ΠΡΑΚΤΙΚΗ ΑΣΦΑΛΕΙΑ

Διδάσκοντες: Δ. Ζήνδρος

Επιμέλεια διαφανειών: Π. Αγγελάτος, Δ. Ζήνδρος

Λύκειο Πεδινής 2014

Ποιος είμαι;

- Διονύσης
- Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών
- Εθνικός Μετσόβιο Πολυτεχνείο
- Ομάδα ασφάλειας προϊόντος, Twitter

Στόχος της ώρας

- Έννοιες στη φυσική ασφάλεια
- Κωδικοί πρόσβασης
- LastPass
- AdBlock
- 2 Factor Authentication
- Κρυπτογράφηση δίσκου (TrueCrypt)

Όσο ξεκινάμε...

- Κατεβάστε το TrueCrypt για το σύστημά σας:
  - http://www.truecrypt.org/

- Εγκαταστήστε το

Ας χακάρουμε το Facebook

Παραβίαση λογαριασμών

- Η παραβίαση λογαριασμών μπορεί να γίνει με δύο τρόπους:
- **Τεχνικούς τρόπους**
- **Ψυχολογικούς τρόπους**

Τεχνικοί τρόποι

- Βασιζόμαστε σε κάποιο bug που έχει το σύστημα
- Κάποιο πρόβλημα ασφάλειας του λογισμικού του Facebook

Ας δούμε έναν τεχνικό τρόπο

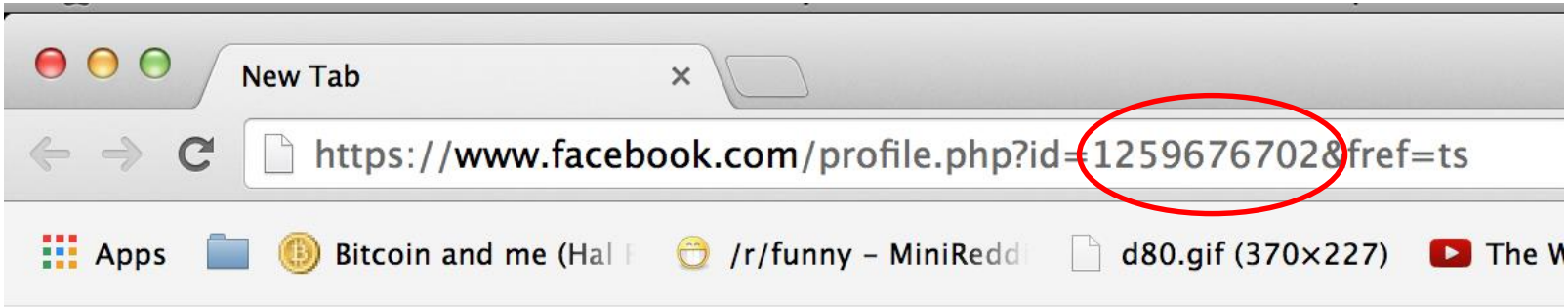
- Παράδειγμα τεχνικού τρόπου:
- “Hack 632” του Facebook
- Αξιοποιεί τη δυνατότητα “Flag for Spam” του Facebook
- Πρέπει ο θύτης και το θύμα να είναι «φίλοι»
- Υποκλέπτει το friendid ανάμεσα στο θύμα και το θύτη
- Προκύπτει ένας κρυπτογραφημένος κωδικός
- Μπορούμε στη συνέχεια να τον αποκρυπτογραφήσουμε

Hack 632

- Δεν χρειάζεται να έχουμε τεχνικές γνώσεις!
- Θα χρειαστούμε 2 εθελοντές: Έναν θύτη και ένα θύμα
- Που να είναι μεταξύ τους φίλοι στο Facebook

Hack 632

- Ο θύτης επισκέπτεται το:
- http://facebook.endofcodes.com/hack632
- Πληκτρολογεί το id του θύματος



Hack 632

- Στη συνέχεια συνδέεται με το **δικό του** λογαριασμό
- Κάνοντας Connect with Facebook
- Οι δύο λογαριασμοί **πρέπει** να είναι φίλοι μεταξύ τους στο Facebook
- Λαμβάνει τον κρυπτογραφημένο κωδικό

…αποκρυπτογραφώντας τον κωδικό

Μα, για μισό λεπτό!

- Ποιος έκλεψε τίνος τον κωδικό;
- Θα ήταν ποτέ δυνατό το Facebook να έχει ένα τόσο τετριμμένο πρόβλημα ασφάλειας;
- Όχι - το Facebook έχει μία δυνατή ομάδα ασφάλειας
- Είναι σχεδόν αδύνατο να βρούμε τεχνικά προβλήματα εκτός αν είμαστε ειδικοί
- Οι επιθέσεις στηρίζονται αποκλειστικά στην **ψυχολογία**

Το Hack632 είναι ένα ψέμα

- Μόλις πέσατε θύματα social engineering
- Πληκτρολογήσατε **τον δικό σας κωδικό** σε ένα κακόβουλο website
- **Αυτή η επίθεση ονομάζεται phishing**
- **Ηλεκτρονικό «ψάρεμα»**

Social engineering

- “Hackάροντας” τον ανθρώπινο παράγοντα
- Οι **άνθρωποι** είναι το πιο ευπαθές κομμάτι ενός συστήματος
- Προσέχετε πού βάζετε τον κωδικό σας!

