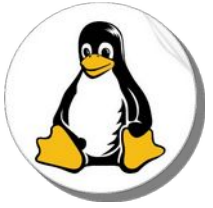
GreekLUG

Ελεύθερο Λογισμικό &



Λογισμικό Ανοικτού Κώδικα

Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Ενότητες

#Εισαγωγή - Γενική προστασία
Γενικά θέματα για την ασφάλεια και ιδιωτικότητα

#Κανόνες ασφαλείας
Βήματα και κανόνες ασφαλείας για υπολογιστές και φορητές συσκευές

#Συνθηματικά
Κωδικοί, 2FA/TOTP και εφαρμογές Password manager

#Κρυπτογράφηση συσκευών
Προστασία συσκευής

#Κρυπτογράφηση επικοινωνίας
HTTPS/SSL, Email/SSL, PGP

Ενότητες

#Ασφάλεια σε κοινωνικά δίκτυα
Διαμοιρασμός, παραπλανητικά μηνύματα, ψευδείς ειδήσεις

#Spam & Phishing (Ηλεκτρονικό «ψάρεμα»)
E-mail και παραπλάνηση, προστασία τραπεζικών συναλλαγών

#Παραβίαση
Βήματα μετά από παραβίαση

Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Εισαγωγή - Γενική προστασία

Εισαγωγή - Γενική προστασία

Η σύγχρονη κοινωνία μεταβαίνει όλο και περισσότερο σε ψηφιακή κατάσταση. Κάθε ημέρα ακόμη περισσότεροι χρήστες εισέρχονται στον ψηφιακό κόσμο ή επεκτείνουν την ψηφιακή τους παρουσία δημιουργώντας νέους λογαριασμούς και προσβάσεις σε ψηφιακά μέσα.

Φυσικό επακόλουθο του παραπάνω είναι το θέμα της **Ασφάλειας** να επεκτείνεται και να περιλαμβάνει σε σημαντικό ποσοστό τον ψηφιακό κόσμο.

Η ραγδαία ανάπτυξη του παγκόσμιου διαδικτύου, νέων μεθόδων επικοινωνίας και ανταλλαγής δεδομένων, δημιουργεί συνεχώς νέες προκλήσεις ασφαλείας, καθώς ένα σημαντικό τμήμα της ζωής μας εξαρτάται και στηρίζεται σε ψηφιακές υπηρεσίες και περιεχόμενο.

Η προσωπική μας ασφάλεια, οι ιδιωτικές μας πληροφορίες, η περιουσία μας, τα προσωπικά μας δεδομένα και πολλά ακόμα, μπορεί να κινδυνεύουν και λόγω αυτού θα πρέπει να ενημερωνόμαστε αλλά και να ακολουθούμε κανόνες ασφαλείας για την προστασία μας.

Εισαγωγή - Γενική προστασία

Η **ηλεκτρονική ασφάλεια** αποτελεί ένα σύνθετο παζλ που περιλαμβάνει διάφορους μηχανισμούς.

Δεν υπάρχει μία "*μαγική*" λύση που εφαρμόζοντάς την μπορούμε να λύσουμε το θέμα.

Υπάρχουν πολλαπλά σημεία που συνδυάζονται ώστε να δημιουργήσουν ένα προφίλ ασφαλείας.

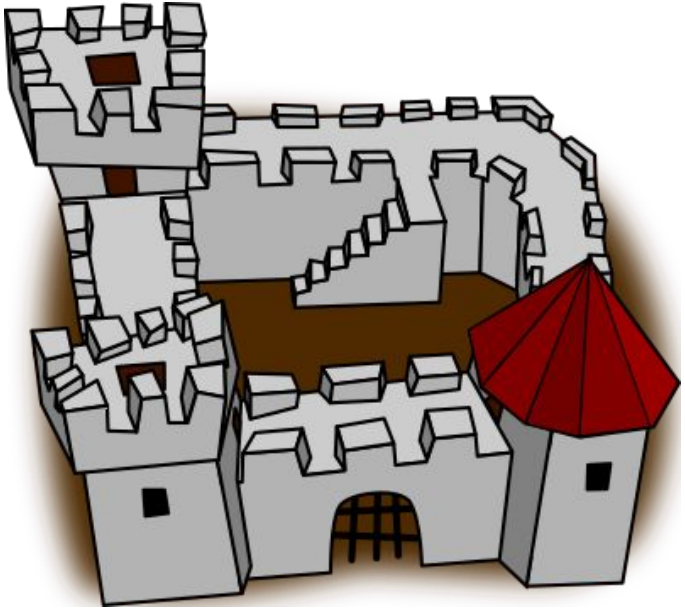
Αυτό που μπορούμε να κάνουμε από την πλευρά μας είναι να ελέγξουμε και να κατανοήσουμε τα χαρακτηριστικά και τις "*επιφάνειες*" που έχουμε εκτεθειμένες και να αναζητήσουμε λύσεις που βελτιώνουν την ασφάλειά μας.

Αυτή εξαρτάται από πολλαπλούς παράγοντες, όπως το υλικό (hardware) της συσκευής μας, το λειτουργικό σύστημα και τις εφαρμογές που χρησιμοποιούμε (software), την σύνδεση στο διαδίκτυο (τρόπος σύνδεσης) και τον τρόπο επικοινωνίας μας μέσω αυτού αλλά και τις πληροφορίες που διαμοιραζόμαστε στο διαδίκτυο (ψηφιακό αποτύπωμα).

Εισαγωγή - Γενική προστασία

Μερικές παραδοχές…

- Η **ασφάλεια** και η **ευχρηστία**, συνήθως τείνουν να είναι αντίθετες
- "*Όλα σπάνε*"



Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Κανόνες ασφαλείας

Κανόνες ασφαλείας

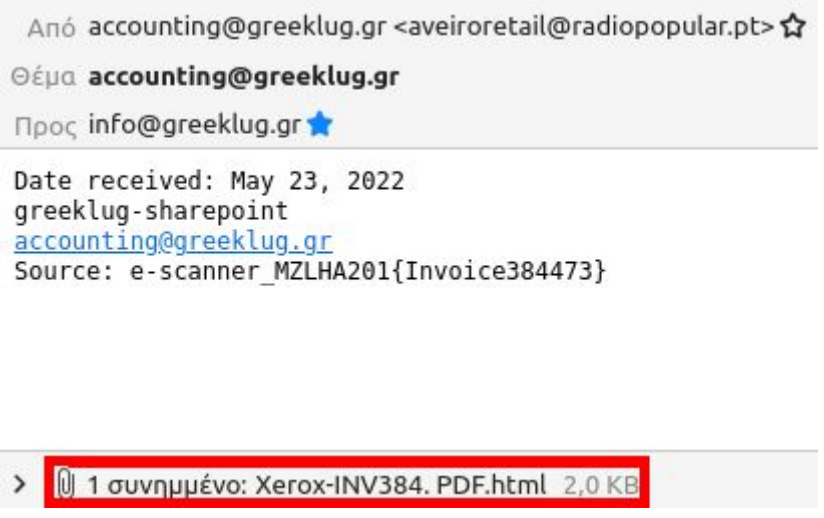
Δεν εκτελούμε προγράμματα και εφαρμογές που δεν αναγνωρίζουμε ως οικεία

πχ δεν ανοίγουμε άγνωστα αρχεία ή (ύποπτα) συνημμένα από email

Τα περισσότερα από αυτά είναι σε εκτελέσιμα αρχεία, πχ .exe, ή κεκαλυμμένα εκτελέσιμα, πχ .jpg.exe

Πλοηγούμαστε με προσοχή σε άγνωστες σελίδες

δεν ανοίγουμε άμεσα κάθε σύνδεσμο που υπάρχει σε μια σελίδα ή μας έχει σταλθεί πχ μέσω email



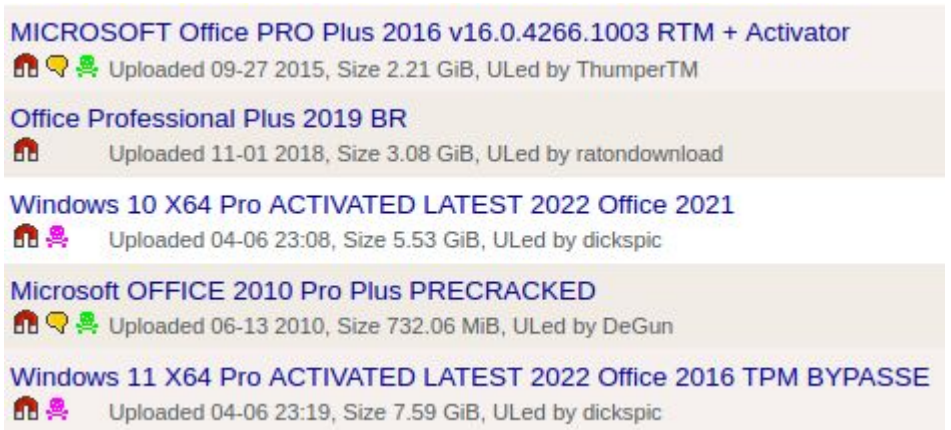
Κανόνες ασφαλείας

Δεν εγκαθιστούμε προγράμματα από τυχαίες σελίδες

Προτιμούμε την εγκατάσταση από το εκάστοτε market εφαρμογών ή την επίσημη σελίδα

Δεν εγκαθιστούμε “σπασμένα” Λ/Σ & προγράμματα

Πολλά από τα *crack* περιέχουν κακόβουλο κώδικα, όπως ιούς, που πέραν του “ξεκλειδώματος” που μας προσφέρουν μπορεί να μολύνουν την συσκευή μας



Κανόνες ασφαλείας

Χρησιμοποιούμε εφαρμογές ασφαλείας

Καθώς τα κακόβουλα προγράμματα είναι... “εκεί έξω”, χρησιμοποιούμε εφαρμογές ασφαλείας, όπως **antivirus**, για να προστατεύσουμε την συσκευή μας

Ενημερώσεις ασφαλείας

Κάνουμε τακτικά ενημερώσεις, ειδικότερα το συντομότερο δυνατό τις **ενημερώσεις ασφαλείας**

Κανόνες ασφαλείας

Εκτελούμε περιοδικά έλεγχο ασφαλείας

Ανά κάποιο χρονικό διάστημα, πχ 1 φόρα το εξάμηνο, ελέγχουμε τις ρυθμίσεις αλλά και σκανάρουμε όλα τα αρχεία μας

Ελέγχουμε τις ρυθμίσεις

Πολλές εφαρμογές εφαρμόζουν από προκαθορισμένα συλλογή πληροφοριών ή άλλες μη-ασφαλείς λειτουργίες

Κανόνες ασφαλείας

Προστατεύουμε την συσκευή μας με κωδικούς πρόσβασης

πχ ορίζουμε κωδικό πρόσβασης στην προφύλαξη οθόνης

Επιλέγουμε την κρυπτογράφηση

όπου αυτό είναι εφικτό, για προστασία πρόσβασης τρίτων,

πχ σε περίπτωση κλοπής

Κανόνες ασφαλείας

Αποφεύγουμε/προσέχουμε τα άγνωστα/δημόσια δίκτυα

αρκετοί δημόσιοι ή κοινόχρηστοι χώροι (καφετέριες, ξενοδοχεία, αεροδρόμια κτλ) παρέχουν ανοιχτά (ασύρματα ή ενσύρματα) δίκτυα με δωρεάν πρόσβαση στο διαδίκτυο, ωστόσο…
η ασφάλειά τους είναι πολλές φορές περιορισμένη, με αποτέλεσμα κακόβουλοι χρήστες να μπορούν να τα χρησιμοποιήσουν ώστε να υποκλέψουν στοιχεία πρόσβασης ή να μολύνουν μη προστατευμένες συσκευές

Αποφεύγουμε/προσέχουμε στους δημόσιους υπολογιστές

αρκετοί χώροι, όπως βιβλιοθήκες, παρέχουν πρόσβαση σε κοινόχρηστους υπολογιστές.
Αν ο υπολογιστής δεν τηρεί τις ενημερώσεις ασφαλείας ή ακόμα είναι ήδη μολυσμένος(!) μπορεί κάποιος κακόβουλος χρήστης να κρατάει το ιστορικό μας ή ακόμα και να δει οτιδήποτε πληκτρολογούμε(!)… με αποτέλεσμα να λάβει πρόσβαση σε κωδικούς μας!

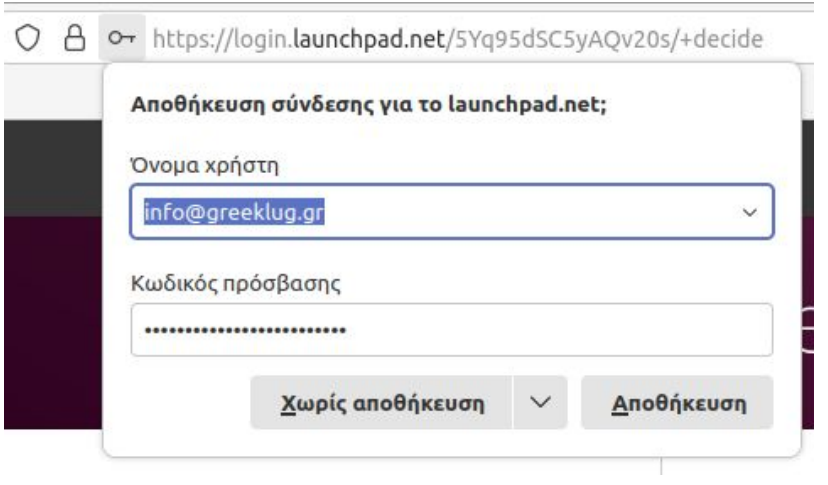
Κανόνες ασφαλείας

<u>Δεν αποθηκεύουμε τα στοιχεία μας</u>

όταν συνδεόμαστε σε έναν λογαριασμό μας (πχ μπαίνουμε στο facebook), δεν επιλέγουμε **ΠΟΤΕ** στην επιλογή να αποθηκευτούν τα στοιχεία εισόδου στον περιηγητή διαδικτύου.

Ακολούθως, όταν τελειώσουμε την περιήγησή μας, **κάνουμε αποσύνδεση** από όλους τους λογαριασμούς μας.

* συνιστάται η χρήση ιδιωτικής περιήγησης στον περιηγητή όπου δεν αποθηκεύεται το ιστορικό περιήγησης



Κανόνες ασφαλείας σε φορητές συσκευές

Ρύθμιση για κλείδωμα φορητής συσκευής

Στην πρώτη εκκίνηση της φορητής συσκευής μας, επιλέγουμε πάντα την ρύθμιση κλειδώματος και ξεκλειδώματος (είτε με χρήση pin, κωδικού μοτίβου, δακτυλικού αποτυπώματος, ή face unlock).

Προσοχή στις εφαρμογές που εγκαθίστανται στις φορητές συσκευές

Συστήνεται η εγκατάσταση εφαρμογών από το market του λειτουργικού συστήματος και από έμπιστους δημιουργούς / επίσημες εταιρίες

Προσοχή στα δικαιώματα που εκχωρούνται στις εφαρμογές

Αποφεύγουμε να εγκαθιστούμε / χρησιμοποιούμε εφαρμογές που απαιτούν παράλογα δικαιώματα για την λειτουργία τους

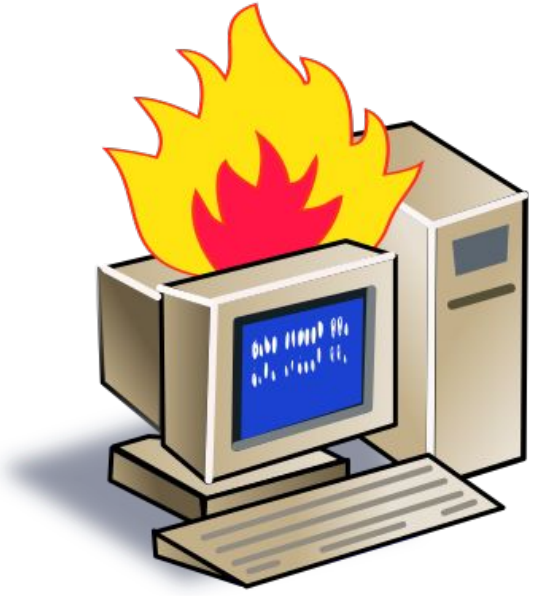
Κακόβουλο Λογισμικό

Κακόβουλο λογισμικό ή malware

- Λογισμικό που είναι κατασκευασμένο για να προκαλεί μη εξουσιοδοτημένες ενέργειες σε ένα μηχάνημα (μείωση απόδοσης Η/Υ, υποκλοπή/διαγραφή δεδομένων, απομακρυσμένος έλεγχος κα)

- Malware = ιός, trojan horse, ransomware, phishing, spyware, keyloggers κα

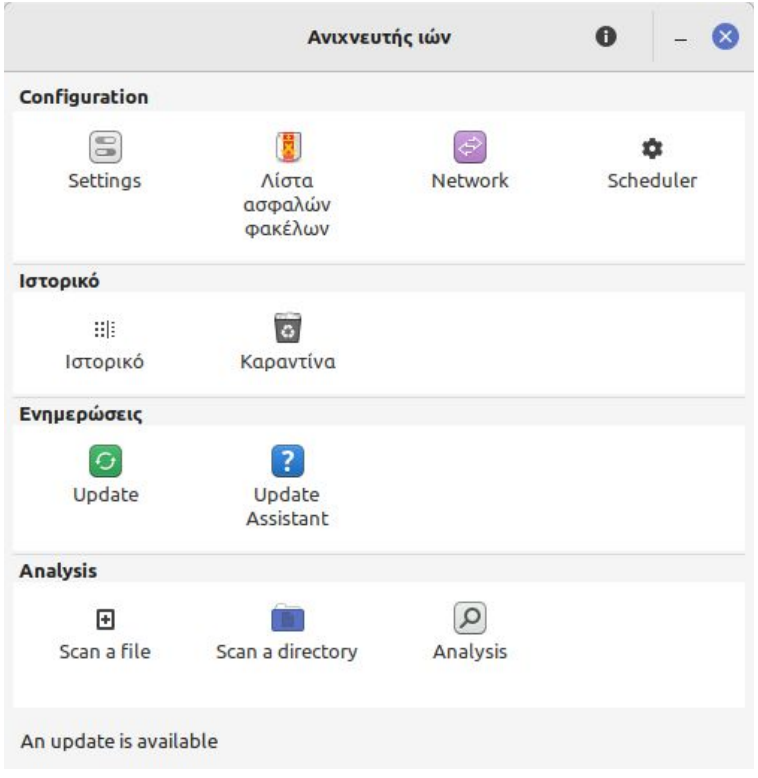
- Απαιτούν συνήθως ανθρώπινη παρέμβαση για την λειτουργία τους (άνοιγμα συνδέσμου, εκτέλεση αρχείου, εγκατάσταση κακόβουλου προγράμματος)



Αντιμετώπιση malware

- Εγκατάσταση προγραμμάτων προστασίας από ιούς (**antivirus**)

Προλαβαίνουν την εγκατάσταση ιού σε Η/Υ, σκανάρει για κακόβουλα αρχεία, προστασία antiphishing, αποκλεισμός κακόβουλων διαφημίσεων



- Συχνή ενημέρωση λειτουργικού συστήματος και εφαρμογών
- Αποφυγή εγκατάστασης “σπασμένων” προγραμμάτων

- Ενεργοποίηση firewall

Ασπίδα προστασίας που φιλτράρει την κίνηση του δικτύου μεταξύ του Η/Υ μας και του internet

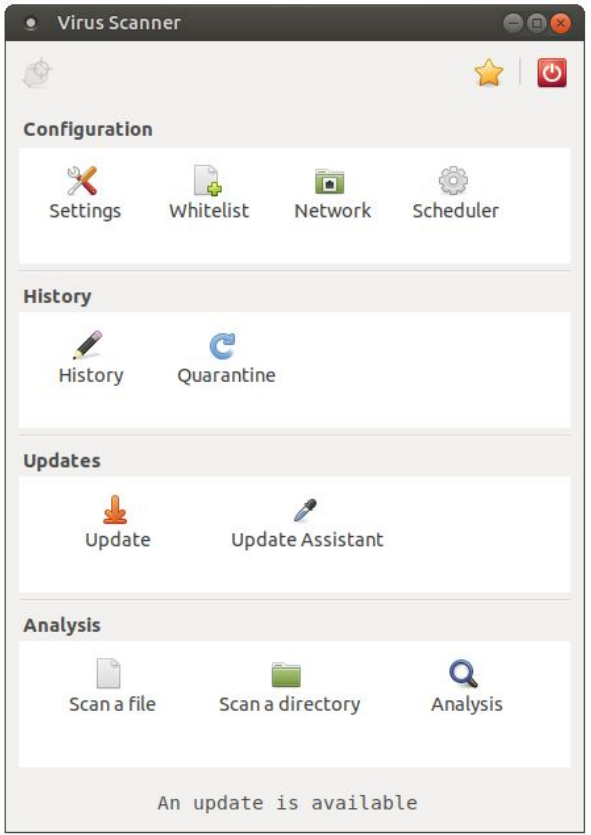
Αντιμετώπιση malware

Clamav

Ανοικτού κώδικα antivirus σε μορφή cli και γραφικού gui

Διαθέσιμο για όλα τα γνωστά Λ/Σ

```
[redacted]:~/Εικόνες/Wallpapers$ clamscan -v 'Wallpapers - Ubuntu'/

Scanning Ubuntu-Gloss/gloss-no-panel.png
Ubuntu-Gloss/gloss-no-panel.png: OK
Scanning Ubuntu-Gloss/ubuntu-gloss-1440 - 900.png
Ubuntu-Gloss/ubuntu-gloss-1440 - 900.png: OK
Scanning Ubuntu-Gloss/ubuntu-gloss.png
Ubuntu-Gloss/ubuntu-gloss.png: OK
Scanning Ubuntu-Gloss/ubuntu-gloss-1440 - 900.jpg
Ubuntu-Gloss/ubuntu-gloss-1440 - 900.jpg: OK
Scanning Ubuntu-Gloss/ubuntu-gloss-no-panel.png
Ubuntu-Gloss/ubuntu-gloss-no-panel.png: OK



----------- SCAN SUMMARY -----------
Known viruses: 6512356
Engine version: 0.99.2
Scanned directories: 1
Scanned files: 172
Infected files: 0
Data scanned: 68.82 MB
Data read: 67.97 MB (ratio 1.01:1)
Time: 12.277 sec (0 m 12 s)
```



