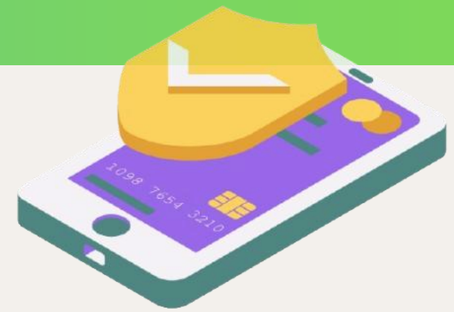
FinaLY
Empowering Financial Literacy in Youth

Ψηφιακή & Διαδικτυακή Συμπεριφορά



Χρηματοδοτείται από την Ευρωπαϊκή Ένωση. Ωστόσο, οι απόψεις και οι γνώμες που εκφράζονται είναι αποκλειστικά του/των συγγραφέα/ων και δεν αντικατοπτρίζουν απαραίτητα εκείνες της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Ούτε η Ευρωπαϊκή Ένωση ούτε ο EACEA μπορούν να θεωρηθούν υπεύθυνοι για αυτές.
Αριθμός Έργου: 2023-3-CY02-KA210-YOU-000185401

Co-funded by the European Union

Χρηματοδοτείται από :

Co-funded by the European Union

Κοινοπραξία

FinaLY

ECECT

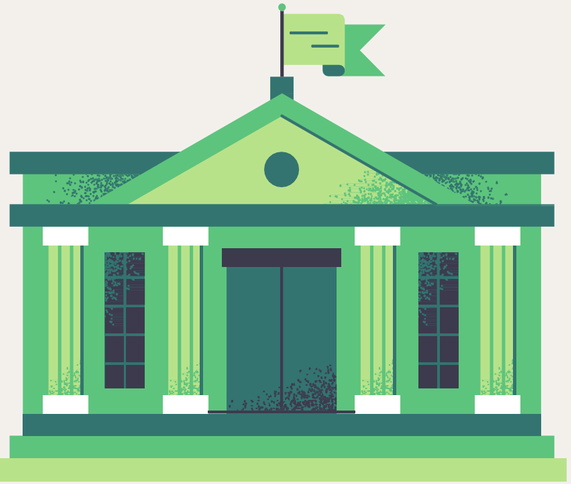
comhairle chontae na mí
meath county council

YouthNet Cyprus

Εισαγωγή

- Ο στόχος του FinaLY είναι να κάνει τους νέους πιο έξυπνους με τις οικονομικές αποφάσεις

- Οι νέοι αρχίζουν να κάνουν βασικές επιλογές χρημάτων, όπως αποταμίευση και δαπάνες, σε έναν οικονομικό κόσμο γεμάτο κινδύνους και ευκαιρίες



- Πολλοί νέοι στην Ευρώπη δεν κατανοούν πλήρως βασικά οικονομικά θέματα όπως η αποταμίευση, ο προϋπολογισμός ή η χρήση πίστωσης

- Σύμφωνα με διεθνή μελέτη του Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD) το 2020, περίπου οι μισοί ενήλικες της ΕΕ δυσκολεύονται με τις οικονομικές γνώσεις

Co-funded by the European Union

Στόχοι

Με το τέλος αυτής της παρουσίασης, θα είστε σε θέση να:

- Προσδιορίζετε ασφαλείς ιστότοπους και τρόπους πληρωμής
- Δημιουργείτε και διαχειρίζεστε ισχυρούς κωδικούς πρόσβασης
- Αναγνωρίζετε και αποφεύγετε τις διαδικτυακές απάτες και τις απόπειρες phishing
- Χρησιμοποιήτε τα ψηφιακά πορτοφόλια (PayPal, Revolut, Apple Pay, Google Pay) με ασφάλεια
- Κατανοείτε και προστεύετε το απόρρητο των προσωπικών δεδομένων
- Να είστε ενήμεροι για τους οικονομικούς κανονισμούς και τα δίχτυα ασφαλείας.

Co-funded by the European Union

Καλώς ήρθατε στον κόσμο του ψηφιακού χρήματος

Ζούμε σε μια εποχή όπου τα χρήματα κινούνται με ένα μόνο **κλικ!**
Από τις ηλεκτρονικές αγορές μέχρι το mobile banking, αγοράζουμε, **εξοικονομούμε** και **στέλνουμε** χρήματα ψηφιακά καθημερινά.

Αλλά με την ευκολία έρχεται και η ευθύνη!
Ας μάθουμε πώς να παραμένουμε:

- **έξυπνοι**
- **ασφαλής**
- **υπό έλεγχο**

όταν χρησιμοποιούμε χρήματα στο διαδίκτυο.

Co-funded by the European Union

Γιατί αυτό έχει σημασία?

Σήμερα μπορείτε να διαχειριστείτε ολόκληρη την οικονομική σας ζωή από το τηλέφωνό σας.

- **Ένα λάθος κλικ = χαμένα χρήματα**

  Το να πατήσετε κατά λάθος σε έναν ψεύτικο σύνδεσμο ή να εισαγάγετε τα στοιχεία σας σε λάθος ιστότοπο μπορεί να εξαντλήσει το υπόλοιπό σας.
- **Οι νέοι αποτελούν βασικό στόχο**

  Οι απατεώνες ξέρουν ότι οι νέοι περνούν πολύ χρόνο online και γίνονται ολοένα και πιο έξυπνοι. Χρησιμοποιούν ψεύτικα δώρα, προσφορές εργασίας, ακόμη και ψεύτικες τραπεζικές εφαρμογές.
- **Οι εγκληματίες του κυβερνοχώρου δεν χρειάζεται να διαρρήξουν το σπίτι σας**

  Απλώς χρειάζονται να εμπιστευτείτε το λάθος μήνυμα ή εφαρμογή.

Γιατί αυτό έχει σημασία?

Το τηλέφωνό μας είναι πλέον το πορτοφόλι μας - ψωνίζουμε, στέλνουμε χρήματα και διαχειριζόμαστε τον τραπεζικό μας λογαριασμό από αυτό.

Αλλά με τη μεγάλη άνεση, έρχεται και ο μεγάλος κίνδυνος. Ένα λάθος πάτημα μπορεί να ανοίξει την πόρτα σε απατεώνες και οι νέοι στοχοποιούνται περισσότερο από ποτέ.

Αυτός είναι ο λόγος για τον οποίο ο χρηματοοικονομικός αλφαβητισμός είναι μια απαραίτητη δεξιότητα στον σημερινό κόσμο.

- **Ένα λάθος κλικ = κλεμμένα χρήματα ή ταυτότητα**
- **Οι απατεώνες επικεντρώνονται πλέον στους νέους - όχι μόνο στους ηλικιωμένους**
- **Οι ψηφιακές μας συνήθειες επηρεάζουν την οικονομική μας ασφάλεια**
- **Μαθαίνοντας τα βασικά, προστατεύουμε το μέλλον μας**

Το να είμαστε έξυπνοι με τα χρήματά σας ξεκινά με το να γνωρίζουμε πώς να εντοπίζουμε τους κινδύνους και να αποφεύγουμε δαπανηρά λάθη.
Ας μην περιμένουμε μέχρι να είναι πολύ αργά!

Co-funded by the European Union

Τι θα μάθετε σήμερα

✅ Πώς να εντοπίζετε ασφαλείς ιστότοπους και τρόπους πληρωμής

✅ Πώς να δημιουργείτε ισχυρούς κωδικούς πρόσβασης

✅ Πώς να αναγνωρίζετε τις διαδικτυακές απάτες

✅ Πώς να χρησιμοποιείτε τις εφαρμογές Revolut, PayPal και άλλες με σύνεση

✅ Πώς να προστατεύετε τα προσωπικά σας δεδομένα στο διαδίκτυο

Co-funded by the European Union

Ποιες είναι οι ασφαλείς διαδικτυακές πρακτικές;

Η ασφάλεια στο διαδίκτυο δεν έχει να κάνει μόνο με την αποφυγή ιών - έχει να κάνει με την προστασία των **χρημάτων, της ταυτότητας και του μέλλοντός** μας.