Πού βάζουμε τον κωδικό μας;

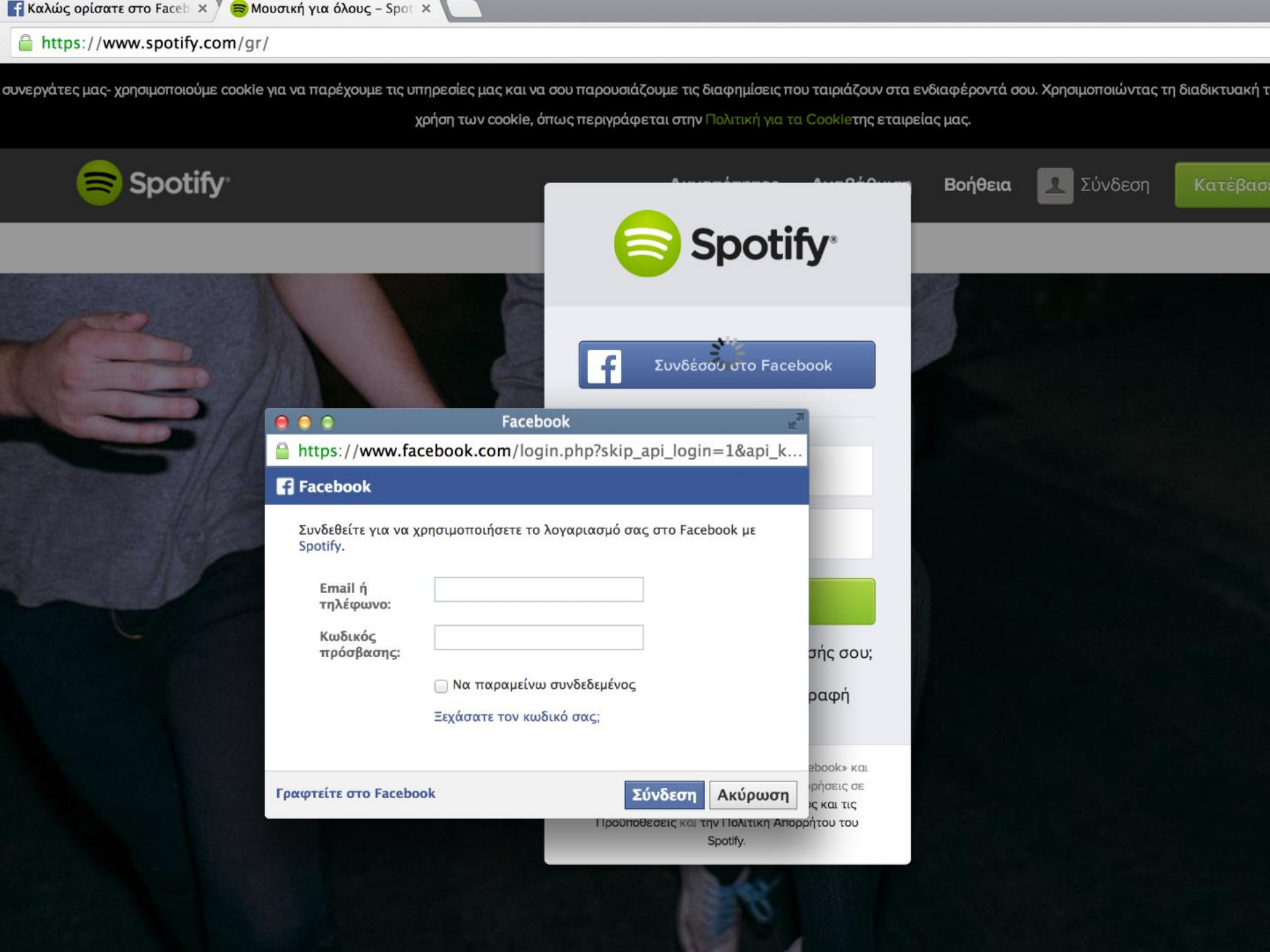
- Προσοχή!
- Μόνο όταν βλέπουμε τη σωστή διεύθυνση!
- Κοιτάμε το όνομα του site:
- Ανάμεσα στο https:// και στο πρώτο /
- https://**facebook.com/**
- Εδώ η σελίδα είναι το facebook.com

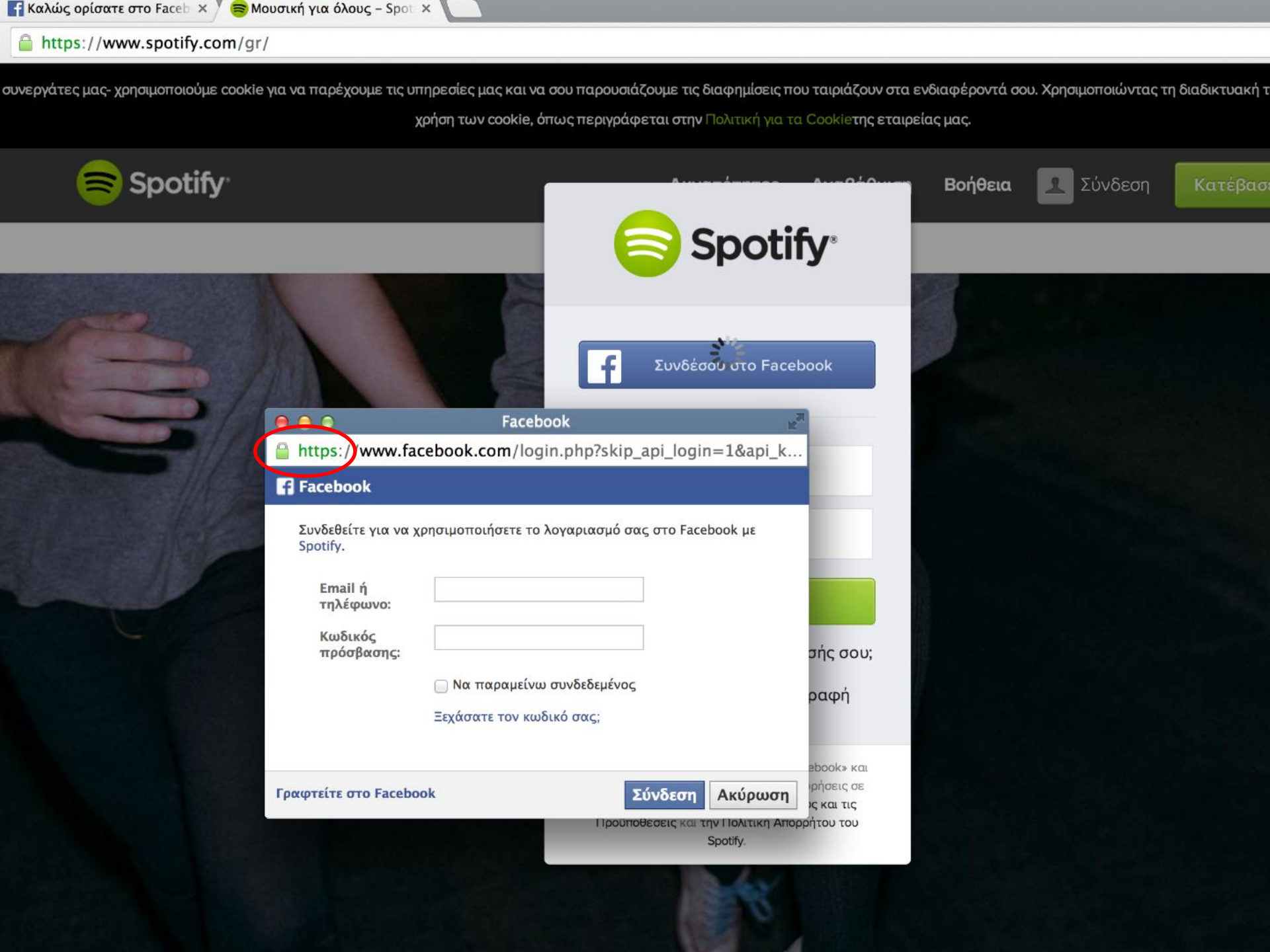
Πού θα βάζατε τον κωδικό σας;