Αντιμετώπιση malware

rkhunter

Έλεγχος για rootkits, backdoors και πιθανές τοπικές ευπάθειες

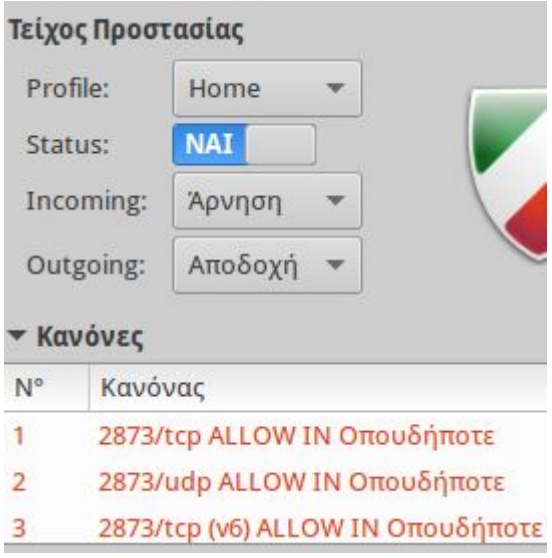
```
dimos99@dimosPC:~$ sudo rkhunter --check
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                               [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                        [ None found ]
    Checking for preloaded libraries                         [ None found ]
    Checking LD_LIBRARY_PATH variable                        [ Not found ]

  Performing file properties checks
    Checking for prerequisites                               [ OK ]
    /usr/sbin/adduser                                        [ OK ]
    /usr/sbin/chroot                                         [ OK ]
    /usr/sbin/cron                                           [ OK ]
    /usr/sbin/groupadd                                       [ OK ]
    /usr/sbin/groupdel                                       [ OK ]
    /usr/sbin/groupmod                                       [ OK ]
    /usr/sbin/grpck                                          [ OK ]
    /usr/sbin/nologin                                        [ OK ]
    /usr/sbin/pwck                                           [ OK ]
    /usr/sbin/rsyslogd                                       [ OK ]
    /usr/sbin/sshd                                           [ OK ]
    /usr/sbin/useradd                                        [ OK ]
    /usr/sbin/userdel                                        [ OK ]
    /usr/sbin/usermod                                        [ OK ]
    /usr/sbin/vipw                                           [ OK ]
    /usr/sbin/unhide                                         [ OK ]
    /usr/sbin/unhide-linux                                   [ OK ]
    /usr/sbin/unhide-posix                                   [ OK ]
    /usr/sbin/unhide-tcp                                     [ OK ]
    /usr/bin/awk                                             [ OK ]
    /usr/bin/basename                                        [ OK ]
```

Αντιμετώπιση malware

IPTables

Το λογισμικό που παρέχει δυνατότητες firewall σε διανομές GNU/Linux

Διαθέτει διάφορες διεπαφές για εύκολη ρύθμιση, όπως το **UFW** / **GUFW**




```
:/$ sudo iptables -L

Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere

Chain ufw-after-forward (1 references)
target     prot opt source               destination
```

Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Συνθηματικά

Συνθηματικά

Οι κωδικοί (password) που επιλέγουμε θα πρέπει να είναι… σύνθετοι και μεγάλοι…

- τουλάχιστον 8 χαρακτήρων
- να περιέχουν γράμματα (μικρά | κεφαλαία), αριθμούς και ειδικούς χαρακτήρες

Μη ασφαλής κωδικός → 1234 ή nikos2021 ή maria15

Ασφαλής κωδικός → Dg!c20#Rz4

Χρησιμοποιούμε διαφορετικούς κωδικούς ανά λογαριασμό

πχ ορίζουμε διαφορετικό κωδικό σε κάθε ιστοσελίδα που είμαστε εγγεγραμμένοι

Αλλάζουμε περιοδικά τους κωδικούς

τουλάχιστον μια φορά κάθε χρόνο είναι καλό να αλλάζουμε τους κωδικούς

Συνθηματικά

Αριθμός Χαρακτήρων	Μόνο Αριθμοί	Μόνο Πεζά γράμματα	Κεφαλαία και Πεζά Γράμματα	Αριθμοί, Πεζά και Κεφαλαία Γράμματα	Σύμβολαμ Αριθμοί, Πεζά και Κεφαλαία Γράμματα
4	Απευθείας	Απευθείας	Απευθείας	Απευθείας	Απευθείας
5	Απευθείας	Απευθείας	Απευθείας	Απευθείας	Απευθείας
6	Απευθείας	Απευθείας	Απευθείας	1 δευτ	5 δευτ
7	Απευθείας	Απευθείας	25 δευτ	1 λεπτό	6 λεπτά
8	Απευθείας	5 δευτ	22 λεπτά	1 ώρα	8 ώρες
9	Απευθείας	2 λεπτά	19 ώρες	3 ημέρες	3 εβδομάδες
10	Απευθείας	58 λεπτά	1 μήνα	7 μήνες	5 χρόνια
11	2 δευτ	1 ημέρες	5 χρόνια	41 χρόνια	400 χρόνια
12	25 δευτ	3 εβδομάδες	300 χρόνια	2.000 χρόνια	34.000 χρόνια
13	4 λεπτά	1 χρόνο	16.000 χρόνια	100.000 χρόνια	2 εκ.χρόνια
14	41 λεπτά	51 χρόνια	800.000 χρόνια	9 εκ. Χρόνια	200 εκ. Χρόνια
15	6 ώρες	1.000 χρόνια	43 εκ. Χρόνια	600 εκ.χρόνια	15 δις χρόνια
16	2 ημέρες	34.000 χρόνια	2 δις χρόνια	37 δις χρόνια	1 τρις χρόνια
17	4 εβδομάδες	800.000 χρόνια	100 δις χρόνια	2 τρις χρόνια	93 τρις χρόνια
18	9 μήνες	23 εκ.χρόνια	6 τρις χρόνια	100 τρις χρόνια	7 τετρακις χρόνια

Συνθηματικά

Δεν εισάγουμε τα στοιχεία μας σε τρίτες ιστοσελίδες ή εφαρμογές

Συχνές απάτες περιλαμβάνουν την αποστολή ευαίσθητων στοιχείων από τους χρήστες μέσω τεχνικών “ψαρέματος” (phishing)

* Δεν δίνουμε **ΠΟΤΕ** στοιχεία λογαριασμών τραπεζών (όνομα χρήστη και κωδικό) σε κανέναν

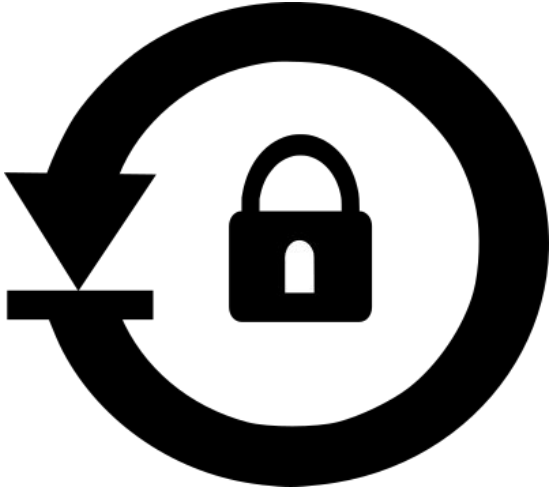
Συνθηματικά

Χρησιμοποιούμε επαλήθευση δύο βημάτων

όπου είναι εφικτό ενεργοποιούμε την **ασφάλεια δύο βημάτων**, πχ αποστολή ειδικού κωδικού μέσω sms στο κινητό μας ή email, για επαλήθευση

Χρησιμοποιούμε password managers

εφόσον σημειώνουμε ηλεκτρονικά τους κωδικούς, προτιμάμε τις ειδικές εφαρμογές “**password managers**”, όπου κρατάμε τους κωδικούς με ασφάλεια και όχι σε μη κρυπτογραφημένα αρχεία όπως .txt



Επαλήθευση 2 βημάτων

MFA (Multi Factor Autentication)

Μέθοδος ταυτοποίησης όπου αποκτούμε πρόσβαση σε έναν λογαριασμό μας με την εισαγωγή 2 ή παραπάνω στοιχείων

Τρόποι MFA

a) Λήψη κωδικού ή pin με ισχύ μερικά δευτερόλεπτα/λεπτά (TOTP – Time based One Time Password) μέσω sms, εφαρμογών αποστολής μηνυμάτων, push notification, App Authenticators

b) Φυσικές συσκευές που χρησιμεύουν ως κλειδί

c) Βιομετρικά δεδομένα (δακτυλικό αποτύπωμα, face unlock κα)

Password Managers

Διαχειριστές Κωδικών (Password Managers)

Ένα πρόγραμμα ή υπηρεσία που δημιουργεί, αποθηκεύει και διαχειρίζεται τους κωδικούς μας

- Αντικαθιστά παραδοσιακές και λιγότερο ασφαλείς μεθόδους διατήρησης κωδικών (απλό αρχείο κειμένου, αρχείο υπολογιστικού φύλλου, κομμάτι χαρτί)
- Αποθηκεύει τους κωδικούς σε μια κρυπτογραφημένη βάση προστατευμένη από έναν κύριο κωδικό
- Απαιτείται να θυμόμαστε μόνο τον κύριο κωδικό, που ξεκλειδώνει όλους τους υπόλοιπους

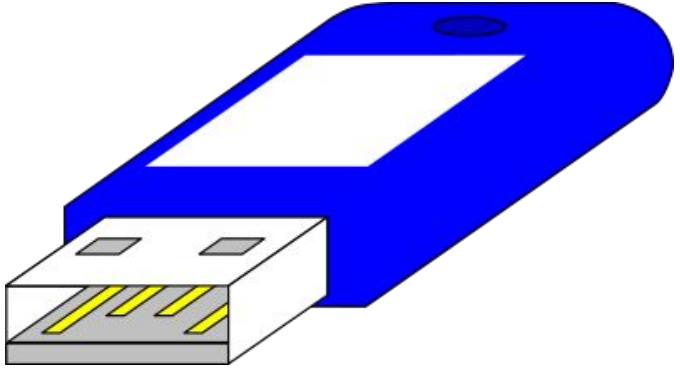
Password Managers

Είδη Διαχειριστών κωδικών

a) Εφαρμογές που υπάρχουν τοπικά στη συσκευή μας (Η/Υ, Laptop, Smartphone κτλ)

b) Online υπηρεσίες προσβάσιμες μέσω περιηγητών διαδικτύου

c) Hardware συσκευές που είναι / παράγουν ένα κλειδί προς χρήση για ξεκλείδωμα λογαριασμού



Password Managers

Password Managers που εγκαθιστώνται τοπικά στο μηχάνημά μας:

- Η κρυπτογραφημένη βάση βρίσκεται είτε τοπικά στον Η/Υ μας (μειωμένο ρίσκο υποκλοπής της, αφού δεν απαιτείται σύνδεση στο διαδίκτυο) και μπορούμε να την μεταφέρουμε σε ένα usb stick, είτε στο cloud σε μια υπηρεσία φιλοξενίας αρχείων (μπορούμε να την χρησιμοποιήσουμε από οπουδήποτε υπάρχει σύνδεση στο internet και συνήθως και από οποιαδήποτε συσκευή)

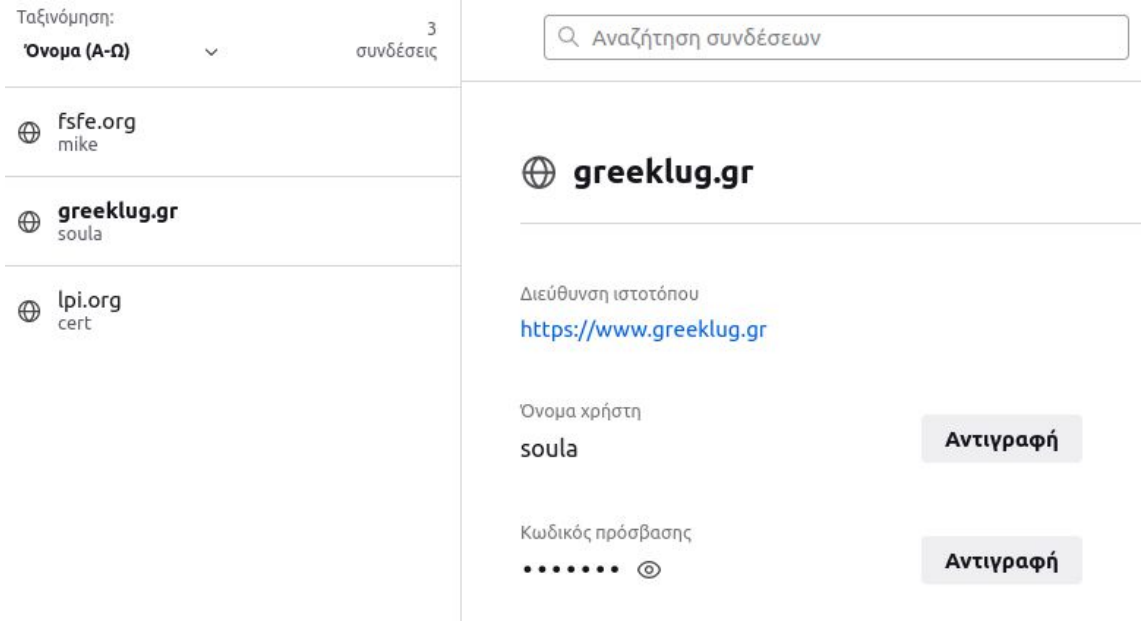
- Η διαχείριση γίνεται αποκλειστικά από την εγκατεστημένη εφαρμογή

Password Managers

Password Managers προσβάσιμοι αποκλειστικά μέσω περιηγητών διαδικτύου:

- Δεν χρειάζεται να εγκατασταθεί κάποιο πρόγραμμα. Η αποθήκευση των κωδικών γίνεται σε μια ιστοσελίδα ή υπηρεσία

- Αυξημένο ρίσκο υποκλοπής των κωδικών σε περίπτωση παραβίασης του server που είναι αποθηκευμένοι



Password Managers

Φυσικές συσκευές που χρησιμεύουν ως κλειδί

- Όχι ακριβώς password manager αλλά περισσότερο “διπλή επαλήθευση”

- Συνήθως είναι μια μικρή συσκευή ή ένα usb stick που παράγει έναν κωδικό στην οθόνη του ή αποτελεί το ίδιο ένα κλειδί για πρόσβαση σε ένα λογαριασμό

- Είναι σχεδόν αδύνατο για κάποιον κακόβουλο χρήστη να αποκτήσει πρόσβαση σε έναν λογαριασμό, χωρίς να έχει στην κατοχή του το κλειδί

- Απώλειά του, σημαίνει ότι δεν μπορούμε και εμείς να μπούμε στον λογαριασμό μας!

Password Managers

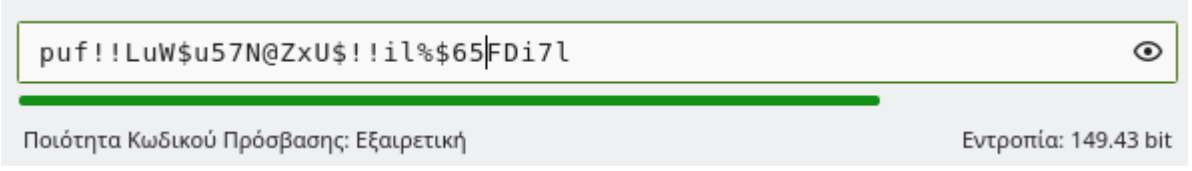
Πρόσθετα χαρακτηριστικά των password managers:

- Κλειδώνεται η εφαρμογή μετά από συγκεκριμένο αριθμό αποτυχημένων προσπαθειών εισόδου, για αποφυγή παραβίασης
- Οι κωδικοί αποθηκεύονται σε μια κρυπτογραφημένη βάση, που απεικονίζεται σε ένα εύχρηστο γραφικό περιβάλλον και είναι ταξινομημένοι σε κατηγορίες για μεγαλύτερη απλούστευση
- Δυνατότητα για αποθήκευση σημειώσεων στοιχεία πιστωτικών καρτών, ταυτότητας κτλ
- Δεν απαιτείται να θυμόμαστε όλους τους κωδικούς, παρά μόνο τον κύριο

Password Managers

Πρόσθετα χαρακτηριστικά των password managers:

- Παράγει **σύνθετους** κωδικούς (γεννήτρια κωδικών) για χρήση σε νέους λογαριασμούς μας και ενημερώνει για την ασφάλεια των παλαιών μας
- Συμπληρώνουν αυτόματα τα συνθηματικά σε ιστοσελίδες, εφαρμογές κτλ, χωρίς να απαιτείται να τους πληκτρολογούμε
- Μειώνεται η πιθανότητα να εισέλθουμε σε κακόβουλη ιστοσελίδα phishing με διαφορετική διεύθυνση από την σωστή, αφού ο password manager δεν θα συμπληρώσει αυτόματα τα στοιχεία



Password Managers

Αδυναμίες και μειονεκτήματα των password managers:

- Ένας χάκερ αν μάθει τον κύριο κωδικό, τότε αποκτά άμεσα πρόσβαση σε όλους τους κωδικούς μας. Αρκετοί password managers υποστηρίζουν 2FA και λύνουν το πρόβλημα

- Κίνδυνος να υποκλαπεί η κρυπτογραφημένη βάση (είτε μέσω παραβίασης του Η/Υ, είτε του server φιλοξενίας της)

Συνθηματικά

Διαχειριστής κωδικών KeePassXC

Το KeePassXC είναι ένα λογισμικό διαχείρισης κωδικών

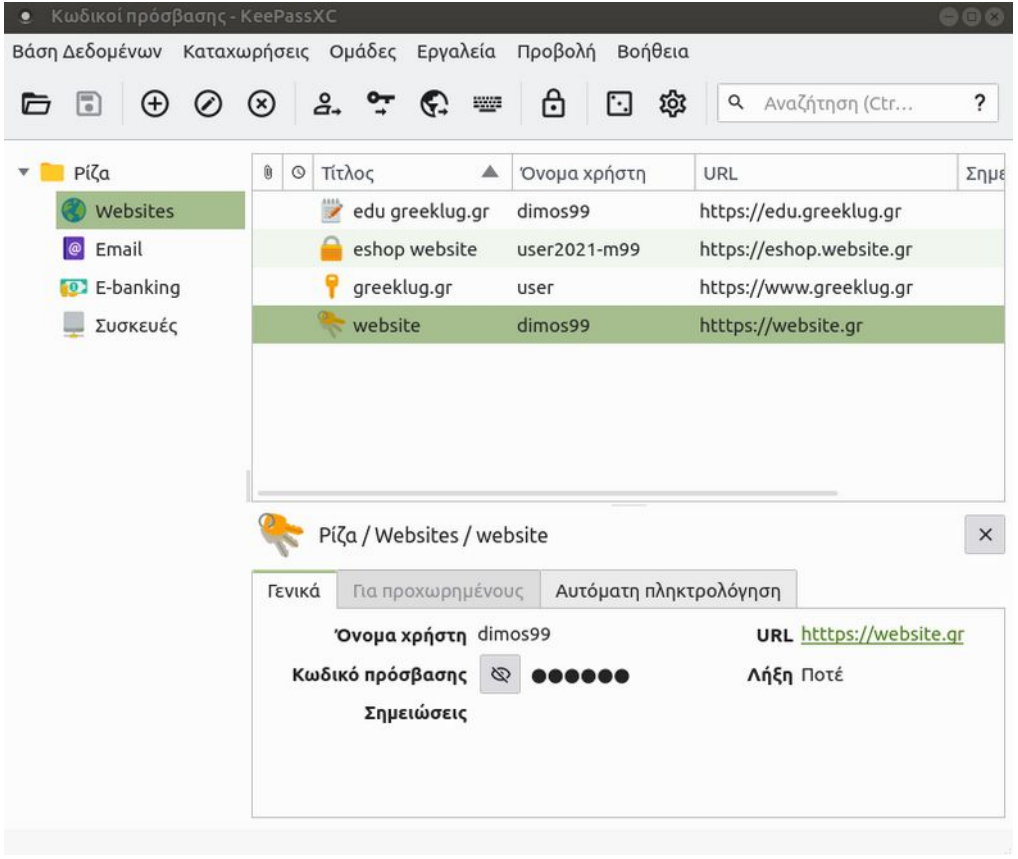
Αποθηκεύει ονόματα χρήστη, κωδικούς πρόσβασης, τομείς, σημειώσεις και πολλά άλλα στοιχεία, σε μια ασφαλή κρυπτογραφημένη βάση δεδομένων, που προστατεύεται από ένα μόνο κύριο κωδικό πρόσβασης ή/και αρχείο κλειδιού.
Η κρυπτογραφημένη βάση δεδομένων αποθηκεύεται σε τοπικό επίπεδο.

