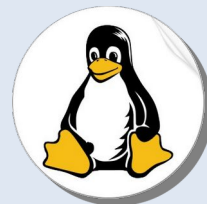




GreekLUG



Ελεύθερο Λογισμικό &



Λογισμικό Ανοικτού Κώδικα



Μάθημα 10ο



Διαδίκτυο 3 & Συσκευές



Ύλη Μαθημάτων Χ

• Μαθ. 8/9/10 : Διαδίκτυο 1, 2 & 3

- Διαδίκτυο γενικά και χρήση με παραδείγματα,
- Ρύθμιση Δικτύου (βασικά),
- Πλοήγηση / περιηγητής Firefox,
- Αναζήτηση, Wikipedia
- Email / εφαρμογή Thunderbird,
- Εφαρμογές άμεσων μηνυμάτων & συνομιλίας
- Βίντεο Chat και επικοινωνία,
- Κοινωνικά δίκτυα και ασφάλεια,
- Χρήση Smartphone





Βίντεο Chat και επικοινωνία I

Γρήγορος και δωρεάν τρόπος επικοινωνίας μέσω διαδικτύου...

- αποστολή μηνυμάτων κειμένου,
- κλήσεις φωνής,
- βιντεοκλήσεις,
- ανταλλαγή αρχείων,
- διαμοιρασμός οθόνης,
- ψηφιακές τηλεφωνικές κλήσεις (VOIP)



Βίντεο Chat και επικοινωνία II

Τυπικά χαρακτηριστικά...

- λίστα επαφών-“φίλων”
- ομάδες
- ασύγχρονη επικοινωνία
- διαθεσιμότητα σε πολλαπλά Λ/Σ





Εισαγωγή - Γενική προστασία I

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.

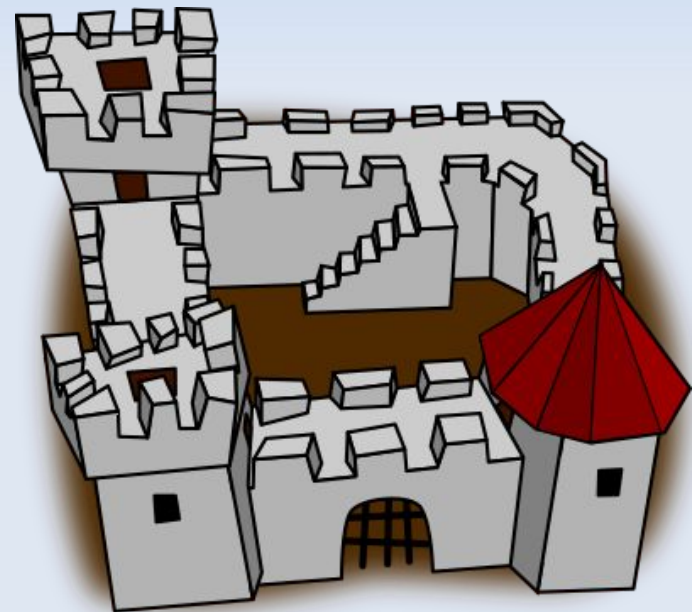
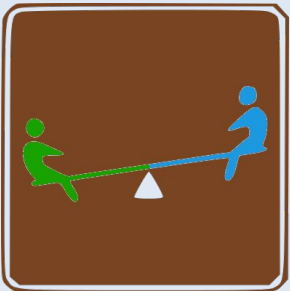
Η προσωπική μας ασφάλεια, οι ιδιωτικές μας πληροφορίες, η περιουσία μας, τα προσωπικά μας δεδομένα και πολλά ακόμα, μπορεί να κινδυνεύουν και λόγω αυτού θα πρέπει να ενημερωνόμαστε αλλά και να ακολουθούμε κανόνες ασφαλείας για την **προστασία** μας.



Εισαγωγή - Γενική προστασία II

Μερικές παραδοχές...