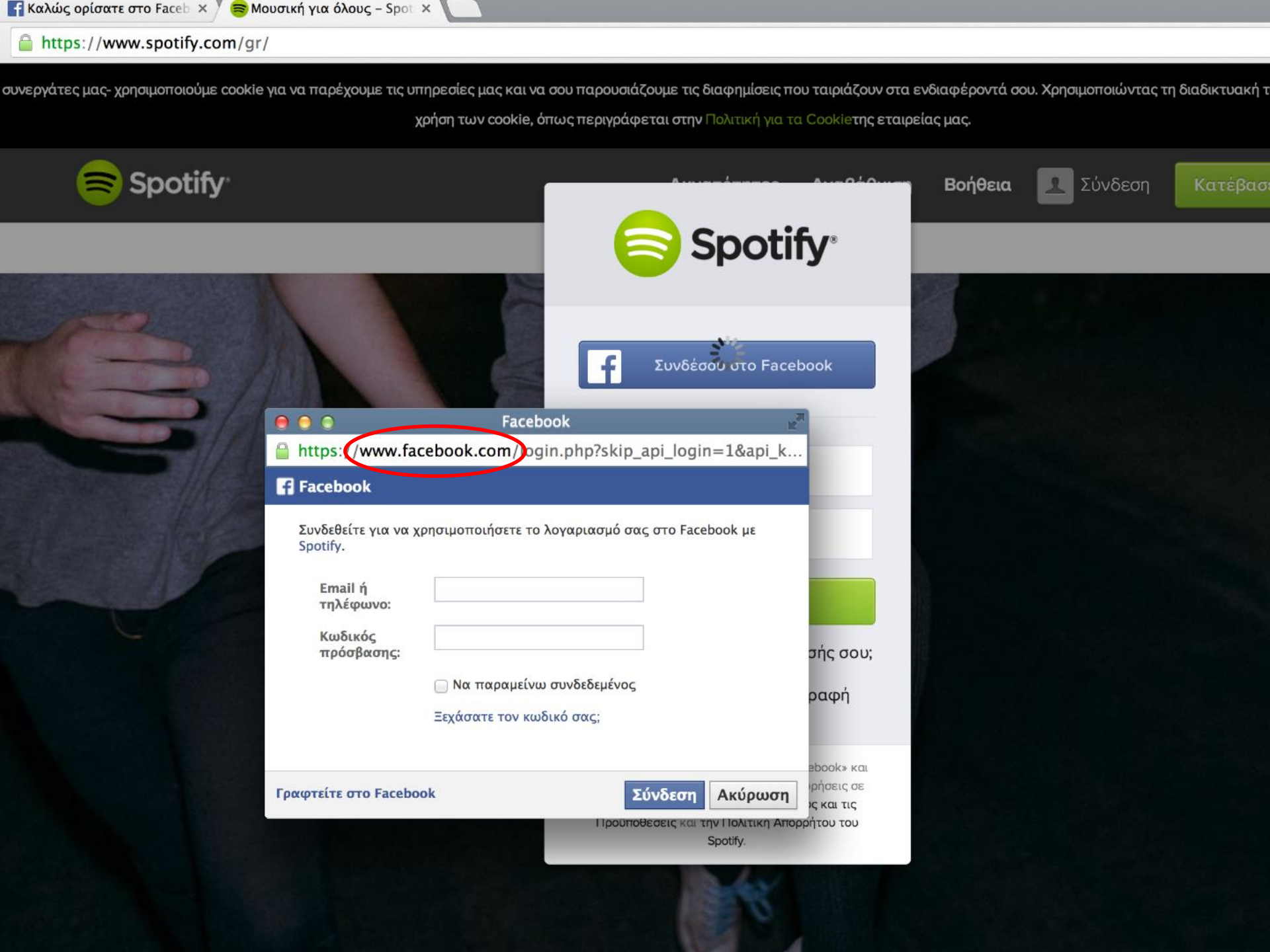
- https://**facebook.com**
- https://**twitter.com**
- https://login.**facebook.com**
- https://**facebook.com**/login/form?id=381
- https://secure.**facebook.com**/login/form?id=981
- https://secure.facebook.com.**dionyziz.com**/login/form
- https://facebook.**endofcodes.com**/hack
- http://facebook.com

Πού θα βάζατε τον κωδικό σας;

