ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Προστασία προσωπικών δεδομένων στο Διαδίκτυο

Δρ. Κωνσταντίνος Λιμνιώτης

Ειδικός Επιστήμονας Πληροφορικής, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

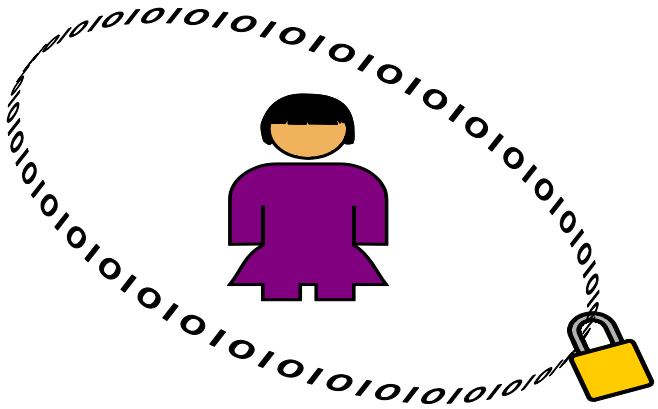
Εισαγωγικά

- Η έννοια της προστασίας προσωπικών δεδομένων είναι στενά συνυφασμένη (αν και δεν ταυτίζεται) με την έννοια της ιδιωτικότητας
- Η προστασία προσωπικών δεδομένων είναι θεμελιώδες ανθρώπινο δικαίωμα (Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης)
- Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) – γνωστός ως GDPR
  - Ν. 4624/2019 (ρυθμίζει επιμέρους θέματα που ο ΓΚΠΔ «αφήνει» στον εθνικό νομοθέτη)
  - Ν. 3471/2006 για την προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες (ενσωματώνει τη λεγόμενη e-Privacy Οδηγία της ΕΕ)
- Αρμόδια εποπτική Αρχή: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Το νομικό πλαίσιο θέτει προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων, ορίζει υποχρεώσεις και αντίστοιχα δικαιώματα
  - **Η ασφάλεια των προσωπικών δεδομένων είναι μία βασική απαίτηση**
  - Όμως: ένας απλός χρήστης δεν πρέπει να επαφίεται στο ότι όσοι επεξεργάζονται προσωπικά του δεδομένα τηρούν το νομικό πλαίσιο…..

Τι είναι προσωπικά δεδομένα;

Προσωπικά δεδομένα είναι κάθε πληροφορία που μας χαρακτηρίζει, όπως για παράδειγμα:

- το όνομά μας,
- η διεύθυνσή μας,
- το τηλέφωνό μας,
- τα ενδιαφέροντά μας,
- φωτογραφίες ή video που μας περιέχουν,
- οι απόψεις μας (σε οποιοδήποτε τομέα)
- …



- Η έννοια είναι πολύ πιο ευρεία από ό,τι ίσως νομίζουμε
  - Ένα «ψευδώνυμο» (nick name) που επιλέγουμε, ακόμα και αν δεν «αντανακλά» από μόνο του την ταυτότητά μας
  - Πληροφορίες που «εκπέμπει» η συσκευή μας από την οποία πλοηγούμαστε στο Διαδίκτυο
    - Π.χ. διεύθυνση IP, MAC address, Android ID,….

Επεξεργασία προσωπικών δεδομένων

Οποιαδήποτε «ενέργεια» επί προσωπικών δεδομένων συνιστά επεξεργασία τους

Σε όλους τα δεδομένα μας υφίστανται επεξεργασία από «κάποιον» – είμαστε δηλαδή υποκείμενα των δεδομένων

Οι ίδιοι όμως ενδεχομένως επεξεργαζόμαστε δεδομένα άλλων – γινόμαστε υπεύθυνοι επεξεργασίας

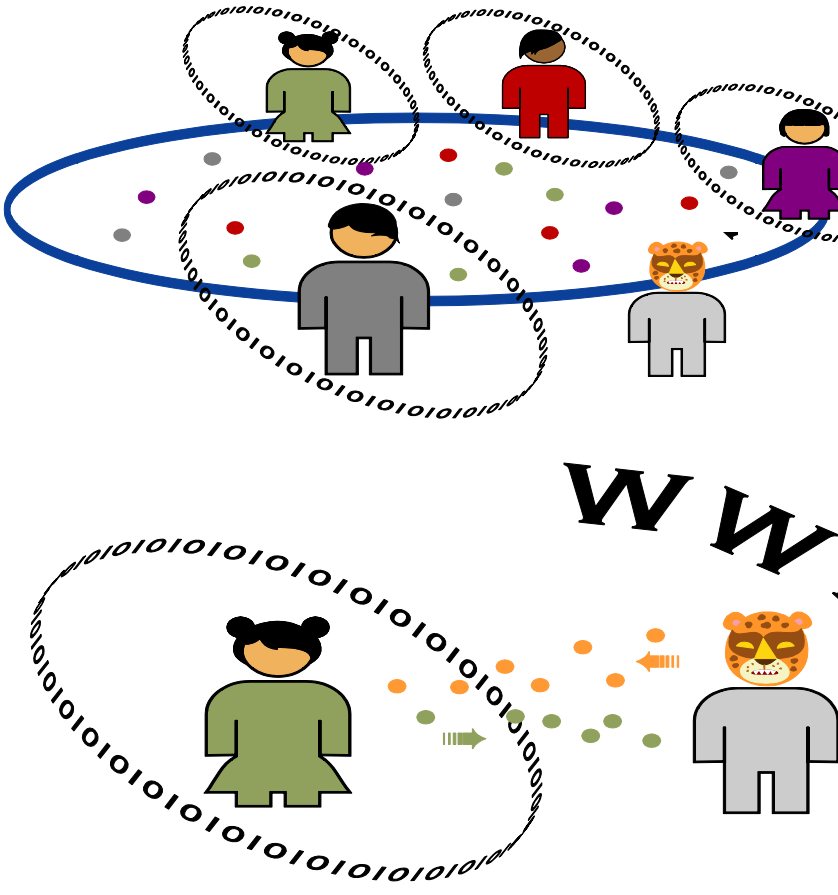
Ειδικά στο Διαδίκτυο, η επεξεργασία προσωπικών μας δεδομένων είναι συνεχής

Ένα «περίπου» τυπικό 24ωρο

7:15	**Διαβάζεις το e-mail σου** – ο πάροχος ηλεκτρονικών επικοινωνιών καταγράφει την ώρα που μπήκες στο λογαριασμό σου, τον αποστολέα του μηνύματός σου, καθώς και την ώρα που σου έστειλε το μήνυμα.
7:30	**«Σερφάρεις» στο Facebook** – πατάς «like» σε ένα άρθρο γνώμης επειδή συμφωνείς. Όλοι όσοι μπορούν να δουν το προφίλ σου αποκτούν μία εικόνα για τις απόψεις σου επί του συγκεκριμένου ζητήματος.
7:50	**Πηγαίνεις με το αυτοκίνητο στο στην εργασία σου** – το αυτοκίνητο διαθέτει συσκευή GPS που καταγράφει τη διαδρομή σας από το σπίτι στο σχολείο. Σε κάποια σημεία της διαδρομής υπάρχουν κάμερες ρύθμισης της κυκλοφορίας και ελέγχου παραβιάσεων του Κώδικα Οδικής Κυκλοφορίας.
8:30	**Μπαίνεις στο γραφείο σου** – έχεις ήδη «χτυπήσει» την κάρτα για την προσέλευσή σου. Όταν «ανοίγεις» το σταθμό εργασίας σου και συνδέεσαι στο δίκτυο, καταγράφεται εσωτερικά ότι ο υπολογιστής σου ενεργοποιήθηκε, τι διεύθυνση δικτύου έλαβε κ.α.
12:00	**Πραγματοποιείς τηλεδιάσκεψη για τη δουλειά** – η εικόνα σου, ο ήχος σου, ό,τι γράφεις στο chat τα βλέπουν όλοι οι συμμετέχοντες. Πληροφορίες τηρεί και ο πάροχος της υπηρεσίας τηλεδιάσκεψης (ενδεχομένως να έχει την τεχνική δυνατότητα να καταγράψει και να δει επακριβώς την τηλεδιάσκεψη)
15:00	**Σερφάρεις στο διαδίκτυο από το γραφείο σου** – ο browser που χρησιμοποιείς καταγράφει τις σελίδες που επισκέπτεσαι. Κάποιες σελίδες εγκαθιστούν στον υπολογιστή σου μικρά αρχεία (cookies) ώστε να μπορούν να σε αναγνωρίζουν όταν θα τις ξαναεπισκεπτείς.
15:15	**Κλικάρεις μια διαφήμιση που έχει ενδιαφέρον** – η διαφημιστική εταιρεία καταγράφει τις προτιμήσεις σου ώστε να μπορεί να σου στέλνει προσφορές για προϊόντα που σε ενδιαφέρουν.
15:30	**«Κατεβάζεις» μία εφαρμογή στο κινητό σου** – δηλώνεις ότι δίνεις άδεια (permission) στην εφαρμογή να έχει πρόσβαση σε διάφορα στοιχεία της συσκευής σου (gps location, camera, contacts….)
16:00	**Ψάχνεις στοιχεία για την αναφορά που πρέπει να παραδώσεις αύριο** – στο google καταγράφονται όλες οι αναζητήσεις που πραγματοποιείς, μαζί με την χρονική στιγμή της αναζήτησης και τη διεύθυνση δικτύου (IP) με την οποία ο υπολογιστής σου συνδέεται, μέσω του Παρόχου, στο διαδίκτυο.
18:00	**Μπαίνεις σε ένα κατάστημα** – στην είσοδο υπάρχει κάμερα που καταγράφει όσους μπαίνουν και βγαίνουν. Σου ζητάνε να συμπληρώσεις μία φόρμα με στοιχεία σου, για να σε ενημερώνουν για προσφορές που θα έχει το κατάστημα στο μέλλον.
19:30	**Κάνεις διαδικτυακή αγορά** – εισάγεις στοιχεία όπως την πιστωτική σου κάρτα. Για την εύρεση του προϊόντος που έψαχνες, έκανες αναζήτηση σε διάφορα συναφή προϊόντα για τα οποία συνεχίζεις στις επόμενες ημέρες να λαμβάνεις διαφημίσεις.
22:00	**Μπαίνεις στο Facebook** – «ανεβάζεις» μία φωτογραφία σου, η οποία απεικονίζει και άλλους (μήπως και τα παιδιά σου;)

Internet: ποιοι κίνδυνοι υπάρχουν;

- Αποκάλυψη δεδομένων
  - Κάποιος «κρυφακούει» με κάποιον τρόπο ή «παρεισφρύει» στον υπολογιστή μας και ανακαλύπτει δεδομένα μας που δεν θα έπρεπε
    - Π.χ. με κακόβουλο λογισμικό ή «αναγκάζοντάς» μας να μεταβούμε σε όχι ασφαλείς ιστοσελίδες κ.α.
  - Κάποιος υποδύεται κάποιον άλλον στο Διαδίκτυο με σκοπό να μας ξεγελάσει (π.χ. για κλοπή προσωπικών δεδομένων, χρημάτων κλπ.)
    - Παραπλανητικά (phishing) e-mail, «ψεύτικοι» λογαριασμοί χρηστών, μηνύματα που φαίνονται να προέρχονται από φίλους μας κ.α.
  - Μόνοι μας αποκαλύπτουμε προσωπικά δεδομένα, γιατί θεωρούμε ότι «δεν πειράζει»
    - Ενδεχομένως να αποκαλύπτουμε και δεδομένα άλλων, χωρίς να έχουμε τη συγκατάθεσή τους!
    - Π.χ. σε μία «απλή» εφαρμογή κοινωνικής δικτύωσης..