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





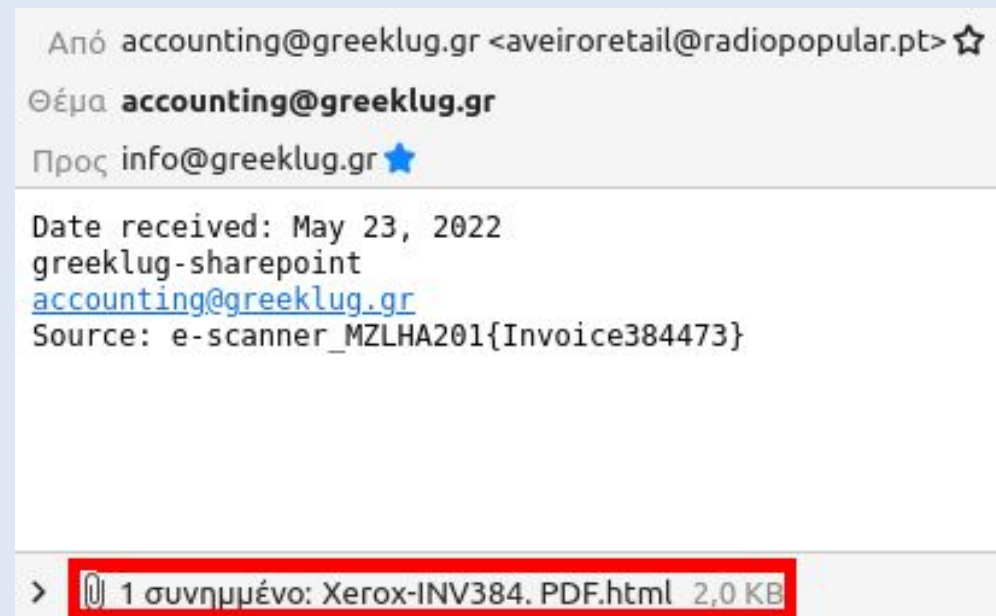
Κανόνες ασφαλείας I

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 II



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

MICROSOFT Office PRO Plus 2016 v16.0.4266.1003 RTM + Activator

   Uploaded 09-27 2015, Size 2.21 GiB, ULed by ThumperTM




Office Professional Plus 2019 BR

 Uploaded 11-01 2018, Size 3.08 GiB, ULed by ratondownload

Windows 10 X64 Pro ACTIVATED LATEST 2022 Office 2021

  Uploaded 04-06 23:08, Size 5.53 GiB, ULed by dickspic

Microsoft OFFICE 2010 Pro Plus PRECRACKED

   Uploaded 06-13 2010, Size 732.06 MiB, ULed by DeGun

Windows 11 X64 Pro ACTIVATED LATEST 2022 Office 2016 TPM BYPASSE

  Uploaded 04-06 23:19, Size 7.59 GiB, ULed by dickspic



Κανόνες ασφαλείας III

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 IV

Εκτελούμε περιοδικά έλεγχο ασφαλείας

Ανά κάποιο χρονικό διάστημα, πχ 1 φορά 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 V

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 VI

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



Κανόνες ασφαλείας VII

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 VIII

Δεν αποθηκεύουμε τα στοιχεία μας

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

https://login.launchpad.net/5Yq95dSC5yAQv20s/+decide

Αποθήκευση σύνδεσης για το launchpad.net;

Όνομα χρήστη
info@greeklug.gr

Κωδικός πρόσβασης
.....

Χωρίς αποθήκευση ▼ Αποθήκευση



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)





Συνθηματικά I

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



Συνθηματικά II

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 III

Εύκολη ... προς ... δύσκολη παραβίαση

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 IV

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





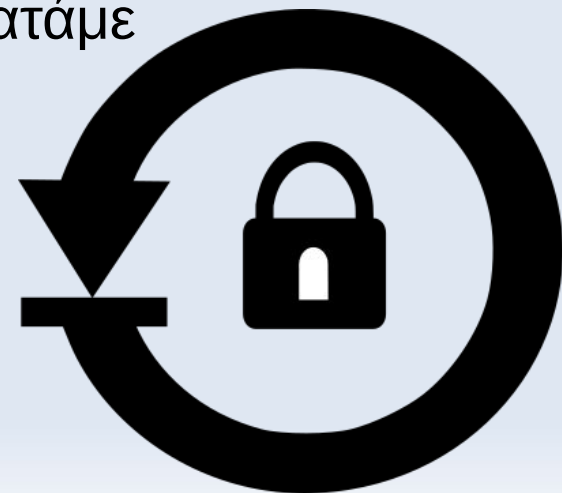
Συνθηματικά V

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

- Λήψη κωδικού ή pin με ισχύ μερικά δευτερόλεπτα/λεπτά (TOTP – Time based One Time Password) μέσω sms, εφαρμογών αποστολής μηνυμάτων, push notification, App Authenticators
- Φυσικές συσκευές που χρησιμεύουν ως κλειδί
- 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



Ασφάλεια σε κοινωνικά δίκτυα I

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 II

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

Συνοπτικά...