- https://**facebook.com** **-** ναι
- https://**twitter.com** **-** ναι
- https://login.**facebook.com** **-** ναι
- https://**facebook.com**/login/form?id=381 - ναι
- https://secure.**facebook.com**/login/form?id=981 - ναι
- https://secure.facebook.com.**dionyziz.com**/login/form - όχι
- https://facebook.**endofcodes.com**/hack **-** όχι
- http://facebook.com - όχι


Καλώς ορίσατε στο Faceb
Μουσική για όλους – Spot
https://www.spotify.com/gr/
συνεργάτες μας- χρησιμοποιούμε cookie για να παρέχουμε τις υπηρεσίες μας και να σου παρουσιάζουμε τις διαφημίσεις που ταιριάζουν στα ενδιαφέροντά σου. Χρησιμοποιώντας τη διαδικτυακή τ
χρήση των cookie, όπως περιγράφεται στην Πολιτική για τα Cookieτης εταιρείας μας.
Spotify
Βοήθεια
Σύνδεση
Κατέβασ
Spotify
Συνδέσου στο Facebook
Facebook
https://www.facebook.com/login.php?skip_api_login=1&api_k...
Facebook
Συνδεθείτε για να χρησιμοποιήσετε το λογαριασμό σας στο Facebook με Spotify.
Email ή τηλέφωνο:
Κωδικός πρόσβασης:
Να παραμείνω συνδεδεμένος
Ξεχάσατε τον κωδικό σας;
Γραφτείτε στο Facebook
Σύνδεση
Ακύρωση
σής σου;
αφή
ebook» και
ρήσεις σε
ς και τις
Προϋποθέσεις και την Πολιτική Απορρήτου του Spotify.


Καλώς ορίσατε στο Faceb
Μουσική για όλους – Spot
https://www.spotify.com/gr/
συνεργάτες μας- χρησιμοποιούμε cookie για να παρέχουμε τις υπηρεσίες μας και να σου παρουσιάζουμε τις διαφημίσεις που ταιριάζουν στα ενδιαφέροντά σου. Χρησιμοποιώντας τη διαδικτυακή τ
χρήση των cookie, όπως περιγράφεται στην Πολιτική για τα Cookieτης εταιρείας μας.
Spotify
Βοήθεια
Σύνδεση
Κατέβασ
Spotify
Συνδέσου στο Facebook
Facebook
https://www.facebook.com/login.php?skip_api_login=1&api_k...
Facebook
Συνδεθείτε για να χρησιμοποιήσετε το λογαριασμό σας στο Facebook με Spotify.
Email ή τηλέφωνο:
Κωδικός πρόσβασης:
Να παραμείνω συνδεδεμένος
Ξεχάσατε τον κωδικό σας;
Γραφτείτε στο Facebook
Σύνδεση
Ακύρωση
σής σου;
αφή
ebook» και
ρήσεις σε
ς και τις
Προϋποθέσεις και την Πολιτική Απορρήτου του Spotify.


Καλώς ορίσατε στο Faceb
Μουσική για όλους – Spot
https://www.spotify.com/gr/
συνεργάτες μας- χρησιμοποιούμε cookie για να παρέχουμε τις υπηρεσίες μας και να σου παρουσιάζουμε τις διαφημίσεις που ταιριάζουν στα ενδιαφέροντά σου. Χρησιμοποιώντας τη διαδικτυακή τ
χρήση των cookie, όπως περιγράφεται στην Πολιτική για τα Cookieτης εταιρείας μας.
Spotify
Βοήθεια
Σύνδεση
Κατέβασ
Spotify
Συνδέσου στο Facebook
Facebook
https://www.facebook.com/login.php?skip_api_login=1&api_k...
Facebook
Συνδεθείτε για να χρησιμοποιήσετε το λογαριασμό σας στο Facebook με Spotify.
Email ή τηλέφωνο:
Κωδικός πρόσβασης:
Να παραμείνω συνδεδεμένος
Ξεχάσατε τον κωδικό σας;
Γραφτείτε στο Facebook
Σύνδεση
Ακύρωση
σής σου;
αφή
ebook» και
ρήσεις σε
ς και τις
Προϋποθέσεις και την Πολιτική Απορρήτου του Spotify.

Διπλοί κωδικοί

- Χρησιμοποιείτε τον ίδιο κωδικό του Facebook σε άλλες σελίδες;
- Κακή ιδέα!
- Αν κάποιος κακόβουλος κλέψει τον έναν κωδικό, έχει πρόσβαση παντού!

Μοναδικός κωδικός σε κάθε σελίδα

- Καλό είναι να έχουμε διαφορετικό κωδικό σε κάθε σελίδα
- Ο κάθε κωδικός να μην μπορεί να προκύψει από τους άλλους εύκολα!
- Κάθε κωδικός πρέπει να είναι μεγάλος (π.χ 15 χαρακτήρες)
- Πώς μπορούμε να θυμόμαστε όλους αυτούς τους κωδικούς;

LastPass

- Είναι αδύνατο να θυμόμαστε όλους τους κωδικούς!
- Αλλά δεν χρειάζεται
- Το LastPass…
- Θυμάται τους κωδικούς μας
- Ας το χρησιμοποιήσουμε

LastPass

- Ξεκινήστε να το χρησιμοποιείτε για νέες σελίδες που γράφεστε
- Σιγά σιγά αλλάξτε τους παλιούς σας κωδικούς

