Two factor authentication

Γιώργος Σπηλιώτης

IT Consultant

TFA - Τι είναι;

- Αυξημένη ασφάλεια κατά την διαπίστευση.
- Περισσότερα του ενός αποδεικτικά
  - Κάτι που μόνο εγώ ξέρω.
  - Κάτι που μόνο εγώ έχω στην κατοχή μου (π.χ. κάρτα ή δακτυλικό αποτύπωμα).
- Το γνωρίζουμε ήδη από την χρήση ATM (PIN + κάρτα).
- Μια μέθοδος χρήσης κοινόχρηστου εξοπλισμού με ασφάλεια.
- Δεν μας προστατεύει από man-in-the middle attacks ή session hijacking.

TFA - Χαρακτηριστικά

- Μικρή επιβάρυνση της «ευκολίας» σε σχέση με τα οφέλη (ασφάλεια).
- Η πιθανότητα για brute force attack είναι η δεσμευμένη πιθανότητα του συνδυασμού όλων των factors.
- Όσο ισχυρότερα είναι τα factors τόσο και η συνολική ασφάλεια που προσφέρουν.
- Επιτρέπει την διαρροή ενός factor χωρίς την πλήρη κατάρρευση του συστήματος.

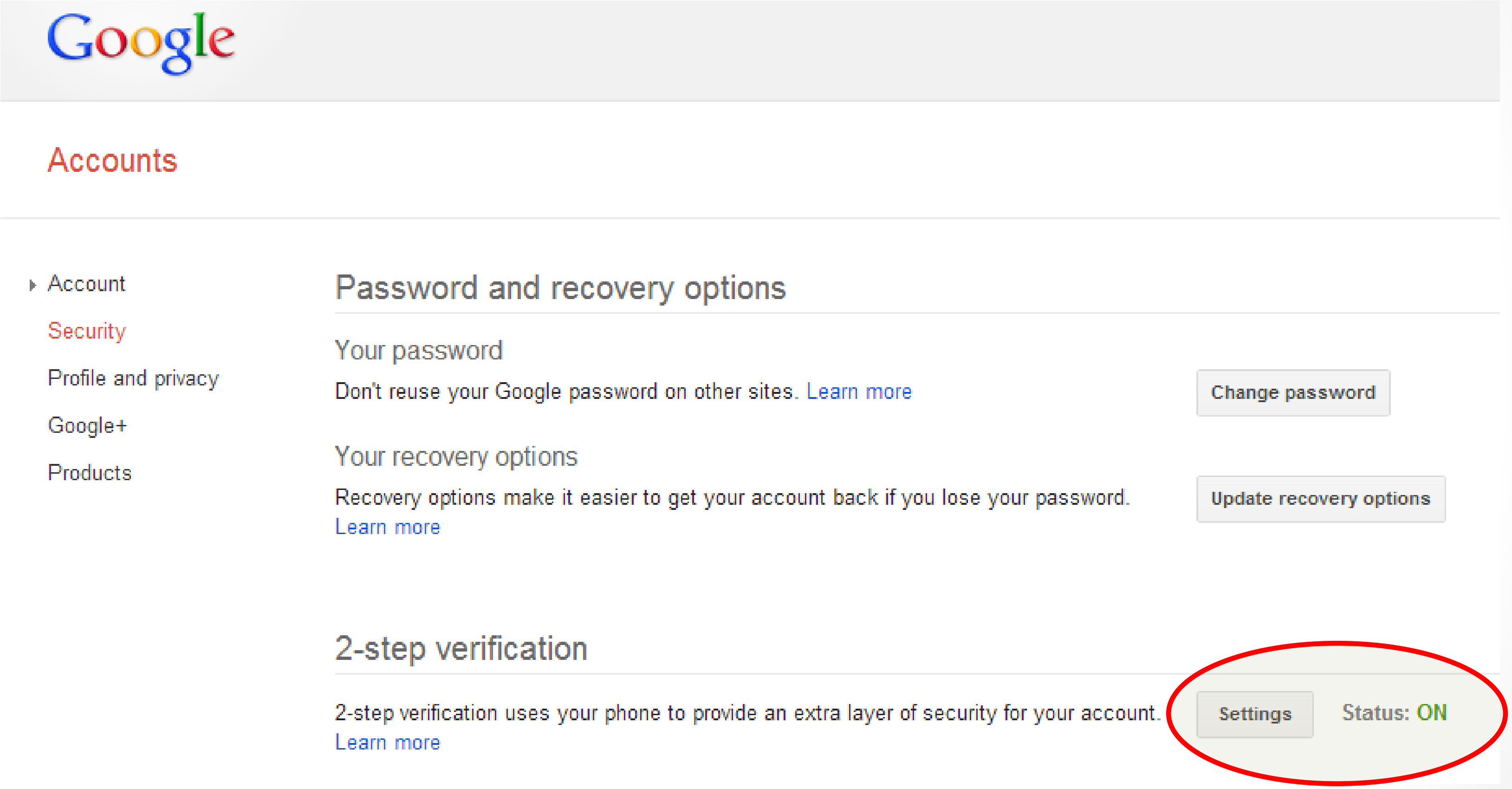
Το δεύτερο factor…

- Πολλαπλά πρότυπα (δυστυχώς)
- Οικογένεια πρωτοκόλλων OATH (όχι OAuth!)
    - HOTP [HMAC based Pass=ReducedSize(f(k,c))]
    - TOTP [TIME HMAC, c=time]
    - ORCA [Challenge-Response based]
- Yubikey [Παραλλαγή HMAC ($c_n > c_{n-1}$)]
- RSA & Clones [παραλλαγές TOTP]
- SMS code
- Τηλεφωνική ανακοίνωση κωδικού