Πώς εξασφαλίζω ασφάλεια;

- **Υπάρχουν τεχνικές που να εξασφαλίζουν την απόλυτη ασφάλεια;**

- **Η απάντηση είναι: σωστή και «μυαλωμένη» χρήση**
- **Βασικές αρχές:**
  - «Δικτυωνόμαστε» με ασφάλεια – προσέχουμε τι «κλικάρουμε» και πού «σερφάρουμε»..
  - Γνωρίζουμε με ποιον μιλούμε
  - Σκεφτόμαστε προτού αναρτήσουμε (είτε δικά μας προσωπικά δεδομένα είτε άλλων)
  - Γνωρίζουμε (τουλάχιστον) τα βασικά που πρέπει να εφαρμόζουν οι πάροχοι υπηρεσιών/εφαρμογών

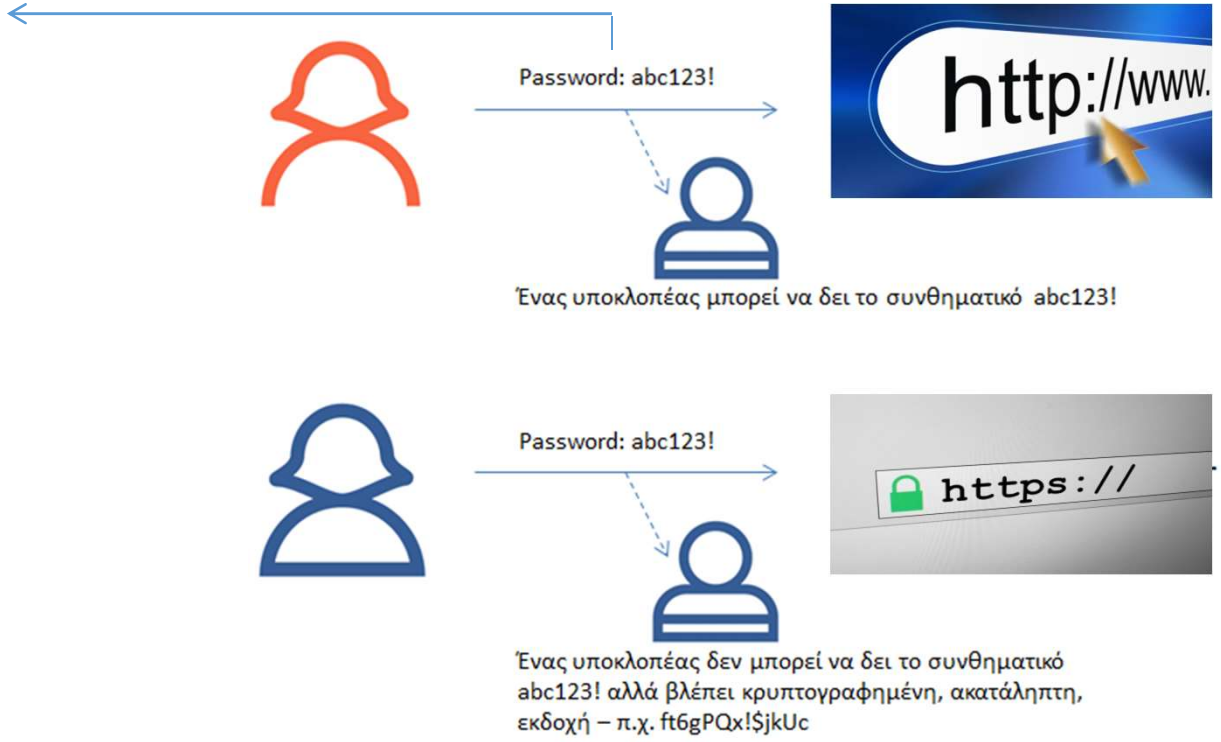
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ασφαλής πλοήγηση

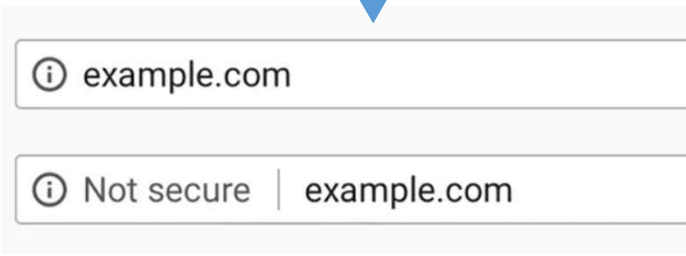
Επίσκεψη σε ασφαλείς (https) ιστοσελίδες

- Γνωρίζετε τη διαφορά μεταξύ http και https για μία ιστοσελίδα;

ή! Δεν είναι
ς συνθηματικό
α δούμε σε



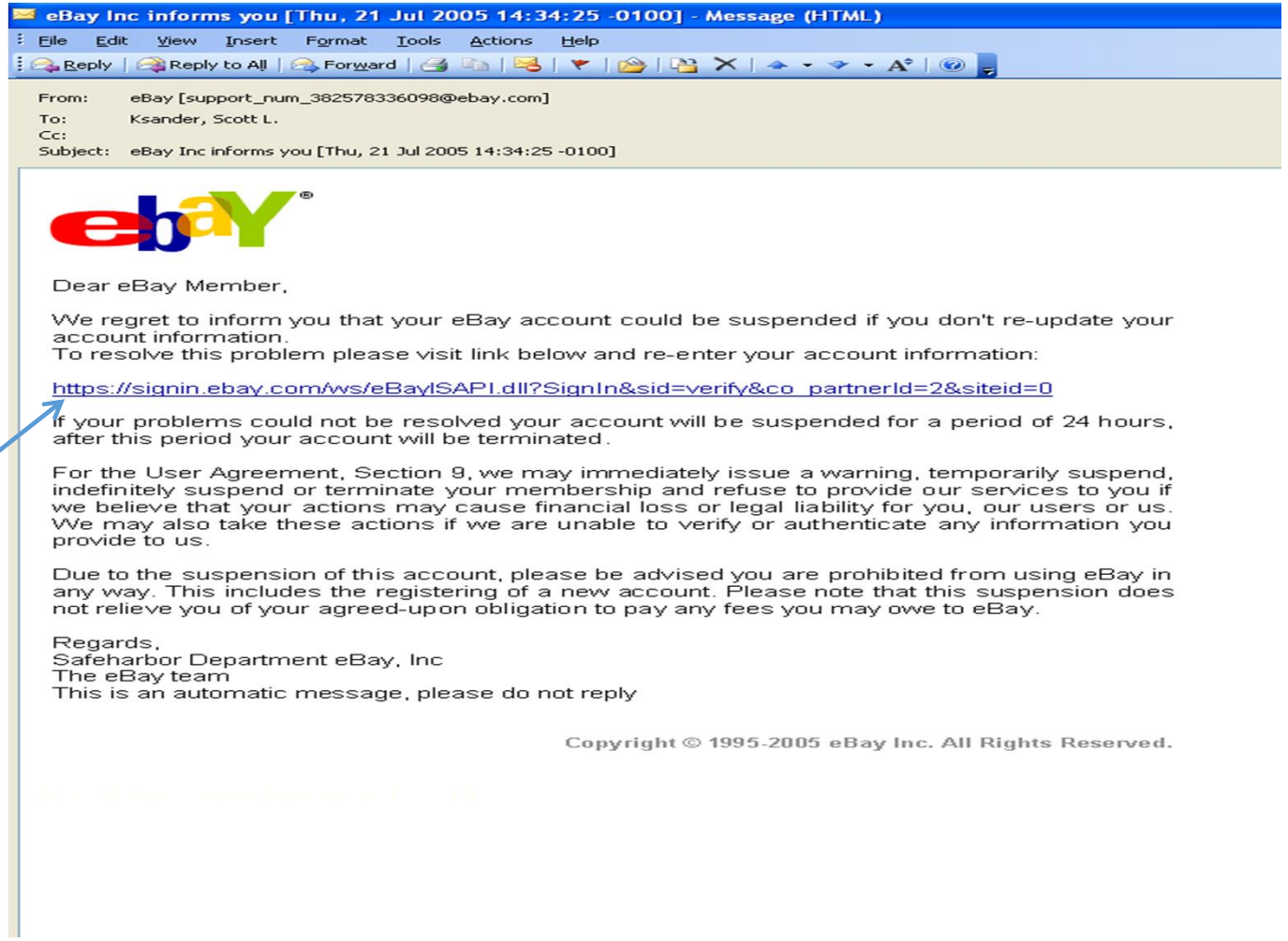
- Κανείς δεν μπορεί να διαβάσει τα δεδομένα που πληκτρολογούμε
- Είμαστε σίγουροι ότι έχουμε συνδε στη σωστή ιστοσελίδα
  - Διαφορετικά, το πρόγραμμα πλοήγησής μας θα «διαμαρτύρονταν» ότι υπάρχ ζήτημα ασφάλειας…