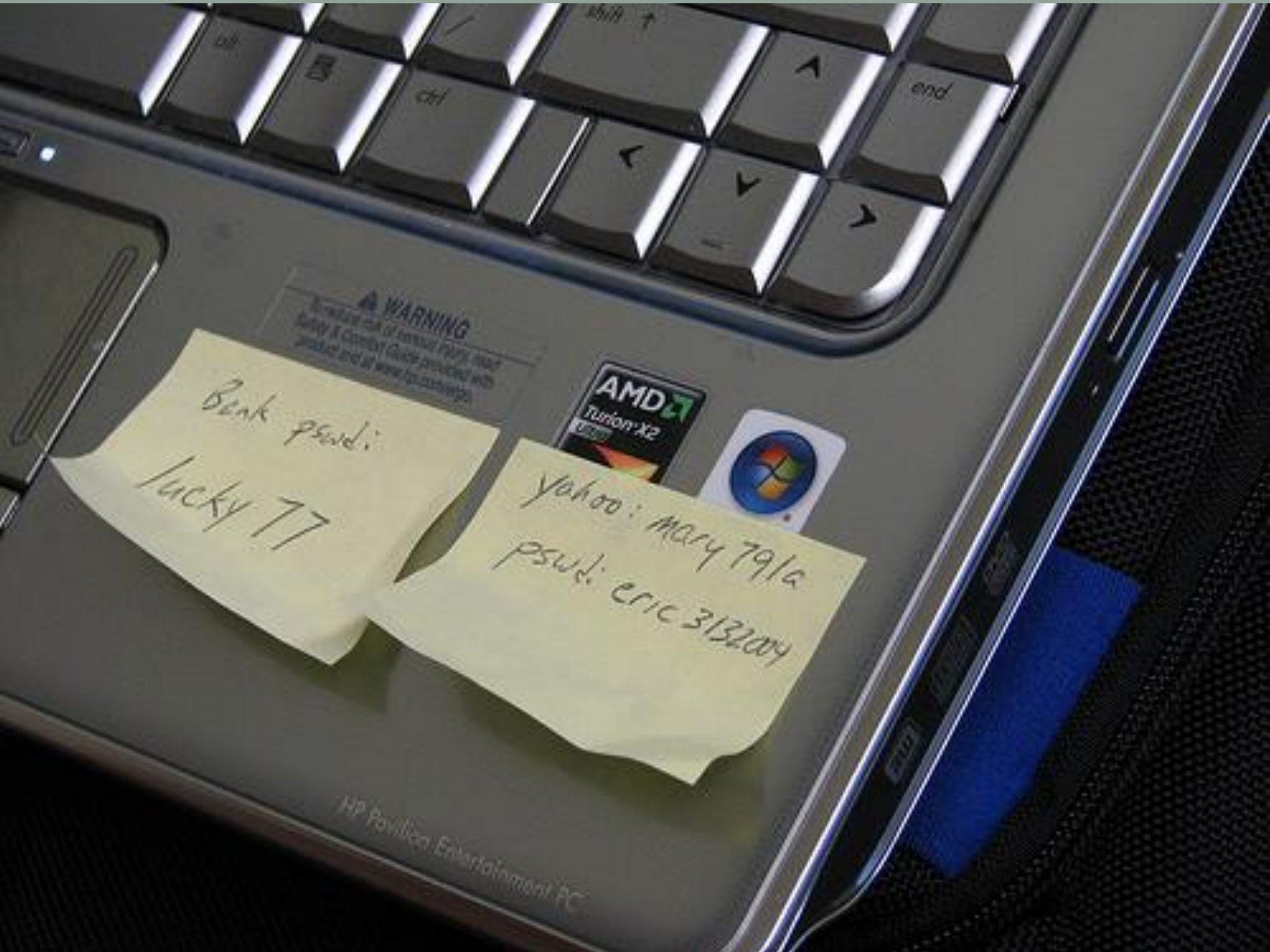
LastPass Demo

Φυσική ασφάλεια

- Προστασία από φυσικές απειλές
- Προσέξτε τα αδιάκριτα βλέμματα

Κλοπή κωδικών πρόσβασης

- Κοιτάζοντας πάνω από τον ώμο μας
- Φωτογραφία από το παράθυρο
- Post-it με κωδικούς πρόσβασης
- Keyloggers