Online presence: security

- "We've seen a single attacker using stolen passwords to attempt to break into a million different Google accounts every single day, for weeks at a time."
- "A different gang attempted sign-ins at a rate of more than 100 accounts per second.“
- Security researcher Elie Bursztein: 18.4% of U.S. Internet users have had at least one of their online accounts broken into.
- Πωλούνται Facebook account: 500 για 200 rubles ($6.2) και 250 rubles ($7.7) για 500 twitter account…

TFA in the cloud: Google



Google

Accounts

- Account
- Security
- Profile and privacy
- Google+
- Products

Password and recovery options

Your password

Don't reuse your Google password on other sites. Learn more

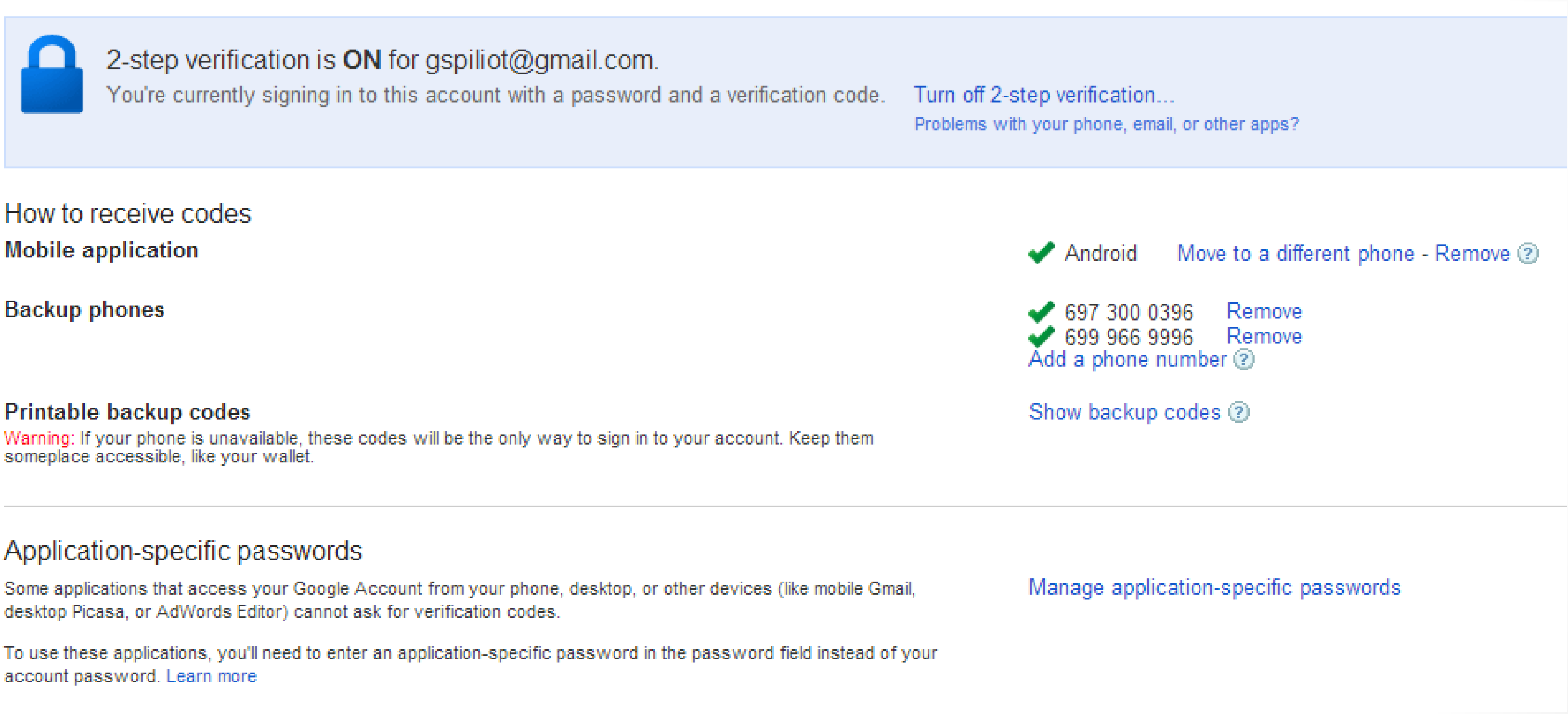
Your recovery options

Recovery options make it easier to get your account back if you lose your password. Learn more

2-step verification

2-step verification uses your phone to provide an extra layer of security for your account. Learn more

TFA in the cloud: Google



2-step verification is **ON** for gspiliot@gmail.com.

You're currently signing in to this account with a password and a verification code.

Turn off 2-step verification...

Problems with your phone, email, or other apps?

How to receive codes

Mobile application

✓ Android Move to a different phone - Remove ⓘ

Backup phones

✓ 697 300 0396 Remove

✓ 699 966 9996 Remove

Add a phone number ⓘ

Printable backup codes

Warning: If your phone is unavailable, these codes will be the only way to sign in to your account. Keep them someplace accessible, like your wallet.