Τελευταία έκδοση: v2.7.1, Μάιος 2022

Υποστήριξη για Λ/Σ: Windows, Mac OS, GNU/Linux

Url: https://keepassxc.org/

Συνθηματικά



Ενδεικτικό παράθυρο του λογισμικό διαχείρισης κωδικών KeePassXC

Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Κρυπτογράφηση συσκευών

Κρυπτογράφηση συσκευών

Η **κρυπτογράφηση δεδομένων** διασφαλίζει ότι τα αρχεία αποθηκεύονται πάντα στο δίσκο μίας συσκευής σε κρυπτογραφημένη μορφή.

Τα αρχεία γίνονται διαθέσιμα στο λειτουργικό σύστημα και τις εφαρμογές σε αναγνώσιμη - εγγράψιμη μορφή, μόνο όταν το σύστημα εκτελείται και ξεκλειδώνεται από έναν αξιόπιστο χρήστη.

Ένας μη εξουσιοδοτημένος χρήστης που θα δει τα περιεχόμενα του δίσκου, θα βρει μόνο αλλοιωμένα τυχαία δεδομένα αντί για τα πραγματικά αρχεία.

Κρυπτογράφηση συσκευών

Η **προστασία** που μπορεί να παρέχει η κρυπτογράφηση δεδομένων μπορεί να αποτρέψει τη μη εξουσιοδοτημένη προβολή τους σε περιπτώσεις, όπως η συσκευή μας:

•βρίσκεται σε ένα μέρος στο οποίο ενδέχεται να αποκτήσουν πρόσβαση μη αξιόπιστα άτομα όσο λείπετε
•χαθεί ή κλαπεί, όπως συμβαίνει με φορητούς υπολογιστές, netbook ή εξωτερικές συσκευές αποθήκευσης
•στο συνεργείο επισκευής
•απορρίπτεται μετά το τέλος της ζωής του

Επίσης, μπορεί να χρησιμοποιηθεί για να προσθέσει κάποια ασφάλεια έναντι μη εξουσιοδοτημένων προσπαθειών παραβίασης του λειτουργικού σας συστήματος, για παράδειγμα, την εγκατάσταση keyloggers ή δούρειων ίππων από εισβολείς που μπορούν να αποκτήσουν φυσική πρόσβαση στο σύστημα ενώ είστε μακριά.

Προειδοποίηση: Η κρυπτογράφηση δεδομένων δεν προστατεύει τα δεδομένα σας από όλες τις απειλές.

Κρυπτογράφηση συσκευών

Η προστασία που **δεν** μπορεί να παρέχει η κρυπτογράφηση δεδομένων αφορά περιπτώσεις όπως:

•Επιτιθέμενοι μπορούν να παραβιάσουν το σύστημά σας (π.χ. μέσω διαδικτύου) ενώ εκτελείται και αφού έχετε ήδη ξεκλειδώσει και προσαρτήσει τα κρυπτογραφημένα μέρη του δίσκου.
•Επιτιθέμενοι μπορούν να αποκτήσουν φυσική πρόσβαση στην συσκευή ενώ εκτελείται (ακόμα και αν χρησιμοποιείτε κλείδωμα οθόνης) ή πολύ σύντομα μετά την εκκίνησή της, και να εκτελέσουν μια επίθεση ψυχρής εκκίνησης (Cold boot attack).
•Κάποιος κακόβουλος χρήστης μπορεί επίσης απλώς να σας αναγκάσει να παραδώσετε τα κλειδιά/φράσεις πρόσβασης χρησιμοποιώντας διάφορες τεχνικές εξαναγκασμού.

Απαιτείται μια πολύ ισχυρή ρύθμιση κρυπτογράφησης δίσκου (π.χ. πλήρης κρυπτογράφηση συστήματος με έλεγχο γνησιότητας και χωρίς διαμέρισμα εκκίνησης απλού κειμένου) για να έχετε μια ευκαιρία ενάντια σε επαγγελματίες εισβολείς που είναι σε θέση να παραβιάσουν το σύστημά σας προτού το χρησιμοποιήσετε. Και ακόμη και τότε δεν μπορεί να αποτρέψει όλους τους τύπους παραβίασης (π.χ. keyloggers υλικού).

Κρυπτογράφηση συσκευών

Η **κρυπτογράφηση συσκευής** που συναντάμε σε Η/Υ αποτελεί μια λειτουργία με βάση την οποία τα δεδομένα μας αποθηκεύονται κρυπτογραφημένα σε μια συσκευή μπλοκ, διαμέρισμα δίσκου (partition) ή φάκελο αρχείων.

Παραδείγματα συσκευών μπλοκ είναι οι σκληροί δίσκοι, τα usb flash και τα CD/DVD.

Αποτελεί πρόσθετο χαρακτηριστικό στους υπάρχοντες μηχανισμούς ασφαλείας ενός λειτουργικού συστήματος, το οποίο επικεντρώνεται στην εξασφάλιση των δεδομένων σε επίπεδο φυσικής πρόσβασης.

Συνεχίσει ωστόσο να βασίζεται σε άλλα μέρη του συστήματος για την παροχή στοιχείων, όπως η ασφάλεια δικτύου και ο έλεγχος πρόσβασης/δικαιώματα χρήστη.

Πάνω σε αυτή στηρίζεται και η πλήρης κρυπτογράφηση δίσκου (FDE) που αφορά την κρυπτογράφηση ολόκληρου του συστήματος.

Κρυπτογράφηση συσκευών

MS Windows | κρυπτογράφηση BitLocker

Η κρυπτογράφηση BitLocker είναι διαθέσιμη σε υποστηριζόμενες συσκευές με Windows 10 ή 11 Pro, Enterprise ή Education.

Σε υποστηριζόμενες συσκευές, το BitLocker θα ενεργοποιηθεί αυτόματα την πρώτη φορά που συνδέεστε σε έναν προσωπικό λογαριασμό Microsoft (όπως @outlook.com ή @hotmail.com) ή στον λογαριασμό εργασίας ή σχολείου.

Το BitLocker δεν ενεργοποιείται αυτόματα με τοπικούς λογαριασμούς, ωστόσο μπορείτε να το ενεργοποιήσετε μη αυτόματα στο εργαλείο Διαχείριση BitLocker.

https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

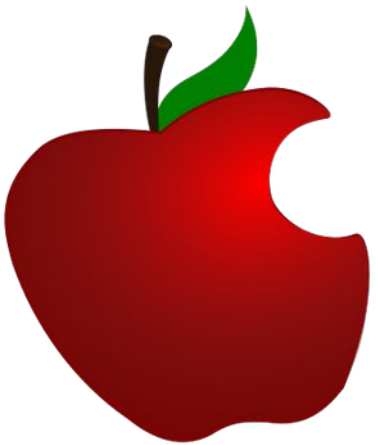
Κρυπτογράφηση συσκευών

Mac | κρυπτογράφηση FileVault

Η κρυπτογράφηση FileVault είναι διαθέσιμη σε υποστηριζόμενες συσκευές με Mac OS X 10.7 Lion ή νεότερες.

Σημείωση: Αν διαθέτετε iMac Pro ή άλλο Mac με chip ασφαλείας T2 Apple, τα δεδομένα στον δίσκο σας κρυπτογραφούνται ήδη αυτόματα. Ωστόσο, η ενεργοποίηση του FileVault παρέχει επιπλέον προστασία ζητώντας το συνθηματικό εισόδου σας για αποκρυπτογράφηση των δεδομένων.

https://support.apple.com/en-us/HT204837



Κρυπτογράφηση συσκευών

Ανάγκη για ασφάλεια

- Κωδικοί και δεδομένα
- Αρχεία και φάκελοι

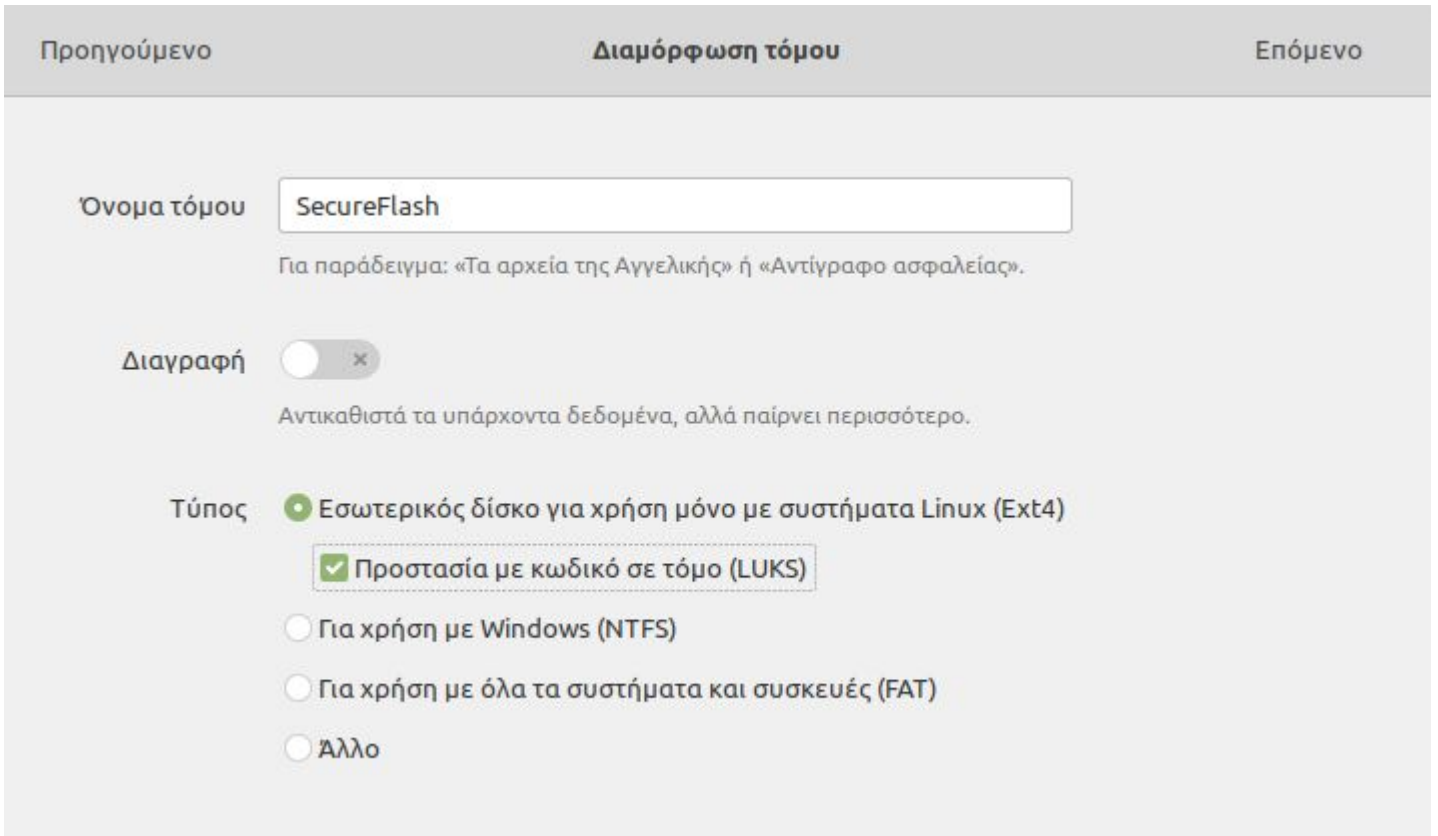
ΣΥΣΤΗΜΑ ΑΡΧΕΙΩΝ

- Τμήμα του συστήματος
- Όλο το σύστημα

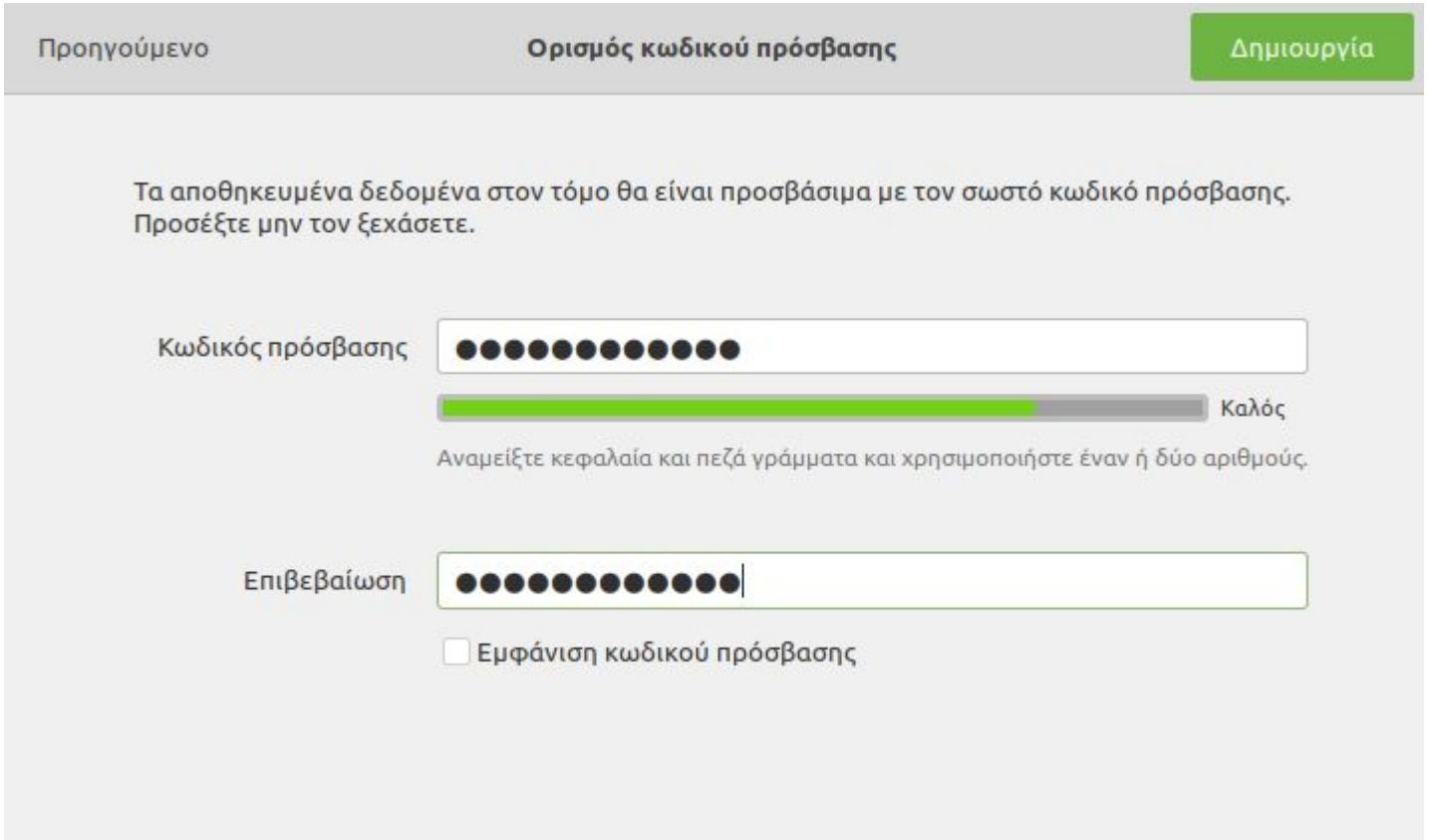
ΣΥΣΚΕΥΕΣ		ΑΡΧΕΙΑ	
Loop-AES	dm-crypt +/- LUKS	eCryptfs	EncFs

https://wiki.archlinux.org/index.php/Disk_encryption

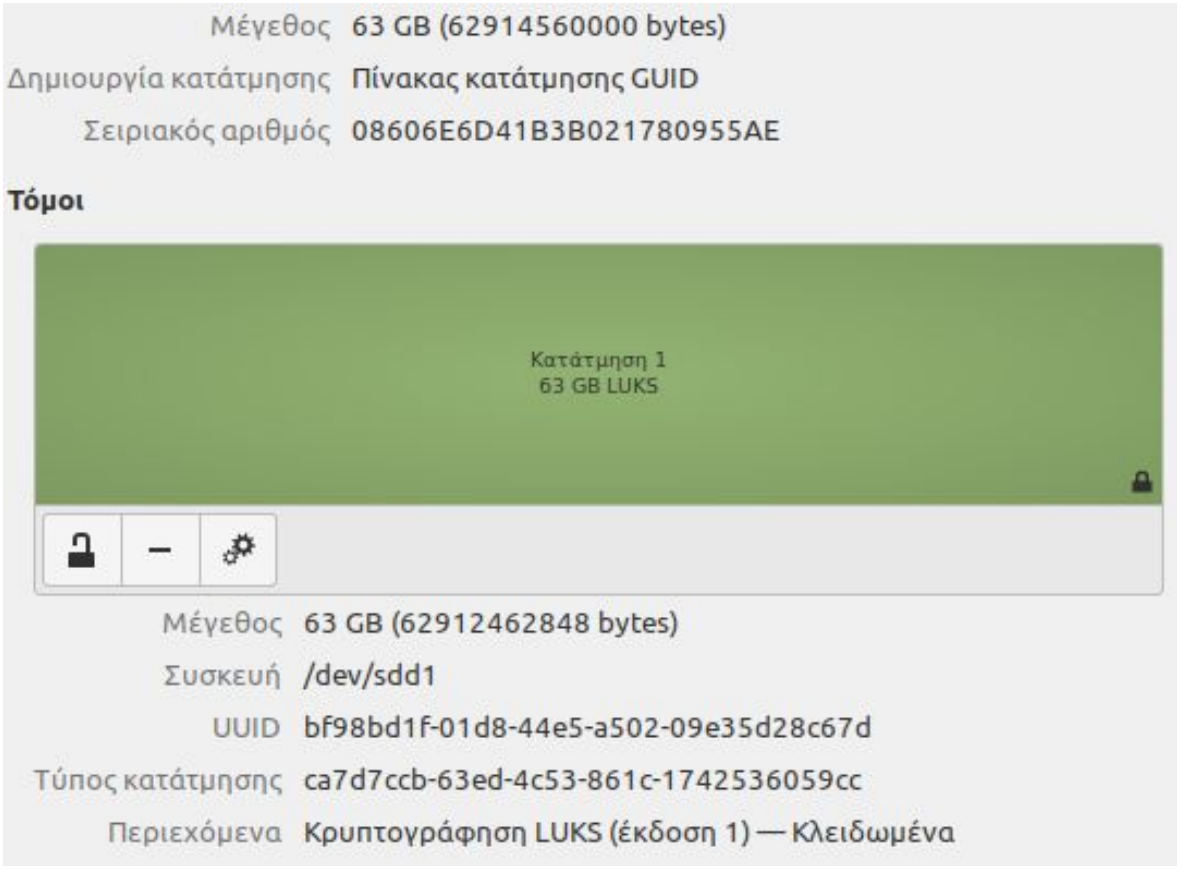
Κρυπτογράφηση συσκευών



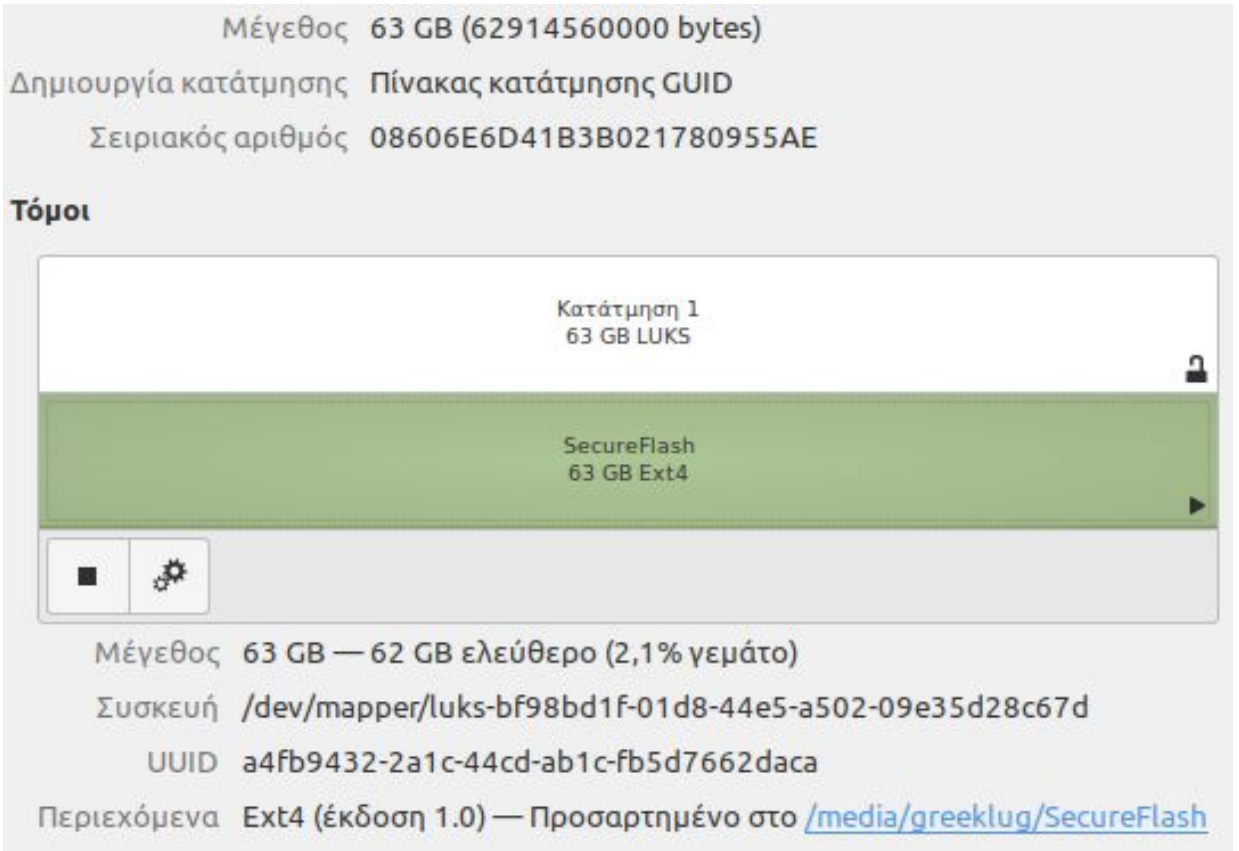
Κρυπτογράφηση συσκευών



Κρυπτογράφηση συσκευών



Κρυπτογράφηση συσκευών



Κρυπτογράφηση συσκευών

Κρυπτογράφηση: GEncfsM

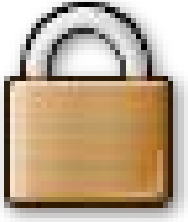
Το Gnome Encfs Manager (GEncfsM) είναι μια δωρεάν και ανοικτού κώδικα εφαρμογή διαχείρισης κρυπτογραφημένων φακέλων που στηρίζεται στο σύστημα EncFS.