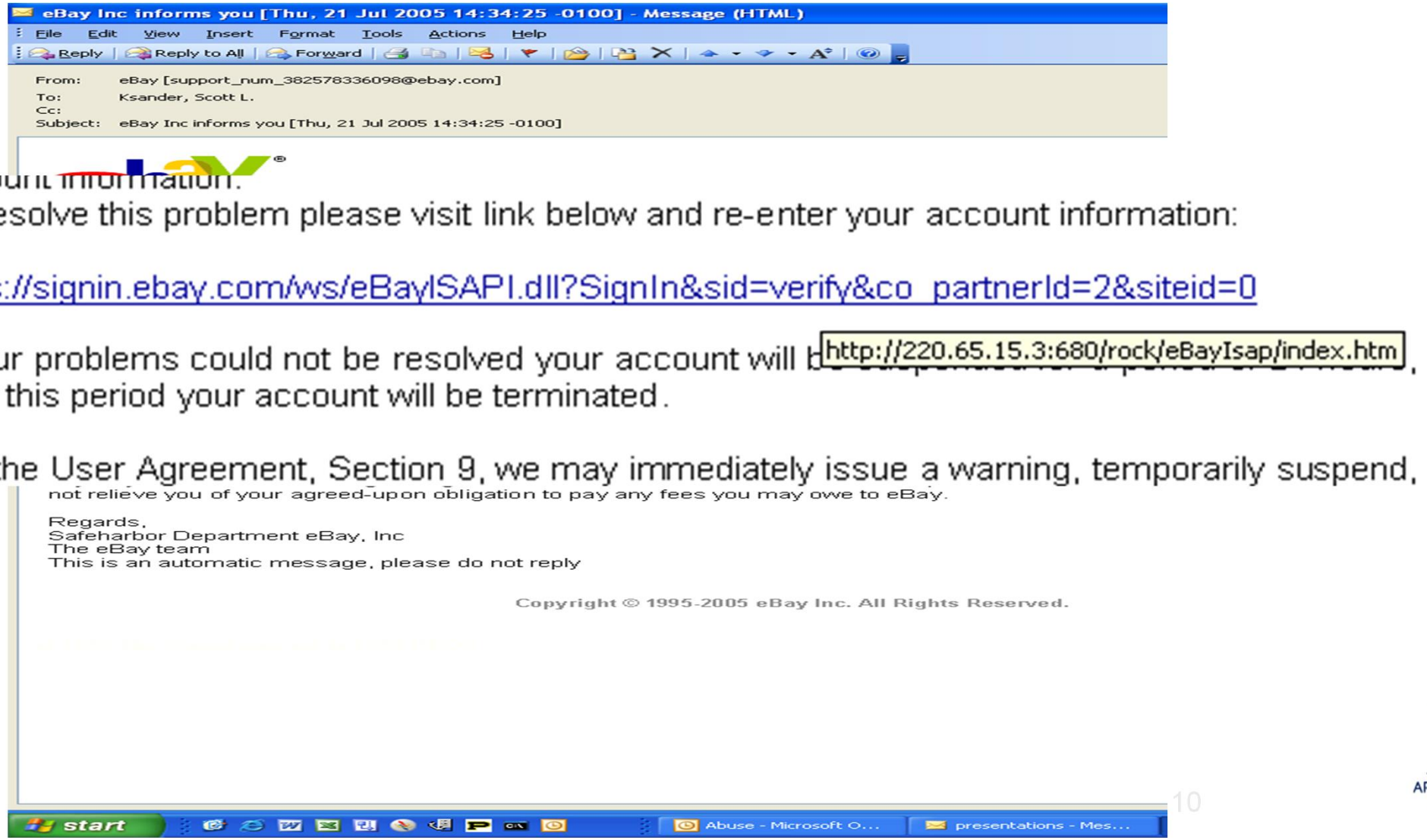
Δεν πρέπει να εισάγουμε ποτέ προσωπικά μας δεδομένα σε http ιστοσελίδες!

«Επιθέσεις» σε απλούς χρήστες – «ψάρεμα»

Φαινομενικά γνησιο e-mail… Μας «προτρέπει» να κλικάρουμε σε σύνδεσμο που φαίνεται έγκυρος (και είναι και https…) Ομως…



Προσοχή στο σύνδεσμο που μας προτρέπει να επισκεφτούμε!



“Ψάρεμα” (Phishing)

- Phishing: αποστολή παραπλανητικών μηνυμάτων (e-mail), με στόχο την εξαπάτηση χρηστών
  - Τα μηνύματα μπορούν είτε να μας προτρέπουν να δώσουμε άμεσα δικές μας πληροφορίες (π.χ. για να «αποφύγουμε» απενεργοποίηση λογαριασμού τραπέζης ή για να «ελέγξουμε» υποτιθέμενη ύποπτη συναλλαγή) είτε να πατήσουμε κάποιο link (π.χ. για ενεργοποίηση λογαριασμού ή για να κερδίσουμε ένα δώρο)
    - «Πατώντας» όμως στο link μπορεί:
      - να μεταφερθούμε σε μία ψεύτικη ιστοσελίδα που «μιμείται» κάποια γνήσια και να εισάγουμε σε αυτή τα στοιχεία μας
      - να εγκατασταθεί στον υπολογιστή μας κακόβουλο λογισμικό που θα υποκλέψει δεδομένα μας

- Να θυμόμαστε πάντα ότι:
  - Κανείς οργανισμός δεν θα μας ζητήσει μέσω e-mail προσωπικά δεδομένα (κωδικούς, ονοματεπώνυμο κτλ.)
  - Δεν έχει σημασία ποιος «φαίνεται» ότι είναι ο αποστολέας!
    - Κάποια παραπλανητικά μηνύματα είναι πολύ καλά «καμουφλαρισμένα» δυστυχώς….

Παράδειγμα παραπλανητικού μηνύματος

Πρόκειται για μήνυμα που έλαβα στις 22 Ιανουαρίου 2022 (ένα από τα πολλά που λαμβάνω καθημερινά….. Αντίστοιχα μηνύματα λαμβάνω από

τις Τράπεζες)

Θέμα: Η πρόσβαση στον λογαριασμό σας είναι προσωρινά απενεργοποιημένη - 01/22/2022 05:43:15 am
Από: "Alpha Bank GR" <alpha59339911135956@cavedeschamps.ch>
Ημερομηνία: Σαβ, Ιανουάριος 22, 2022 6:43
Προς: klimn@di.uoa.gr
Περισσότερες Επιλογές...

Αγαπητέ πελάτη,

Εντοπίσαμε κάποια ασυνήθιστη δραστηριότητα στον λογαριασμό σας, πρέπει να συνδεθείτε μέσω του παρακάτω συνδέσμου και να επιβεβαιώσετε την ταυτότητά σας, διαφορετικά ο λογαριασμός σας θα τερματιστεί εντός 24 ωρών.

επιβεβαιώστε τώρα

---

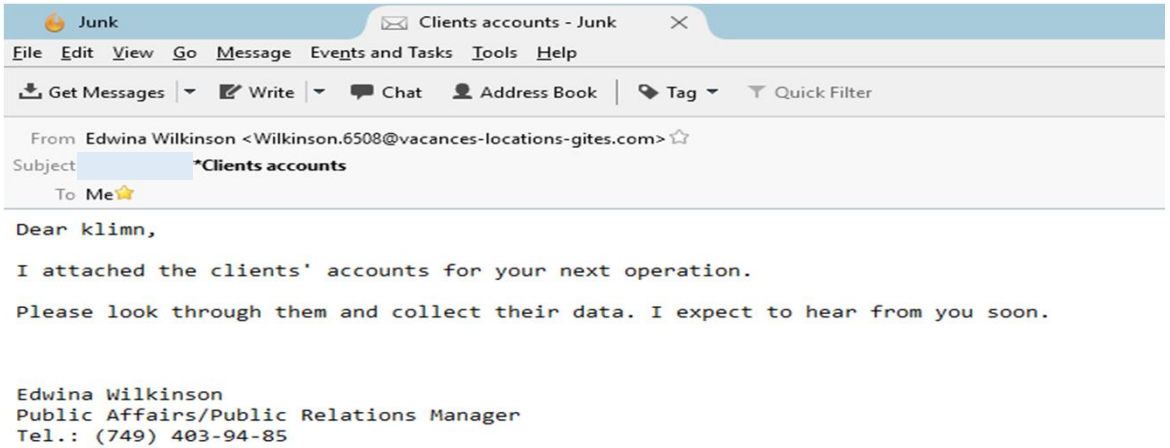
*Αυτό είναι ένα αυτοματοποιημένο μήνυμα και χρειάζεται προσεκτική προσοχή, μην απαντήσετε.

Ευχαριστώ για την εμπιστοσύνη σας,

ALPHA BANK

Ransomware

- Σήμερα, περισσότερα από το 90% των παραπλανητικών (phishing) e-mail είναι τύπου «ramsonware»
  - Ο παραλήπτης τους, «ανοίγοντας» το επισυναπτόμενο αρχείο ενεργοποιεί άθελά του λογισμικό που κρυπτογραφεί σημαντικά αρχεία του υπολογιστή του, χωρίς να μπορεί να τα ανακτήσει
  - Ο επιτιθέμενος ζητάει χρήματα για να αποκρυπτογραφήσει τα αρχεία



Προσοχή στο συνημμένο αρχείο!

Το αποτέλεσμα ενός ransomware…

Άλλες περιπτώσεις παραπλάνησης - «Ψεύτικο» μήνυμα από φίλο

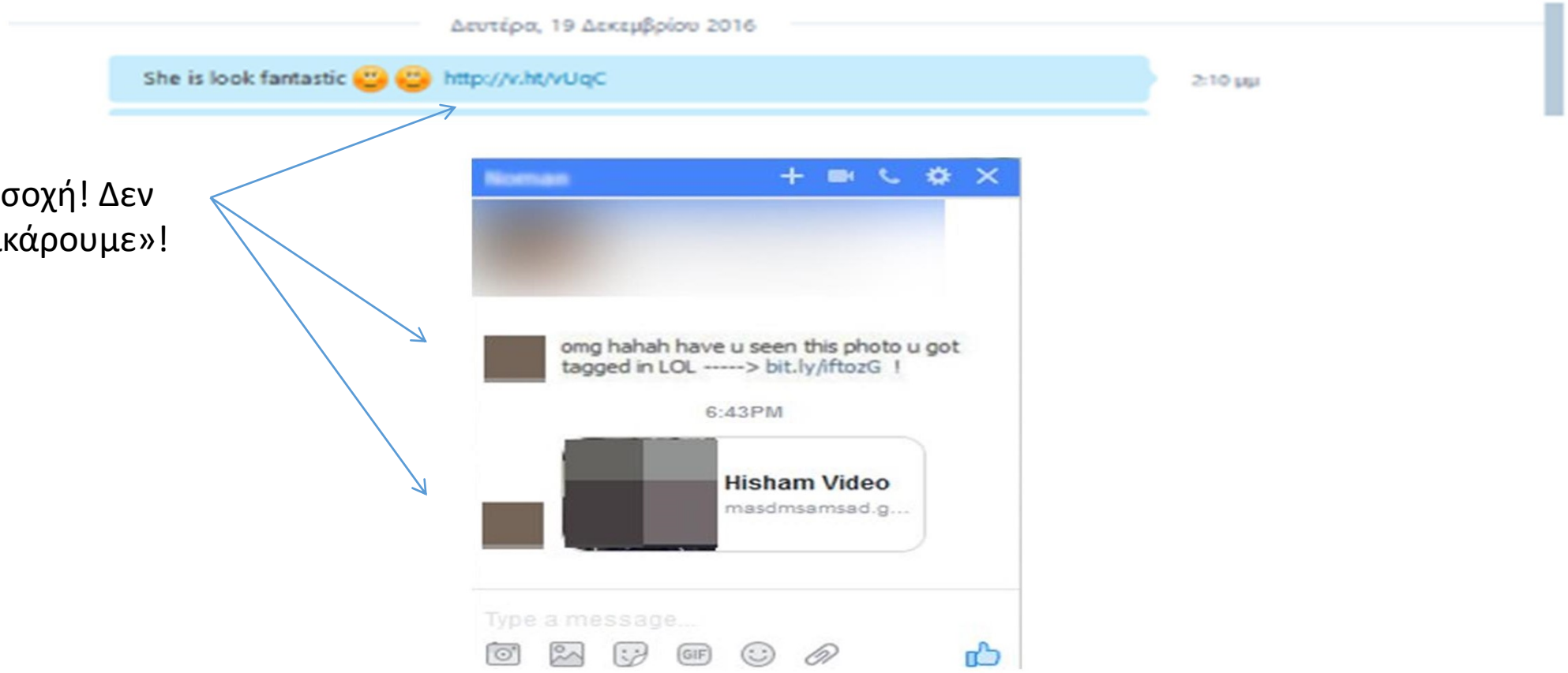
- Ενδεχομένως να λάβουμε ένα «περίεργο» μήνυμα από φίλο σου σε κοινωνικό δίκτυο ή chat
- Έχει συμβεί:

- 8:38pm Rhiannon
  Hi
- 8:38pm Elias
  Hi!
- 8:39pm Rhiannon
  I am stranded in london and i need your help
- 8:40pm Rhiannon
  i was mugged at a gun point in Kentish town, it was a brutal experience, all cash i had on me were stolen and my credit card was collected too now i'm left with no money here. I need you to loan me some money to get a plane ticket

- Πηγή: (http://eliasbizannes.com/blog/2009/01/phishing-for-fraud-on-facebook/)
- Το ότι φαίνεται ότι το στέλνει ο φίλος μας δεν σημαίνει ότι το στέλνει πράγματι!
  - Επικοινωνούμε άμεσα μαζί του να τον ενημερώσουμε – πιθανώς κάποιος να έχει υποκλέψει το συνθηματικό του!