Ακολουθούν ορισμένες βασικές συνήθειες που πρέπει να ακολουθεί κάθε νέος:

- **Αγοράζετε μόνο από ασφαλείς, αξιόπιστους ιστότοπους**

Αναζητήστε «https://» και αποφύγετε ύποπτες προσφορές που φαίνονται πολύ καλές για να είναι αληθινές.

- **Διατηρήστε τα οικονομικά σας στοιχεία απόρρητα**

Ποτέ μην κοινοποιείτε τα στοιχεία της κάρτας σας, τα PIN ή τους κωδικούς πρόσβασης - ακόμα και με φίλους.

- **Μειώστε τον κίνδυνο απάτης ή κλοπής**

Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης, ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων (2FA) και αποφύγετε το δημόσιο Wi-Fi για ενέργειες που σχετίζονται με χρήματα.

- **Ελέγξτε διπλά πριν πατήσετε "Πληρωμή" και ελέγχετε πάντα τις τραπεζικές σας κινήσεις για ύποπτη δραστηριότητα.**

Co-funded by the European Union

Πώς να εντοπίσετε ασφαλείς ιστότοπους

Πριν εισαγάγετε προσωπικά στοιχεία ή στοιχεία πληρωμής στο διαδίκτυο, βεβαιωθείτε ότι ο ιστότοπος είναι ασφαλής.

Δείτε πώς μπορείτε να το καταλάβετε:

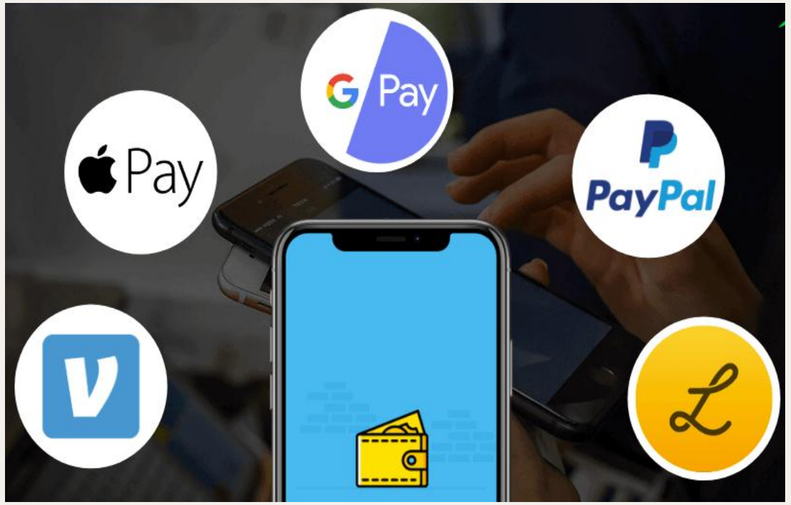
- **Αναζητήστε το "https://" στη διεύθυνση URL**
  Το "s“ (secure) σημαίνει ασφαλές - μην εμπιστεύεστε ποτέ ιστότοπους χωρίς αυτό.
- **Ελέγξτε για εικονίδιο λουκέτου στη γραμμή διευθύνσεων**
  Αυτό σημαίνει ότι ο ιστότοπος διαθέτει πιστοποιητικό SSL και κρυπτογραφεί τα δεδομένα σας.
- **Μένετε σε γνωστούς και αξιόπιστους ιστότοπους**
  Εάν δεν το έχετε ακούσει ποτέ και φαίνεται πρόχειρο, εμπιστευτείτε το ένστικτό σας - μην το ρισκάρετε.
- **Προσέξτε για περίεργα αναδυόμενα παράθυρα, τυπογραφικά λάθη ή κακό σχεδιασμό**
  Αυτά μπορεί να είναι προειδοποιητικά σημάδια ότι ο ιστότοπος δεν είναι νόμιμος.

✅ https://www.trusted-shop.com
❌ http://www.trust3d-sh0p-deals.example

Co-funded by the European Union

Ασφαλείς πύλες πληρωμής

Δεν είναι όλοι οι τρόποι πληρωμής εξίσου ασφαλείς. Η επιλογή του κατάλληλου μπορεί να προστατεύσει τόσο τα χρήματά σας όσο και τα προσωπικά σας στοιχεία.



Τι πρέπει να έχετε κατά νου:

- **Χρησιμοποιήστε ασφαλείς, αξιόπιστες μεθόδους πληρωμής**
  Μείνετε σε πλατφόρμες όπως το PayPal, πιστωτικές/χρεωστικές κάρτες, το Apple Pay ή το Google Pay - προσφέρουν ενσωματωμένη ασφάλεια και προστασία αγοραστών.

- **Επιβεβαιώστε τις πληρωμές απευθείας στην επίσημη πλατφόρμα**
  Να ολοκληρώνετε πάντα τις συναλλαγές εντός του ιστότοπου ή της εφαρμογής. Ποτέ μέσω εξωτερικών συνδέσμων ή αναδυόμενων παραθύρων.

Co-funded by the European Union

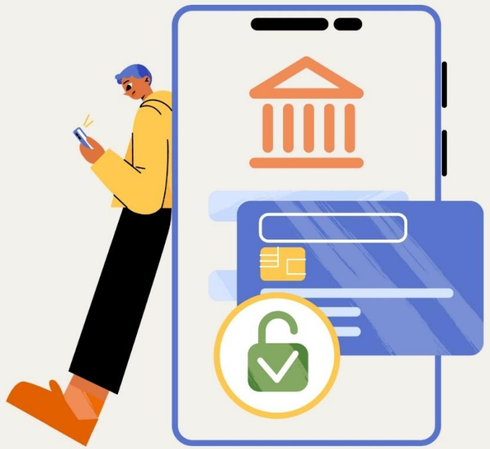
Ασφαλείς πύλες πληρωμής

- **Αποφύγετε τις πληρωμές μέσω email, κειμένου ή τηλεφώνου**
  Εάν κάποιος σας ζητήσει να στείλετε χρήματα με αυτόν τον τρόπο, είναι σοβαρή προειδοποιητική ένδειξη - συχνά είναι μη ανιχνεύσιμο και μη ασφαλές.

- **Διατηρήστε ψηφιακές αποδείξεις και παρακολουθήστε τις συναλλαγές**
  Τα screenshots ή τα μηνύματα ηλεκτρονικού ταχυδρομείου επιβεβαίωσης μπορούν να βοηθήσουν εάν υπάρξει ποτέ διαφωνία.

Co-funded by
the European Union

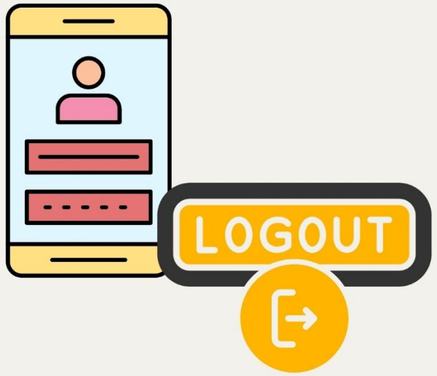
Συμβουλές για να παραμείνετε ασφαλείς στο διαδίκτυο



1. Διατηρήστε **ενημερωμένο το λογισμικό προστασίας από ιούς**: Βοηθά στον αποκλεισμό κακόβουλου λογισμικού, απόπειρες phishing και ύποπτες λήψεις.