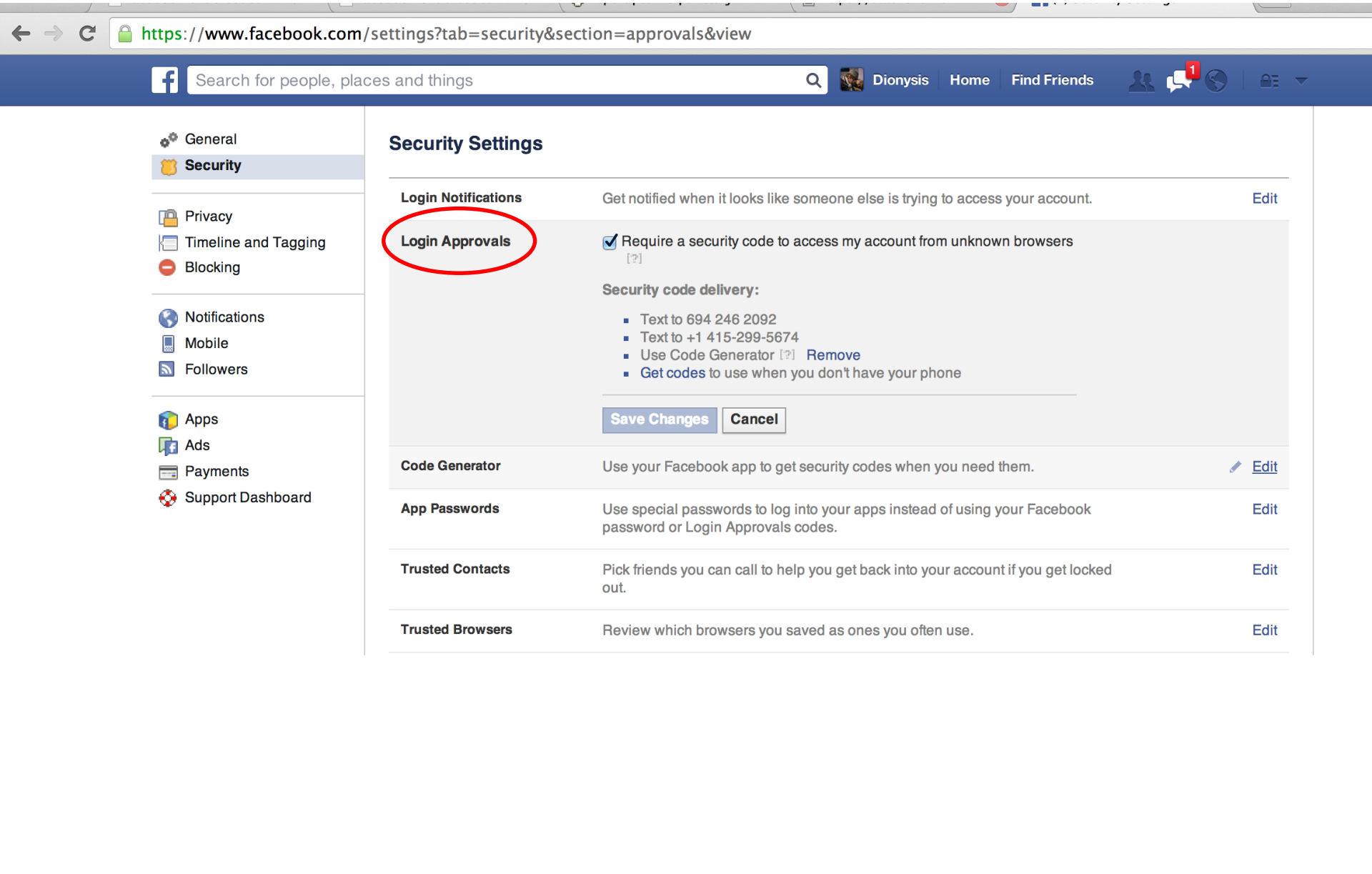

WARNING
AMD
Turion X2
Bank psw:
lucky 77
Yahoo: mary 79/a
psw: eric 3/3/2004
HP Pavilion Entertainment PC

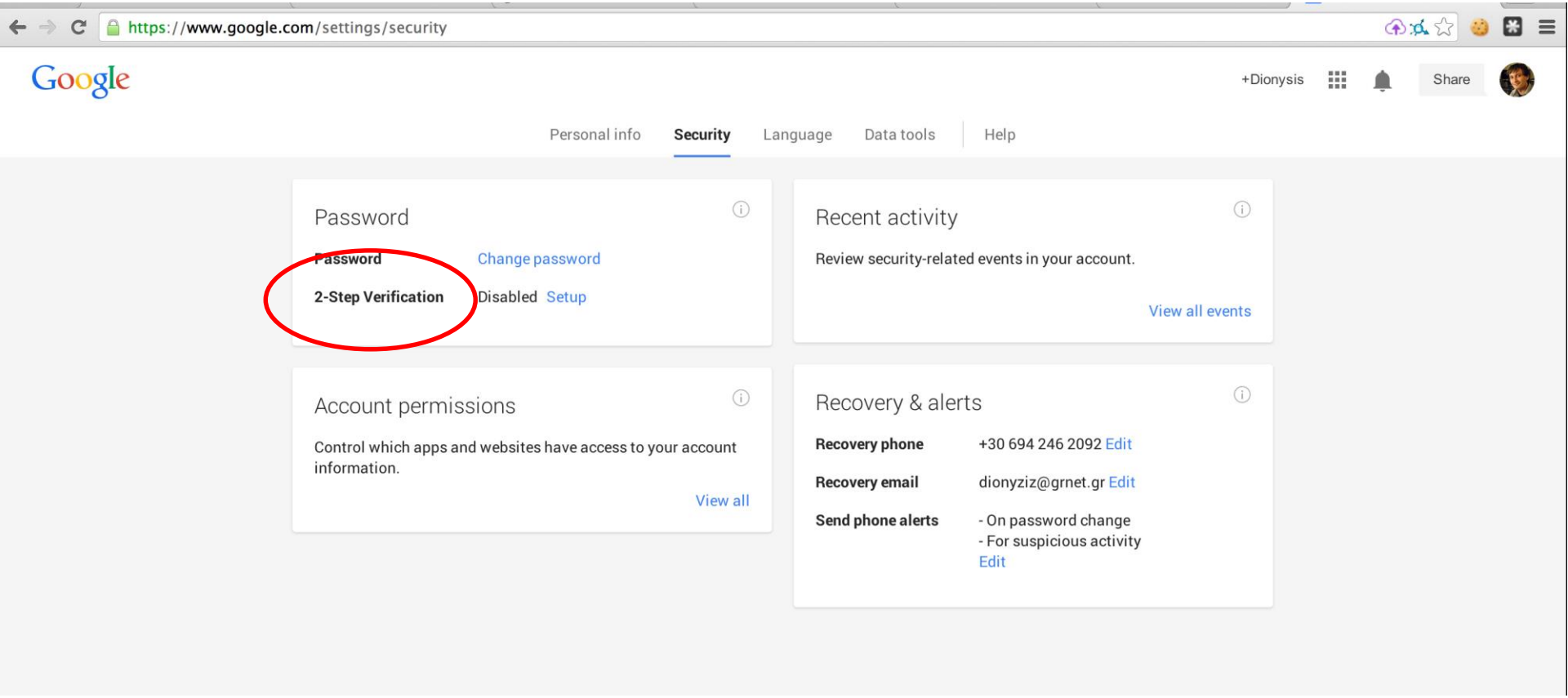
Key loggers

- Τρόπος κλοπής του τι γράφεται στο πληκτρολόγιο:
  - Κωδικοί πρόσβασης
  - Πιστωτικές κάρτες
- Hardware keylogging (σε Internet café)
  - Αλλαγή πληκτρολογίου
  - Παρεμβολή στο καλώδιο πληκτρολογίου
  - Αποθηκεύουν τους κωδικούς στο hardware μέχρι να ανακτηθούν
  - Ή τους στέλνουν μέσω WiFi
- Software keylogging
  - Ιός - malware
  - Αποθηκεύει τους κωδικούς σε αρχείο
  - Τους στέλνει μέσω Internet στο θύτη