Show backup codes ⓘ

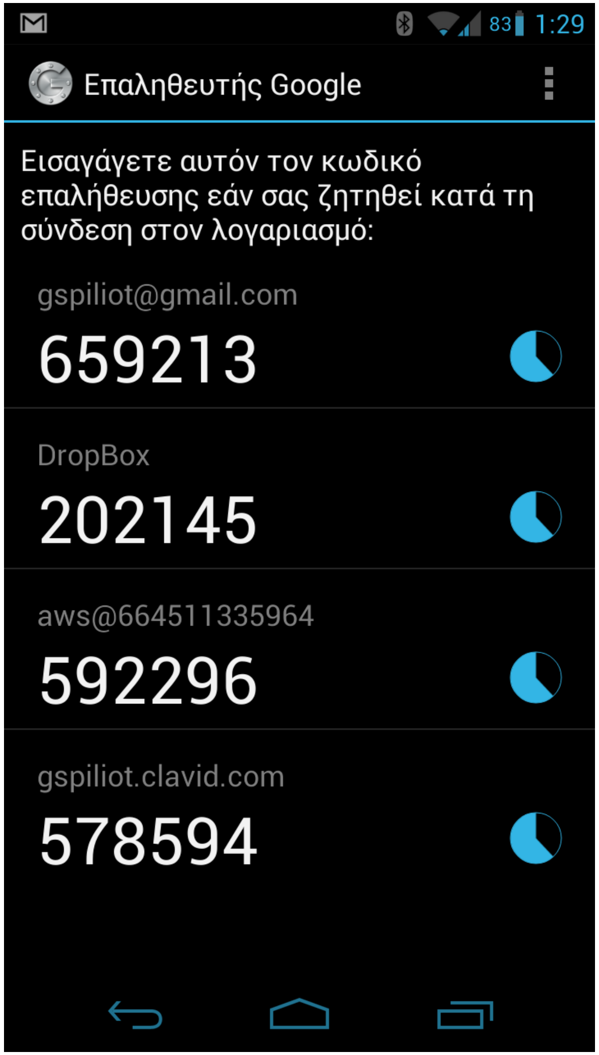
Application-specific passwords

Some applications that access your Google Account from your phone, desktop, or other devices (like mobile Gmail, desktop Picasa, or AdWords Editor) cannot ask for verification codes.

To use these applications, you'll need to enter an application-specific password in the password field instead of your account password. Learn more

Manage application-specific passwords

TFA in the cloud: Google



1:29

Επαληθευτής Google

Εισαγάγετε αυτόν τον κωδικό επαλήθευσης εάν σας ζητηθεί κατά τη σύνδεση στον λογαριασμό:

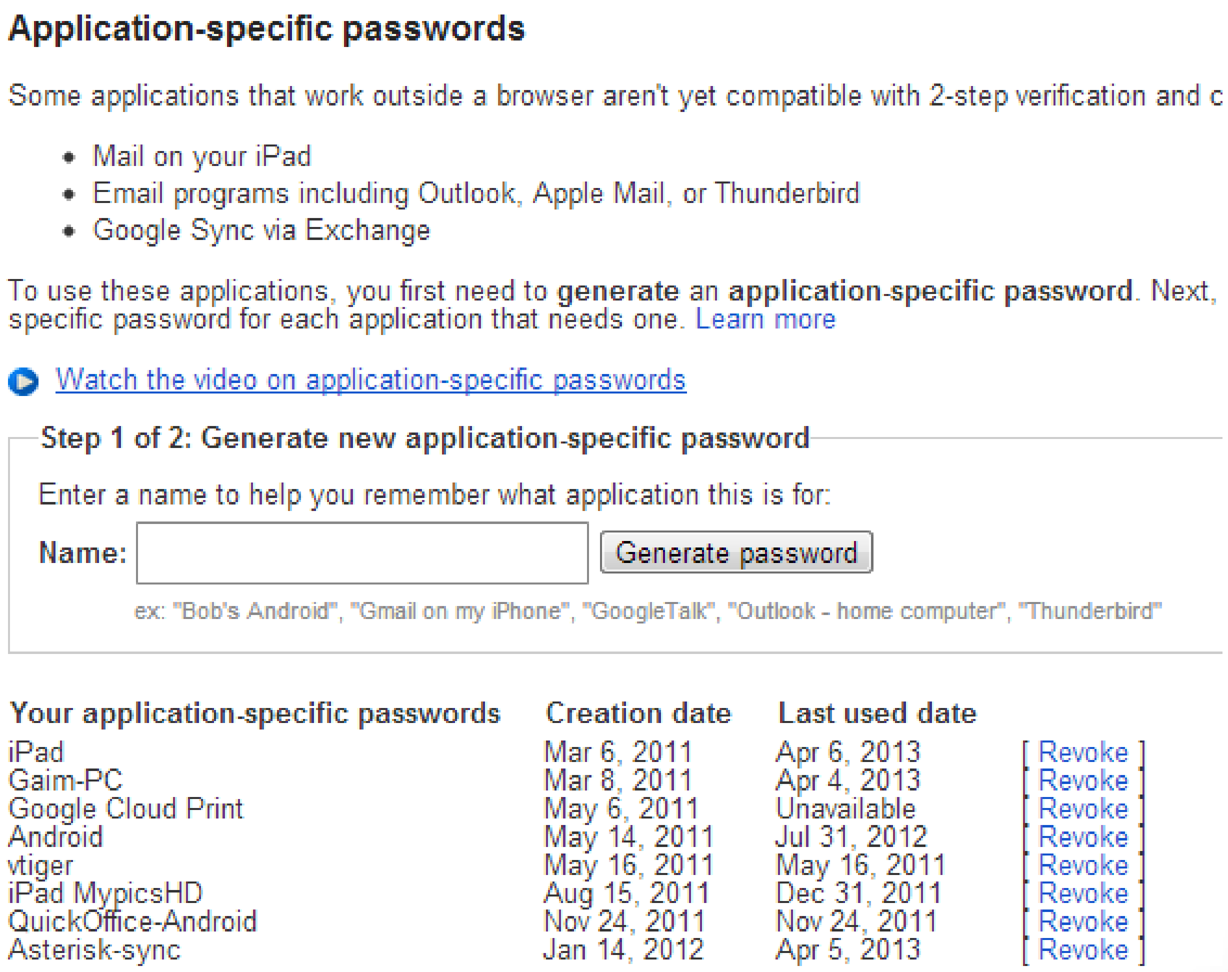
gspiliot@gmail.com
659213

DropBox
202145

aws@664511335964
592296

gspiliot.clavid.com
578594

TFA in the cloud: Google



Application-specific passwords

Some applications that work outside a browser aren't yet compatible with 2-step verification and c

- Mail on your iPad
- Email programs including Outlook, Apple Mail, or Thunderbird
- Google Sync via Exchange

To use these applications, you first need to **generate** an **application-specific password**. Next, specific password for each application that needs one. Learn more

Watch the video on application-specific passwords

Step 1 of 2: Generate new application-specific password

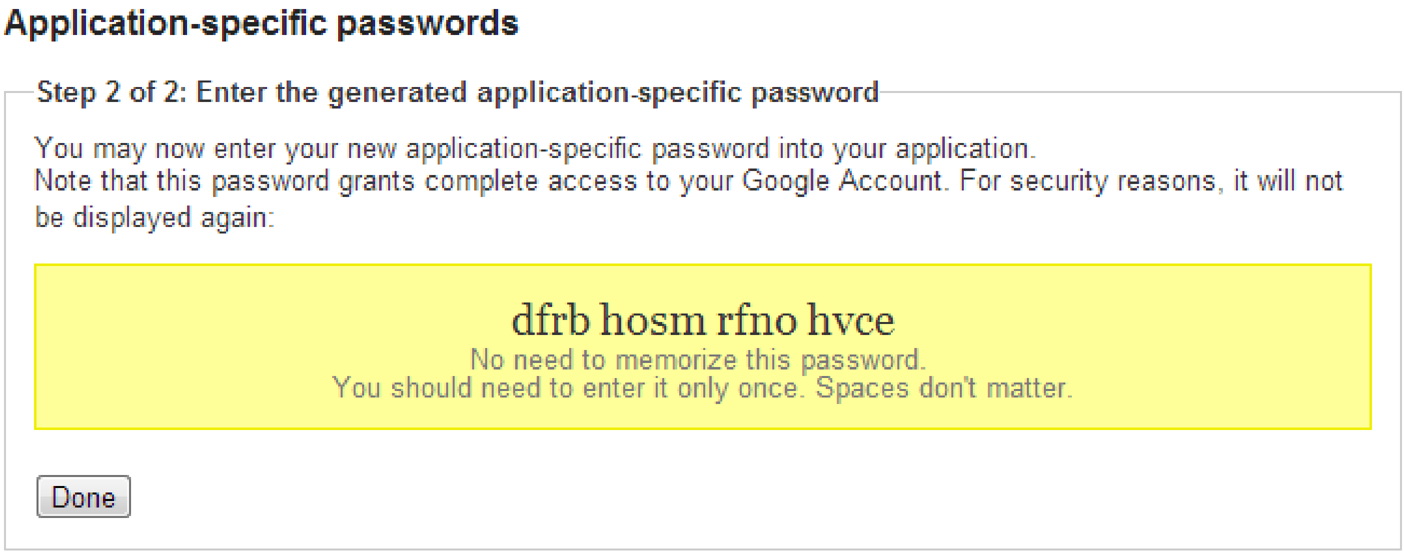
Enter a name to help you remember what application this is for:

Name:

ex: "Bob's Android", "Gmail on my iPhone", "GoogleTalk", "Outlook - home computer", "Thunderbird"

Your application-specific passwords	Creation date	Last used date	
iPad	Mar 6, 2011	Apr 6, 2013	[Revoke]
Gaim-PC	Mar 8, 2011	Apr 4, 2013	[Revoke]
Google Cloud Print	May 6, 2011	Unavailable	[Revoke]
Android	May 14, 2011	Jul 31, 2012	[Revoke]
vtiger	May 16, 2011	May 16, 2011	[Revoke]
iPad MypicsHD	Aug 15, 2011	Dec 31, 2011	[Revoke]
QuickOffice-Android	Nov 24, 2011	Nov 24, 2011	[Revoke]
Asterisk-sync	Jan 14, 2012	Apr 5, 2013	[Revoke]