2. Ασφάλεια κωδικού πρόσβασης: Χρησιμοποιήστε **ισχυρούς, μοναδικούς κωδικούς πρόσβασης** για κάθε λογαριασμό, αποφύγετε την επαναχρησιμοποίησή τους και ενημερώστε τους τακτικά.

3. Παρακολουθήστε τον τραπεζικό σας λογαριασμό για **ασυνήθιστη δραστηριότητα**: Ελέγχετε συχνά τις καταστάσεις σας



4. Ενεργοποίηση **ελέγχου ταυτότητας δύο παραγόντων** (2FA): Ένα επιπλέον επίπεδο προστασίας για το ηλεκτρονικό ταχυδρομείο, τα μέσα κοινωνικής δικτύωσης και τις τραπεζικές εφαρμογές σας, όπως:
   - Face ID / Δακτυλικό αποτύπωμα (βιομετρικά στοιχεία)
   - Κωδικοί μίας χρήσης που αποστέλλονται με SMS ή email
   - Εφαρμογές ελέγχου ταυτότητας (π.χ. Google Authenticator, Microsoft Authenticator, Authy)
   - Κλειδιά ασφαλείας (όπως YubiKey ή Titan Key)

5. **Αποσυνδεθείτε** όταν χρησιμοποιείτε κοινόχρηστες ή δημόσιες συσκευές

Ασφάλεια κωδικών πρόσβασης;

Η σωστή διαχείριση κωδικών πρόσβασης σημαίνει την υιοθέτηση έξυπνων συνηθειών ώστε να διατηρείτε τους λογαριασμούς σας ασφαλείς.
Είναι η πρώτη σας γραμμή άμυνας ενάντια στις διαδικτυακές απειλές.

Βέλτιστες πρακτικές για ισχυρούς κωδικούς πρόσβασης:

- **Μακρύ και περίπλοκο:** Χρησιμοποιήστε τουλάχιστον 12 χαρακτήρες, συμπεριλαμβανομένων κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων (π.χ. *M!cr0S@fe2025!*)

- **Μην επαναχρησιμοποιείτε ποτέ κωδικούς πρόσβασης:** One hack = πρόσβαση σε όλα εάν χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε όλους τους ιστότοπους.

- **Αποφύγετε πληροφορίες που είναι εύκολα προβλέψιμες:** Αποφύγετε ονόματα, γενέθλια, ονόματα κατοικίδιων ζώων ή οτιδήποτε μπορεί να βρει κάποιος στα μέσα κοινωνικής δικτύωσης.

Co-funded by the European Union

Ασφάλεια κωδικών πρόσβασης;

- **Ενεργοποίηση ελέγχου ταυτότητας δύο παραγόντων (2FA):** Προσθέστε ένα επιπλέον επίπεδο ασφάλειας απαιτώντας ένα δεύτερο βήμα ταυτοποίησης (όπως έναν κωδικό από το τηλέφωνό σας ή μια εφαρμογή ελέγχου ταυτότητας) εκτός από τον κωδικό πρόσβασής σας.

- **Διατηρήστε ενημερωμένες τις επιλογές ανάκτησης:** Βεβαιωθείτε ότι το εφεδρικό email και ο αριθμός τηλεφώνου σας είναι ενημερωμένα.

- **Χρησιμοποιήστε έναν αξιόπιστο διαχειριστή κωδικών πρόσβασης (password manager):** Αποθηκεύει όλους τους κωδικούς πρόσβασης με ασφάλεια και τους κρυπτογραφεί.

- **Αποφύγετε την αποθήκευση απλού κειμένου:** Μην διατηρείτε κωδικούς πρόσβασης σε εφαρμογές σημειώσεων, documents ή email.

Co-funded by the European Union

Συμβουλές για ισχυρούς κωδικούς πρόσβασης που μπορείτε να θυμάστε

1. Αντικαταστήστε τα γράμματα με αριθμούς ή σύμβολα
Πάρτε μια λέξη ή φράση που μπορείτε εύκολα να θυμάστε και αντικαταστήστε ορισμένα γράμματα με παρόμοιους αριθμούς ή σύμβολα.
Για παράδειγμα:
Λέξη: “sunflower"
ΚΩΔΙΚΟΣ: sunf10w3r

2. Συνδυάστε άσχετες λέξεις
Διαλέξτε 3-4 τυχαίες λέξεις και συνδυάστε τις. Όσο πιο ασυνήθιστος είναι ο συνδυασμός, τόσο το καλύτερο.
Για παράδειγμα:
Λέξεις: βιβλίο, τυρί, δέντρο!!!
Κωδικός πρόσβασης: BookCheeseTree!!!

3. Χρησιμοποιήστε ένα αξέχαστο γεγονός με μια φράση
Συνδυάστε μια σημαντική ημερομηνία με μια φράση που σχετίζεται με αυτήν την ημερομηνία.
Για παράδειγμα:
Εκδήλωση: Επέτειος γάμου στις 15 Ιουνίου 1980
Κωδικός: WeddingDay15061980
Σημείωση: Αποφύγετε να χρησιμοποιείτε μόνο μια εύκολα απομνημονεύσιμη ημερομηνία και αποφύγετε πληροφορίες που κάποιος θα μπορούσε να βρει, για παράδειγμα, από το Facebook, όπως τα γενέθλιά σας.

4. Χρησιμοποιήστε τη μέθοδο Όνομα-Ημερομηνία-Τόπος
Συνδυάστε το όνομα κάποιου σημαντικού για εσάς, μια σημαντική ημερομηνία και ένα σημαντικό μέρος.
Για παράδειγμα:
Όνομα: Μαίρη
Ημερομηνία: Γεννημένη το 1950
Τόπος: (είχαμε το μήνα του μέλιτος στο) Κέιμπριτζ
Κωδικός: Mary1950Cambridge

Πηγή: AbilityNet. (2025, Φεβρουάριος). *Συμβουλές για τη δημιουργία ισχυρών κωδικών πρόσβασης που μπορείτε να θυμάστε*. AbilityNet. https://abilitynet.org.uk/factsheets/tips-creating-strong-passwords-you-can-remember

Co-funded by the European Union

Password Strength Chart

SANDSTORM IT
power on

This is based on the average brute forcing (botnet) power in 2019.

123456 Top 10,000 password	0.20 milliseconds	Unsafe
qwerty123456 Longer "common" password	13 hours	Unsafe
ITFunSom3times Longer password with numbers	48 thousand years	Risky
ITifun0m3times! Longer password with numbers and special characters	13 trillion years	Good
imusingalongpasswordtoday Even Longer password	913 trillion years	Better
imu$inga1ongpa$$word+oday! Even Longer password with numbers and special characters	2 octillion years	Best

Please Note: These passwords are for demonstration purposes ONLY and are not to be used.

Τι είναι οι απάτες και οι παραπλανήσεις;

Οι απατεώνες είναι παντού στο διαδίκτυο
Ο στόχος τους είναι απλός: να σας ξεγελάσουν ώστε να δώσετε τα χρήματά σας ή τα προσωπικά σας στοιχεία.

- **Οι phishers και οι απατεώνες στοχεύουν την εμπιστοσύνη σας**
  Προσποιούνται ότι είναι τράπεζες, υπηρεσίες παράδοσης ή ακόμα και φίλοι για να λάβουν τα δεδομένα σας.

- **Χρησιμοποιούν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή συνδέσμους**
  Αυτά μπορεί να σας οδηγήσουν σε παρόμοιους ιστότοπους ή να σας ζητήσουν να "επαληθεύσετε" τις πληροφορίες σας.

- **Συχνά υπόσχονται πράγματα που φαίνονται πολύ καλά για να είναι αληθινά**
  Όπως δωρεάν iPhone, δωροκάρτες ή εύκολα χρήματα - είναι σχεδόν πάντα παγίδα.