2 Factor Authenticator

- Βάζουμε έναν επιπλέον κωδικό που στέλνεται στο κινητό μας
- Μπορούμε να το ενεργοποιήσουμε για:
  - Facebook
  - Twitter
  - Gmail
  - Blizzard
  - Και άλλα
- Ας το ενεργοποιήσουμε τώρα


https://www.facebook.com/settings?tab=security&section=approvals&view
Search for people, places and things
Dionysis
Home
Find Friends
General
Security
Privacy
Timeline and Tagging
Blocking
Notifications
Mobile
Followers
Apps
Ads
Payments
Support Dashboard
Security Settings
Login Notifications
Get notified when it looks like someone else is trying to access your account.
Edit
Login Approvals
Require a security code to access my account from unknown browsers
Security code delivery:
Text to 694 246 2092
Text to +1 415-299-5674
Use Code Generator
Remove
Get codes to use when you don't have your phone
Save Changes
Cancel
Code Generator
Use your Facebook app to get security codes when you need them.
Edit
App Passwords
Use special passwords to log into your apps instead of using your Facebook password or Login Approvals codes.
Edit
Trusted Contacts
Pick friends you can call to help you get back into your account if you get locked out.
Edit
Trusted Browsers
Review which browsers you saved as ones you often use.
Edit


https://www.google.com/settings/security
Google
+Dionysis
Share
Personal info
Security
Language
Data tools
Help
Password
Password
Change password
2-Step Verification
Disabled
Setup
Recent activity
Review security-related events in your account.
View all events
Account permissions
Control which apps and websites have access to your account information.
View all
Recovery & alerts
Recovery phone
+30 694 246 2092 Edit
Recovery email
dionyziz@grnet.gr Edit
Send phone alerts
- On password change
- For suspicious activity
Edit

2 Factor Authentication demo

Προστασία από ιούς

- Δεν τρέχουμε προγράμματα ή αρχεία που μας στέλνουν!
- Είτε με e-mail είτε μέσω Facebook
- Επιβεβαιώνουμε ότι ο αποστολέας μας το έστειλε
- Ρωτάμε: Μου έστειλες κάποιο αρχείο?
- Ενημερώνουμε **πάντα** τον υπολογιστή μας
- Ενημέρωση σε:
  - Windows
  - Linux / Ubuntu
  - Adobe Flash / Adobe Acrobat
  - Java
- Μην ξεχνάτε να τρέχετε τις ενημερώσεις!
- Ενεργοποιήστε τις αυτόματες ενημερώσεις

AdBlock

- Μπλοκάρει τις διαφημίσεις στον browser
- Μας προστατεύει από παραπλανητικά μηνύματα / malware

Προστασία από φυσικές επιθέσεις

- Κρυπτογράφηση δίσκου
- Σε περίπτωση κλοπής εξοπλισμού, τα δεδομένα είναι ασφαλή
- Δυνατοί κωδικοί πρόσβασης
- Ορθή πολιτική χρήσης κωδικών πρόσβασης

Κρυπτογράφηση δίσκου

- Πλήρης ή μερική
- **Πλήρης**: Κρυπτογραφεί όλο το σύστημα αρχείων
- **Μερική**: Κρυπτογραφεί επιλεγμένα αρχεία
- Για την κρυπτογράφηση χρησιμοποιείται ένας κωδικός πρόσβασης

TrueCrypt

- Επιτρέπει μερική/πλήρη κρυπτογράφηση δίσκου
- Είναι ανοιχτού κώδικα
- Υποστηρίζει Linux, Mac, Windows

TrueCrypt demo

Αποκάλυψη κλειδιού

- Κάποιος που βλέπει το δίσκο μπορεί να καταλάβει ότι είναι κρυπτογραφημένος
- Αν υπάρχει υποψία ότι έχουμε παράνομα δεδομένα, μπορεί να μας ζητηθεί ο κωδικός πρόσβασης από κάποια αρχή (αστυνομία, δικαστήριο...)
- Δεν μπορούμε πάντα να αρνηθούμε!

Full Disk Encryption (FDE)

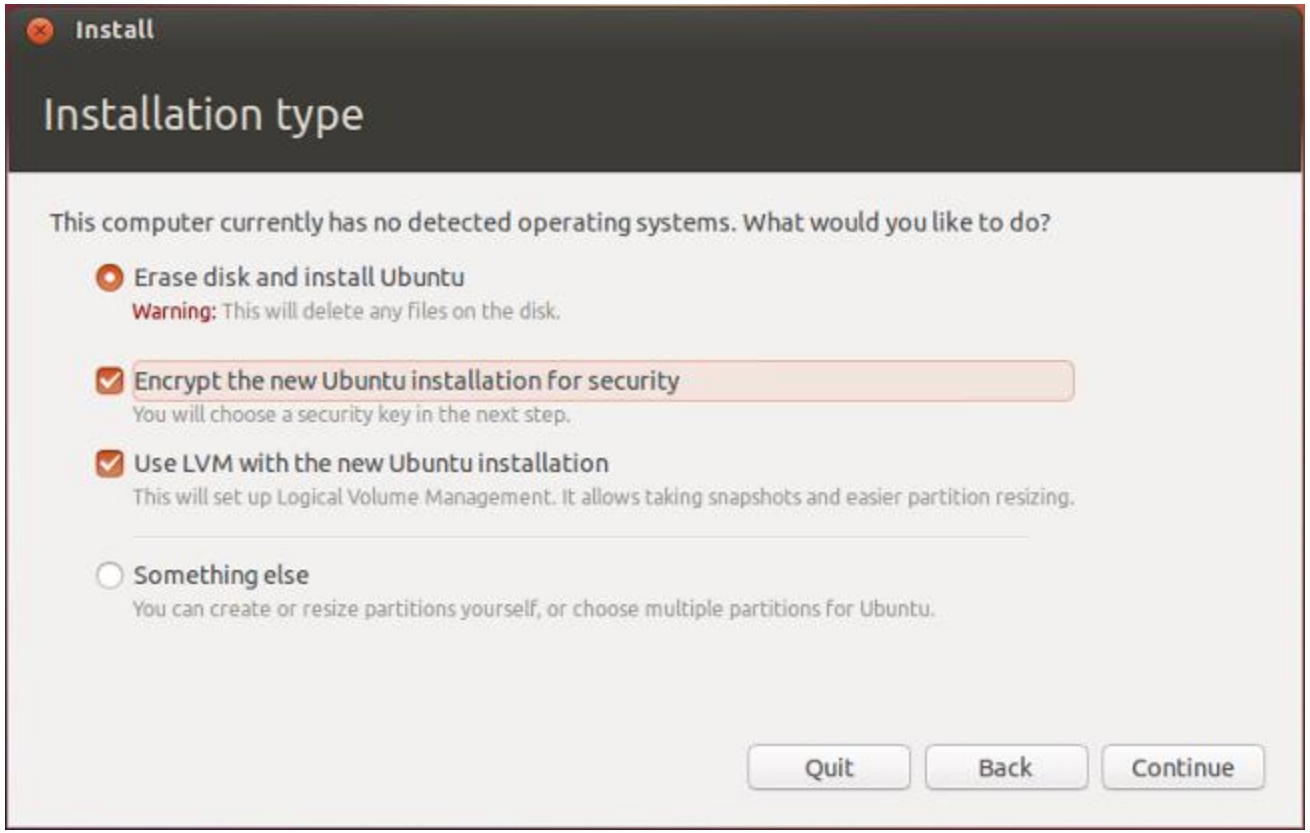
- Όλος ο δίσκος κρυπτογραφείται
  - Λειτουργικό σύστημα
  - Προγράμματα
  - Δεδομένα του χρήστη