TFA in the cloud: Google



Application-specific passwords

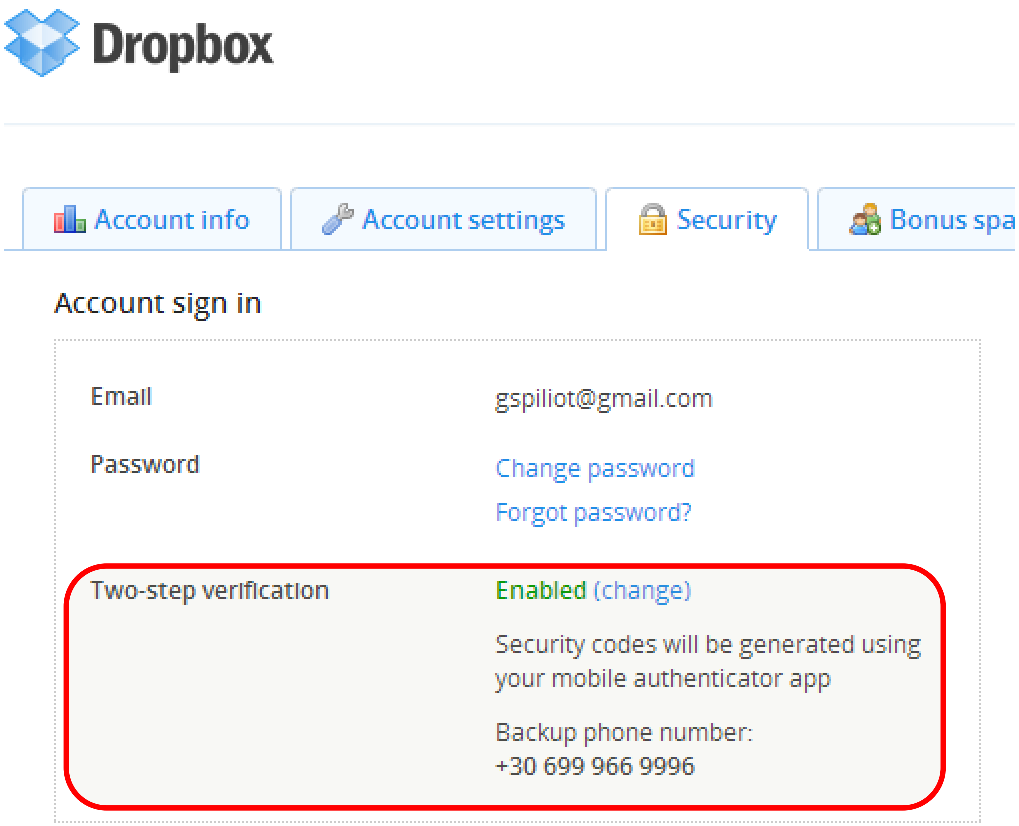
Step 2 of 2: Enter the generated application-specific password

You may now enter your new application-specific password into your application.
Note that this password grants complete access to your Google Account. For security reasons, it will not be displayed again:

dfrb hosm rfno hvce

No need to memorize this password.
You should need to enter it only once. Spaces don't matter.