- **Εάν κάτι σας φαίνεται ύποπτο - κάντε παύση και ελέγξτε ξανά**
  Καλύτερα να είσαι ασφαλής παρά να μετανιώσεις όταν πρόκειται για την ασφάλειά σου στο διαδίκτυο.

FinaLY

Co-funded by
the European Union

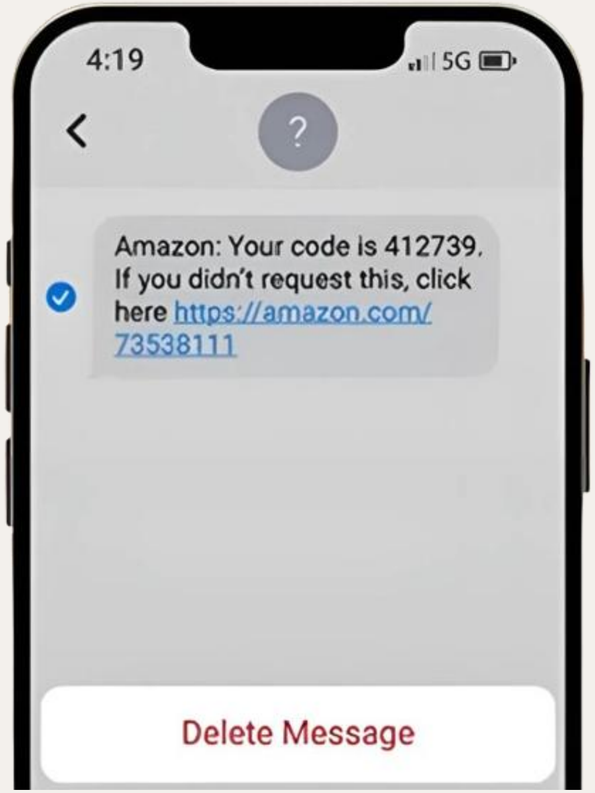
Πώς να εντοπίσετε τους phishers

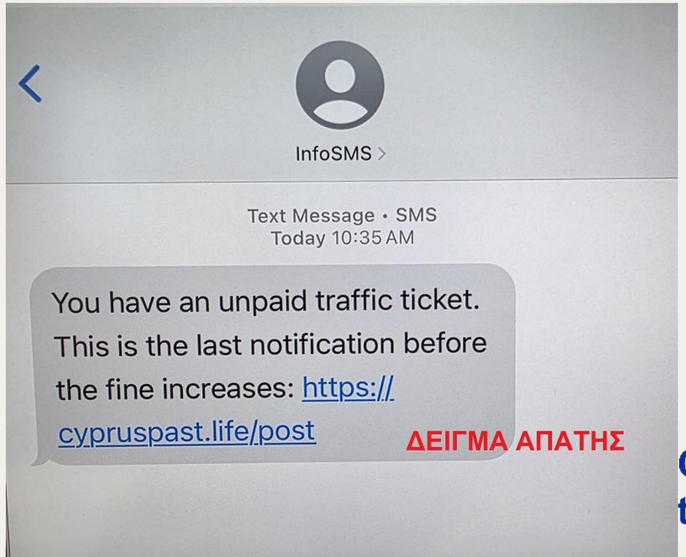
Ελέγξτε τη διεύθυνση email του αποστολέα
Είναι ανορθόγραφο, άγνωστο ή λίγο περίεργο; Αυτό είναι μια κόκκινη σημαία. *(π.χ. support@paypall.com)*

Προσέξτε για επείγοντα ή απειλιτικά μηνύματα
"Ο λογαριασμός σας θα κλείσει!" ή "Δράσε τώρα!" - οι τακτικές πίεσης είναι κλασικές κινήσεις απάτης.

Να είστε προσεκτικοί με ύποπτους συνδέσμους ή συνημμένα
Τοποθετήστε το δείκτη του ποντικιού πάνω από συνδέσμους πριν κάνετε κλικ - αν φαίνεται περίεργο, μην τον ανοίξετε.

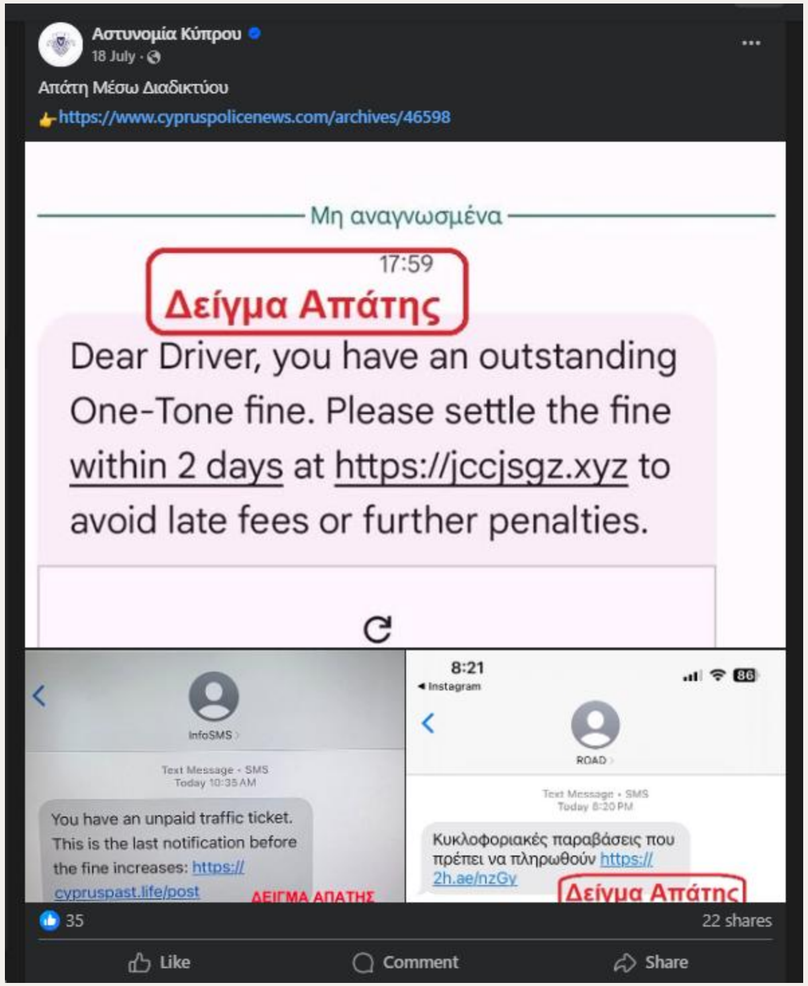
Σκεφτείτε πριν μοιραστείτε προσωπικές ή οικονομικές πληροφορίες
Καμία νόμιμη εταιρεία δεν θα ζητήσει τους κωδικούς πρόσβασης ή τα στοιχεία της πιστωτικής σας κάρτας μέσω email ή κειμένου.