Παρέχει την δυνατότητα δημιουργίας κρυπτογραφημένων φακέλων ή συσκευών, τα οποία προστατεύονται με έναν κωδικό-κλειδί.
Μέσω της προσάρτησης ενεργοποιούμε την πρόσβαση στο κρυπτογραφημένο φάκελο όπου μπορούμε να μεταφέρουμε ή να διαχειριστούμε τα δεδομένα μας.

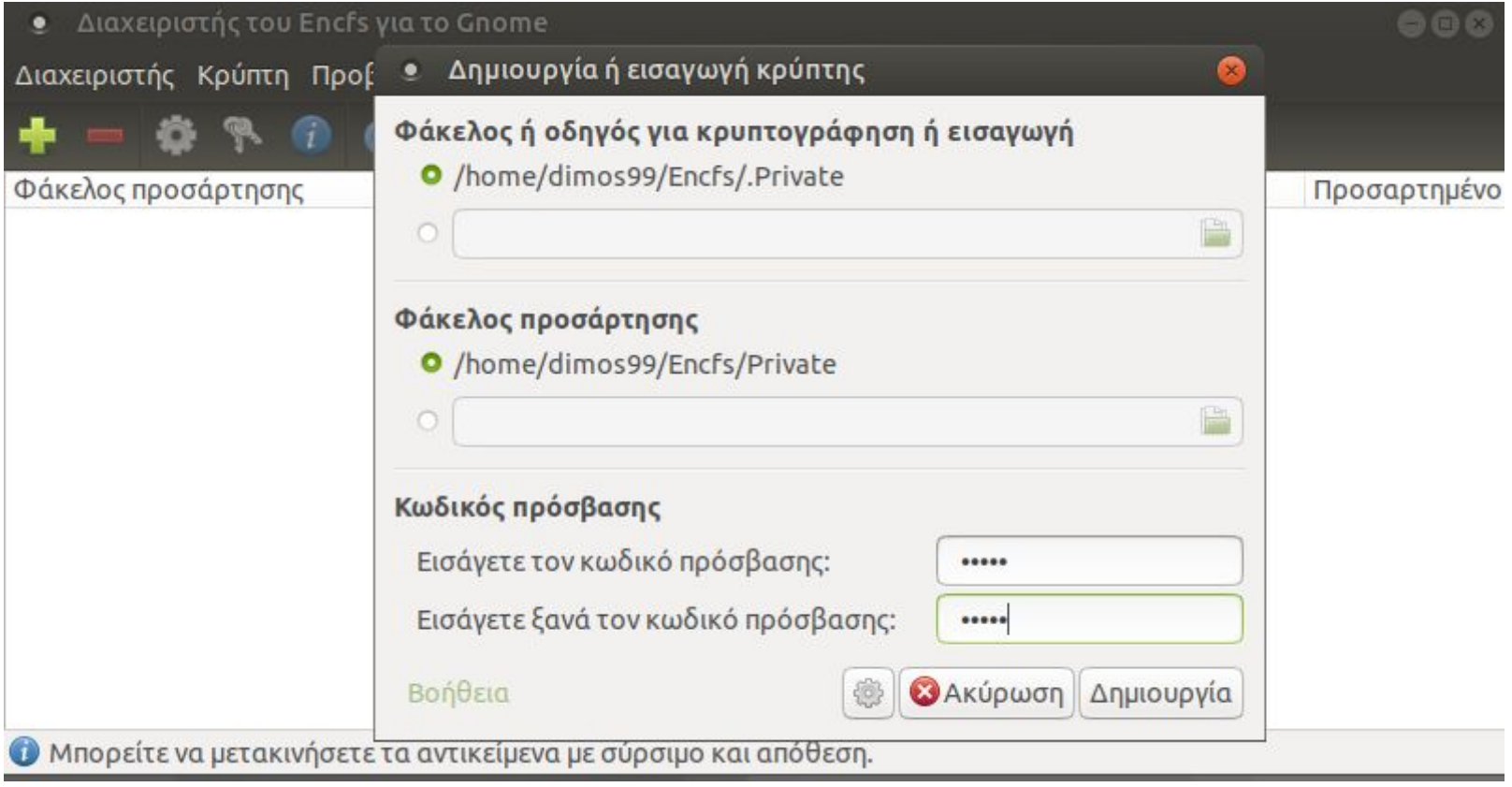
Τελευταία έκδοση: v1.9

Υποστήριξη για Λ/Σ: GNU/Linux

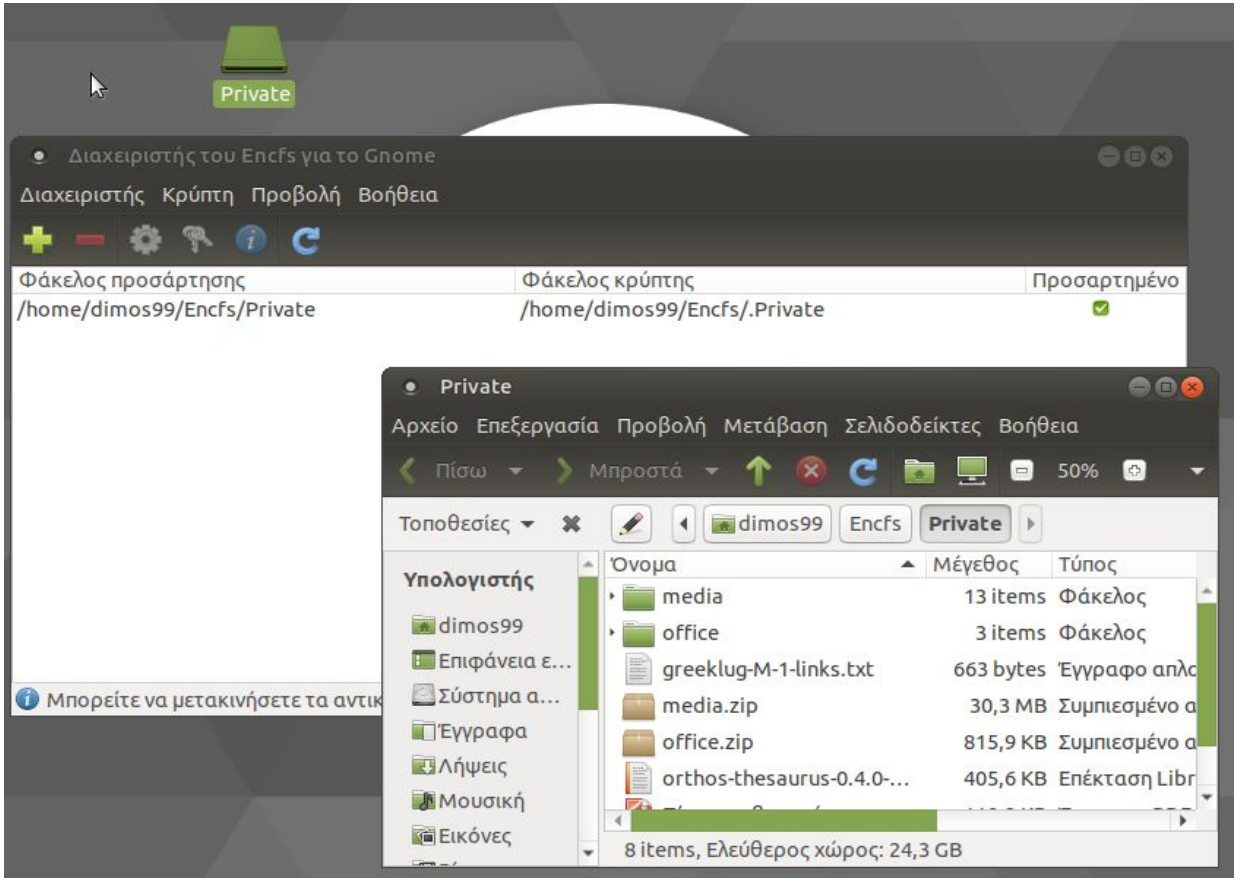
Url: https://moritzmolch.com/apps/gencfsm.html



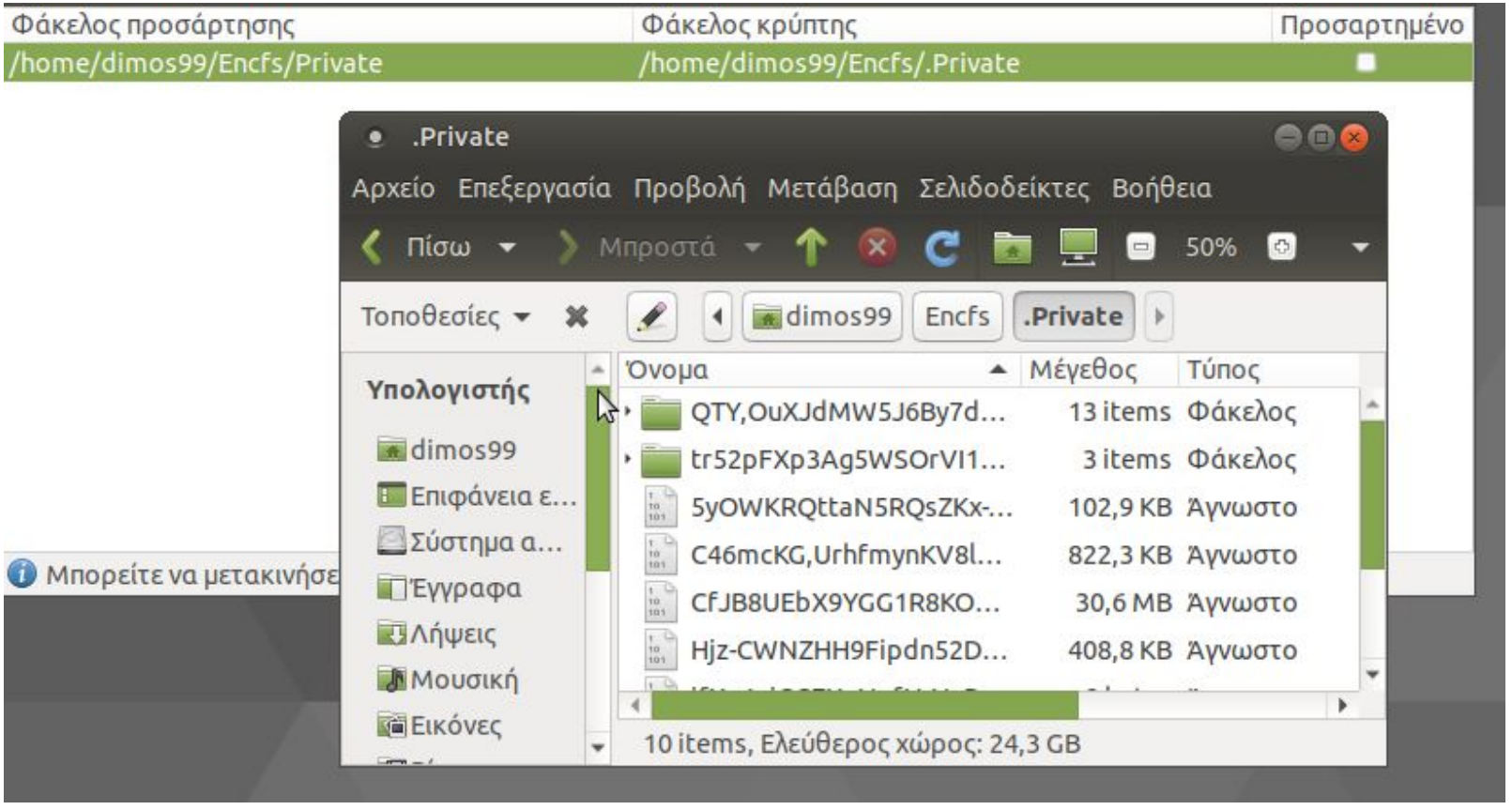
Κρυπτογράφηση συσκευών



Κρυπτογράφηση συσκευών



Κρυπτογράφηση συσκευών



Κρυπτογράφηση συσκευών

Android | κρυπτογράφηση

Το Android 5.0 έως 9.0 υποστηρίζει την πλήρη κρυπτογράφηση δίσκου (dm-crypt). Από την έκδοση 10.0 η λειτουργία δεν παρέχεται πλέον αλλά μόνο η κρυπτογράφηση αρχείων (FBE).

Ο επίσημος λόγος κατάργησης του παραπάνω, παρόλο που είναι εξαιρετικό για την ασφάλεια, στηρίζεται ότι οι περισσότερες από τις βασικές λειτουργίες του τηλεφώνου δεν είναι άμεσα διαθέσιμες όταν οι χρήστες επανεκκινούν τη συσκευή τους. Επειδή η πρόσβαση στα δεδομένα τους προστατεύεται πίσω από τα διαπιστευτήρια ενός χρήστη, λειτουργίες όπως οι συναγερμοί δεν μπορούσαν να λειτουργήσουν, οι υπηρεσίες προσβασιμότητας δεν ήταν διαθέσιμες και τα τηλέφωνα δεν μπορούσαν να δέχονται κλήσεις.

Η κρυπτογράφηση αρχείων (FBE) υποστηρίζεται από την έκδοση 7.0 και είναι προαπαιτούμενη για συσκευές με Android 10.0 ή νεότερο.

https://source.android.com/security/encryption

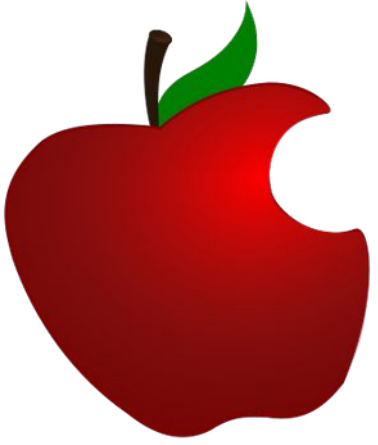
Κρυπτογράφηση συσκευών

iOS και iPadOS | κρυπτογράφηση Data Protection
Δεν υποστηρίζει κάποια τεχνολογία για πλήρη κρυπτογράφηση δίσκου.

Τα προσωπικά δεδομένα στα τηλέφωνα και συσκευές Apple κρυπτογραφούνται από προεπιλογή με την λειτουργία κρυπτογράφησης αρχείων Data Protection (AES).

Κάθε φορά που η συσκευή κλειδώνεται με κωδικό πρόσβασης ή Touch ID, γίνεται κρυπτογράφηση των κλειδιών και συνεπαγωγικά τα δεδομένα προστατεύονται από άμεση πρόσβαση.

https://support.apple.com/el-gr/guide/security/sece3bee0835/web



Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση επικοινωνίας

Η **κρυπτογράφηση επικοινωνίας** διασφαλίζει ότι τα δεδομένα που ανταλλάσουμε με τρίτους μεταφέρονται μέσω **ασφαλών καναλιών επικοινωνίας** (κρυπτογράφηση σύνδεσης) ή και σε **κρυπτογραφημένη μορφή** (κρυπτογράφηση μηνυμάτων).

Στο παρελθόν η επικοινωνία μέσω διαδικτύου γίνονταν συνήθως χωρίς κρυπτογράφηση, ωστόσο με τις νεότερες τεχνολογίες παρακολούθησης/δυνατοτήτων παραβίασης, υπήρξαν πολλαπλές υποθέσεις παραβίασης.

Ενδεικτικό παράδειγμα ήταν η πλοήγηση στο διαδίκτυο, η οποία πραγματοποιούνταν μέσω του πρωτοκόλλου HTTP (πόρτα 80). Η πρόσβαση σε ιστοσελίδες, ειδικά σε αυτές που υπήρχε σύνδεση χρηστών με όνομα χρήστη και κωδικό, μπορούσε να αναγνωστεί με διάφορες τεχνικές, με αποτέλεσμα κακόβουλοι χρήστες να μπορούν να πάρουν πρόσβαση σε λογαριασμούς ή και να καταγράψουν ευαίσθητα δεδομένα, όπως στοιχεία πιστωτικών καρτών.

Το παραπάνω ισχύει και για όλα τα γνωστά πρωτόκολλα επικοινωνίας, όπως το FTP για την μεταφορά αρχείων, τα IMAP/POP3/SMTP για την αποστολή και παραλαβή αλληλογραφίας κ.α.

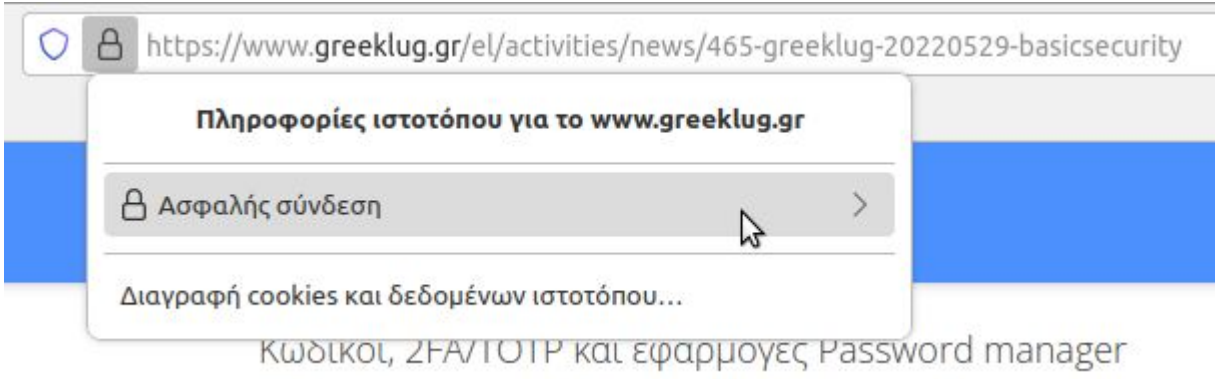
Κρυπτογράφηση επικοινωνίας

Για την εξασφάλιση της επικοινωνίας τα πρωτόκολλα υποστηρίζουν την χρήση κρυπτογράφησης.

Αυτή αναφέρεται συνήθως ως Secure Sockets Layer (**SSL**) ή Transport Layer Security (**TLS**).

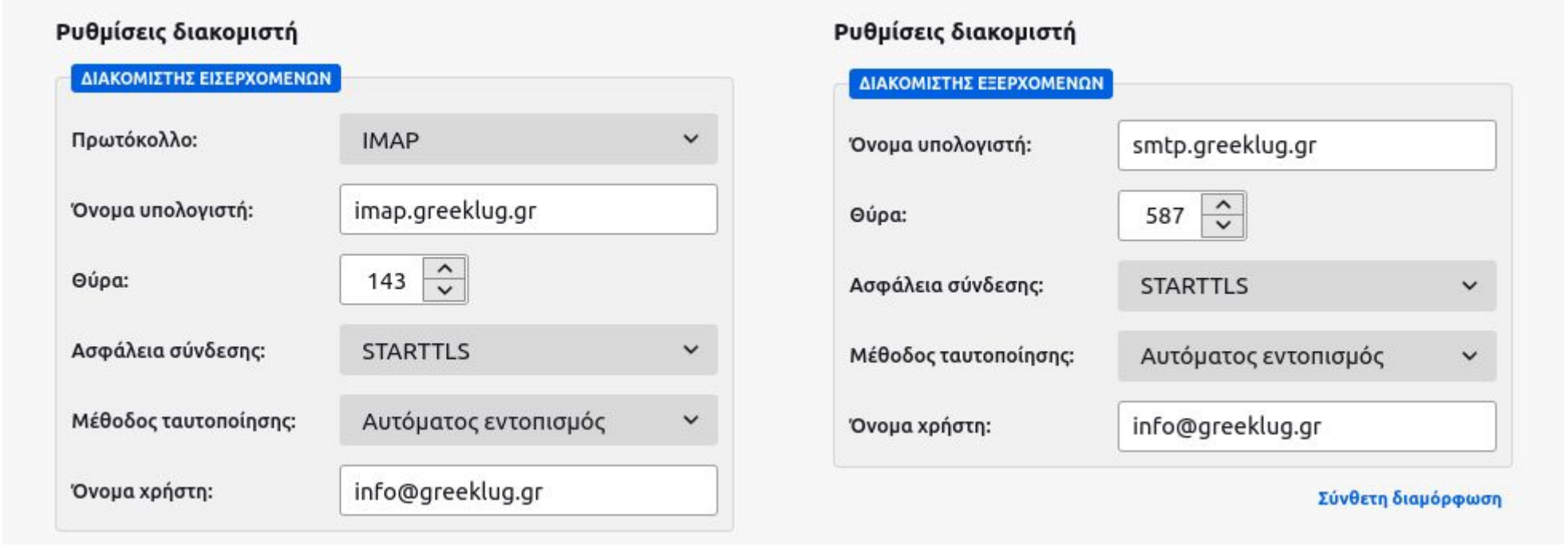
Με βάση το παραπάνω για την πλοήγηση σε ιστοσελίδες χρησιμοποιούμε πλέον το πρωτόκολλο **HTTPS** (πόρτα 443).