Άλλες περιπτώσεις παραπλάνησης - «Ψεύτικο» μήνυμα από φίλο

Προσοχή! Δεν «κλικάρουμε»!



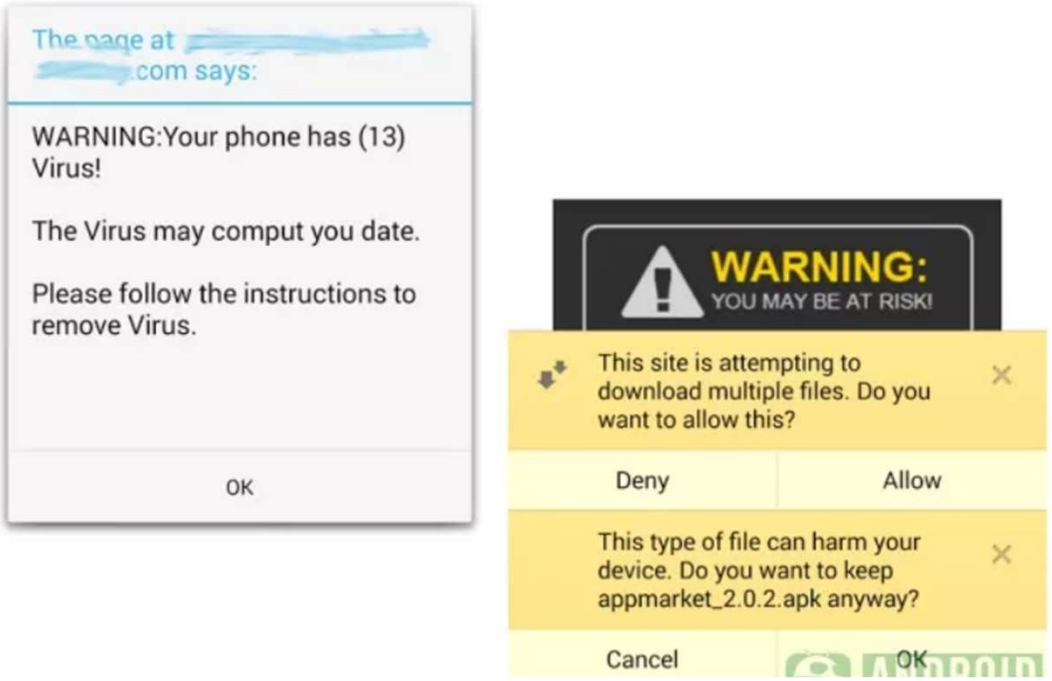
«Ψεύτικες» ειδήσεις

- Ενδεχομένως να δούμε ότι κάποιος - ακόμα και «φίλος» μας - αναρτά κάτι δημόσια ή έδειξε ενδιαφέρον («like») σε κάποιο περιστατικό / είδηση αξιοπερίεργο που «κινεί το ενδιαφέρον»

- Κάποιες «ειδήσεις» φαίνονται αρκετά «ύποπτες» - αν πράγματι ήταν αληθείς, θα εμφανίζονταν σε όλα τα ειδησεογραφικά sites….

Η περίπτωση των «έξυπνων» κινητών

- Αναδυόμενα «παράθυρα» που μας προτρέπουν να κάνουμε κλικ, επικαλούμενα ως και θέματα ασφάλειας!
  - Και όχι μόνο στα «έξυπνα» κινητά αλλά και σε Η/Υ… (ιδίως αν επισκεφτεί κανείς ιστοσελίδες που προσφέρουν «δωρεάν» χρήσιμα προγράμματα λογισμικού…)



Τι πραγματικά συμβαίνει;

- Σε όλες τις προηγούμενες περιπτώσεις, απλά «πατώντας» πάνω σε αυτά τα links πιθανότατα θα εγκατασταθεί αυτόματα κακόβουλο λογισμικό στον υπολογιστή μας!
  - Με συνέπειες απρόβλεπτες (έως, πιθανώς, και υποκλοπή στοιχείων της συσκευής μας αλλά «παραβίαση» του λογαριασμού μας)
- Αν αυτό το link «προέρχεται» από φίλο μας, πιθανότατα ο ίδιος έχει ήδη κάνει αυτό το λάθος και αποστέλλει, χωρίς να το ξέρει, τέτοια μηνύματα
  - Θα πρέπει να τον ειδοποιήσουμε αμέσως!
- Πολύ προσοχή στις αναρτήσεις – προσκλήσεις των άλλων!
  - Τα «περίεργα» μηνύματα δεν είναι ποτέ αθώα, από όποιον κι αν (φαίνεται ότι) προέρχονται

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ

Προστασία συνθηματικών

Συνθηματικά (Passwords)

- Δεν δίνουμε ποτέ το συνθηματικό μας σε κανέναν, ούτε σε φίλο μας
  - Ακόμα και αν μας το ζητήσουν για «σοβαρό» λόγο – π.χ. για να μην «κλειδώσει» ο λογαριασμός μας
  - Κανένας φορέας δεν θα μας ζητήσει το συνθηματικό με e-mail ή μέσω κοινωνικού δικτύου/chat
- Δεν γράφουμε το συνθηματικό σε κάποιο χαρτί ή σε αρχείο στον υπολογιστή – μπορεί να «πέσει» στα χέρια οποιουδήποτε!

- Το συνθηματικό μας πρέπει να είναι μη προβλέψιμο
  - Δεν πρέπει να περιέχει κατά κανένα τρόπο το όνομά μας, το τηλέφωνό μας, την ημερομηνία γέννησής μας, την αγαπημένη ομάδα, το αγαπημένο μας μουσικό συγκρότημα, το όνομα των παιδιών μας κτλ.
    - Δηλαδή, να μην έχει κανένα προσωπικό μας δεδομένο!!
    - Πολλές από αυτές τις πληροφορίες μπορεί να τις έχουμε ήδη, έμμεσα, κοινοποιήσει και σε κοινωνικό δίκτυο!!

Μη προβλέψιμα συνθηματικά

ς επιλέγουμε μη προβλέψιμα συνθηματικά;

- Δυστυχώς, τα συνθηματικά που μπορούμε να αποστηθίσουμε εύκολα είναι προβλέψιμα
- Λίστα με τα πιο συχνά χρησιμοποιούμενα συνθηματικά στον κόσμο (από το site https://nordpass.com/most-common-passwords-list/)

RANK	PASSWORD
1	123456
2	123456789
3	12345
4	qwerty
5	password
6	12345678
7	111111

RANK	PASSWORD
8	123123
9	1234567890
10	1234567
11	qwerty123
12	000000
13	1q2w3e
14	aa12345678

RANK	PASSWORD
15	abc123
16	password1
17	1234
18	qwertyuiop
19	123321
20	password123
21	1q2w3e4r5t

RANK	PASSWORD
22	iloveyou
23	654321
24	666666
25	987654321
26	123
27	123456a
28	qwe123
29	1q2w3e4r

- Αν έχετε κάποιο από αυτά, αλλάξτε το αμέσως!

έπει λοιπόν να έχουμε συνθηματικά που δεν μπορεί να μαντέψει κανείς (ούτε άνθρωπος ούτε υπολογιστής)

- Να μην είναι λέξη, να έχει μέγεθος τουλάχιστον 8 γράμματα, να έχει και αριθμούς εκτός από γράμματα,…
- Να μην σχετίζεται με προσωπικές μας πληροφορίες!

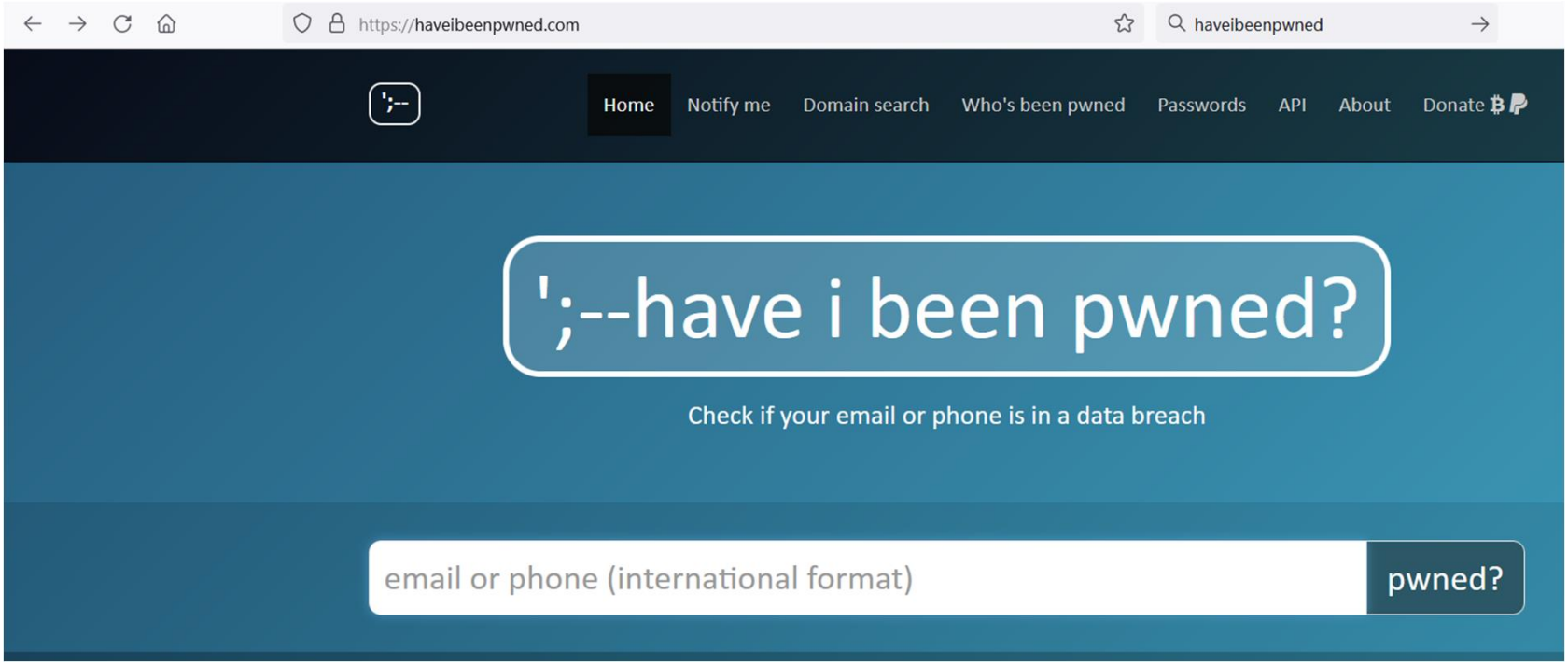
Άρα;