Co-funded by the European Union

Τα Νέα της Αστυνομίας Κύπρου



Co-funded by the European Union

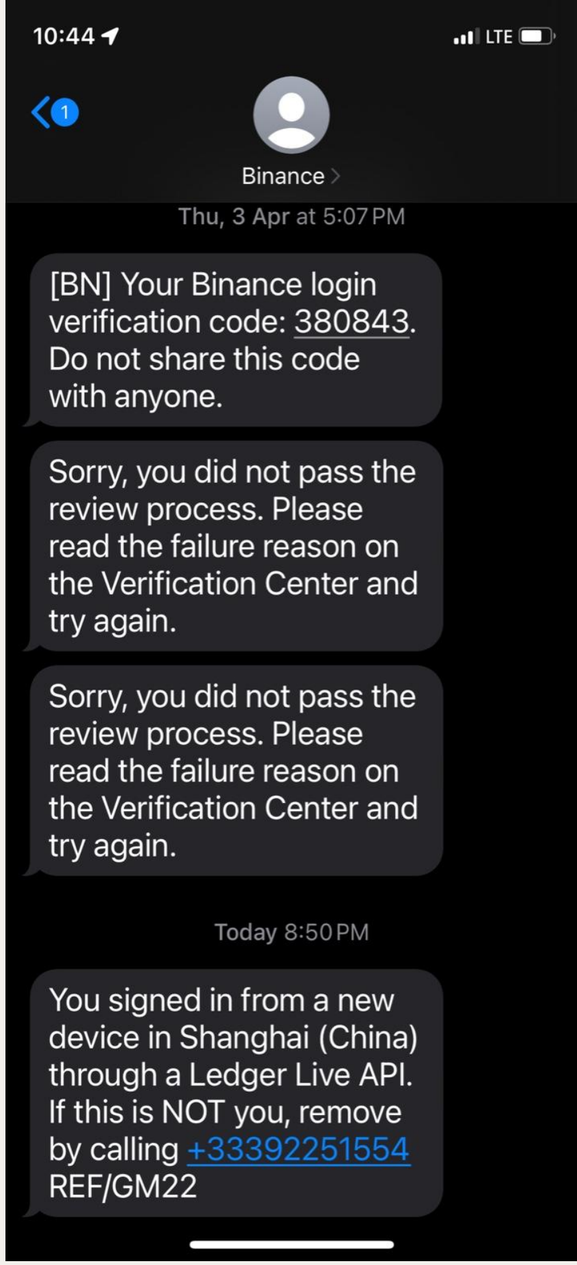
Πώς να εντοπίσετε τους phishers

Το διπλανό μήνυμα στο screenshot είναι **απάτη**.

- **Τακτικές επείγουσας ανάγκης και φόβου**: Ισχυρίζεται ότι έγινε σύνδεση από μια ύποπτη τοποθεσία (π.χ. Σαγκάη, Κίνα), κάτι που είναι μια συνηθισμένη τακτική εκφοβισμού για να προκαλέσει γρήγορη αντίδραση από το πιθανό θύμα.
- **Ύποπτος αριθμός τηλεφώνου**: Σας ζητά να καλέσετε έναν αριθμό που δεν ανήκει στην Binance (+33392251554). Νόμιμες εταιρείες όπως η Binance **δεν** ζητούν ποτέ από τους χρήστες να καλούν τυχαίους διεθνείς αριθμούς για την ασφάλεια του λογαριασμού τους.
- **Ασυνήθιστος κωδικός αναφοράς**: Η χρήση ενός κωδικού π.χ. "REF/GM22" προσθέτει στην ψεύτικη επείγουσα ανάγκη και νομιμότητα. Αυτό το είδος φράσης είναι χαρακτηριστικό στα μηνύματα phishing.
- **Ασυνέπεια στο στυλ μηνύματος**: Τα νόμιμα μηνύματα Binance πάνω από αυτό είναι σαφή, συνοπτικά και δεν σας ζητούν να προβείτε σε ενέργειες όπως η κλήση ενός αριθμού.

Τι να κάνω:

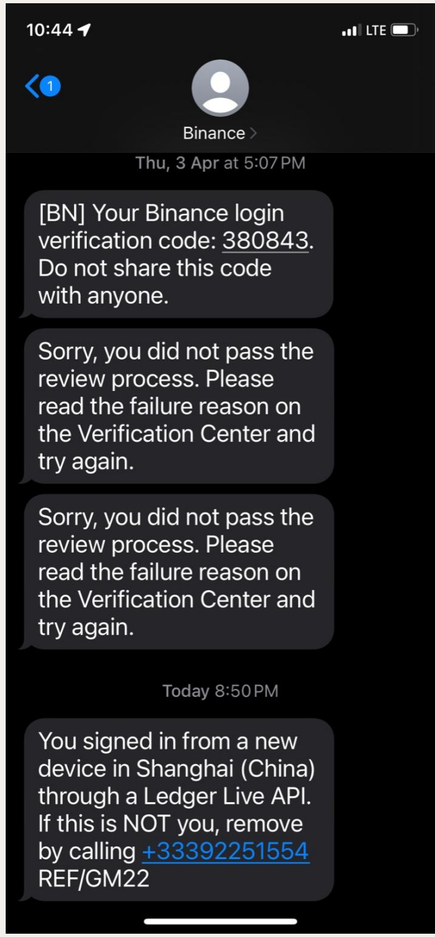
- **Μην καλέσετε τον αριθμό.**
- **Μην κάνετε κλικ σε καμία σύνδεση** εάν το μήνυμα είχε κάποια.
- **Αναφέρετε αμέσως το μήνυμα στην Υποστήριξη της Binance** μέσω του επίσημου ιστότοπού της.
- Εξετάστε το ενδεχόμενο να ενεργοποιήσετε το **2FA (Έλεγχος ταυτότητας δύο παραγόντων)** και να αλλάξετε τον κωδικό πρόσβασής σας στην Binance για κάθε ενδεχόμενο.



Co-funded by the European Union

Πώς να εντοπίσετε τους phishers

Οι απατεώνες μπορούν να **πλαστογραφήσουν τα αναγνωριστικά αποστολέα,** που σημαίνει ότι μπορούν να κάνουν ένα ψεύτικο μήνυμα να **εμφανίζεται κάτω από το ίδιο thread** με τα νόμιμα μηνύματα (όπως αυτά από την Binance).



Πώς το κάνουν:

- **Πλαστογράφηση αποστολέα:** Ο απατεώνας χρησιμοποιεί λογισμικό για να στείλει ένα SMS που φαίνεται να προέρχεται από το "Binance". Τα συστήματα SMS δεν είναι πάντα ασφαλή έναντι τέτοιου είδους τα κόλπων.
- **Αυτόματο νήμα**: Το τηλέφωνό σας ομαδοποιεί τα μηνύματα κατά όνομα/αναγνωριστικό αποστολέα. Επομένως, εάν το πλαστό όνομα ταιριάζει με το "Binance", το τηλέφωνό σας το συνδέει με νόμιμα μηνύματα, ακόμα κι αν στην πραγματικότητα δεν προέρχεται από το Binance.

Γιατί είναι επικίνδυνο:

- Φαίνεται πιο αξιόπιστο επειδή εμφανίζεται στην ίδια συνομιλία.
- Οι άνθρωποι υποθέτουν ότι πρέπει να είναι αληθινό επειδή είναι ομαδοποιημένο με προηγούμενες νόμιμες ειδοποιήσεις.

Τι να κάνω:

- Ελέγχετε πάντα **τα επίσημα κανάλια** (εφαρμογή Binance, ιστότοπος ή επαληθευμένο email υποστήριξης) αντί να εμπιστεύεστε το περιεχόμενο SMS.
- Ποτέ μην καλείτε ή κάνετε κλικ σε οτιδήποτε σε ένα μήνυμα, εκτός εάν είστε απολύτως βέβαιοι ότι προέρχεται από νόμιμη πηγή.