Αντίστοιχα στην μεταφορά αρχείων FTP υπάρχει πλέον το **FTPS** (FTP με χρήση SSL/TLS), αλλά και στην αλληλογραφία τα IMAP/POP3/SMTP υποστηρίζουν την χρήση SSL ή TLS κ.α.



Κρυπτογράφηση επικοινωνίας

Ενδεικτικές ρυθμίσεις αλληλογραφίας στην εφαρμογή Thunderbird:



Κρυπτογράφηση επικοινωνίας

Πρωτόκολλο	**Χωρίς** κρυπτογράφηση	**Με** κρυπτογράφηση **SSL/TLS**
Web/Ιστοσελίδες	HTTP (80)	HTTPS (443)
Email	IMAP (143) | POP3 (110) SMTP (25)	IMAP (143) | POP3 (110) SMTP (587)
Μεταφορά αρχείων	FTP (21)	FTPS (21)
Απομακρυσμένη εκτέλεση εντολών/μεταφορά δεδομένων	--	SSH/SFTP (22)

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης

Χρήστης Α

Μη κρυπτογραφημένη Επικοινωνία

Κείμενο

Χρήστης Β

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης

Χρήστης Α

Μη κρυπτογραφημένη Επικοινωνία

Κείμενο

Χρήστης Β

Χρήστης Α

Κρυπτογραφημένη Επικοινωνία με SSL/TLS

Κείμενο

Χρήστης Β

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση μηνυμάτων με την μέθοδο δημοσίου κλειδιού
Κάθε χρήστης έχει το δικό του κλειδί, που αποτελείται από δύο τμήματα:
•ένα **ιδιωτικό**
•ένα **δημόσιο**

Σημεία κρυπτογράφησης:
•Κείμενο
•Υπογραφή

Κείμενο
Παρουσίαση Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα - 29/05/2022

Κείμενο με κρυπτογράφηση
-----BEGIN PGP MESSAGE-----
wcFMA0JrV2MGhiq6AQ9G0hd4Af2nFDsUNuMhDQw2lstu3JZdSqk0lQ8NvwRuMYeYG9ZtF8dpSqLy
DePuP6OhguL6gK+vGmrCuC6FFTy1EYovEB4qPc1IntcrBInDvTu7vy7wXsE+wp8Hpy2YGsHp3...
-----END PGP MESSAGE-----

Κρυπτογράφηση επικοινωνίας

Βήματα κρυπτογράφησης δημοσίου κλειδιού

•Ο **Χρήστης Α** θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον **Χρήστη Β**
•Ο **Χρήστης Α** κρυπτογραφεί το απλό κείμενο με το δημόσιο κλειδί του **Χρήστη Β** και στέλνει το μήνυμα
•Ο **Χρήστης Β** λαμβάνει το μήνυμα και αποκρυπτογραφεί το κωδικοποιημένο κείμενο με το ιδιωτικό κλειδί του
•Τρίτοι χρήστες βλέπουν μόνο το **κωδικοποιημένο** κείμενο

Σημαντικό
Το ιδιωτικό κλειδί παραμένει στον εκάστοτε χρήστη και δεν διαμοιράζεται

* Ο **Χρήστης Α** θα πρέπει να γνωρίζει το δημόσιο κλειδί του **Χρήστη Β** για να μπορέσει να επικοινωνήσει μαζί του

Κρυπτογράφηση επικοινωνίας

Βήματα ψηφιακής υπογραφής δημοσίου κλειδιού

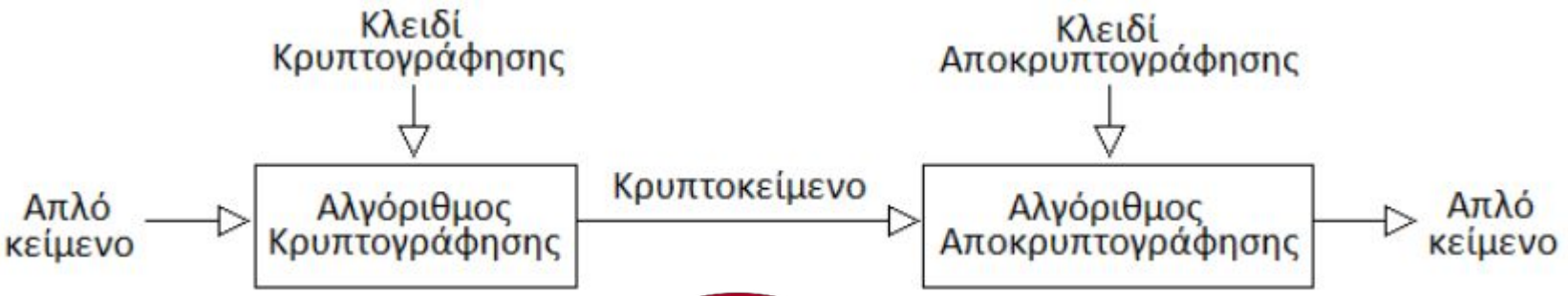
•Ο **Χρήστης Α** θέλει να στείλει ένα μήνυμα, ψηφιακά υπογεγραμμένο, στον **Χρήστη Β**
•Ο **Χρήστης Α** υπογράφει το μήνυμα με το ιδιωτικό κλειδί του και στέλνει το μήνυμα
•Ο **Χρήστης Β** λαμβάνει το μήνυμα και χρησιμοποιεί το δημόσιο κλειδί του **Χρήστη Α** για να επιβεβαιώσει ότι το μήνυμα στάλθηκε από αυτόν

Σημαντικό
Η υπογραφή εξαρτάται από το περιεχόμενο του μηνύματος. Εάν αυτό τροποποιηθεί τότε η εγκυρότητα της υπογραφής δεν ισχύει

* Ο **Χρήστης Β** θα πρέπει να γνωρίζει το δημόσιο κλειδί του **Χρήστη Α** για να μπορέσει να επιβεβαιώσει την εγκυρότητα του μηνύματος

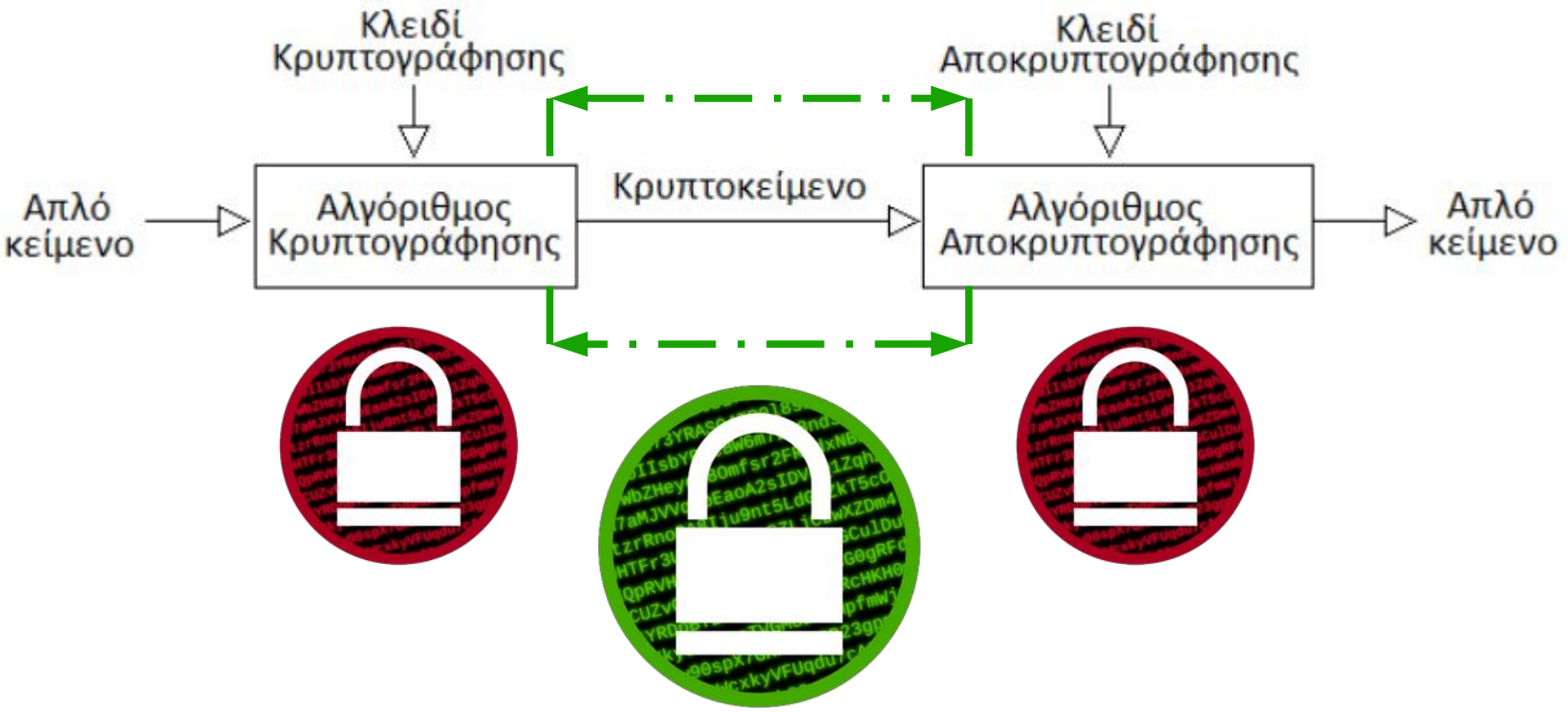
Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Μηνυμάτων



Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης
Κρυπτογράφηση Μηνυμάτων



Κρυπτογράφηση επικοινωνίας

Η εφαρμογή αλληλογραφίας **Mozilla Thunderbird** έχει την δυνατότητα χρήσης της κρυπτογράφησης **OpenPGP**.

Μέσω αυτής το Thunderbird μπορεί να κρυπτογραφεί, αποκρυπτογραφεί και να υπογράφει ψηφιακά μηνύματα.

Δημιουργεί επίσης και διαχειρίζεται τα δημόσια και ιδιωτικά κλειδιά που απαιτούνται για το σκοπό αυτό.

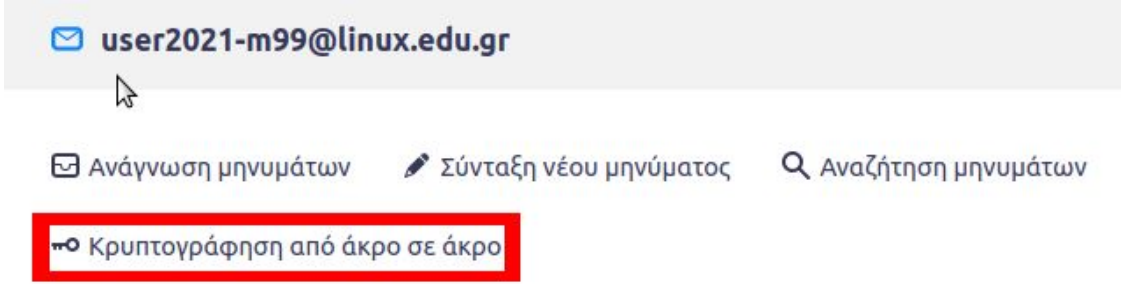
Η λειτουργία και σχετικές ρυθμίσεις παρέχονται από την επιλογή “Κρυπτογράφηση από άκρο σε άκρο”.

https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq

Thunderbird & OpenPGP

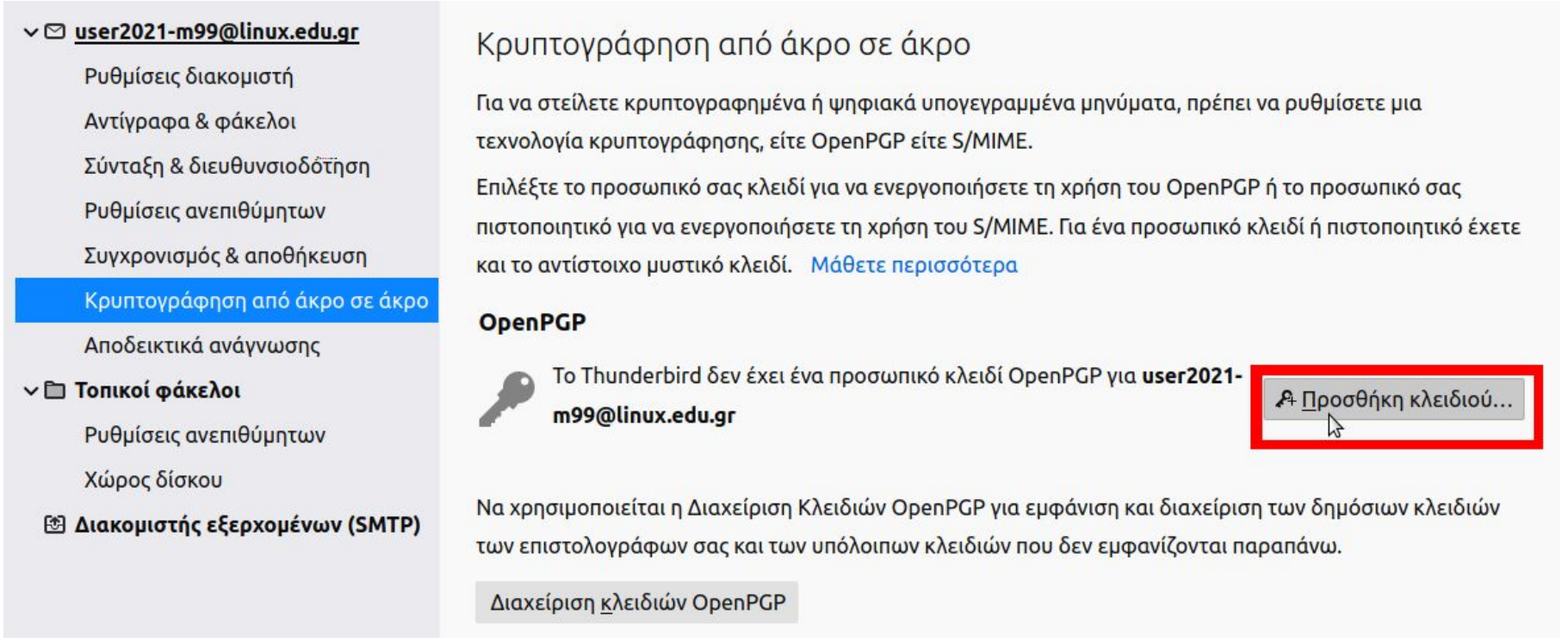
Κρυπτογράφηση επικοινωνίας

Αρχικά δημιουργούμε το δικό μας κλειδί OpenPGP που στηρίζεται στο μοντέλο δημόσιου κλειδιού (περιλαμβάνει δύο μέρη, το ιδιωτικό και το δημόσιο κλειδί).

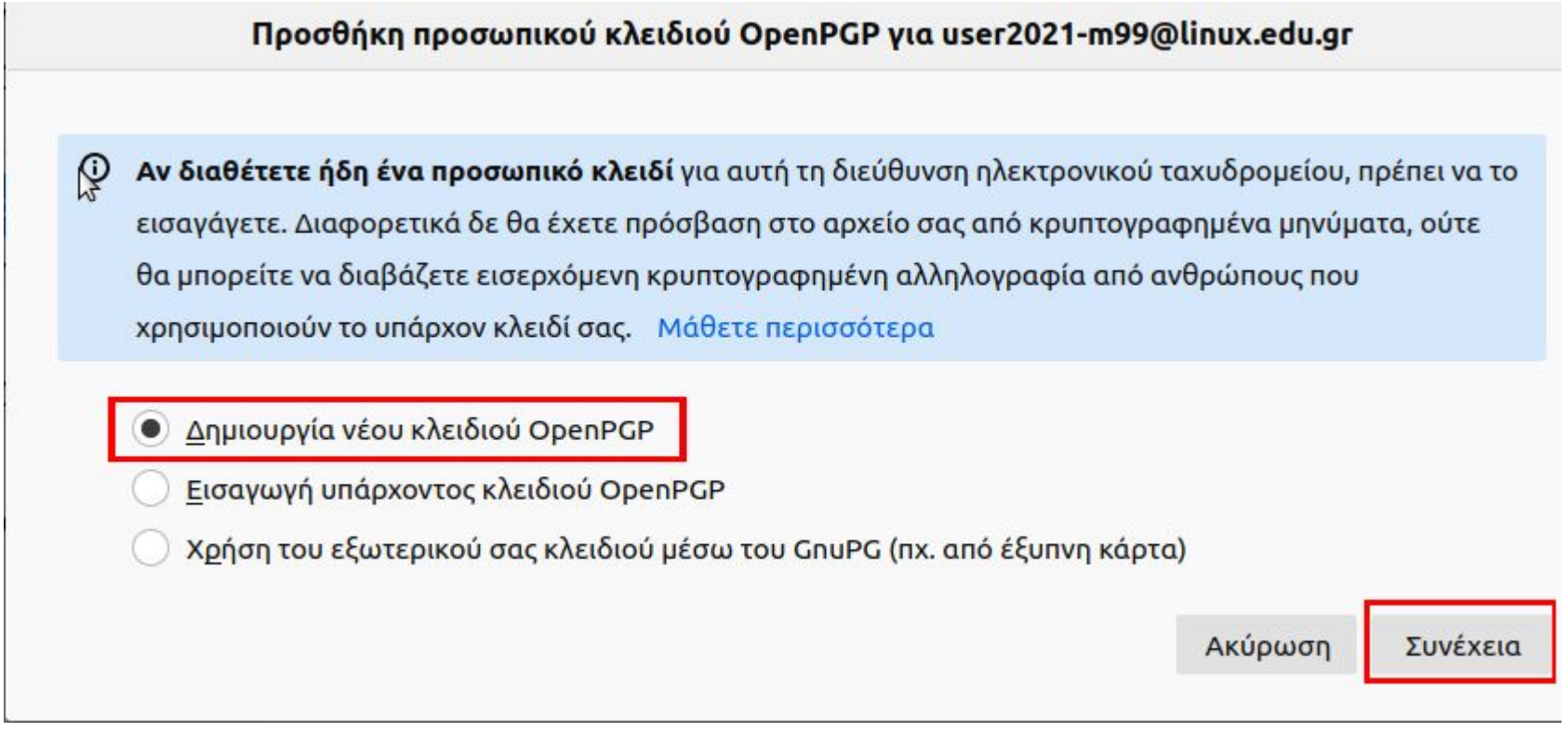


Κρυπτογράφηση επικοινωνίας

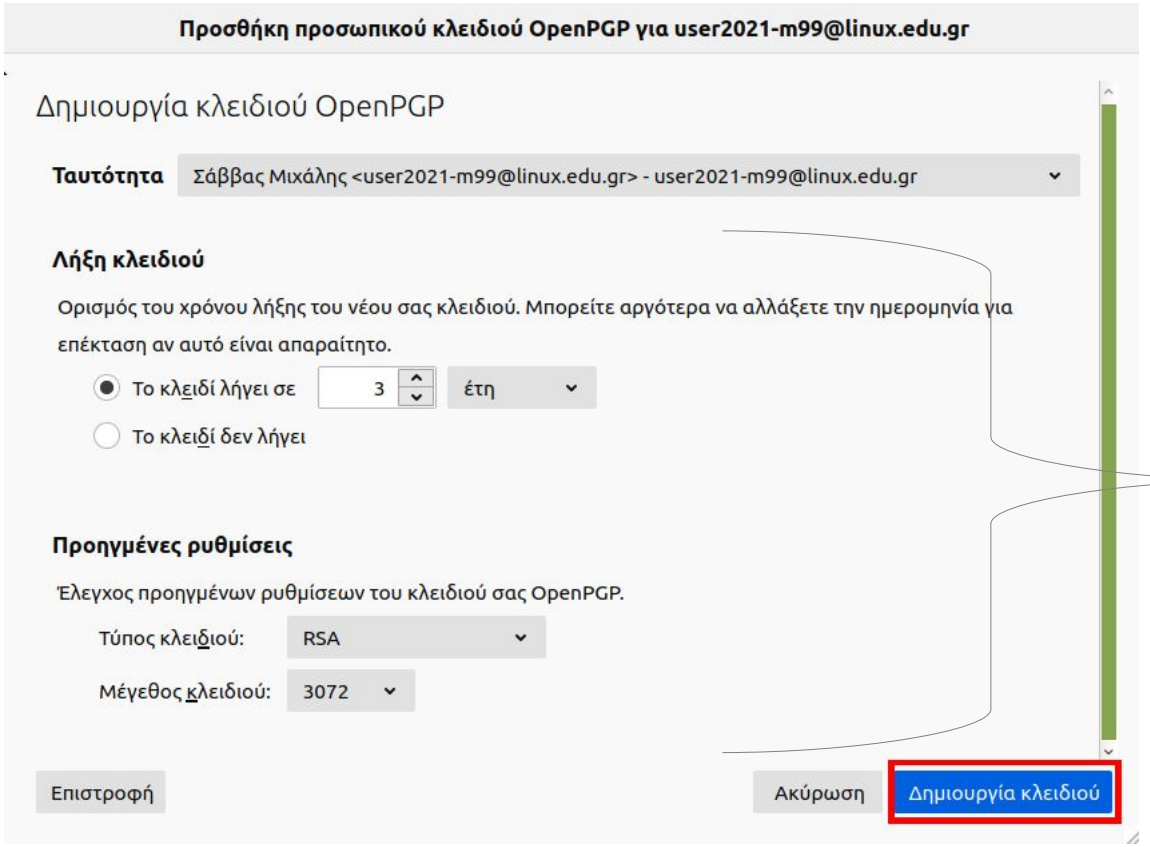
Αρχικά δημιουργούμε το δικό μας κλειδί OpenPGP που στηρίζεται στο μοντέλο δημόσιου κλειδιού (περιλαμβάνει δύο μέρη, το ιδιωτικό και το δημόσιο κλειδί).