Full Disk Encryption (FDE)

- Mac
  - FileVault

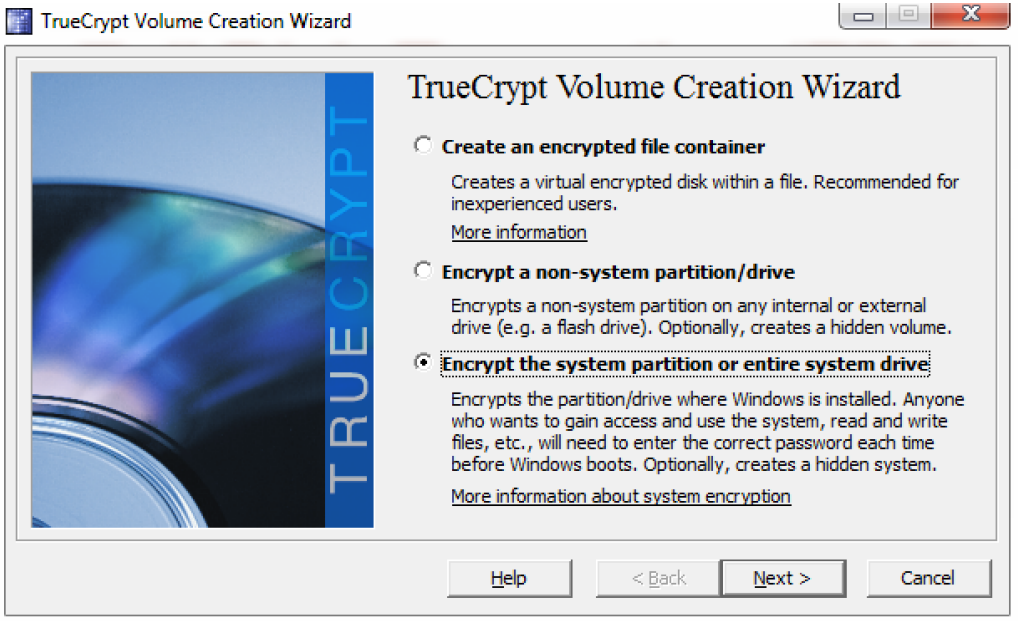
Full Disk Encryption (FDE)

- Linux
  - LUKS/dm-crypt
  - Υποστηρίζεται από τον πυρήνα



Full Disk Encryption (FDE)

- Windows
  - TrueCrypt



“You can always be a little more paranoid.”

Tom Lowenthal

Quiz

- Υπάρχει περίπτωση να κρυπτογραφηθεί ο δίσκος μας χωρίς να το θέλουμε;

Ransomware

- Ιός που βασίζεται στην κρυπτογραφία
- Κρυπτογραφεί τα αρχεία μας

- Δεν περιέχει το private key
- Μας ζητάει λύτρα για να ξεκλειδώσουν τα αρχεία μας

CryptoLocker

Your personal files are encrypted!

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50

Your important files **encryption** produced on this computer: photos, videos, documents, etc. **Here** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

Μάθαμε

- LastPass
- AdBlock
- Social engineering
- Κωδικούς πρόσβασης
- Κρυπτογράφηση δίσκου (TrueCrypt)
- 2 factor authentication

Σε ενδιαφέρει η ασφάλεια;

- Tor
  - Ανώνυμη περιήγηση στο διαδίκτυο
- Hidden Volumes
  - Κρυμμένοι σκληροί δίσκοι που δεν φαίνεται ότι υπάρχουν
- Bitcoin
  - Ασφαλείς, αποκεντρωμένες πληρωμές
- HTTPS / ARP / HSTS / BREACH
  - Ασφάλειας δικτύων
- OTR
  - Ασφαλές, κρυπτογραφημένο chat
- GPG
  - Κρυπτογράφηση e-mail, ψηφιακές υπογραφές

Ευχαριστώ που με παρακολουθήσατε!

- Ενδιαφέρεστε για ασφάλεια;
- 10 ώρες μαθημάτων ασφάλειας στο:
- http://security-class.gr

- Παραμένω διαθέσιμος:
  - dionyziz@gmail.com
  - https://twitter.com/dionyziz
  - https://facebook.com/dionyziz
  - https://dionyziz.com

- Creative Commons 3.0 Attribution