Co-funded by the European Union

Μείνετε ασφαλείς στο διαδίκτυο

✅ Να σκέφτεστε πάντα **πριν κάνετε κλικ**

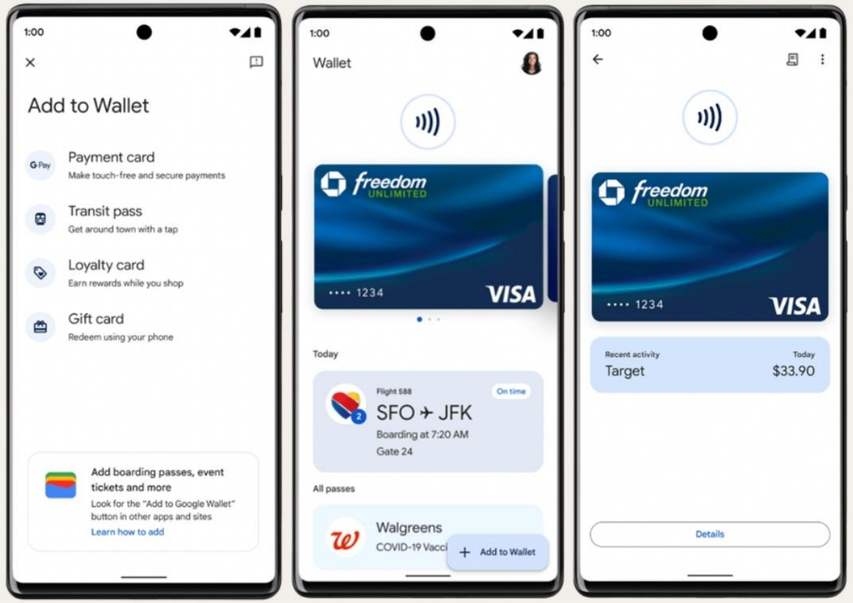
✅ Διατηρήστε **ενημερωμένες τις συσκευές και τα antivirus σας.**

✅ Αναφορά ύποπτων μηνυμάτων ή email

✅ Σε περίπτωση αμφιβολίας - **ζητήστε βοήθεια** (γονείς, τράπεζα ή αρχές)

Co-funded by the European Union

Ψηφιακά πορτοφόλια



Εικόνα: Google
YouTube: Τηλέφωνο, κλειδιά... Πορτοφόλι Google | H Google
https://www.youtube.com/watch?v=3eKF_kEjy-I

➢ Τι είναι ένα ψηφιακό πορτοφόλι;

Ένα ψηφιακό ή ηλεκτρονικό πορτοφόλι είναι μια εφαρμογή ή λογισμικό που αποθηκεύει με ασφάλεια τα στοιχεία πληρωμής σας, όπως πιστωτικές, χρεωστικές ή δωροκάρτες και μερικές φορές ακόμη και άλλα στοιχεία όπως κάρτες επιβράβευσης, εισιτήρια, ταυτότητα και κρυπτονομίσματα.

➢ Πως δουλεύει

- Μόλις προσθέσετε την κάρτα σας, οι συναλλαγές χρησιμοποιούν **tokenization**, το οποίο αντικαθιστά τα πραγματικά στοιχεία της κάρτας σας με ένα μοναδικό διακριτικό. Αυτό διατηρεί τα δεδομένα σας ασφαλή, ακόμα κι αν ένα κατάστημα παραβιαστεί.
- Οι πληρωμές επιβεβαιώνονται χρησιμοποιώντας ασφαλείς **μεθόδους ελέγχου ταυτότητας** όπως Face ID, Touch ID ή PIN.

➢ Καθημερινά παραδείγματα

- **Apple Wallet / Apple Pay** – Αποθηκεύστε και χρησιμοποιήστε κάρτες, ταυτότητες και πάσο απρόσκοπτα και με ασφάλεια.
- **Google Wallet / Google Pay, PayPal, Revolut** – Δημοφιλή ψηφιακά πορτοφόλια που προσφέρουν ανέπαφες πληρωμές, μεταφορές και διαχείριση χρημάτων.

Οφέλη από τη χρήση τους

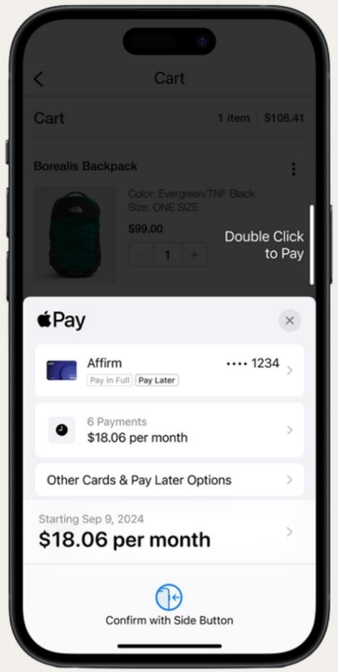
- **Εξαιρετικά γρήγορο και βολικό**:
  Πληρώνετε άμεσα χωρίς να έχετε μαζί σας μετρητά ή κάρτες.

- **Παρακολουθείτε τις δαπάνες σας σε πραγματικό χρόνο**
  Δείτε ακριβώς πού πηγαίνουν τα χρήματά σας - απευθείας από το τηλέφωνό σας.

- **Λαμβάνετε ειδοποιήσεις άμεσης πληρωμής**
  Μπορεί να επιβεβαιώσει ότι η πληρωμή σας ολοκληρώθηκε και το ποσό που χρεωθήκατε

- **Ιδανικό για online αγορές και ταξίδια**
  Ψωνίστε σε όλο τον κόσμο με ασφάλεια και πληρώστε σε πολλά νομίσματα.

- **Εύκολος διαχωρισμός λογαριασμών με φίλους**
  Τέλος στις άβολες συζητήσεις για τα λεφτά - μοιραστείτε τα έξοδα άμεσα



Εικόνα: www.apple.com/apple-pay/

Εικόνα: www.apple.com/wallet/

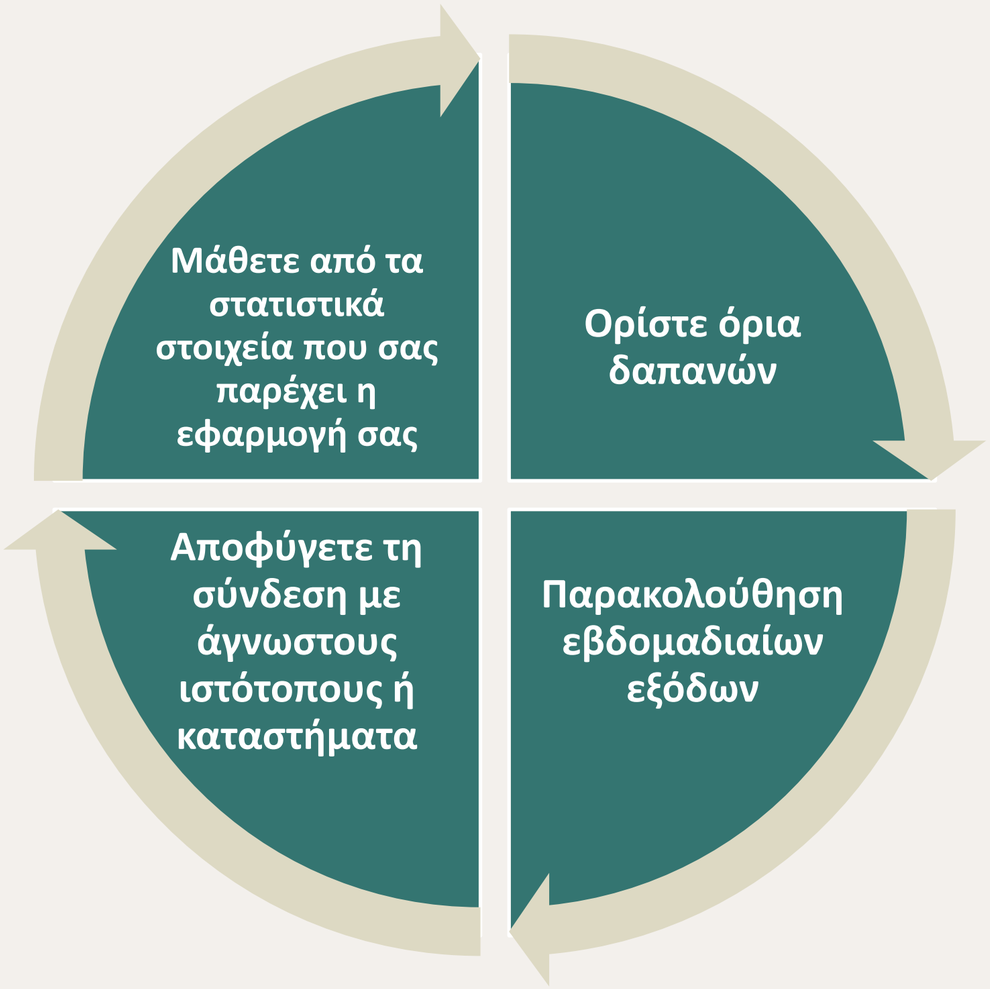
Εικόνα: www.revolut.com/apple-and-google-pay/