Κρυπτογράφηση επικοινωνίας

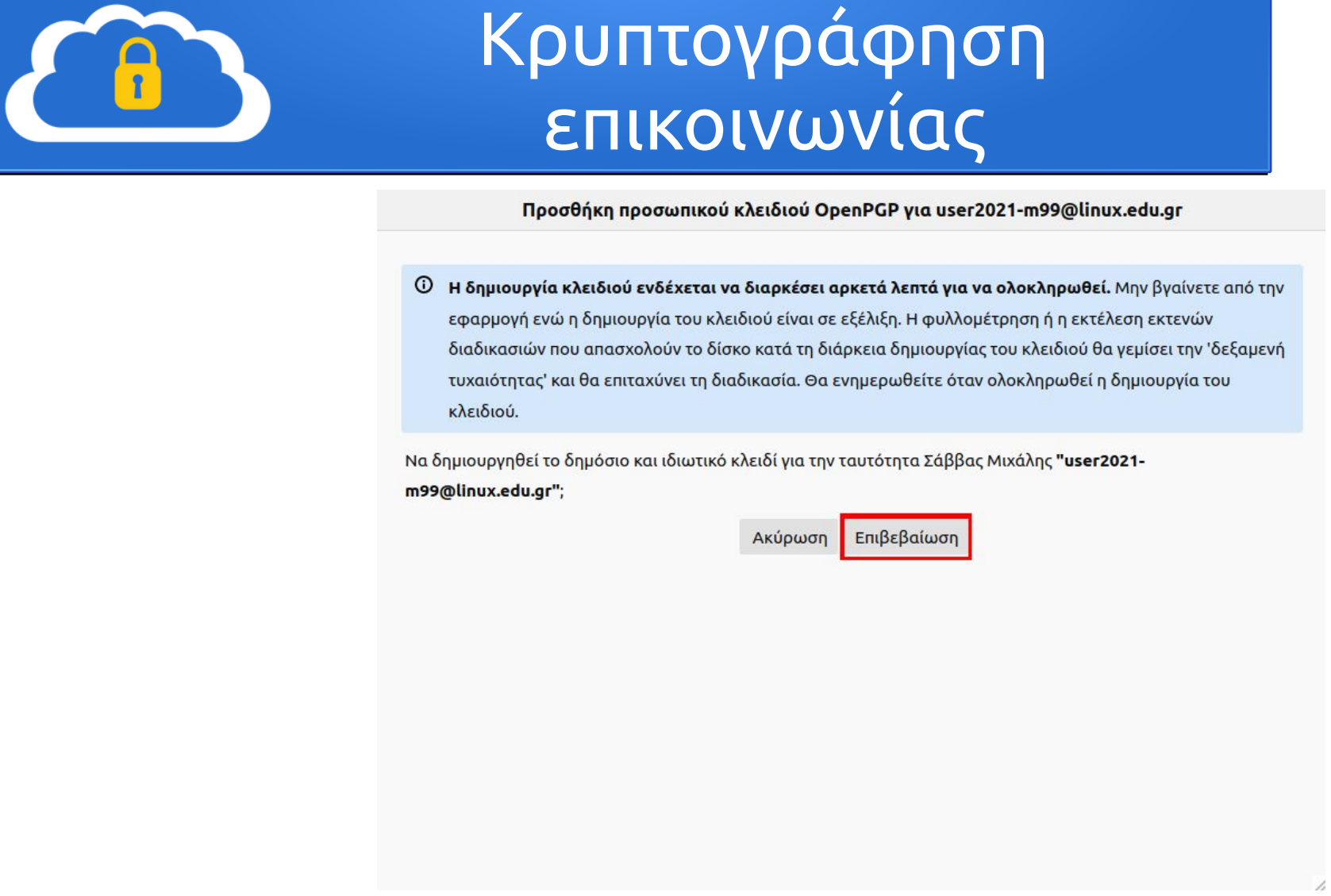


Κρυπτογράφηση επικοινωνίας

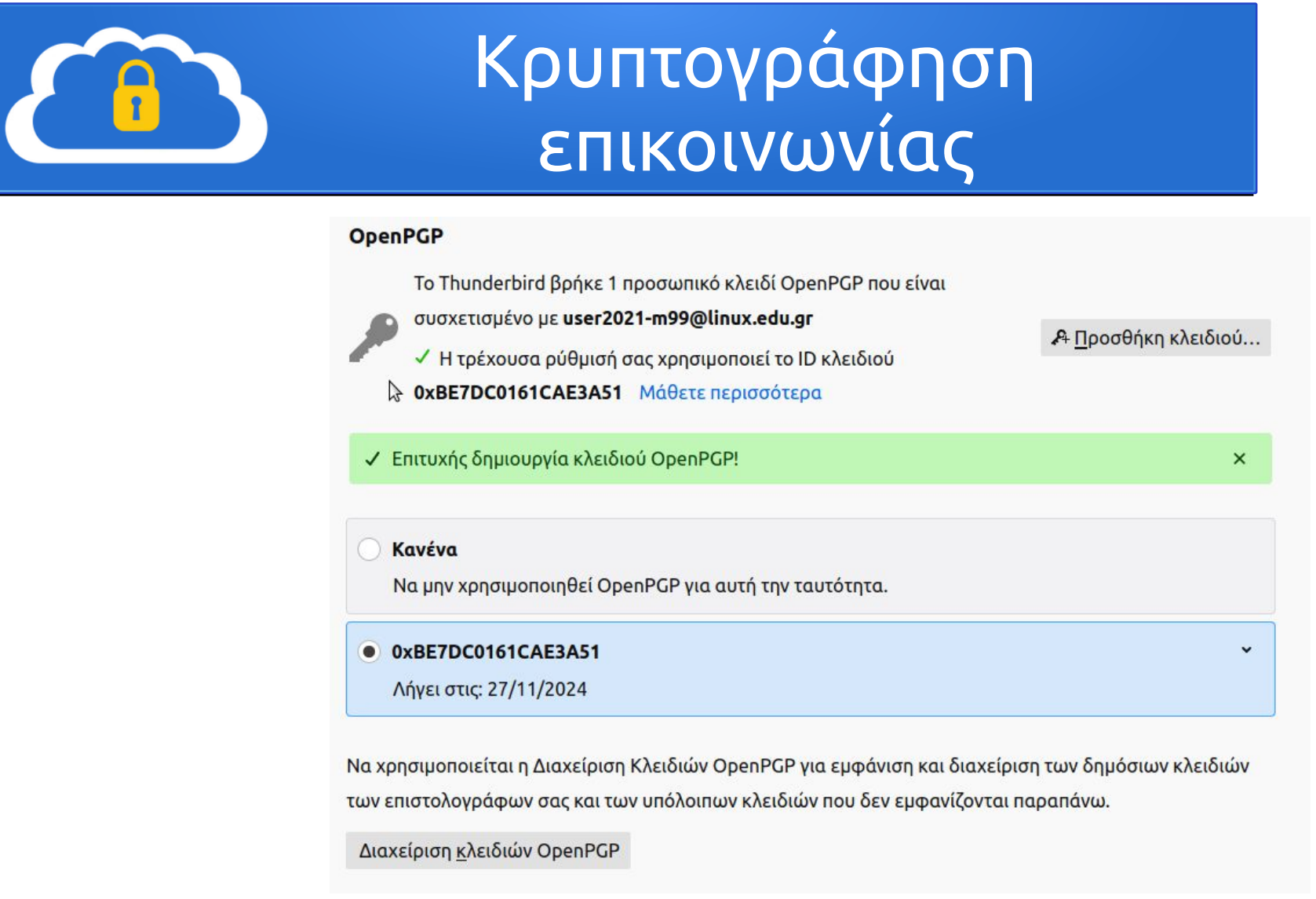


Δυνατότητα επιλογής διάρκειας & τύπου κρυπτογράφησης

Κρυπτογράφηση επικοινωνίας



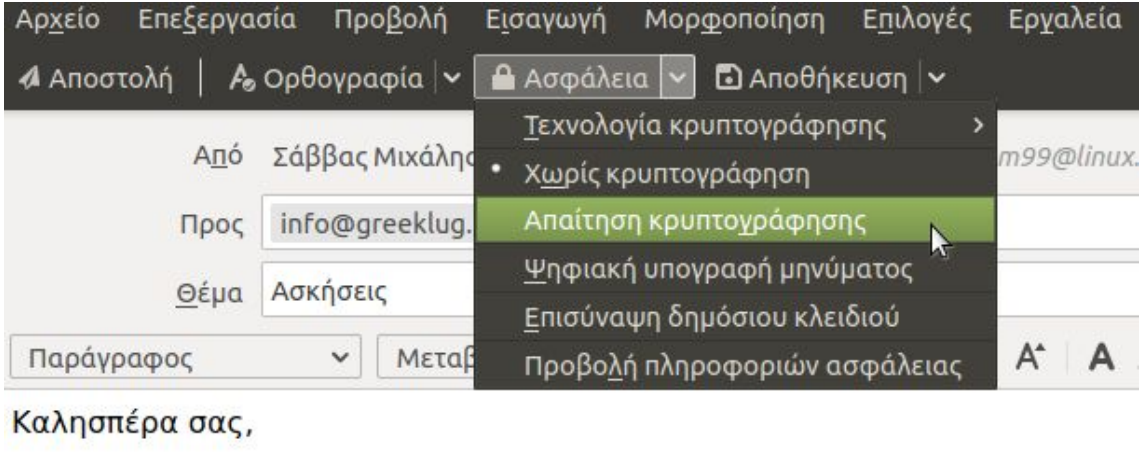
Κρυπτογράφηση επικοινωνίας



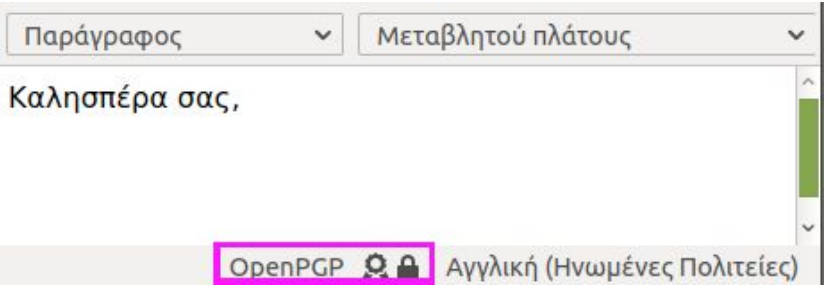
Κρυπτογράφηση επικοινωνίας

Κατά την σύνταξη ενός μηνύματος, μπορούμε να επιλέξουμε:
•“Απαίτηση κρυπτογράφησης”, ώστε το μήνυμά μας να κρυπτογραφηθεί
•“Ψηφιακή υπογραφή μηνύματος”, ώστε να υπογράψουμε το μήνυμα (το περιεχόμενο του μηνύματος δεν κρυπτογραφείται)

Επίσης έχουμε την δυνατότητα να επισυνάψουμε το δημόσιο κλειδί μας, εφόσον ο παραλήπτης δεν το διαθέτει, πχ είναι η πρώτη φορά επικοινωνίας μαζί του.

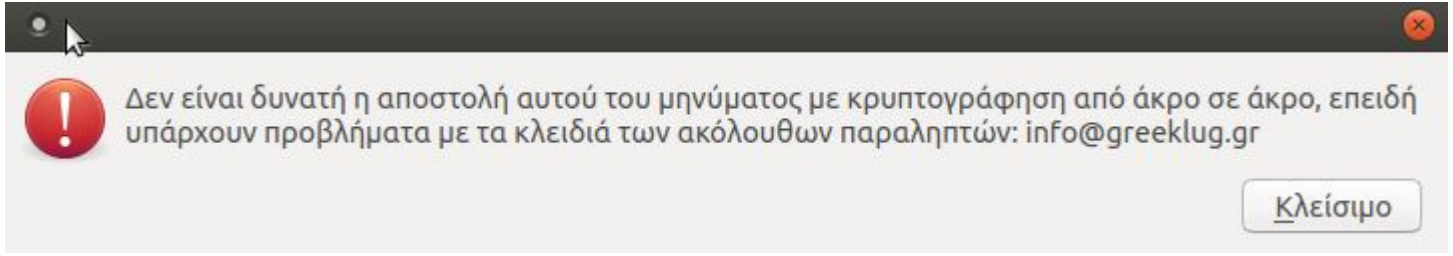


Εφόσον επιλέξουμε κάποια ασφάλεια εμφανίζεται στο κάτω μέρος σχετική ένδειξη χρήσης του OpenPGP.



Κρυπτογράφηση επικοινωνίας

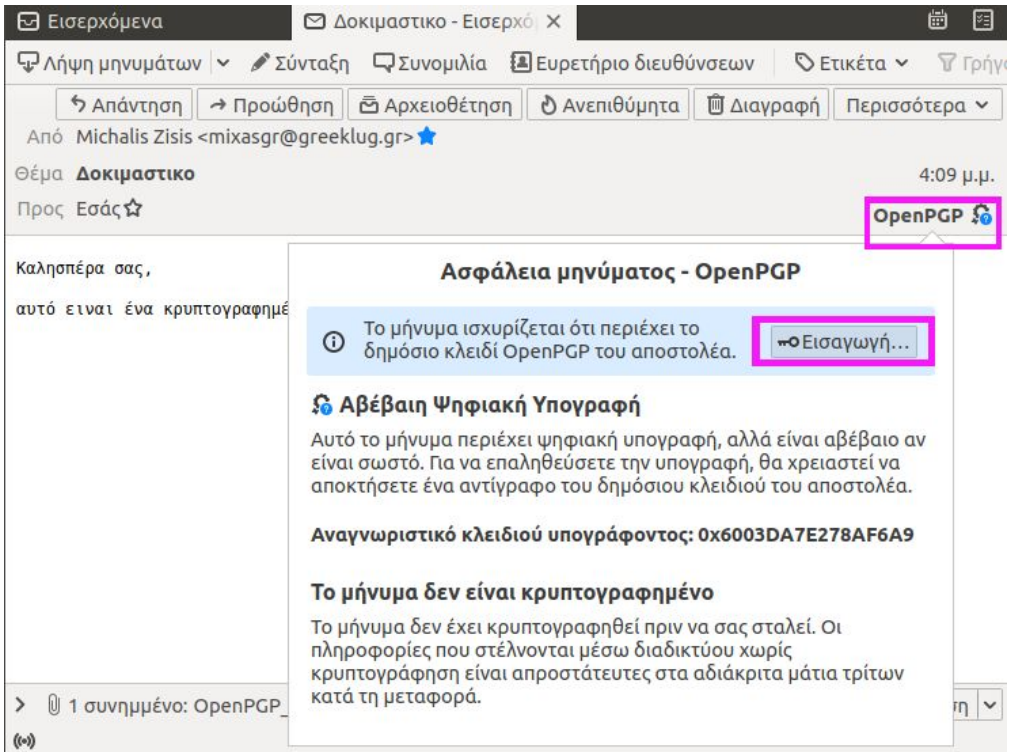
Για να είναι εφικτή η αποστολή ενός κρυπτογραφημένου μηνύματος σε κάποιον θα πρέπει να διαθέτουμε το δημόσιο κλειδί του στην κλειδοθήκη μας. Διαφορετικά η αποστολή αποτυγχάνει.



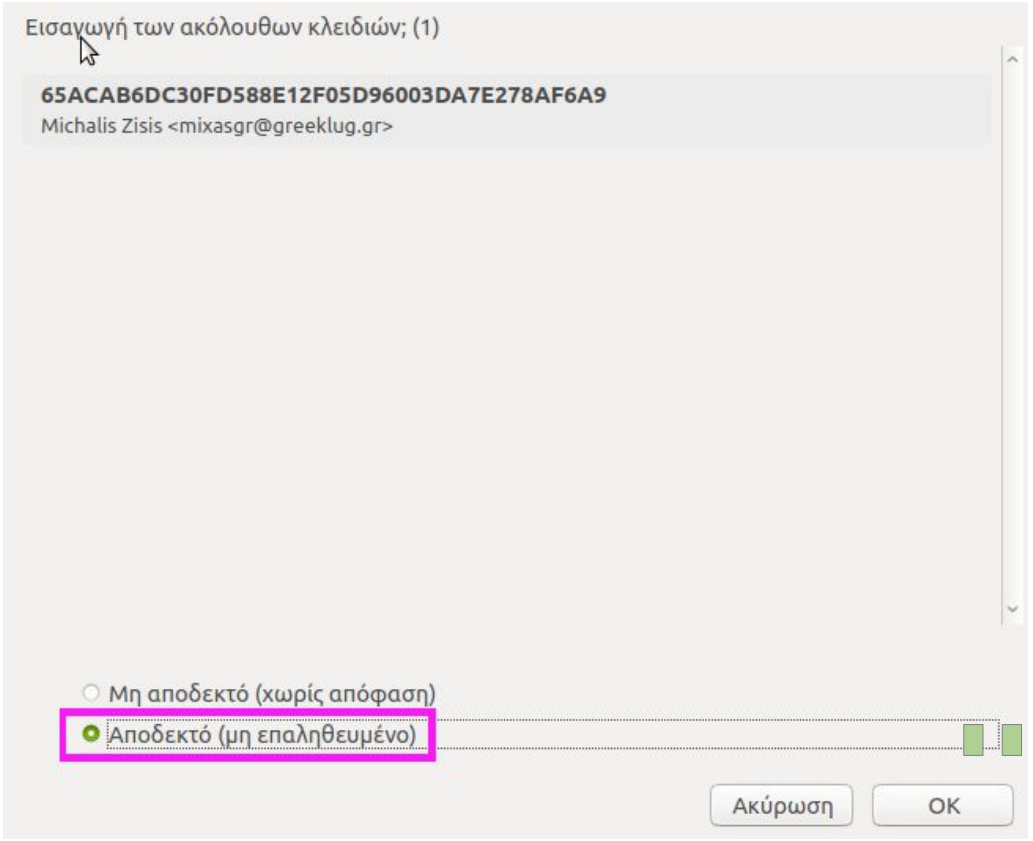
Θα πρέπει αντίστοιχα να εισάγουμε το δημόσιο κλειδί, είτε χειροκίνητα, είτε μέσω κάποιου μηνύματος που μας είχε προωθηθεί από τον παραλήπτη, που να έχει συνημμένο το κλειδί του.

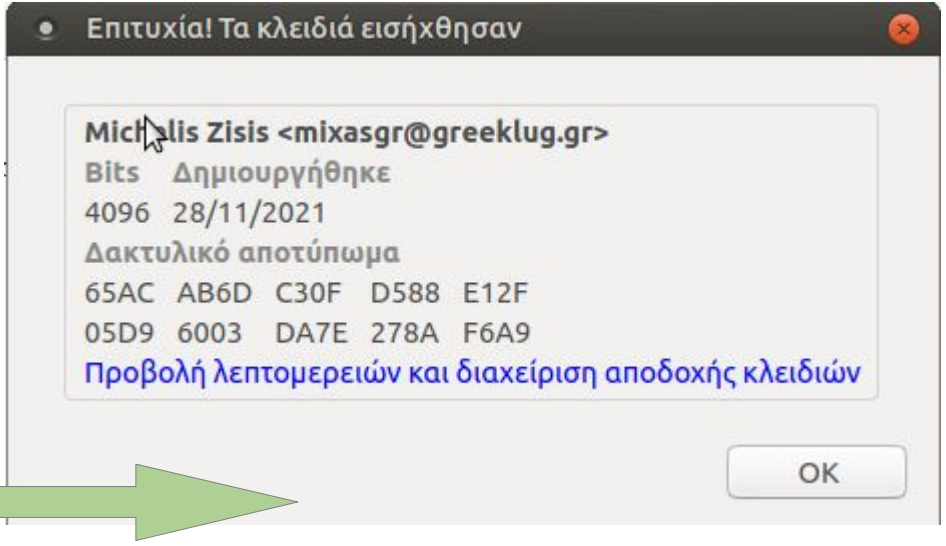
Κρυπτογράφηση επικοινωνίας

Εφόσον ένα μήνυμα περιέχει κάποιο κλειδί OpenPGP εμφανίζεται σχετική ένδειξη. Επίσης μέσω αυτής μπορούμε να δούμε πληροφορίες για την υπογραφή και να το εισάγουμε στην κλειδοθήκη μας.