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

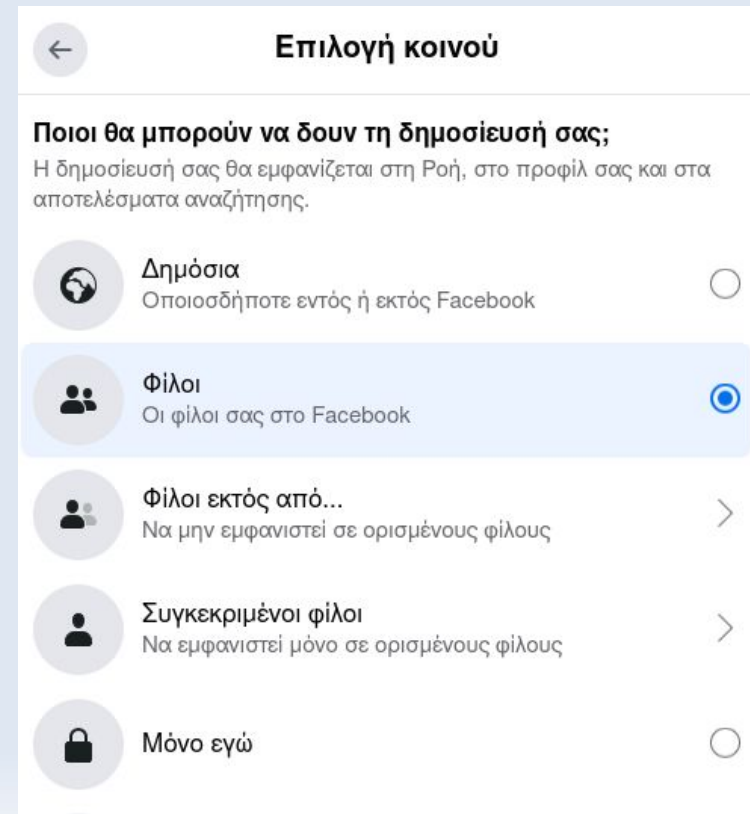




Ασφάλεια σε κοινωνικά δίκτυα III

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





Ασφάλεια σε κοινωνικά δίκτυα IV

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 V

Για την επικοινωνία με άλλους χρήστες προτιμούμε την αποστολή προσωπικών μηνυμάτων και όχι μέσω της δημοσίευσης μηνυμάτων ή σχολίων στο προφίλ τους

αλλιώς... οποιοδήποτε βλέπει την συνομιλία μας

Προσέχουμε την χρήση τρίτων εφαρμογών

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.(!)



Ασφάλεια σε κοινωνικά δίκτυα VI

Αποφεύγουμε να δημοσιεύουμε “τα πάντα”

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 VII

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

Σύνδεση



Αλλαγή κωδικού πρόσβασης

Καλό είναι να χρησιμοποιήσετε έναν ισχυρό κωδικό πρόσβασης που δεν χρησιμοποιείτε αλλού



Αποθήκευση στοιχείων σύνδεσης

Ενεργό • Θα αποθηκευτούν μόνο στα προγράμματα περιήγησης και τις συσκευές που θα επιλέξετε εσείς

Έλεγχος ταυτότητας δύο παραγόντων



Χρησιμοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων

Ενεργό • Θα ζητήσουμε τον κωδικό σύνδεσης αν παρατηρήσουμε κάποια προσπάθεια σύνδεσης από συσκευή ή πρόγραμμα περιήγησης που δεν αναγνωρίζουμε.



Ασφάλεια σε κοινωνικά δίκτυα VIII

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 **περιορισμό** τους.
- Αν θέλουμε να κοινοποιήσουμε μια τέτοια ανάρτηση, συστήνεται να την διασταυρώσουμε πρώτα, ιδιαίτερα αν επηρεάζουμε πολλά άτομα, καθώς η διάδοσή τους μπορεί να αποτελεί πλέον και ποινικό αδίκημα !



Κινητή Τηλεφωνία

Κινητά τηλέφωνα:

1) **ΚΛΑΣΣΙΚΑ** (*FEATUREPHONE*)

2) **ΕΞΥΠΝΑ** (*SMARTPHONE*)





Κινητή Τηλεφωνία & Linux



- **Android**

Λ/Σ για smartphones που βασίζεται στην πυρήνα Linux

- **Android Open Source Project (AOSP)**

<https://source.android.com>

- Προκαθορισμένα κλειδωμένο

έχουμε δικαιώματα χρήστη και όχι διαχειριστή
==>

απόκτηση πλήρους πρόσβασης στο σύστημα, το γνωστό "root"



ΕΛ/ΛΑΚ στο Android



Αν και το Android είναι κυρίως Ελεύθερο Λογισμικό, οι συσκευές συνήθως έρχονται με ιδιοταγές λογισμικό και υπηρεσίες που εμποδίζουν τον κόσμο να τις χρησιμοποιήσει ανεξάρτητα και αυτόνομα.



- Καμπάνια: **Ελευθερώστε το Android σας!**
<https://www.greeklug.gr/el/ellak/associates/84-associate-fsfe-el/395-fsfe-freeyourandroid>
- Εγκατάσταση εφαρμογών ΕΛ/ΛΑΚ
Market: F-Droid (<https://f-droid.org/>)
Γνωστές εφαρμογές: Mozilla Firefox Mobile, Thunderbird/K-9 Mail, Signal, VLC
- Εγκατάσταση ΕΛ/ΛΑΚ Λειτουργικού Συστήματος
LineageOS (<https://lineageos.org/>)



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

Creative Commons Αναφορά Δημιουργού - Μη Εμπορική Χρήση -
Παρόμοια Διανομή 4.0 Διεθνές (CC BY-NC-SA 4.0)

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.el>



Ελληνική Ένωση Φίλων ΕΛ/ΛΑΚ | GreekLUG

<https://www.greeklug.gr/>