσίας των διαδικτυακών μέσων και τα παραπάνω να καθορίζει εξατομικευμένα ο κάθε χρήστης. Σε αυτό τον βαθμό η προσφορά υπηρεσιών και εργαλείων που να απευθύνονται στον κάθε επισκέπτη και στις ανάγκες του δεν έχει κάποιο προηγούμενο στην ιστορία του εμπορίου. Η νέα αυτή οικονομία που βασίζεται στην διαφήμιση, την αγορά και διακίνηση πληροφοριών, προϊόντων και υπηρεσιών σε παγκόσμιο επίπεδο με μόνο σύνορο τις προτιμήσεις και επιλογές των χρηστών δεν έχει προηγούμενο στην ανθρώπινη ιστορία.

Οι ερευνητές αλλά και γενικότερα οι ειδικοί που μελετούν το πεδίο που αφορά την επικοινωνία ανθρώπου-υπολογιστή, την στατιστική, την διαφήμιση και την επικοινωνία γενικότερα δείχνουν ιδιαίτερο ενδιαφέρον για τα cookies και τις λειτουργίες τους. Τα cookies υπάρχουν και χρησιμοποιούνται σε όλους τους διαδικτυακούς τόπους αλλά οι επισκέπτες των διαδικτυακών τόπων ειδικά στην Ελλάδα δεν διαθέτουν επαρκή ενημέρωση.

https://el.wikipedia.org/wiki/HTTP_cookies

Είναι επίσης θεμιτό να προβληθεί και το δεκάλεπτο βίντεο του SaferInternetGreece, το “Παντοπωλείο”.



To Pantopoleion - The Grocery Store subtitled in all EU languages

163.046 προβολές · 28 Ιαν 2015



ΜΟΥ ΑΡΕΣΕΙ

ΔΕΝ ΜΟΥ ΑΡΕΣΕΙ

ΚΟΙΝΟΠΟΙΗΣΗ

ΑΠΟΘΗΚΕΥΣΗ



SaferInternetGreece
1,99 χιλ. εγγεγραμμένοι

ΕΓΓΡΑΦΗΚΑΤΕ



Η παρουσίαση βρίσκεται στο <https://slides.com/anyapp/deck>

[Περισσότερο υλικό μπορείτε να βρείτε εδώ](#)