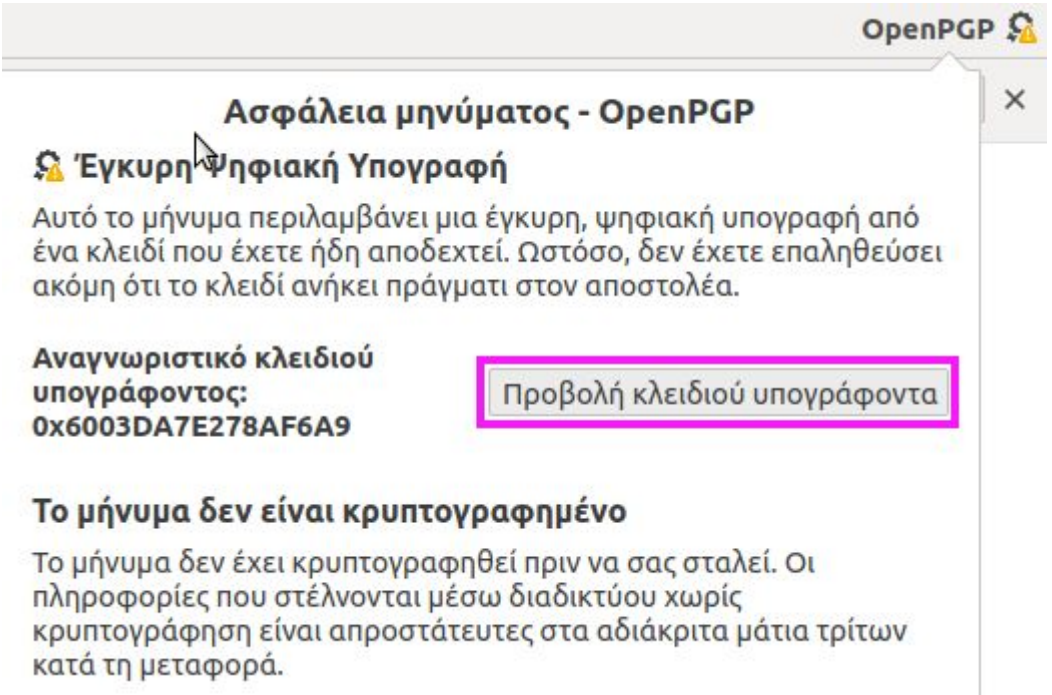
Κρυπτογράφηση επικοινωνίας





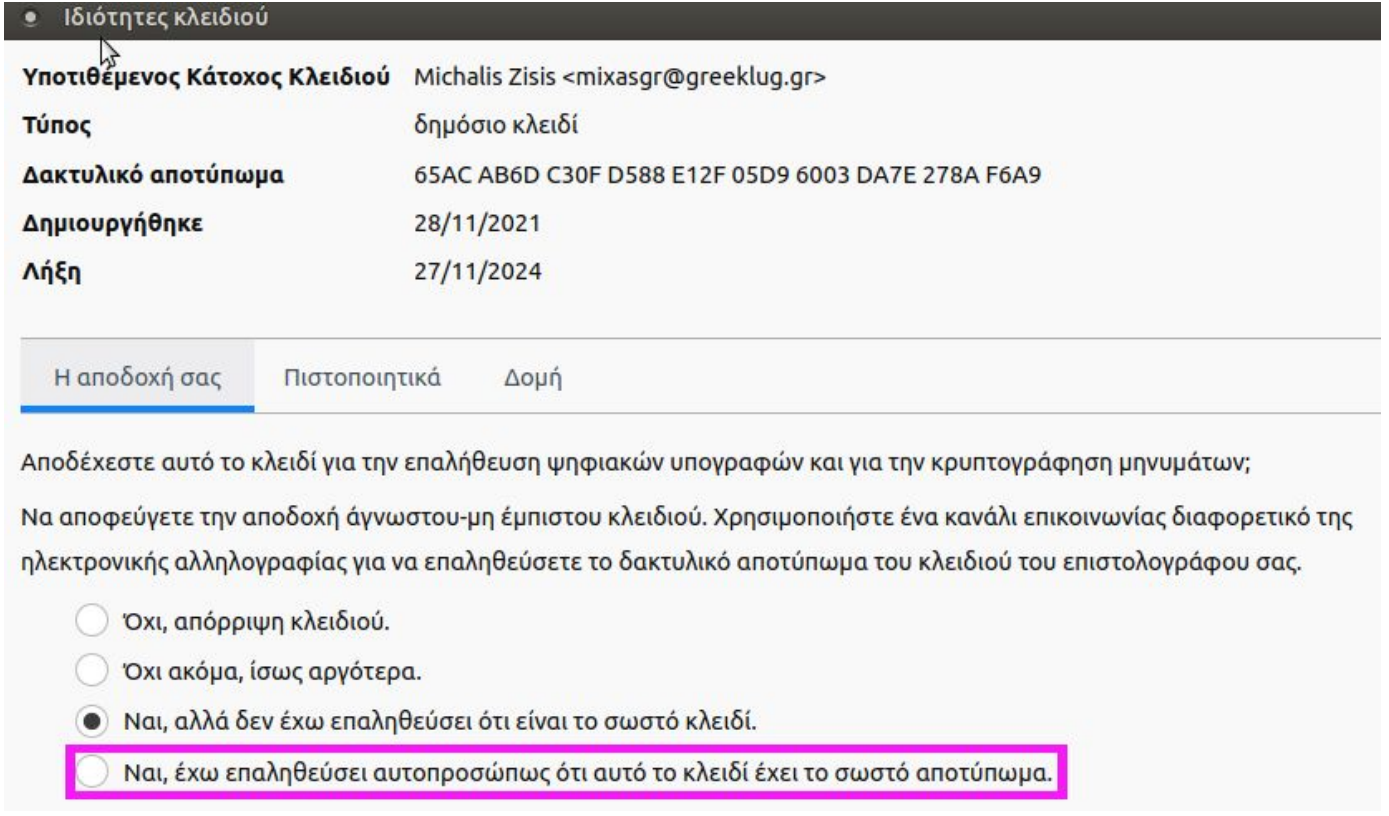
Κρυπτογράφηση επικοινωνίας

Από προκαθορισμένα το κλειδί εισάγεται στην κλειδοθήκη, ωστόσο δεν θεωρείται έγκυρο μέχρι να το ελέγξουμε και να το επαληθεύσουμε με τον κάτοχο.



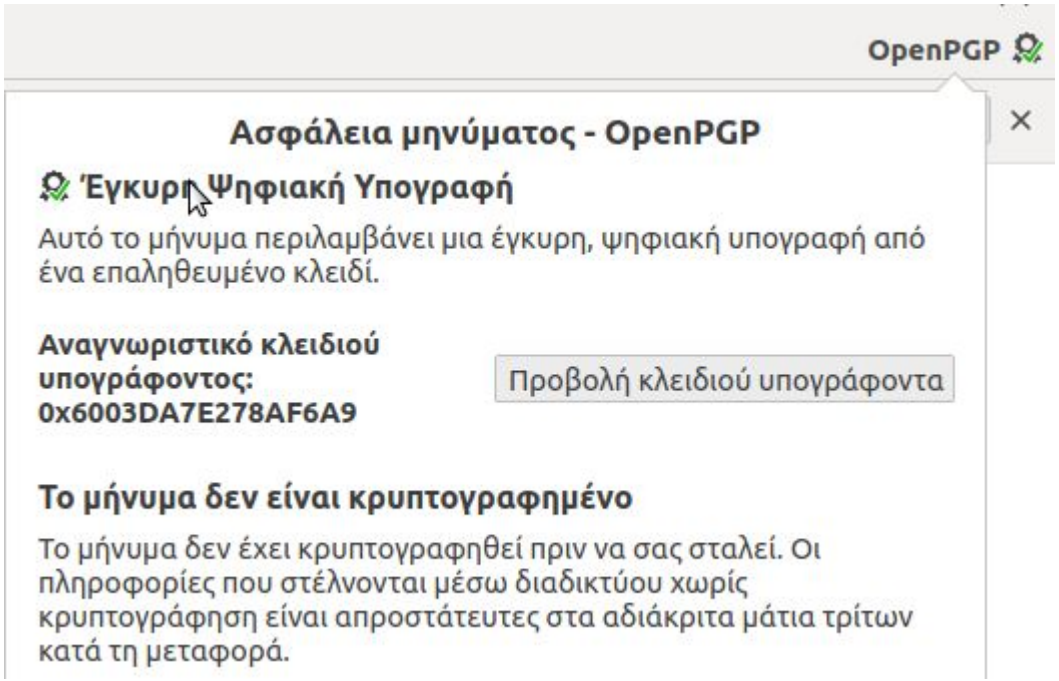
Κρυπτογράφηση επικοινωνίας

Εφόσον επαληθεύσουμε την ορθότητα του κλειδιού, μπορούμε να το αποδεχθούμε πλήρως.



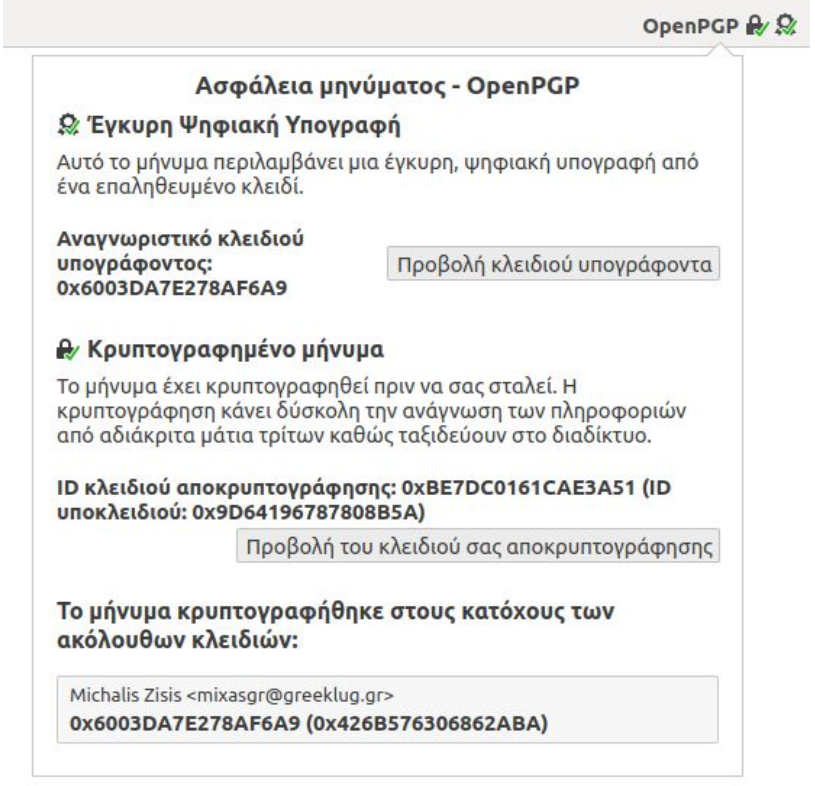
Κρυπτογράφηση επικοινωνίας

Ένδειξη ενός έγκυρου και επαληθευμένου κλειδιού σε μη κρυπτογραφημένο μήνυμα, που περιλαμβάνει ψηφιακή υπογραφή.



Κρυπτογράφηση επικοινωνίας

Ένδειξη ενός έγκυρου και επαληθευμένου κλειδιού σε κρυπτογραφημένο μήνυμα, που περιλαμβάνει επίσης ψηφιακή υπογραφή.



Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Ασφάλεια σε κοινωνικά δίκτυα

Ασφάλεια σε κοινωνικά δίκτυα

Τα κοινωνικά δίκτυα είναι διαδραστικά δίκτυα σε μορφή ιστοσελίδων που αφορούν την ανταλλαγή πληροφοριών ανάμεσα σε ανθρώπους.

Συνήθως αφορούν την διαμοιρασμό περιεχομένου όπως…

- δημοσιεύσεις κειμένου,
- σχόλια,
- φωτογραφίες,
- βίντεο
- ή άλλα δεδομένα, όπως πολυμέσα, που δημιουργούνται με ψηφιακό τρόπο.

Ασφάλεια σε κοινωνικά δίκτυα

Οι χρήστες αλληλεπιδρούν σε επίπεδο ατόμων, κοινοτήτων και οργανισμών, όπου μοιράζονται, δημιουργούν, συζητούν, συμμετέχουν και τροποποιούν ψηφιακό περιεχόμενο.

Συνοπτικά…

- λίστα επαφών-“φίλων” και “ακολούθων”
- κοινοποίηση περιεχομένου
- ομάδες
- σελίδες περιεχομένου
- πρόσθετα, όπως παιχνίδια
- εφαρμογές σε πολλαπλά Λ/Σ

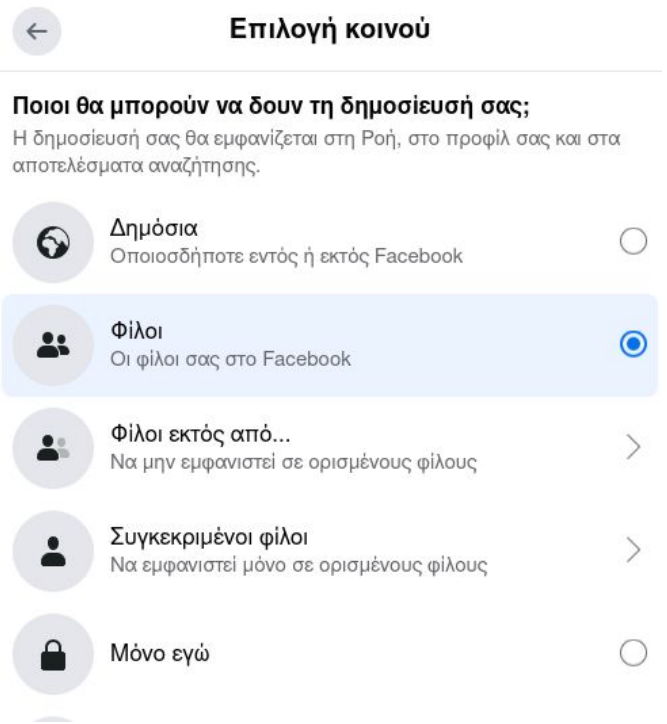
Ασφάλεια σε κοινωνικά δίκτυα

Προσθέτουμε στην λίστα “φίλων” μας μόνο **γνωστά/έμπιστα άτομα** είμαστε αρκετά προσεκτικοί με τις αποδοχές φιλίας και ελέγχουμε την αξιοπιστία ενός προφίλ προτού πατήσουμε "αποδοχή". Υπάρχουν πολλά ψεύτικα προφίλ, που σκοπό έχουν την πρόκληση κακόβουλων ενεργειών εις βάρος μας

Απενεργοποιούμε την δημόσια κοινοποίηση
καθώς οποιοδήποτε στο πλανήτη θα μπορεί να δει τι λέμε και τι κάνουμε

Αποφεύγουμε να δημοσιεύουμε ευαίσθητα προσωπικά δεδομένα
όπως φωτογραφίες των παιδιών μας, σημεία πρόσβασης στο σπίτι μας, μια αγορά που κάναμε πρόσφατα κτλ

Αποφεύγουμε να δημοσιεύουμε περιεχόμενο που "προδίδει" την τοποθεσία μας
...και γενικά το τι κάνουμε την τρέχουσα στιγμή, όπως ενεργοποίηση τοποθεσίας, δημοσίευση στοιχείων εισιτηρίων κτλ



Ασφάλεια σε κοινωνικά δίκτυα

<u>Για την επικοινωνία με άλλους χρήστες προτιμούμε την αποστολή προσωπικών μηνυμάτων και όχι μέσω της δημοσίευσης μηνυμάτων ή σχολίων στο προφίλ τους</u>
αλλιώς… οποιοδήποτε βλέπει την συνομιλία μας

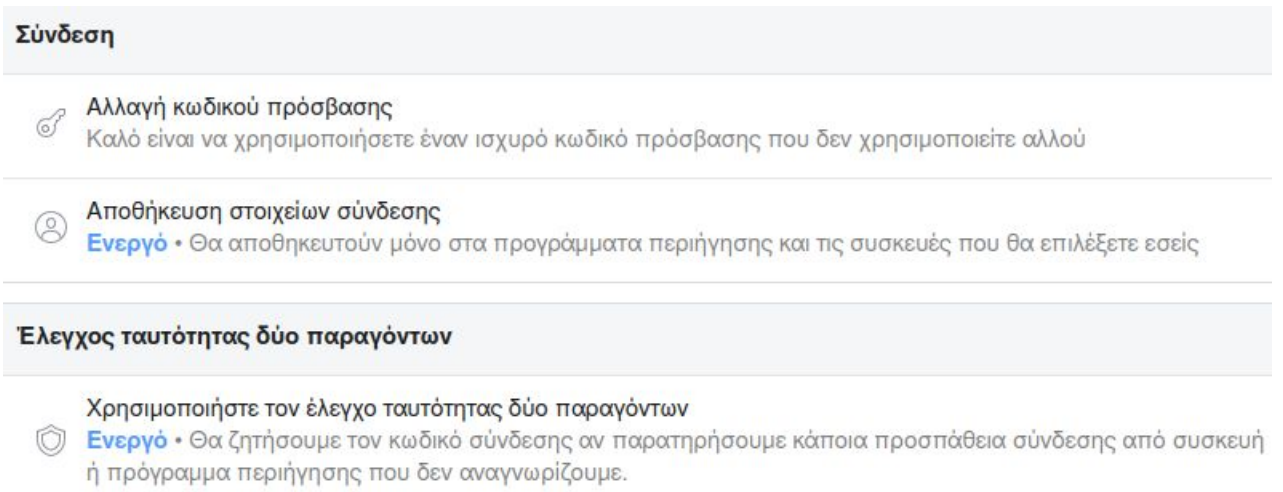
<u>Προσέχουμε την χρήση τρίτων εφαρμογών</u>
πολλά κοινωνικά δίκτυα παρέχουν την δυνατότητα χρήσης εφαρμογών, όπως παιχνίδια, οι οποίες όμως παρέχονται από τρίτους. Με την σειρά τους πολλές από αυτές ζητούν πρόσβαση σε προσωπικές πληροφορίες, όπως η λίστα φίλων μας, ημερομηνία γέννησης κ.α.(!)

<u>Αποφεύγουμε να δημοσιεύουμε “τα πάντα”</u>
με βάση τους όρους χρήσης των περισσότερων κοινωνικών δικτύων η χρήση τους συνεπάγεται μερική ή πλήρη πρόσβαση τους στα δεδομένα που εισάγουμε… ακόμα και η επικοινωνία με προσωπικά μηνύματα για “κουτσομπολιό” ανάμεσα σε κοντινούς μας φίλους
Κάποιος τρίτος ή “φίλος” μας μπορεί να χρησιμοποιήσει δεδομένα μας, πχ μια φωτογραφία μας με οποιοδήποτε τρόπο

Ασφάλεια σε κοινωνικά δίκτυα

Ρυθμίσεις ασφαλείας σε κοινωνικά δίκτυα

- Προβολή και διαχείριση συσκευών που αποκτούν πρόσβαση στον λογαριασμό μας
- Επιλογή **σύνθετου κωδικού πρόσβασης** και **ενεργοποίηση 2FA**
- Ενεργοποίηση ειδοποιήσεων σχετικά με τοποθεσίες ή προγράμματα που δεν αναγνωρίζουμε
- Διάφορες γενικές ρυθμίσεις



Ασφάλεια σε κοινωνικά δίκτυα

Ψευδείς ειδήσεις (fake news) σε κοινωνικά δίκτυα

- Κοινωνικά δίκτυα → νέο έδαφος διάδοσης **ψευδών ειδήσεων**
- Fake news = Σκόπιμη παραπληροφόρηση, με σκοπό την αποκόμιση οικονομικών, πολιτικών κα ωφελών
- Τα κοινωνικά δίκτυα αποτελούν πλατφόρμες ενημέρωσης. Δεν είναι όλες οι ειδήσεις αληθείς, μόνο και μόνο επειδή αναρτήθηκαν από προφίλ με πολλούς ακόλουθους.
- Στοχεύουν στην διάδοσή τους, ώστε να αυξηθεί η επισκεψιμότητα των ιστοσελίδων που φιλοξενούν τα fake news και εν τέλει να μεγιστοποιηθεί το κέρδος μέσω διαφημίσεων.
- Απαιτείται προσοχή στον εντοπισμό τους και **περιορισμός** τους.
- Αν θέλουμε να κοινοποιήσουμε μια τέτοια ανάρτηση, συστήνεται να την διασταυρώσουμε πρώτα, ιδιαίτερα αν επηρεάζουμε πολλά άτομα, καθώς η διάδοσή τους αποτελεί πλέον ποινικό αδίκημα.

Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Spam & Phishing

Spam & Phishing

Ιστορικά ως **Spam** αναφέρεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων που έχουν στόχο την προώθηση κάποιων προϊόντων ή ιδεών.

Λόγω της ευκολίας και του χαμηλού κόστους της, η μαζική αποστολή αλληλογραφίας αποτελεί μια τεχνική που υιοθετήθηκε ευρέως από χρήστες που προσπαθούν να μεγιστοποιήσουν το κοινό που θέλουν να απευθυνθούν. Η αποστολή ωστόσο τέτοιων μηνυμάτων μπορεί όμως να είναι αντίθετη με την επιθυμία των χρηστών και να γίνεται χωρίς την συγκατάθεσή τους συνεπώς είναι ανεπιθύμητη.

Σήμερα χρησιμοποιείται εξίσου και από κακόβουλους χρήστες, οι οποίοι με την χρήση του προσπαθούν να διαδώσουν μαζικά malware ή άλλα κακόβουλα στοιχεία.