Ιδέα για δημιουργία «ισχυρού» συνθηματικού που θα το θυμόμαστε

- Σκεφτόμαστε μια φράση που μας αρέσει
  - Στίχος τραγουδιού, άλλη αγαπημένη μας φράση κτλ.
- Π.χ. Κάλλιο 5 και στο χέρι παρά 10 και καρτέρει
- Σκεφτείτε ένα συνθηματικό που δημιουργείται από το πρώτο γράμμα κάθε λέξης σε αυτή τη φράση:

  K5ksxp10kk
- Είναι μη προβλέψιμο και, ταυτόχρονα, δεν το ξεχνάμε
  - Δεν υπάρχει λοιπόν καμία ανάγκη να το γράψουμε κάπου
- Αν η αγαπημένη μας φράση δεν περιέχει αριθμούς, μπορούμε απλά να προσθέσου
  έναν ή δύο αριθμούς στην αρχή ή στο τέλος
- Καλό είναι να προσθέτουμε και έναν μη αλφαριθμητικό χαρακτήρα (π.χ. !, $, #)
- Αποφεύγουμε να χρησιμοποιούμε το ίδιο συνθηματικό σε όλες τις υπηρεσίες

Πώς μπορώ να ξέρω αν το συνθηματικό μου έχει διαρρεύσει;



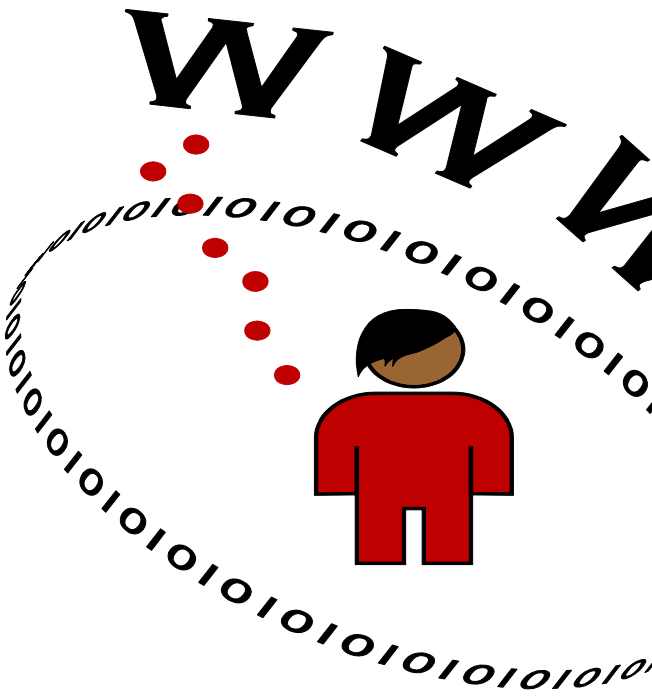
- Σύμφωνα με τον GDPR, αν σε έναν οργανισμό «κλαπούν» τα συνθηματικά των χρηστών του, θα πρέπει να τους ενημερώσει… (εάν δεν είχε ήδη λάβει μέτρα τέτοια ώστε τα συνθηματικά να είναι πλήρως «ακατάληπτα» σε όποιον αποκτήσει πρόσβαση σε αυτά)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Τι πληροφορίες διαμοιράζουμε μόνοι μας;

Σκέφτομαι προτού δημοσιεύσω

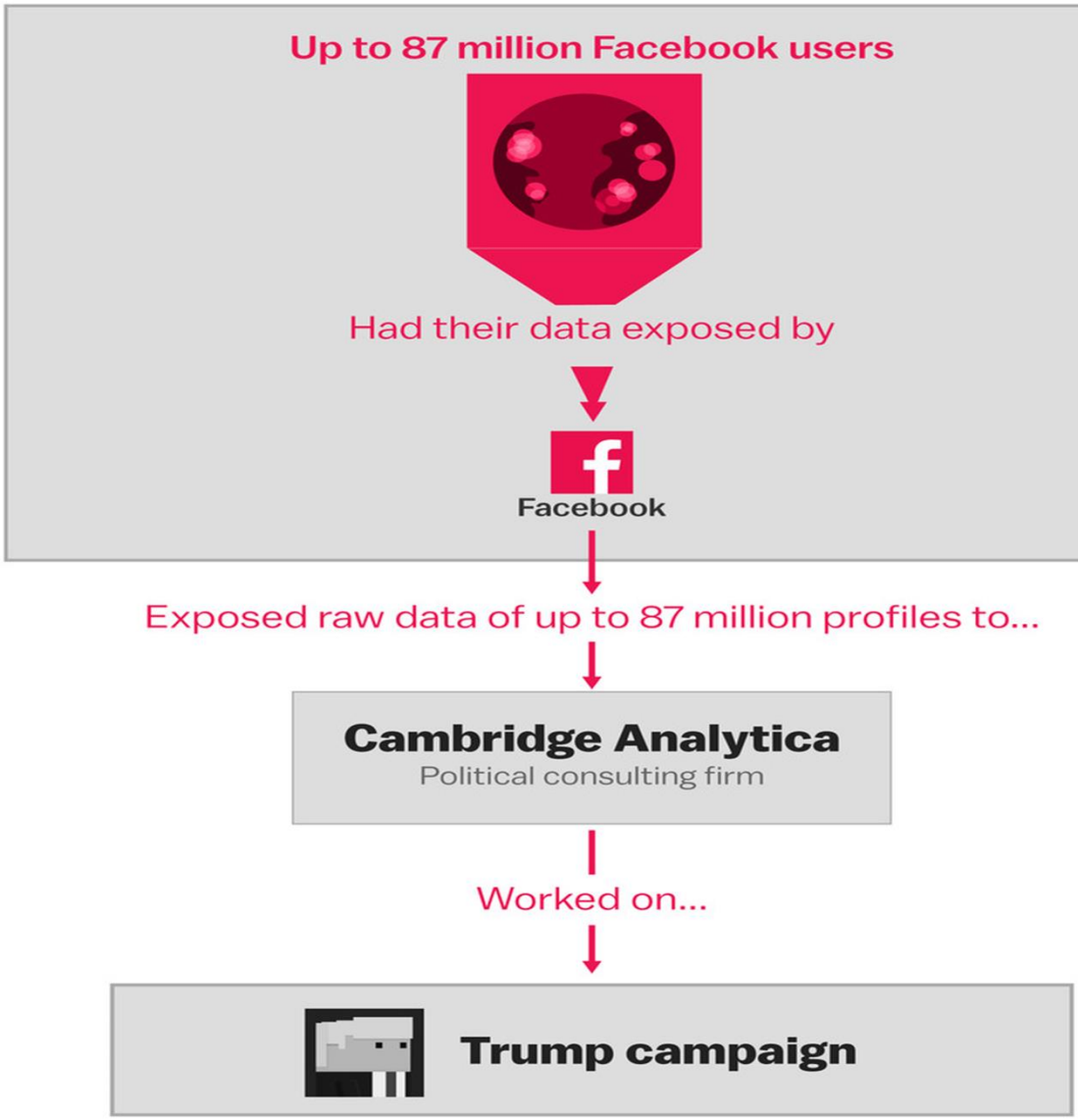
- Το Internet παρέχει τη δυνατότητα να δημοσιοποιήσουμε προσωπικά μας δεδομένα χωρίς, ουσιαστικά, περιορισμούς.
- Δυστυχώς, όσα αναρτούμε μπορούν να χρησιμοποιηθούν για σκοπούς που ίσως δεν τους φανταζόμαστε…
  - Ένα απλό «like» αποκαλύπτει πληροφορίες για εμάς (προτιμήσεις μας, πεποιθήσεις κτλ.)
  - Μόνοι μας «παρέχουμε» πληροφορίες που επιτρέπουν ευχερώς σε άλλους τη δημιουργία ακριβούς προφίλ για εμάς
- Εάν δημοσιεύουμε δεδομένα άλλων (π.χ. φωτογραφίες ή και απλή αναφορά ονόματος άλλου), έχουμε τη συγκατάθεσή τους για αυτό;



- **Τα γραπτά μένουν…**
- Ο GPDR προβλέπει για το «δικαίωμα στη λήθη», αλλά οι νομικές επιταγές είναι αρκετές;
  - **Προτού δημοσιεύσεις… σκέψου!**

Το περιστατικό της Cambridge Analytica (2018)

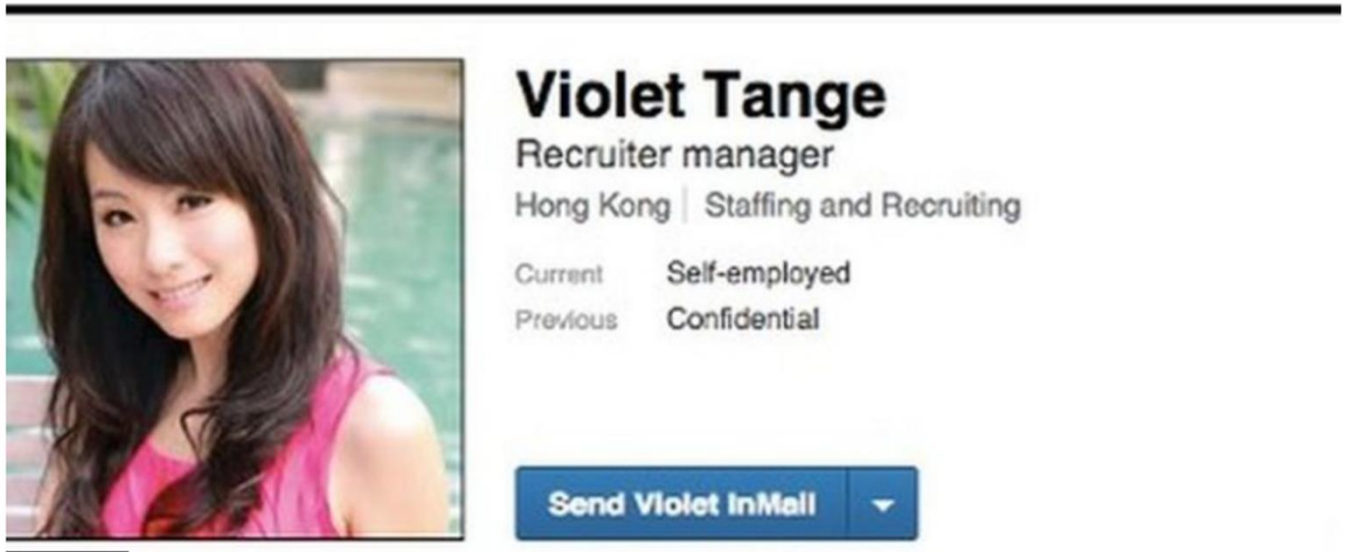
- Μέσω του Facebook, προσωπικά δεδομένα 87 εκατομμυρίων χρηστών του έφτασαν στα χέρια του Aleksandr Kogan, ερευνητή της Cambridge Analytica, η οποία ήταν στην «υπηρεσία» της εκλογικής καμπάνιας του Trump.
- Χρήστες το Facebook «κατέβασαν» μία εφαρμογή, η οποία απέκτησε πρόσβαση στα δεδομένα των φίλων τους, χωρίς οι τελευταίοι να το γνωρίζουν.
- Η εταιρεία πλέον είχε πρόσβαση σε δεδομένα χρηστών τα οποία οι ίδιοι, «απλόχερα», έχουν «διαμοιράσει»
  - Επέτρεπε τη δημιουργία προφίλ (π.χ. ποιες οι απόψεις τους σε συγκεκριμένα ζητήματα)
- Αυτό με τη σειρά του επέτρεπε την «πολιτική χειραγώγησή» τους
  - «Στοχευμένα» διαφημιστικά μηνύματα, προσανατολισμένα στο προφίλ του καθενός, προκειμένου να τον «στρέψουν» σε συγκεκριμένη πολιτική επιλογή



Από την ιστοσελίδα https://www.vox.com

“Ψεύτικα» προφίλ

- Από την ιστοσελίδα του bbc: https://www.bbc.com/news/technology-34994858



- Προσοχή στο τι πληροφορίες μας θα δώσουμε στον «άγνωστο φίλο μας»!
  - Μήπως μόνοι μας δίνουμε «αβίαστα» προσωπικά μας δεδομένα σε αγνώστους?