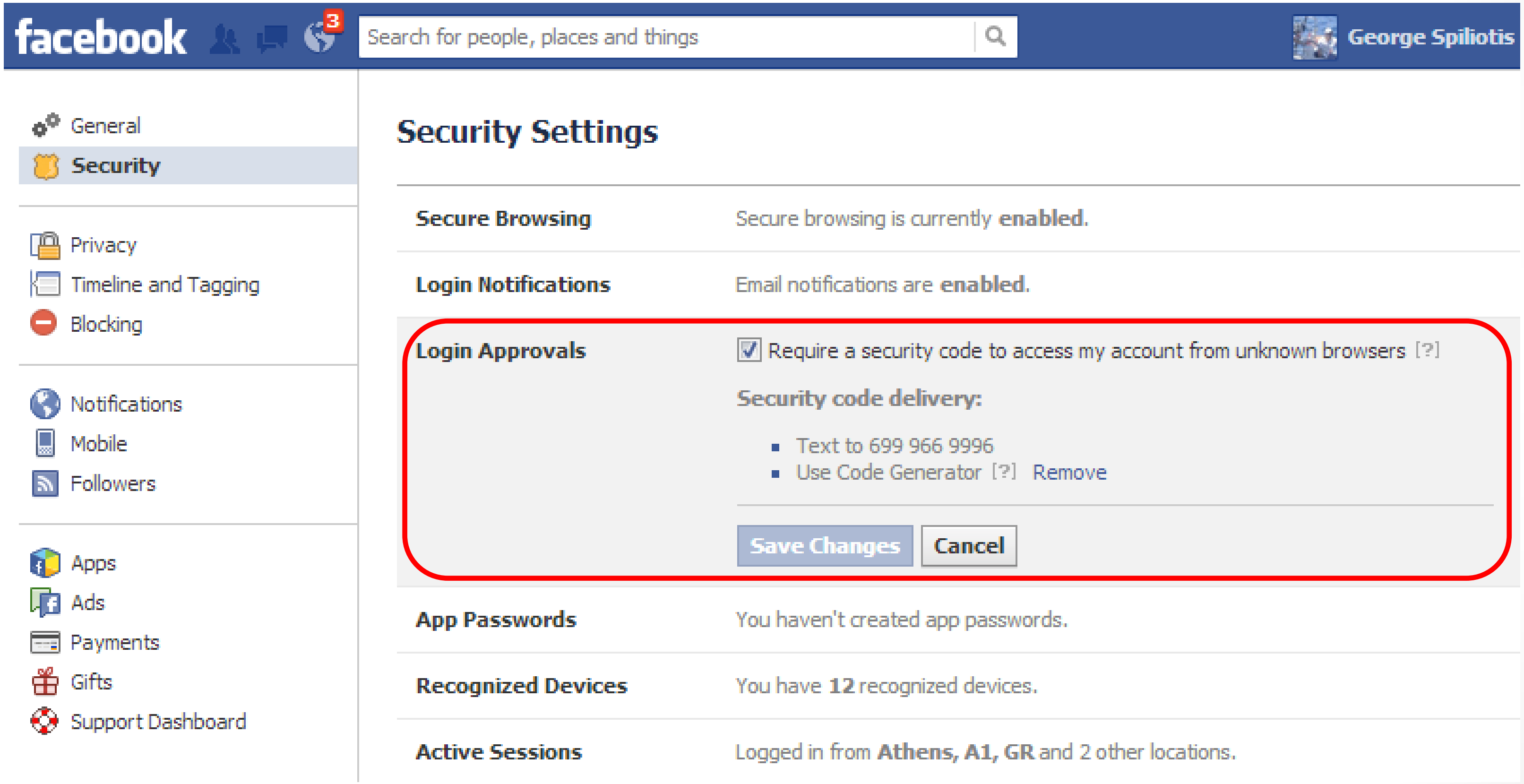
TFA in the cloud: Dropbox



Account sign in

Email	gspiliot@gmail.com
Password	Change password Forgot password?
Two-step verification	Enabled (change) Security codes will be generated using your mobile authenticator app Backup phone number: +30 699 966 9996