Με βάση τα παραπάνω, το spam έχει πλέον ταυτιστεί με την **ανεπιθύμητη αλληλογραφία** και αποτελεί ένα καθημερινό φαινόμενο που επηρεάζει όλους τους χρήστες ηλεκτρονικής αλληλογραφίας.

Για τον περιορισμό του spam έχουν ψηφιστεί νόμοι που ορίζουν τις προδιαγραφές μιας έγκυρης μαζικής αποστολής, όπως η απαίτηση για **double opt-in**, ενώ επίσης η ανεπιθύμητη αποστολή διώκεται νομικά.

Spam & Phishing

Ως **Phishing** ή “ηλεκτρονικό ψάρεμα” αναφέρεται η προσπάθεια εξαπάτησης χρηστών, κατά την οποία οι κακόβουλοι χρήστες δημιουργούν μια παγίδα, πχ ένα ηλεκτρονικό μήνυμα ή μια ιστοσελίδα, που υποδύεται μία άλλη αξιόπιστη οντότητα.

Μέσω διαμοιρασμού της παγίδας, πχ με αποστολή spam μηνυμάτων, προσπαθούν να προσελκύσουν χρήστες, που είτε λόγω άγνοιας, είτε λόγω ελλιπούς προστασίας, κάνουν χρήση της παγίδας, παρέχοντας με αυτόν τον τρόπο, προσωπικά και άλλα στοιχεία τους, στους κακόβουλους χρήστες.

Τυπικό παράδειγμα του παραπάνω είναι ηλεκτρονικά μηνύματα και ιστοσελίδες που προσποιούνται ότι προέρχονται από γνωστά τραπεζικά ιδρύματα και έχουν στόχο να υποκλέψουν τα στοιχεία web banking ή στοιχεία πιστωτικών καρτών των χρηστών.

Συνήθως, χρησιμοποιούνται μαζί με άλλες τεχνικές, όπως το Email spoofing, με βάση το οποίο παράγουν ηλεκτρονικά μηνύματα που φαίνεται να προέρχονται από τον ίδιο τον αποστολέα, ή την αξιόπιστη οντότητα, ενώ στην πραγματικότητα τα μηνύματα προέρχονται από κάποιον κακόβουλο διακομιστή.

Spam & Phishing

Το spam αποτελεί ένα φαινόμενο που έχει επεκταθεί και σε άλλες μορφές, όπως η τηλεφωνία με ανεπιθύμητες/διαφημιστικές κλήσεις ή sms.

Παραπλανητικές τηλεφωνικές κλήσεις (Μητρώο 11)
Στην Ελλάδα υπάρχει σχετική νομοθεσία που αναφέρεται ως Μητρώο 11 (Μητρώο άρθρου 11 Ν. 3471/2006), όπου κάθε πάροχος υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να τηρεί έναν ειδικό κατάλογο συνδρομητών, οι οποίοι έχουν ζητήσει να μην δέχονται τηλεφωνικές κλήσεις για προώθηση προϊόντων και υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς.

Μπορεί κάποιος να ζητήσει να ενταχθεί σε αυτό κατόπιν επικοινωνίας με τον πάροχό του, ενώ επίσης συνήθως υπάρχει η δυνατότητα αυτόματης καταχώρησης από τις εφαρμογές για κινητά των παρόχων.

«Ψάρεμα» μέσω SMS
Γίνεται χρήση παρόμοιων τεχνικών με αυτών των phishing email, με τους χρήστες να λαμβάνουν sms που φαίνεται να προέρχεται από κάποια έγκυρη οντότητα. Συνήθως περιέχουν κάποιον σύνδεσμο που μας οδηγεί σε ιστοσελίδα παγίδα.

Spam & Phishing

Από ALPHA©BANK, <alpha@themintingcompany.com>

Θέμα **Έχετε λάβει (1) νέο μήνυμα !** 25/5/22, 11:54

Προς Εμένα <info@greeklug.gr>

Αγαπητέ πελάτη,

Εντοπίσαμε κάποια ασυνήθιστη δραστηριότητα στον λογαριασμό σας, πρέπει να συνδεθείτε μέσω του παρακάτω συνδέσμου και να επιβεβαιώσετε την ταυτότητά σας, εάν δεν λύσετε το πρόβλημα η τραπεζική σας κάρτα θα αποκλειστεί και δεν θα μπορείτε να κάνετε περαιτέρω συναλλαγές ή να κάνετε ανάληψη μετρητών από το ATM του υποκαταστήματος της τράπεζάς μας.
Πρέπει να διευθετήσετε το θέμα μέσα στις επόμενες 24 ώρες.

Ενημερώστε τον λογαριασμό σας

Σε ευχαριστώ για την εμπιστοσύνη σου,

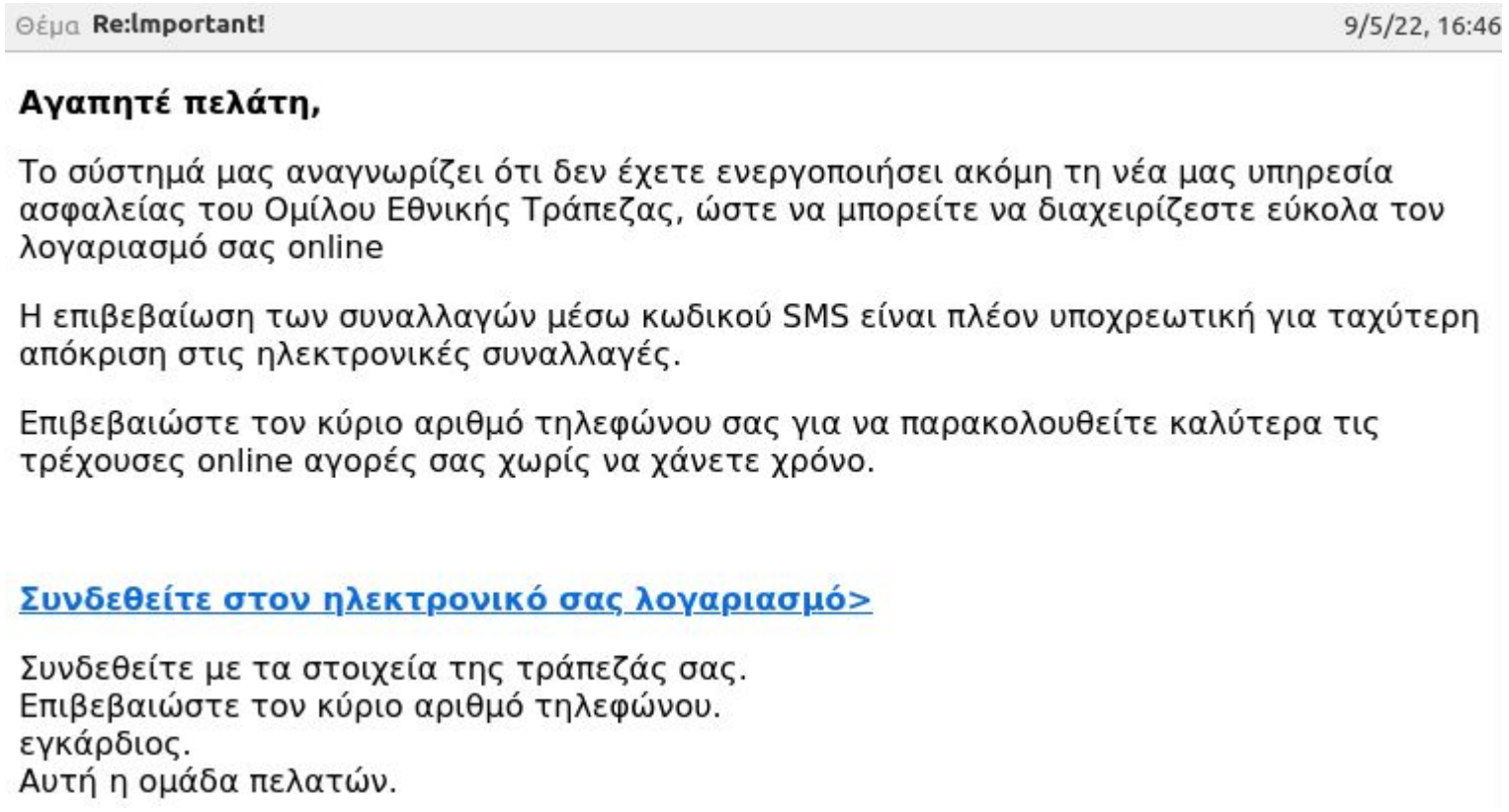
μεταβείτε στη διεύθυνση **AlphaiBank,**

AlphaiBank,

ebanking@alpha.gr

© 2022 - "Alpha bank"

Spam & Phishing



Θέμα **Re:Important!** 9/5/22, 16:46

Αγαπητέ πελάτη,

Το σύστημά μας αναγνωρίζει ότι δεν έχετε ενεργοποιήσει ακόμη τη νέα μας υπηρεσία ασφαλείας του Ομίλου Εθνικής Τράπεζας, ώστε να μπορείτε να διαχειρίζεστε εύκολα τον λογαριασμό σας online

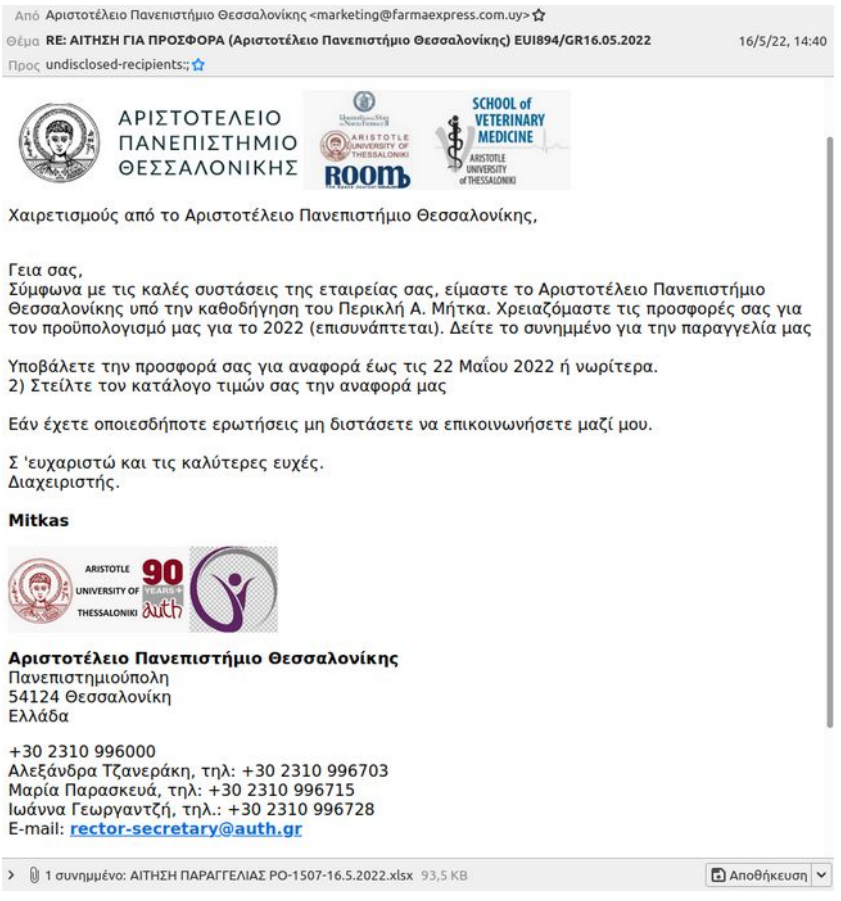
Η επιβεβαίωση των συναλλαγών μέσω κωδικού SMS είναι πλέον υποχρεωτική για ταχύτερη απόκριση στις ηλεκτρονικές συναλλαγές.

Επιβεβαιώστε τον κύριο αριθμό τηλεφώνου σας για να παρακολουθείτε καλύτερα τις τρέχουσες online αγορές σας χωρίς να χάνετε χρόνο.

Συνδεθείτε στον ηλεκτρονικό σας λογαριασμό>

Συνδεθείτε με τα στοιχεία της τράπεζάς σας.
Επιβεβαιώστε τον κύριο αριθμό τηλεφώνου.
εγκάρδιος.
Αυτή η ομάδα πελατών.

Spam & Phishing



Από Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης <marketing@farmaexpress.com.uy>

Θέμα **RE: ΑΙΤΗΣΗ ΓΙΑ ΠΡΟΣΦΟΡΑ (Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης) EUI894/GR16.05.2022** 16/5/22, 14:40

Προς undisclosed-recipients:;

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

Χαιρετισμούς από το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης,

Γεια σας,
Σύμφωνα με τις καλές συστάσεις της εταιρείας σας, είμαστε το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης υπό την καθοδήγηση του Περικλή Α. Μήτκα. Χρειαζόμαστε τις προσφορές σας για τον προϋπολογισμό μας για το 2022 (επισυνάπτεται). Δείτε το συνημμένο για την παραγγελία μας

Υποβάλετε την προσφορά σας για αναφορά έως τις 22 Μαΐου 2022 ή νωρίτερα.
2) Στείλτε τον κατάλογο τιμών σας την αναφορά μας

Εάν έχετε οποιεσδήποτε ερωτήσεις μη διστάσετε να επικοινωνήσετε μαζί μου.

Σ 'ευχαριστώ και τις καλύτερες ευχές.
Διαχειριστής.

Mitkas

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πανεπιστημιούπολη
54124 Θεσσαλονίκη
Ελλάδα

+30 2310 996000
Αλεξάνδρα Τζανεράκη, τηλ: +30 2310 996703
Μαρία Παρασκευά, τηλ: +30 2310 996715
Ιωάννα Γεωργαντζή, τηλ.: +30 2310 996728
E-mail: rector-secretary@auth.gr

1 συνημμένο: ΑΙΤΗΣΗ ΠΑΡΑΓΓΕΛΙΑΣ PO-1507-16.5.2022.xlsx 93,5 KB Αποθήκευση

Spam & Phishing

Πλοηγούμαστε με προσοχή σε άγνωστες σελίδες
δεν ανοίγουμε άμεσα κάθε σύνδεσμο που υπάρχει σε μια σελίδα ή μας έχει σταλθεί πχ μέσω email

Χρησιμοποιούμε ιδιωτική περιήγηση
αποφεύγουμε κατά το δυνατό τις “περίεργες” σελίδες και χρησιμοποιούμε για αυτές την ιδιωτική περιήγηση ή την πλοήγηση από δεύτερο περιηγητή ως ελάχιστο μέτρο προστασίας

Επιθεωρούμε το μήνυμα
ελέγχουμε ότι οι σύνδεσμοι που υπάρχουν στο μήνυμα οδηγούν στην διεύθυνση που θα έπρεπε

Ελέγχουμε τις κεφαλίδες ενός ηλεκτρονικού μηνύματος
Ελέγχουμε τις κεφαλίδες (headers) ώστε να επιβεβαιώσουμε ότι το μήνυμα προήλθε από ορθή διεύθυνση αλληλογραφίας

Spam & Phishing

Received	from frosty-wing.tecnocorp.uy (localhost.localdomain [127.0.0.1]) by frosty-wing.tecnocorp.uy (Postfix) with ESMTP id 9DEEF44093825; Mon, 16 May 2022 07:02:34 -0500 (CDT)
Received	from frosty-wing.tecnocorp.uy ([169.60.33.176]) by frosty-wing.tecnocorp.uy (frosty-wing.tecnocorp.uy [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id kWFN0bfS7qbA; Mon, 16 May 2022 07:02:19 -0500 (CDT)
Received	from webmail.farmaexpress.com.uy (localhost.localdomain [127.0.0.1]) by frosty-wing.tecnocorp.uy (Postfix) with ESMTPSA id CC0E044192631; Mon, 16 May 2022 06:40:39 -0500 (CDT)

Spam & Phishing

Αναχαίτιση Spam και κακόβουλων e-mail

Οι εφαρμογές αλληλογραφίας, όπως το Mozilla Thunderbird, περιέχουν ενσωματωμένη λειτουργία ανεπιθύμητης αλληλογραφίας. Με βάση αυτή, μεταφέρουν στον ειδικό φάκελο ανεπιθύμητων μηνυμάτων όσα μηνύματα εντοπίζουν ως κακόβουλα. Ωστόσο θα πρέπει από την πλευρά μας να εκπαιδεύσουμε την βάση ανεπιθύμητης αλληλογραφίας σημειώνοντας αρχικά τα spam μηνύματα ώστε να μπορεί η εφαρμογή να τα εντοπίσει.

Μπορούμε επίσης να δημιουργήσουμε κάποια φίλτρα, με μοτίβα/κοινά στοιχεία κακόβουλων μηνυμάτων, ώστε αντίστοιχα μηνύματα να χαρακτηρίζονται αυτόματα ως spam ή και να διαγράφονται αυτόματα.

Οι ίδιες λειτουργίες παρέχονται συνήθως και από τον πάροχο της αλληλογραφίας μας.
Για παράδειγμα, μεγάλος αριθμός διακομιστών που στηρίζονται σε Linux κάνουν χρήση των ΕΛ/ΛΑΚ λογισμικών:

- **Spamassasin**, που αποτελεί φίλτρο ελέγχου ανεπιθύμητης αλληλογραφίας
- **ClamAV**, που αποτελεί antivirus για σκανάρισμα συνημμένων αρχείων.

Θα πρέπει να ελέγξουμε τις ρυθμίσεις του λογαριασμού ή φιλοξενίας μας και να ενεργοποιήσουμε τα φίλτρα ασφαλείας εάν αυτά δεν είναι ήδη ενεργά.

Spam & Phishing

☆		Finansowanie z tarczą do 750 000 PLN z de minims	operate-corpor...	24/5/22, 12:03
☆		***SPAM*** Η Sinsay είναι τώρα διαθέσιμη στην Ελλάδα	Sinsay	24/5/22, 13:23
☆		***SPAM*** Jagodina Open Dance Festival-11-12.june 2022.	festival.rs	25/5/22, 05:10
☆		***SPAM*** Έχετε λάβει (1) νέο μήνυμα !	ALPHA©BANK,	25/5/22, 07:20
☆		***SPAM*** Έχετε λάβει (1) νέο μήνυμα !	myAlpha Bank	25/5/22, 08:09
☆		***SPAM*** Jagodina Open Dance Festival-11-12.june 2022.	festival.rs	25/5/22, 08:20
☆	📎	Опалубка, леса строительные. Продажа и аренда	СтальСтрой	25/5/22, 09:15

Spam & Phishing

Sim card swapping

Αποτελεί μια τεχνική παραβίασης μέσω της οποίας κακόβουλοι χρήστες, έχοντας υποκλέψει ήδη κάποια από τα προσωπικά μας στοιχεία, αιτούνται την αντικατάσταση της κάρτας κινητής τηλεφωνίας μας.

Ο πάροχος, παρέχει την νέα κάρτα sim στους κακόβουλους χρήστες, οι οποίοι λαμβάνουν πλέον τις τηλεφωνικές μας κλήσεις, όπως και τα sms επιβεβαίωσης.

Σε περίπτωση που εντοπίσουμε ότι η σύνδεσή μας έχει διακοπεί για αρκετό χρονικό διάστημα, θα πρέπει να επικοινωνήσουμε άμεσα με τον πάροχό μας.

Spam & Phishing

Τραπεζικοί λογαριασμοί/πληρωμές
Με βάση τις ενημερώσεις ασφαλείας των τραπεζών, η ίδια η τράπεζά **δεν πρόκειται να μας ζητήσει ποτέ** να παρέχουμε τους κωδικούς μας.

Σε περίπτωση που δεν είμαστε σίγουροι, ή έχουμε εντοπίσει κάποια ύποπτη δραστηριότητα δεν θα πρέπει να προχωρήσουμε σε συναλλαγή.

Όλες οι τράπεζες παρέχουν εναλλακτικούς τρόπους επαλήθευσης, είτε μέσω SMS, είτε μέσω εφαρμογής ηλεκτρονικών μηνυμάτων (συνήθως Viber), είτε με μηνύματα μέσω των εφαρμογών τους για κινητά τηλέφωνα.

Spam & Phishing

Απαιτείται ισχυρή ταυτοποίησή σας

Σας έχουμε στείλει Κωδικό μιας Χρήσης (OTP) με VIBER ή SMS στον αριθμό κινητού **••••••••••3619** για να ολοκληρώσετε τη συναλλαγή σας.

Συμπληρώστε τον **6ψήφιο κωδικό**:

Ο Κωδικός μιας Χρήσης (OTP) ισχύει για 2 λεπτά.

ΣΥΝΕΧΕΙΑ

Βασική Ασφάλεια στην Ψηφιακή Καθημερινότητα

Παραβίαση

Παραβίαση

Παρά τις προσπάθειές μας και την ακολούθηση των κανόνων ασφαλείας, μπορεί κάποια συσκευή μας να παραβιαστεί, όχι άμεσα από κάποιο δικό μας λάθος αλλά από κενό ασφαλείας στο λειτουργικό σύστημα ή κάποια έμπιστη εφαρμογή.

- Χακάρισμα συσκευής
- Χακάρισμα e-mail λογαριασμού
- Ransomware

GreekLUG

Ευχαριστούμε!

Το αρχείο της παρουσίασης από την
Ελληνική Ένωση Φίλων ΕΛ/ΛΑΚ (GreekLUG) διέπεται από την άδεια

Ελληνική Ένωση Φίλων Ελεύθερου Λογισμικού | GreekLUG
https://www.greeklug.gr/