Τεχνικές «ιχνηλάτησης» χρηστώ

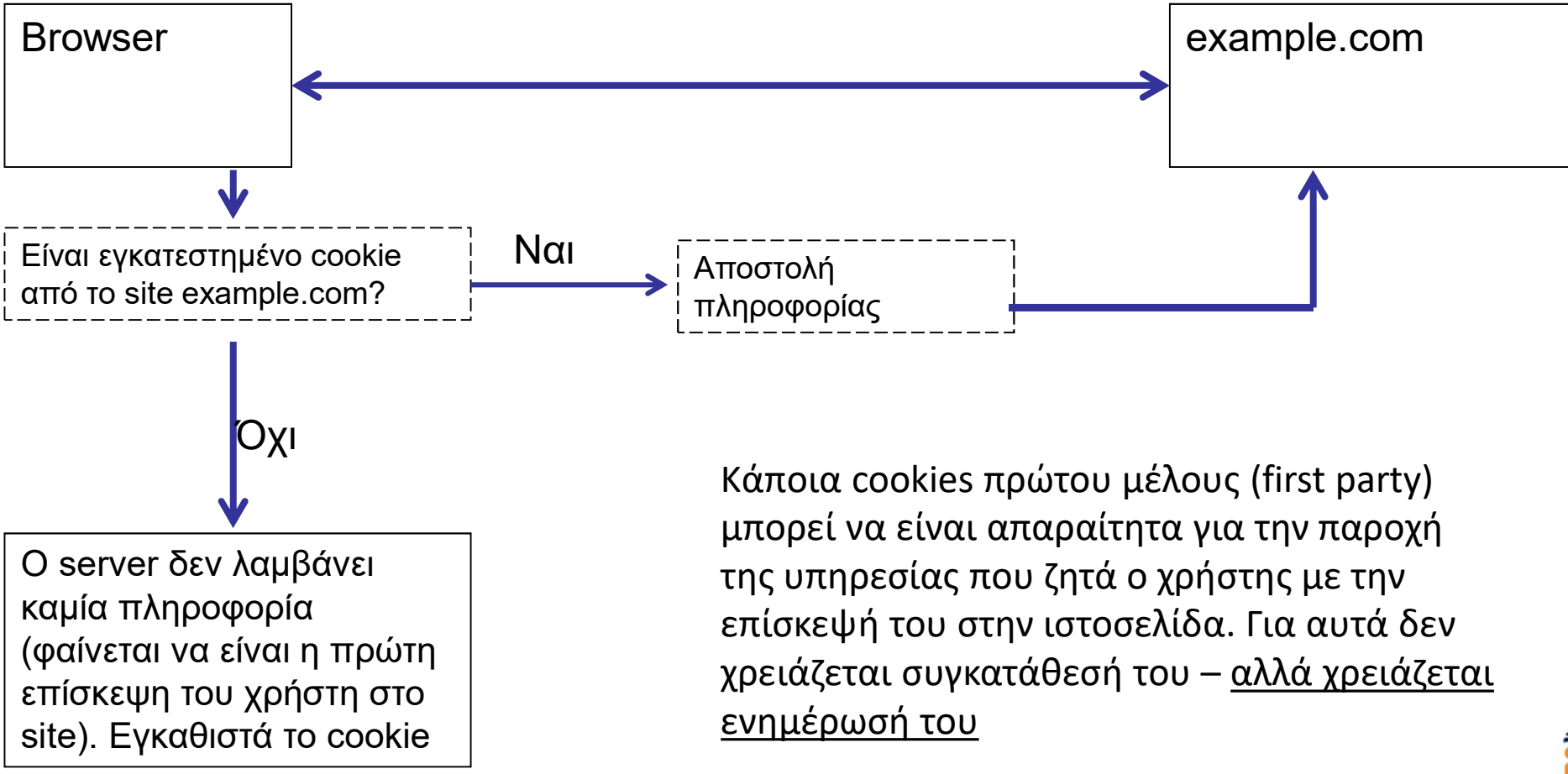
“Ιχνηλάτηση» χρηστών στο Διαδίκτυο

- Πολλοί μηχανισμοί «παρακολούθησης» χρηστών
  - Μέσω αποθήκευσης πληροφορίας στη συσκευή του χρήστη (π.χ. cookies)
  - «Ψηφιακό αποτύπωμα» συσκευής (π.χ. ρυθμίσεις προγράμματος πλοήγησης)

Σε όλες τις συσκευές – ειδικά δε στα «έξυπνα» κινητά, οι προκλήσεις είναι ακόμα μεγαλύτερες

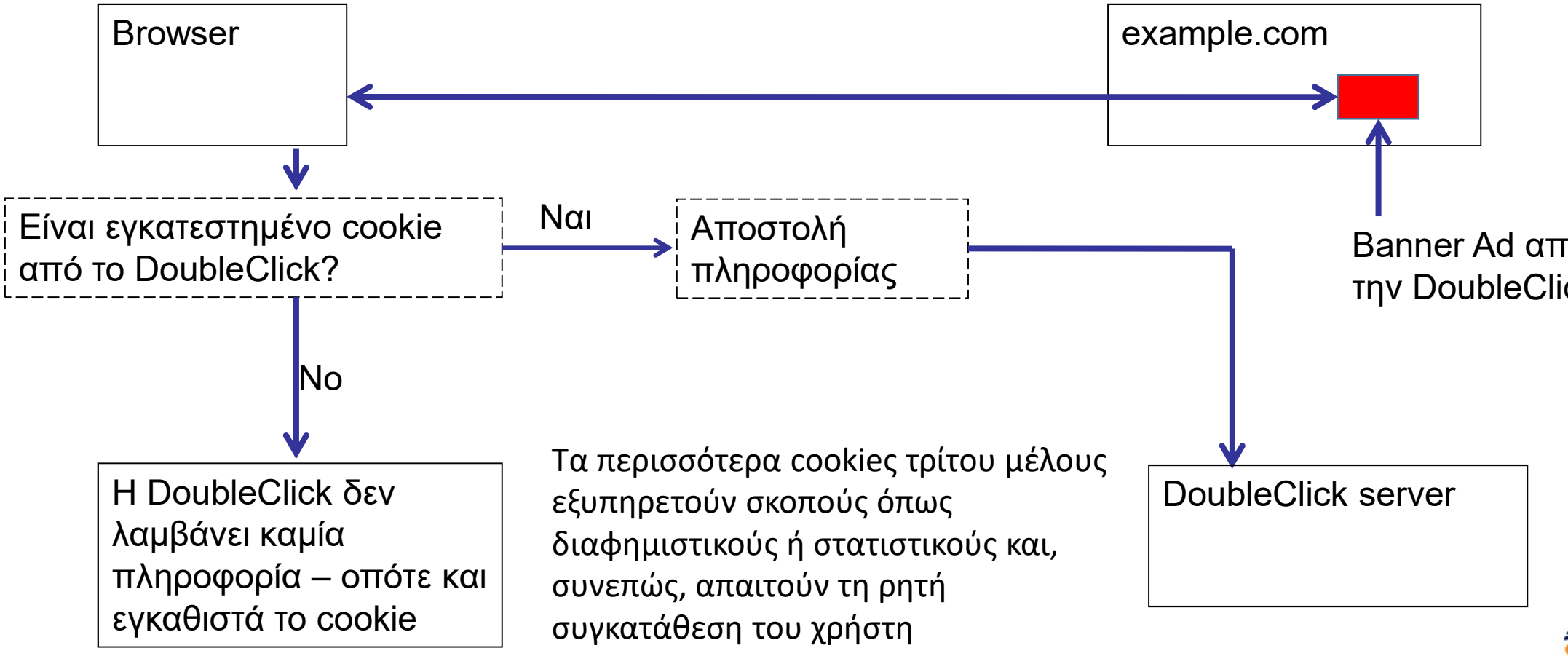
- Υπάρχει σαφές νομικό πλαίσιο – όμως η εμπειρία λέει ότι δεν τηρείται από όλους..
- Ο χρήστης πρέπει να είναι προσεχτικός
  - Να γνωρίζει τι πρέπει να ισχύει
  - Να ελέγχει – στο βαθμό που μπορεί - αν εφαρμόζονται αυτά που πρέπει
  - Να διαβάζει τους όρους προστασίας δεδομένων εφαρμογών/ιστοσελίδων
  - Να ασκεί τα δικαιώματά του (ποιος επεξεργάζεται τα δεδομένα; Για ποιο σκοπό; Ποια δεδομένα; Τι είδους επεξεργασία; Ποιοι οι αποδέκτες;)

First Party Cookies



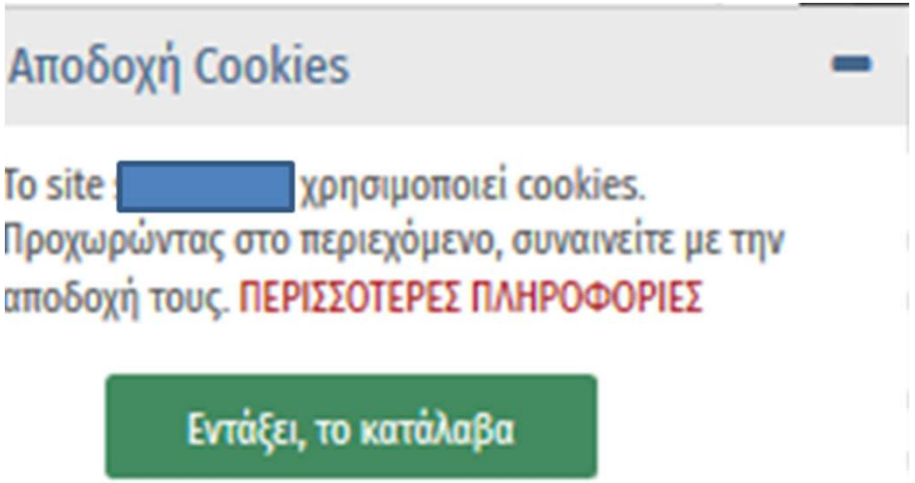
Κάποια cookies πρώτου μέλους (first party) μπορεί να είναι απαραίτητα για την παροχή της υπηρεσίας που ζητά ο χρήστης με την επίσκεψή του στην ιστοσελίδα. Για αυτά δεν χρειάζεται συγκατάθεσή του – αλλά χρειάζεται ενημέρωσή του