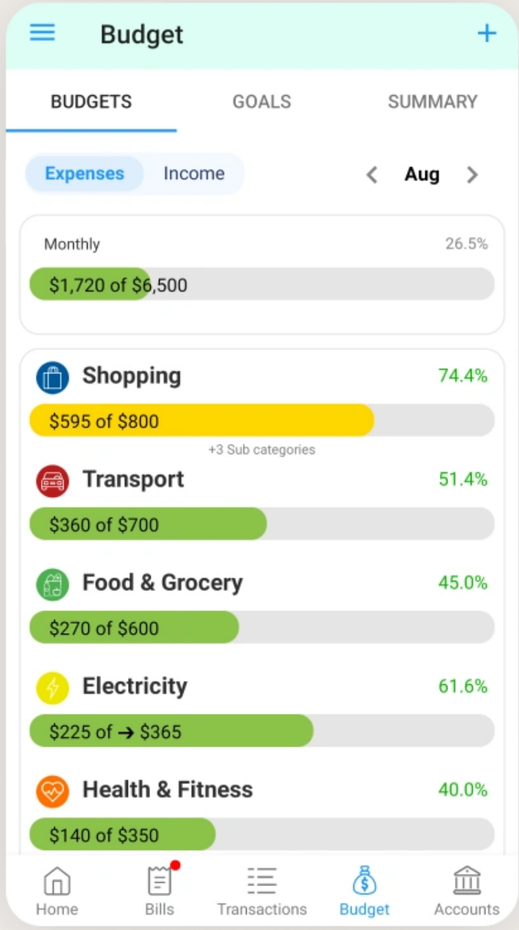
Πώς να τα χρησιμοποιήσετε με ασφάλεια

- Χρησιμοποιήστε ισχυρή ασφάλεια στην συσκευή σας. Κλείδωμα με Face ID, δακτυλικό αποτύπωμα ή PIN
- Ενεργοποίηση ειδοποιήσεων για κάθε συναλλαγή
- Χρησιμοποιήστε έλεγχο ταυτότητας δύο παραγόντων (2FA) και ισχυρούς κωδικούς πρόσβασης
- Λήψη μόνο επίσημων εφαρμογών – Από το Google Play ή το App Store
- Αποφύγετε το δημόσιο Wi-Fi για πληρωμές - Χρησιμοποιήστε δεδομένα κινητής τηλεφωνίας ή προσωπικό δίκυτο

Co-funded by the European Union

Έξυπνες συνήθειες χρημάτων





Εικόνα: www.timelybills.app/budgeting-app

Co-funded by the European Union

Τι είναι το απόρρητο δεδομένων;

Απόρρητο δεδομένων σημαίνει να γνωρίζετε πώς χρησιμοποιούνται, αποθηκεύονται και κοινοποιούνται οι προσωπικές και οικονομικές σας πληροφορίες - και να λαμβάνετε μέτρα για την προστασία τους.

Τα προσωπικά και οικονομικά σας στοιχεία = ευαίσθητα
Στοιχεία όπως το όνομα, η τοποθεσία, τα τραπεζικά στοιχεία και οι συνήθειες δαπανών σας πρέπει να διατηρούνται ασφαλή.

Οι εφαρμογές και οι τράπεζες συλλέγουν δεδομένα για την παροχή υπηρεσιών
Παρακολουθούν τη δραστηριότητά σας για να βελτιώσουν τις λειτουργίες τους - αλλά έχετε το δικαίωμα να ελέγχετε σε τι έχουν πρόσβαση.

Μάθετε τι μοιράζεστε - και με ποιον
Ελέγχετε πάντα τις ρυθμίσεις απορρήτου, τους όρους χρήσης και τα δικαιώματα πριν χρησιμοποιήσετε μια εφαρμογή ή υπηρεσία.

Co-funded by the European Union

Ποιες πληροφορίες πρέπει να προστατεύσετε;

- Ονοματεπώνυμο & διεύθυνση
- Στοιχεία τραπεζικής κάρτας ή λογαριασμού
- Αριθμοί ταυτότητας (διαβατήριο, ταυτότητα)
- Στοιχεία σύνδεσης (email, κωδικοί πρόσβασης)
- Συνήθειες δαπανών & ιστορικό συναλλαγών

Πώς να διατηρήσετε τον έλεγχο

Δεν μπορείτε να σταματήσετε όλη τη συλλογή δεδομένων - αλλά μπορείτε *να* αποφασίσετε ποιος θα πάρει τι.

Πώς να παραμείνετε υπεύθυνοι για το ψηφιακό σας αποτύπωμα:

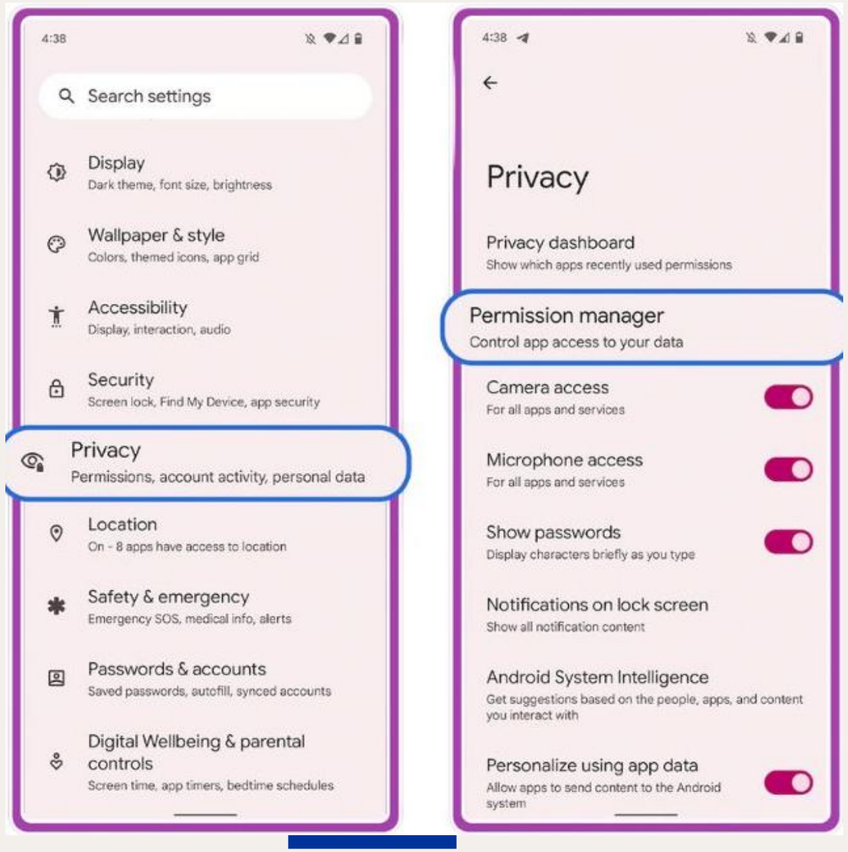
- **Μοιραστείτε πληροφορίες μόνο σε ασφαλείς, αξιόπιστες πλατφόρμες**
  Εάν φαίνεται σκιερό, μάλλον είναι - μην το ρισκάρετε