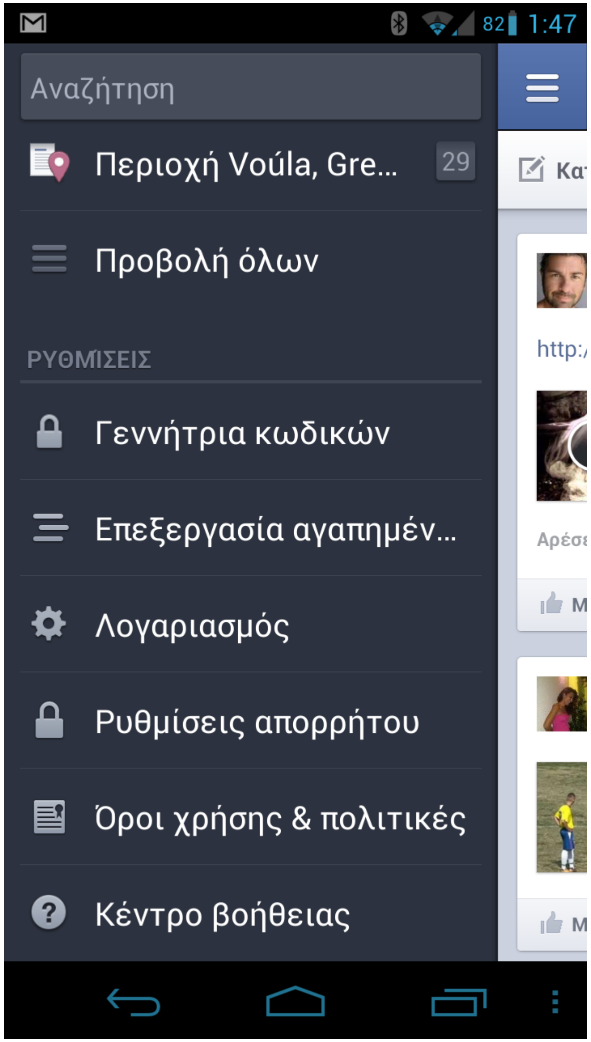
TFA in the cloud: Facebook

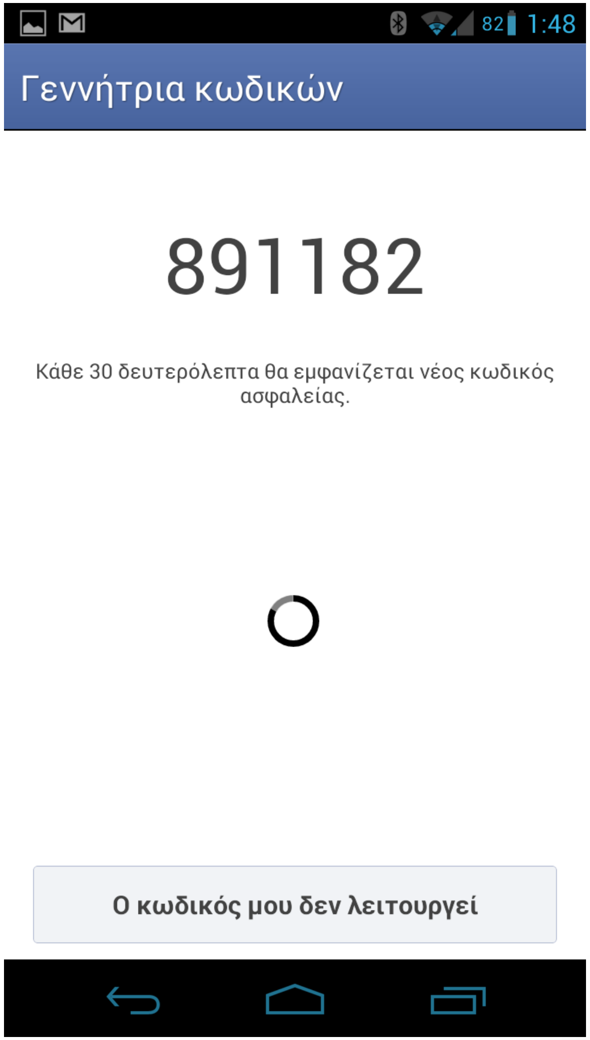


Security Settings

Secure Browsing	Secure browsing is currently **enabled**.
Login Notifications	Email notifications are **enabled**.
Login Approvals	☑ Require a security code to access my account from unknown browsers [?] **Security code delivery:** ▪ Text to 699 966 9996 ▪ Use Code Generator [?] Remove
App Passwords	You haven't created app passwords.
Recognized Devices	You have **12** recognized devices.
Active Sessions	Logged in from **Athens, A1, GR** and 2 other locations.

TFA in the cloud: Facebook

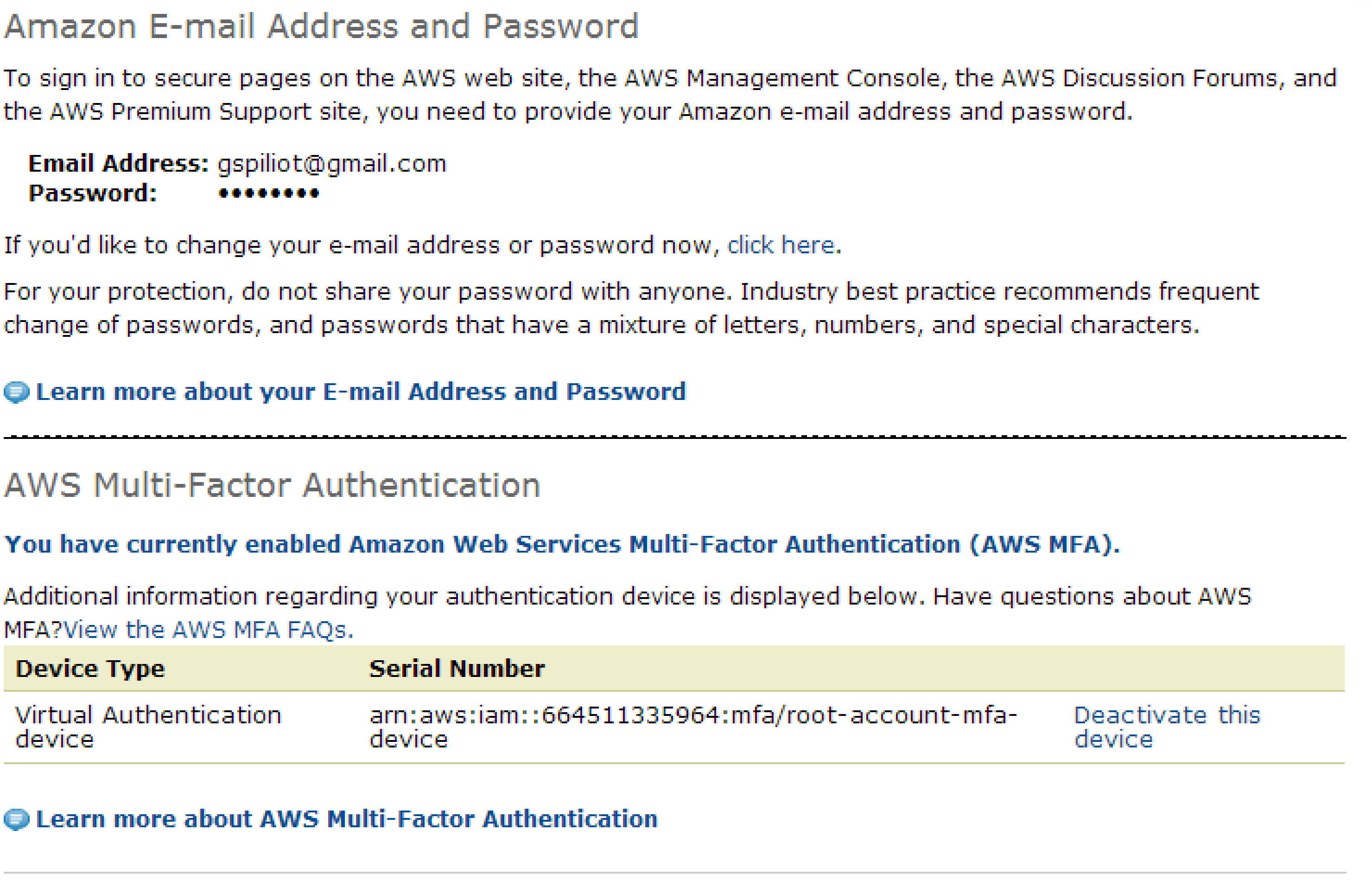




891182

Κάθε 30 δευτερόλεπτα θα εμφανίζεται νέος κωδικός ασφαλείας.

TFA in the cloud: Amazon AWS



Amazon E-mail Address and Password

To sign in to secure pages on the AWS web site, the AWS Management Console, the AWS Discussion Forums, and the AWS Premium Support site, you need to provide your Amazon e-mail address and password.

Email Address: gspiliot@gmail.com
Password: ••••••••

If you'd like to change your e-mail address or password now, click here.

