«ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

ΤΡΙΤΗ 22 ΑΠΡΙΛΙΟΥ 2024, 10:00 – 11:00

ΛΥΚΕΙΟ ΚΑΙ ΤΕΣΕΚ ΑΓΙΟΥ ΧΑΡΑΛΑΜΠΟΥΣ ΕΜΠΑΣ

ΚΑΘΗΓΗΤΕΣ: ΓΙΟΥΚΚΑ ΜΑΡΙΑ, ΕΥΘΥΜΙΟΥ ΣΤΕΦΑΝΟΣ, ΣΠΥΡΟΥ ΣΠΥΡΟΣ, ΧΑΡΑΛΑΜΠΙΔΗ ΘΕΟΦΑΝΩ

InBusinessNews

Έρευνα: Θύμα κυβερνοεπίθεσης μια στις τέσσερις επιχειρήσεις στην Κύπρο

Αποκαλυπτικά τα ευρήματα της «The Digital Cyprus Survey 2023»

26 Jun 2023

InBusinessNews

Θύμα κυβερνοεπίθεσης μία στις δύο επιχειρήσεις στην Κύπρο- Το κατά μέσο όρο οικονομικό κόστος

Μια στις δύο περίπου επιχειρήσεις στην Κύπρο (49%) δέχτηκαν κάποια είδους κυβερνοεπίθεση/παραβίαση τους τελευταίους 12 μήνες σύμφωνα με...

21 Dec 2023

Philenews

Κυβερνοεπίθεση δέχθηκε το Ανοικτό Πανεπιστήμιο Κύπρου | Φιλελεύθερος

Κυβερνοεπίθεση δέχθηκε χθες το Ανοικτό Πανεπιστήμιο Κύπρου. Σε ανακοίνωση του αναφέρει πως «ο ιστοχώρος, η πλατφόρμα τηλεκπαίδευσης,...

28 Mar 2023

Politis

Επίθεση από χάκερς δέχεται το Κτηματολόγιο - Εκτός λειτουργίας η ιστοσελίδα

Την κατάσταση φαίνεται να ελέγχει η Αρχή Ψηφιακής Ασφάλειας. Κυβερνοεπίθεση δέχεται από χθες το βράδυ η ιστοσελίδα του Τμήματος...

9 Mar 2023

iEidiseis

Μεγάλη διαρροή προσωπικών δεδομένων από το Facebook – «Αλλάξτε τους κωδικούς σας»

Ονόματα, αριθμοί τηλεφώνων, διευθύνσεις email, κωδικοί Facebook και άλλα στοιχεία διέρρευσαν στο Dark Web. Συναγερμός έχει σημάνει για τη...

16 Feb 2024

Kathimerini

https://m.kathimerini.com.cy › kypros · Translate this page

Νέα διαδικτυακή απάτη: Απέσπασαν €80.000 από εταιρεία

14 Sept 2023 — Στις 05 Σεπτεμβρίου, η κυπριακή **εταιρεία** έλαβε μήνυμα ηλεκτρονικού ταχυδρομείου, στο οποίο αναφερόταν όπως τα **χρήματα** για πληρωμή των προϊόντων, ...

Λογικό κανείς να αναρωτιέται ....

- **Γιατί** υπάρχει τόσο πολλή ανησυχία;
- **Ποιο**ι είναι μερικοί από τους κινδύνους τους οποίους πρέπει να προσέξει ο χρήστης του Διαδικτύου;
- **Μήπως** πρέπει αυτοί οι κίνδυνοι να σας κάνουν να μη χρησιμοποιείτε το Διαδίκτυο;

Βασικοί Κίνδυνοι Διαδικτύου / ΤΝ

- ✓ Εθισμός
- ✓ Υποκλοπή προσωπικών δεδομένων (**Phishing**)
- ✓ Παραπληροφόρηση
- ✓ Συνομιλίες με αγνώστους
- ✓ Εκφοβισμός (**Cyberbullying**)
- ✓ Ανεπιθύμητα μηνύματα
- ✓ Αποξένωση από τον πραγματικό κόσμο
- ✓ Παραβίαση πνευματικών δικαιωμάτων
- ✓ Αποπλάνηση (**Grooming**)
- ✓ Ακατάλληλο περιεχόμενο
- ✓ Παιδική Πορνογραφία
- ✓ Παρακίνηση σε επιβλαβείς συμπεριφορές
- ✓ Παραβίαση ιδιωτικότητας
- ✓ Ιοί (**Viruses**)
- ✓ Φυσικές παθήσεις
- ✓ Προκλήσεις στη χρήση της Τεχνητής Νοημοσύνης (**AI**)

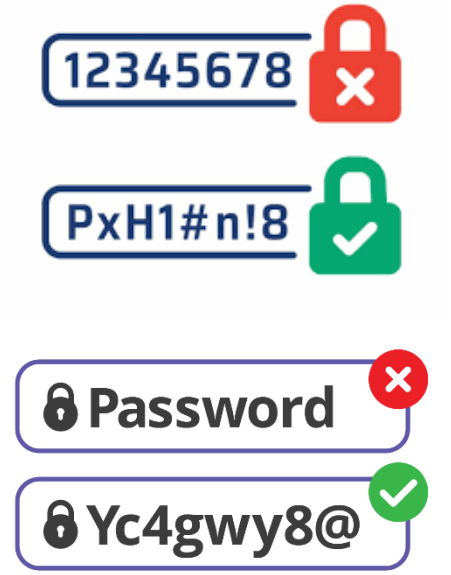
Πως να Παραμείνετε Ασφαλείς στο Διαδίκτυο Εσείς και τα Παιδιά σας