Third Party Cookies

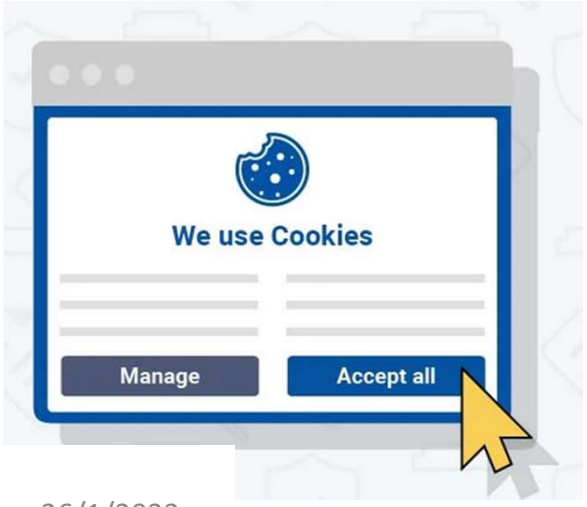


Η περίπτωση των cookies στην πράξη

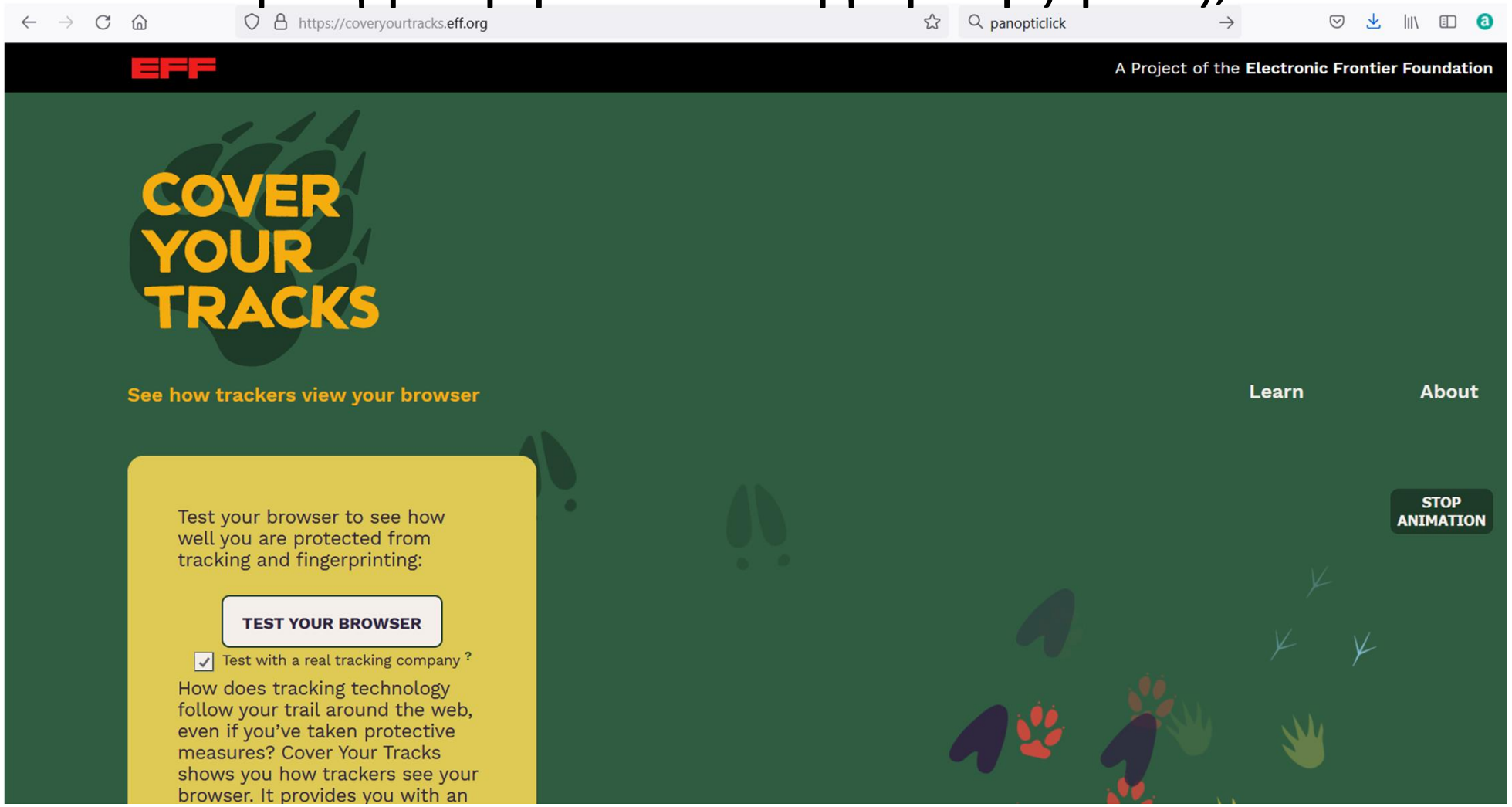
- Μία υλοποίηση **μη σύμφωνη** με το νομικό πλαίσιο
- Δεν ζητείται συγκατάθεση για την εγκατάσταση των cookies, όπως θα έπρεπε (για cookies στατιστικού σκοπού ή σκοπού διαφημίσεων ή «σύνδεσης» με προφίλ κοινωνικού δικτύου, που είναι οι συνηθέστερες περιπτώσεις)



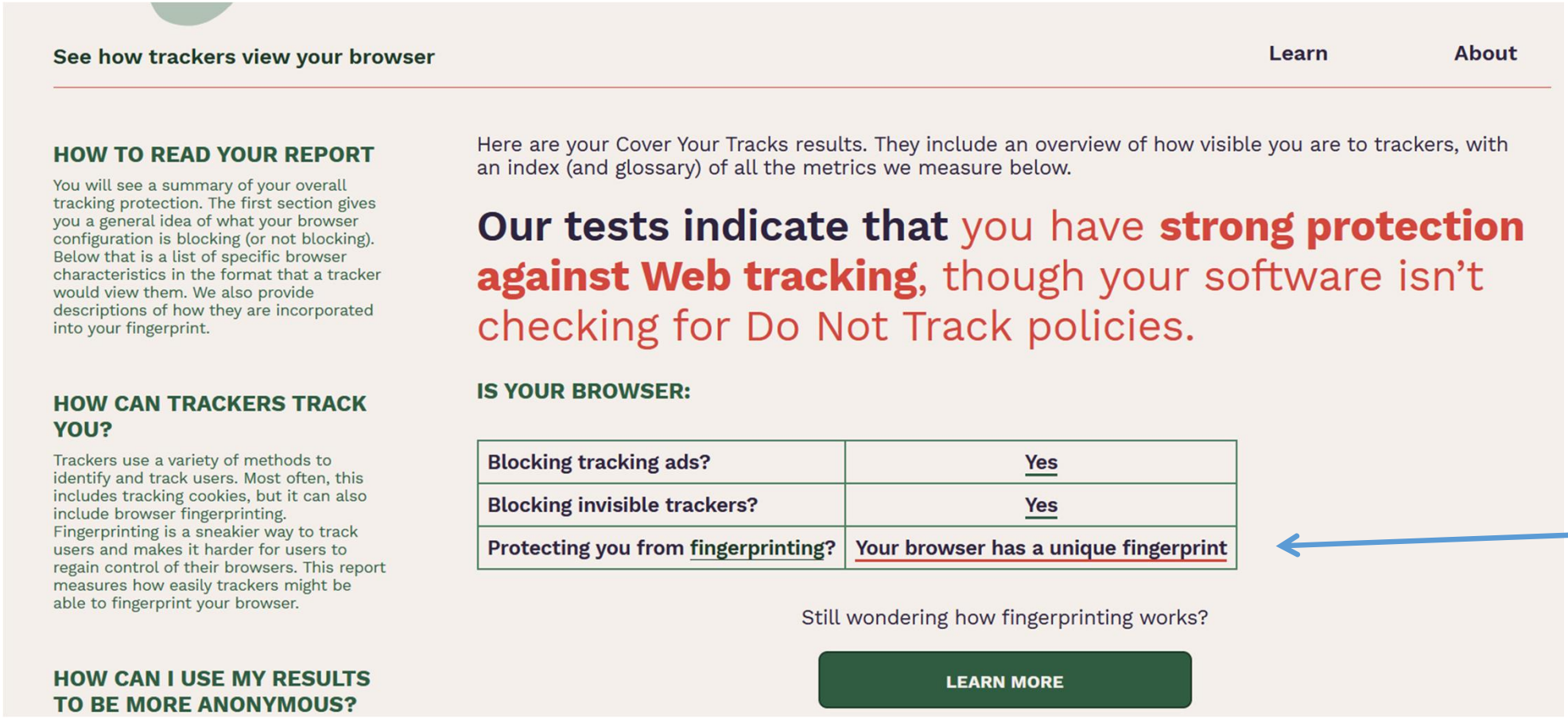
- Μία υλοποίηση **μη σύμφωνη** με το νομικό πλαίσιο
- "Εξαναγκάζεται» συγκατάθεση (οπότε και δεν είναι ελεύθερη, ούτε ειδική)



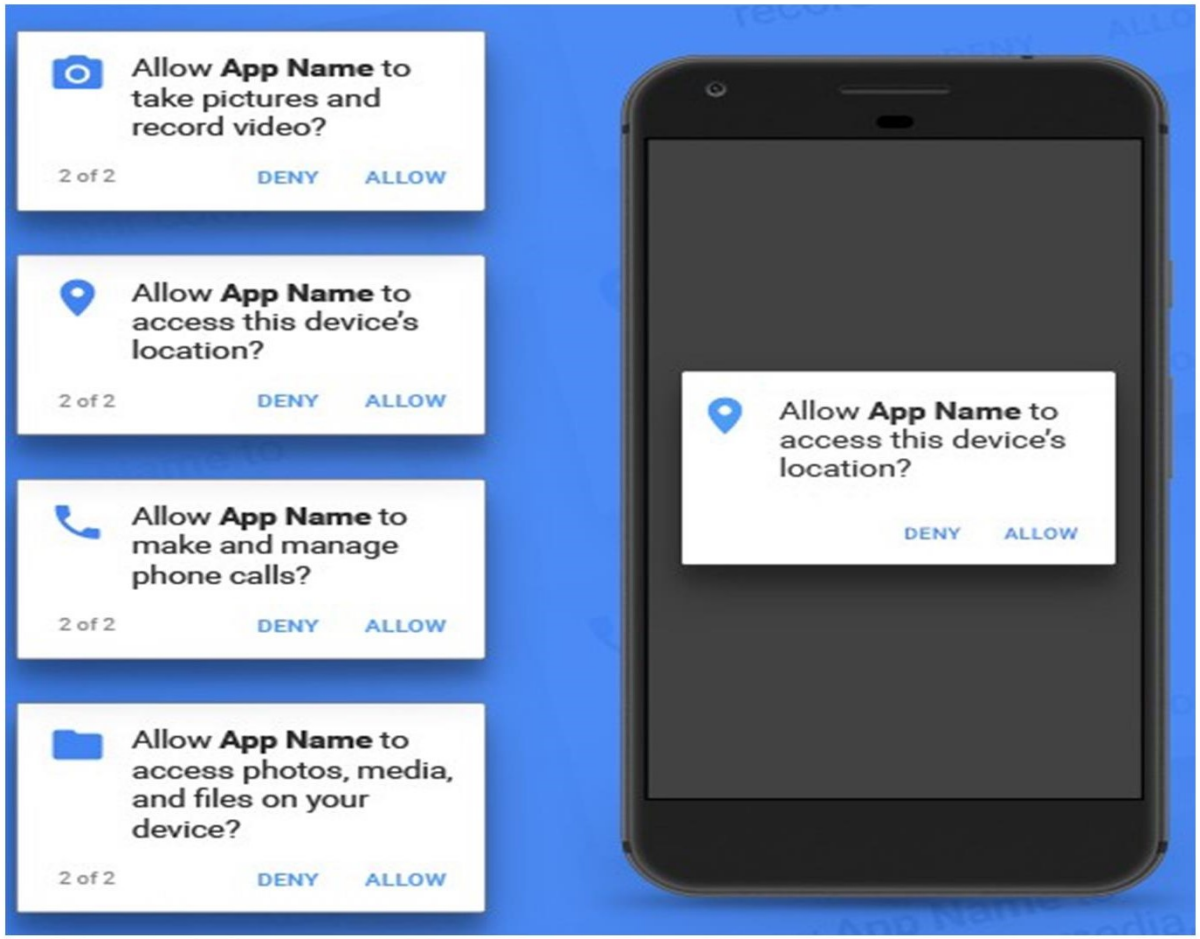
Ψηφιακό αποτύπωμα: Πόσο «μοναδικό» είναι το πρόγραμμα πλοήγησής μας;