For your protection, do not share your password with anyone. Industry best practice recommends frequent change of passwords, and passwords that have a mixture of letters, numbers, and special characters.

Learn more about your E-mail Address and Password

AWS Multi-Factor Authentication

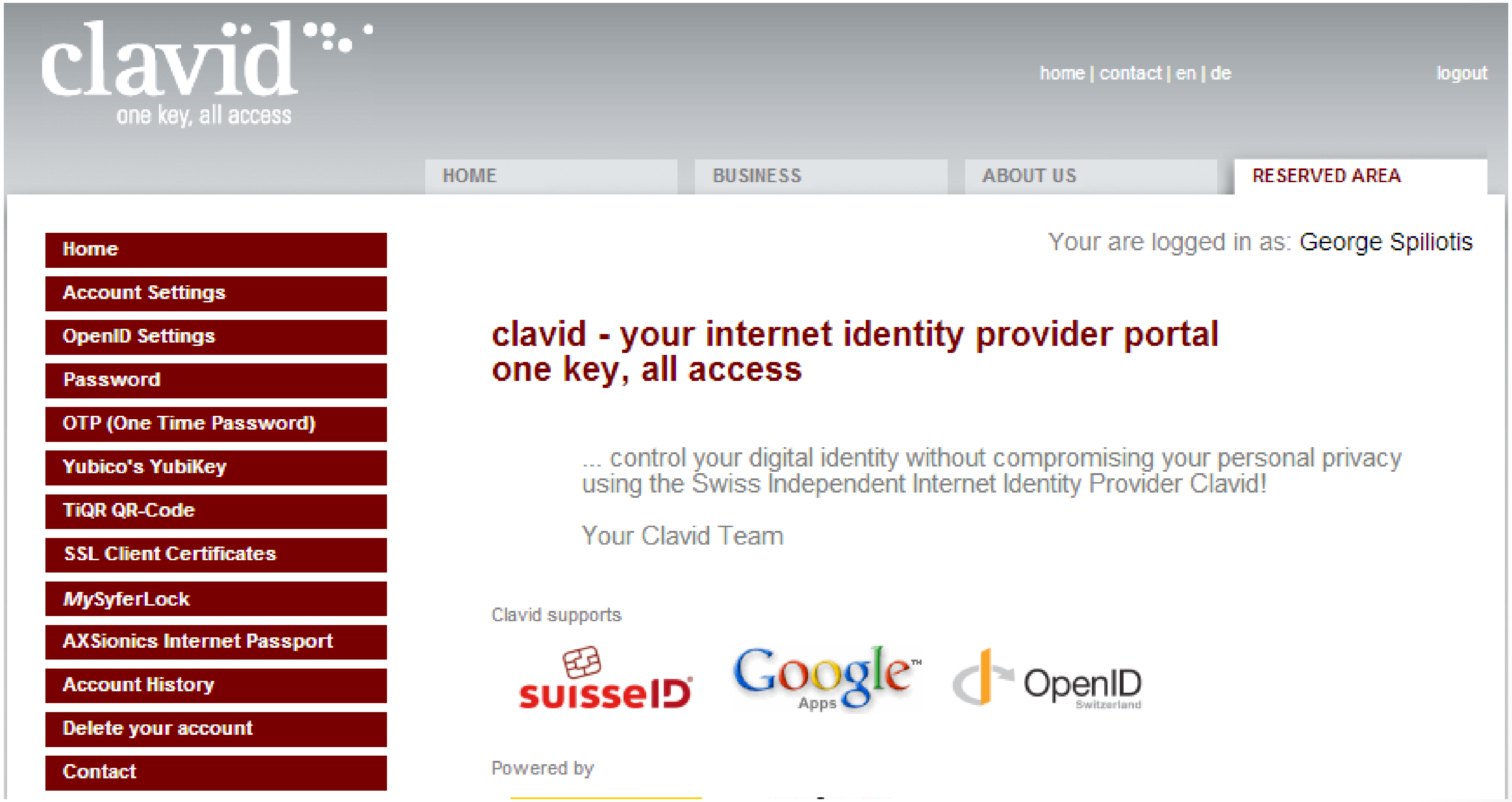
You have currently enabled Amazon Web Services Multi-Factor Authentication (AWS MFA).

Additional information regarding your authentication device is displayed below. Have questions about AWS MFA?View the AWS MFA FAQs.

Device Type	Serial Number	
Virtual Authentication device	arn:aws:iam::664511335964:mfa/root-account-mfa-device	Deactivate this device

Learn more about AWS Multi-Factor Authentication

OpenID MultiFactor provider



Your are logged in as: George Spiliotis

clavid - your internet identity provider portal
one key, all access

... control your digital identity without compromising your personal privacy using the Swiss Independent Internet Identity Provider Clavid!

Your Clavid Team

Clavid supports

Powered by

Corporate Solutions

- Yubikey http://www.yubico.com
  - Δύο personalities σε ένα κλειδί
  - Επανεγγράψιμο
  - Proprietary Yubico protocol, OATH ή Static Secret
  - Radius Server infrastructure χωρίς κόστος
- Mobile OTP (MOTP) http://motp.sourceforge.net
  - Χωρίς έξοδα για Hardware Device
  - TOTP από το κινητό τηλέφωνο (Android, iOS, Windows Phone, Blackberry, παλαιότερα τηλέφωνα με jME)
  - Free Radius Server implementation