- **Ελέγξτε τις ρυθμίσεις απορρήτου σε κάθε εφαρμογή**
  Περιορίστε τις εφαρμογές στις οποίες μπορούν να έχουν πρόσβαση (όπως επαφές, φωτογραφίες ή την κάμερά σας)

- **Διαβάστε με τι συμφωνείτε**
  Οι όροι, οι προϋποθέσεις και τα δικαιώματα έχουν σημασία

- **Απενεργοποιήστε την πρόσβαση τοποθεσίας όταν δεν χρειάζεται**
  Το τηλέφωνό σας δεν χρειάζεται να σας παρακολουθεί 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα

- **Να προσέχετε τι δημοσιεύετε στο διαδίκτυο**



Πώς πρέπει να σας προστατεύουν οι πλατφόρμες

Δεν εξαρτάται μόνο από εσάς - οι πλατφόρμες έχουν επίσης την ευθύνη να διατηρούν τα δεδομένα σας ασφαλή. Οι υπεύθυνες πλατφόρμες θα πρέπει πάντα να παρέχουν τις ακόλουθες προστασίες:

Χρησιμοποιούν κρυπτογράφηση για την προστασία των δεδομένων σας
Οι πληροφορίες σας θα πρέπει να είναι κλειδωμένες, ώστε κανείς να μην μπορεί να έχει πρόσβαση σε αυτές χωρίς άδεια.

Σας επιτρέπουν να ενημερώνετε ή να διαγράφετε τα προσωπικά σας δεδομένα
Θα πρέπει να έχετε τον έλεγχο του τι μένει και τι φεύγει.

Να είναι διαφανείς σχετικά με τον τρόπο χρήσης των δεδομένων σας
Χωρίς κρυφή παρακολούθηση - αξίζετε να γνωρίζετε ακριβώς τι συλλέγεται και γιατί.

Παρέχουν πολιτικές απορρήτου σε απλή γλώσσα
Χωρίς νομική ορολογία - μόνο σαφείς, κατανοητές εξηγήσεις των δικαιωμάτων σας.

Co-funded by the European Union

Τι είναι οι οικονομικοί κανονισμοί;

Προστατεύουν τους καταναλωτές:
Οι κανονισμοί βοηθούν στην πρόληψη απατών, απάτης και αθέμιτων πρακτικών

Βεβαιωθείτε ότι οι τράπεζες και οι χρηματοοικονομικές εφαρμογές είναι ασφαλείς και δίκαιες:
Πρέπει να ακολουθούν αυστηρά πρότυπα κατά τη διαχείριση των χρημάτων σας

Επιβάλλεται από τις οικονομικές αρχές:
Οργανισμοί όπως **οι Κεντρικές Τράπεζες ή οι Χρηματοοικονομικές Ρυθμιστικές Αρχές** παρακολουθούν τον τρόπο λειτουργίας των χρηματικών συστημάτων

Co-funded by the European Union

Πώς σας προστατεύουν

✅ Σταματούν τις απάτες και την παράνομη δραστηριότητα

✅ Κάνουν τις εταιρείες να ακολουθούν τους νόμους περί απορρήτου και ασφάλειας

✅ Βεβαιώνουν ότι τα χρήματά σας αντιμετωπίζονται με υπευθυνότητα

✅ Προσφέρουν υποστήριξη όταν οι εταιρείες παραβιάζουν τους κανόνες

Co-funded by the European Union

Τι είναι τα δίχτυα ασφαλείας;

Ένα **δίχτυ ασφαλείας** είναι η προστασία που σας βοηθά όταν συμβαίνουν απροσδόκητα προβλήματα.

Τύποι διχτυών χρηματοοικονομικής ασφάλειας

1. **Εξοικονόμηση έκτακτης ανάγκης:** Χρήματα που προορίζονται για ξαφνικά έξοδα (π.χ. ιατρικοί λογαριασμοί, επισκευές αυτοκινήτων).
2. **Ασφάλιση:** Η ασφάλιση υγείας, αυτοκινήτου ή κατοικίας σας προστατεύει από μεγάλα απροσδόκητα έξοδα.
3. **Κυβερνητικά προγράμματα:** Παροχές όπως το επίδομα ανεργίας ή οι συντάξεις υποστηρίζουν τους ανθρώπους σε δύσκολες στιγμές.
4. **Συστήματα υποστήριξης:** Οικογένεια, κοινότητα ή κοινωνικές ομάδες που παρέχουν βοήθεια όταν χρειάζεται.

Γιατί έχουν σημασία τα δίχτυα ασφαλείας

- Μειώνουν το άγχος και τον οικονομικό κίνδυνο.
- Βοηθούνν να ανακάμπτουμε πιο γρήγορα από τις αναποδιές.
- Δίνουν ηρεμία και σταθερότητα.

Co-funded by the European Union

Γνωρίστε τα όρια

Οι οικονομικοί κανονισμοί βοηθούν - αλλά δεν καλύπτουν τα πάντα
Είναι σημαντικό να γνωρίζετε τι *δεν* προστατεύεται!

Δεν είναι όλες οι εφαρμογές ή πλατφόρμες ελεγχόμενες
Ορισμένα εργαλεία μπορεί να φαίνονται νόμιμα, αλλά λειτουργούν εκτός των κανόνων

Τα κρυπτονομίσματα και οι ξένες ιστοσελίδες ενδέχεται να στερούνται προστασίας
Εάν κάτι πάει στραβά, είναι πιο δύσκολο να πάρετε τα χρήματά σας πίσω

Πρέπει πάντα να παραμένετε σε εγρήγορση και ενημερωμένοι
Διαβάστε κριτικές, κάντε την έρευνά σας και μάθετε τους κινδύνους

Smart + Safe = Η καλύτερη προστασία σας
Όσο περισσότερα γνωρίζετε, τόσο καλύτερα μπορείτε να προστατεύσετε τα οικονομικά σας.

Co-funded by the European Union

ΟΛΟΚΛΗΡΩΝΟΝΤΑΣ

Co-funded by
the European Union

Εκπαιδευτικά Σεμινάρια

Όλοι οι συμμετέχοντες έχουν δικαίωμα να εγγραφούν για ΔΩΡΕΑΝ εκπαίδευση:

Συμμετοχή:

- Κύπρος και Ιρλανδία
- Σε απευθείας σύνδεση

Συνεδρίες:

- 4 διαδικτυακά σεμινάρια
- Συζητήσεις
- Βεβαίωση συμμετοχής

* Κάθε συμμετέχοντας θα πρέπει να συμπληρώσει μια φόρμα σχολίων στο τέλος κάθε webinar

Co-funded by the European Union

Ανατροφοδότηση και μαθήματα

Θα ήμασταν ευγνώμονες για τα σχόλιά σας, προκειμένου να βελτιώσουμε τις μελλοντικές προπονήσεις

SCAN HERE

Η πλατφόρμα class365 περιέχει όλο το εκπαιδευτικό υλικό στα ελληνικά και στα αγγλικά, συμπεριλαμβανομένων ηχογραφήσεων, πόρων και εργαλείων

www.class365.eu

www.learn.finalyproject.eu

SCAN HERE

Co-funded by the European Union

Για περισσότερες πληροφορίες:

www.finalyproject.eu/
www.facebook.com/finalyproject
www.instagram.com/finalyproject/
www.tiktok.com/@finalyproject?lang=en

ecect.projects@gmail.com
+ 357 96520112 (Κύπρος)

Co-funded by
the European Union