Ψηφιακό αποτύπωμα: Πόσο «μοναδικό» είναι το πρόγραμμα πλοήγησής μας;



«Έγκριση προσβάσεων» σε εφαρμογές Android



- Κάθε άδεια (permission) που εκχωρούμε ουσιαστικά αντιστοιχεί σε επεξεργασία προσωπικών μας δεδομένων
- Είναι κάθε επεξεργασία που ζητείτα απαραίτητη για αυτό που θέλουμε με την εγκατάσταση της εφαρμογή
- Είναι «διαφανής» η επεξεργασία;
- Γνωρίζουμε ότι κάθε τέτοια έγκρισι ουσιαστικά μπορεί – αν η εφαρμογ το επιτρέπει - να εκχωρεί την ίδια ακριβώς πρόσβαση και σε τρίτους (third parties);

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Πρακτικές συμβουλές

«Δικτυωνόμαστε» με ασφάλεια

ε κάθε μας κίνηση στο Διαδίκτυο είμαστε πολύ προσεχτικοί

εν δημοσιεύουμε προσωπικά μας δεδομένα όπως διεύθυνση, ηλέφωνο, το καθημερινό μας πρόγραμμα, την πλήρη μερομηνία γέννησης

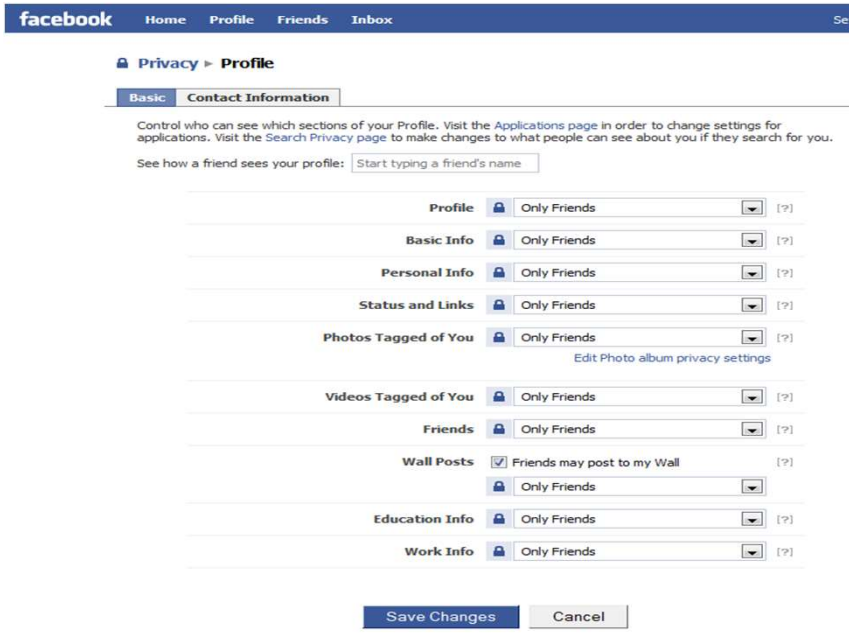
- Δεν δημοσιεύουμε «άκριτα» ούτε προσωπικά δεδομένα άλλων

νά τακτά διαστήματα γράφουμε το όνομά μας σε κάποια ηχανή αναζήτησης (π.χ. Google) για να δούμε τι αποτέλεσμα πιστρέφει.

υθμίζουμε κατάλληλα και αυστηρά τις προσωπικές μας υθμίσεις για ιδιωτικότητα και προστασία προσωπικών εδομένων που μας προσφέρει η υπηρεσία.

ιαβάζουμε την πολιτική προστασίας δεδομένων (privacy policy)

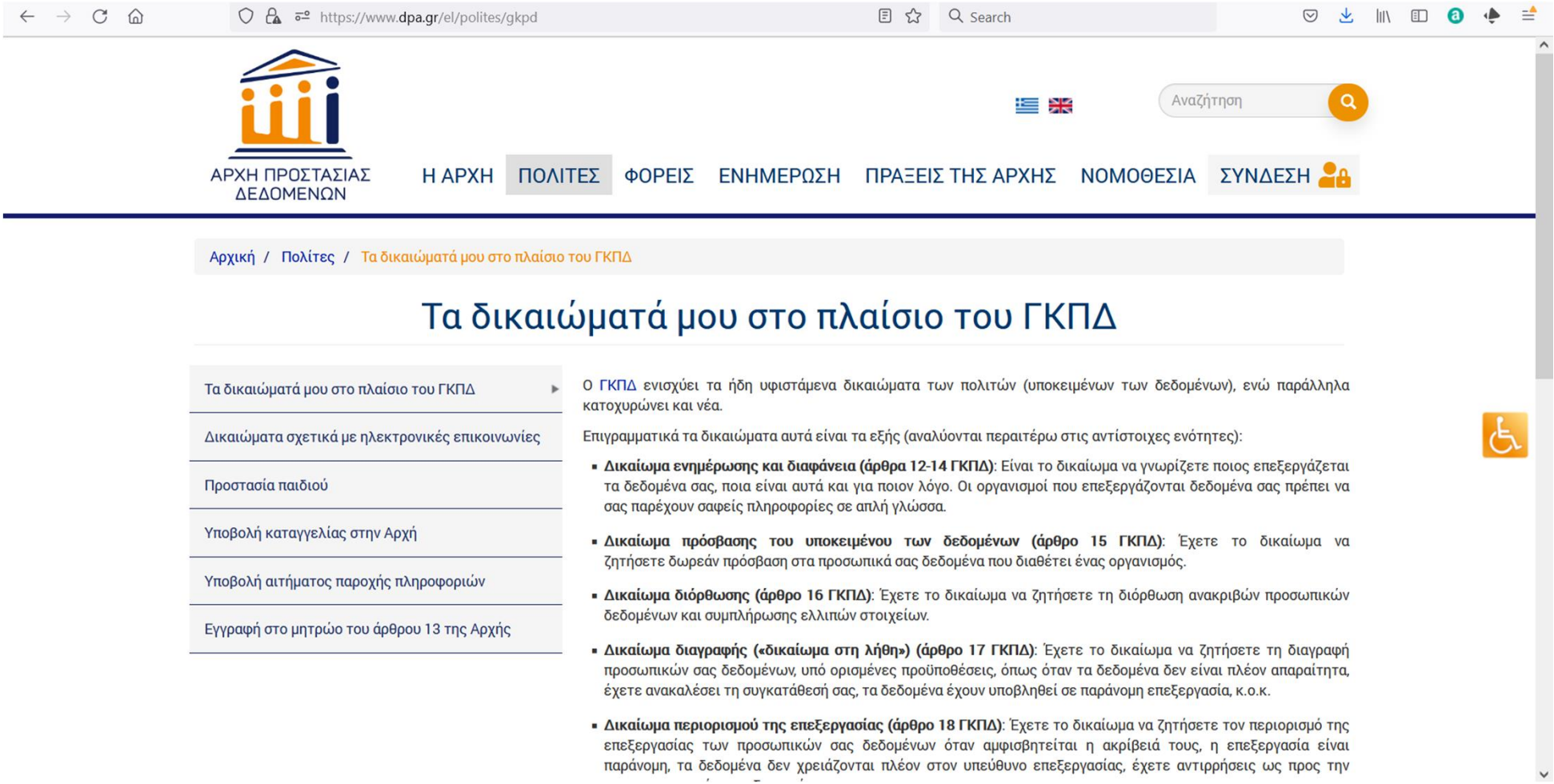
σκούμε τα δικαιώματά μας



Γενικότερες συμβουλές

- Προσοχή στις ιστοσελίδες που επισκεπτόμαστε (π.χ. ένα link μπορεί να μας μεταφέρει σε άλλη σελ από αυτή που δηλώνει). Πληκτρολογούμε οι ίδιοι το link που θέλουμε!
- Δεν στέλνουμε ποτέ μέσω e-mail ή chat οποιοδήποτε προσωπικό δεδομένο (συνθηματικά, αριθμο καρτών κτλ.)
- Σε αναδυόμενα «παράθυρα» που δεν τα ζητήσαμε, δεν κάνουμε καμία ενέργεια!
- "Σωστή" χρήση του e-mail
  - Δεν ανοίγουμε αρχεία οποιουδήποτε τύπου από άγνωστο αποστολέα
    - Ακόμα και αν είναι από φίλο μας, διερευνούμε αν είναι «ύποπτο»
    - Δεν ανοίγουμε **ποτέ** αρχεία τύπου .zip, .exe, .scr
    - Αγνοούμε και σβήνουμε αμέσως κάθε mail που επικαλείται κίνδυνο «κλειδώματος» οποιουδήποτε λογαριασμού μας, επείγουσα ειδοποίηση οποιουδήποτε τύπου, δέλεαρ ότι κερδίσαμε χρηματικό π ή κληρονομιά κτλ.
- Χρησιμοποιούμε ενημερωμένα προγράμματα antivirus, firewall, antispyware
  - «Κατεβάζουμε» κάποιο από τα γνωστά προγράμματα από την επίσημη σελίδα τους, και όχι κάποιο τυχαίο που μας προτείνεται μέσω διαφήμισης
- Ενημερώνουμε διαρκώς το λειτουργικό μας σύστημα με όλα τα updates
- Κρατάμε αντίγραφα ασφαλείας των δεδομένων μας

https://www.dpa.gr



If you reveal your secrets to the wind,
you should not blame the wind for
revealing them to the trees.

Kahlil Gibran