1. Χρησιμοποιείτε **ισχυρούς κωδικούς πρόσβασης.**
2. Κάντε χρήση του **ελέγχου ταυτότητας πολλών παραγόντων** (MFA).
3. Χρησιμοποιήστε τη μέθοδο SLAM για να εντοπίσετε **ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου.**
4. Ασφαλίστε το **πρόγραμμα περιήγησής σας.**
5. Διατηρήστε το πιο **πρόσφατο λογισμικό** στις έξυπνες συσκευές σας.
6. Να γνωρίζετε **ποιες πληροφορίες μοιράζεστε στα μέσα κοινωνικής** δικτύωσης.
7. Αποφύγετε συνομιλίες με αγνώστους.
8. Ποτέ **μην δίνετε προσωπικά σας στοιχεία.**
9. Παραμείνετε **ενημερωμένοι** για τις **Τεχνολογικές Εξελίξεις** της Τεχνητής Νοημοσύνης.
10. Κρατήστε **ανοιχτούς** τους **διαύλους επικοινωνίας**.

Κωδικοί Πρόσβασης

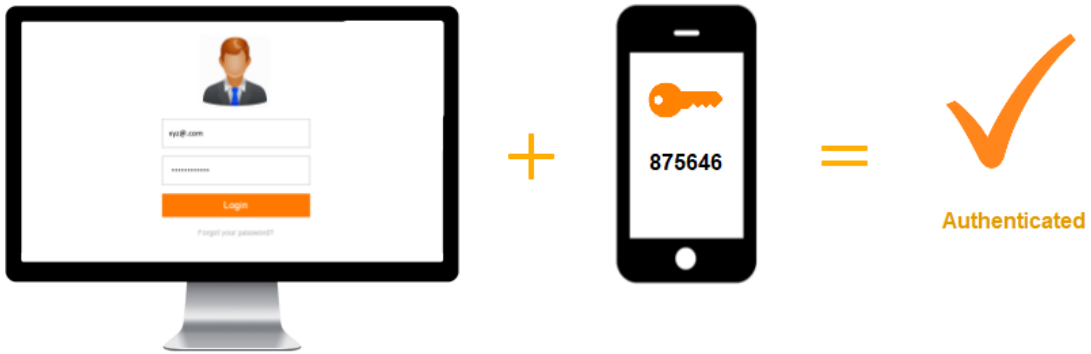
Ισχυροί κωδικοί πρόσβασης

- Θα πρέπει να αποτελούνται από **τουλάχιστον 12 χαρακτήρες** και συστήνεται να μην είναι οι ίδιοι χαρακτήρες σε ακολουθία.
- Να περιέχουν και να συνδυάζουν **γράμματα**, **σύμβολα**, **αριθμούς** και **ειδικούς χαρακτήρες (π.χ** ?, %, *, @**)**.
- Αποφύγετε να χρησιμοποιείτε λέξεις, ειδικά ουσιαστικά.
- Μην συμπεριλάβετε ποτέ στοιχεία προσωπικής ταυτοποίησης.
- Να μην επαναχρησιμοποιούνται.



Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων (MFA)

Ο έλεγχος ταυτότητας πολλών παραγόντων (**Multi-Factor Authentication MFA**) προσθέτει ένα επίπεδο προστασίας στη διαδικασία εισόδου. Κατά την πρόσβαση σε λογαριασμούς ή εφαρμογές, οι χρήστες υποβάλλονται σε πρόσθετες ενέργειες επαλήθευσης ταυτότητας, όπως σάρωση δακτυλικού αποτυπώματος ή εισαγωγή κωδικού που λαμβάνεται μέσω τηλεφώνου.



Η Μέθοδος **SLAM**

Οι επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing) είναι ένα τεράστιο μέρος των σύγχρονων επιθέσεων στον κυβερνοχώρο – ορισμένες είναι εξαιρετικά εξατομικευμένες και μπορεί να περιέχουν αναφορές στα μέλη της οικογένειάς σας, τα χόμπι σας και πολλά άλλα.

Χρησιμοποιήστε τη μέθοδο SLAM για να βοηθήσετε στον εντοπισμό επιθέσεων ηλεκτρονικού ψαρέματος:

- **Sender**: Ελέγξτε τη διεύθυνση (email) του αποστολέα
- **Links**: Τοποθετήστε το δείκτη του ποντικιού και ελέγξτε τυχόν συνδέσμους πριν κάνετε κάποιο κλικ.
- **Attachment**: Μην ανοίγετε συνημμένα από κάποιον που δεν γνωρίζετε ή συνημμένα που δεν περιμένατε.
- **Message**: Ελέγξτε το περιεχόμενο του μηνύματος και προσέξτε για κακή γραμματική ή ορθογραφικά λάθη.

Επιθέσεις ηλεκτρονικού ψαρέματος (**phishing**)

Τετ 25.02.2021 17:04

EuroBank-gr <masayo.t@[redacted].site>

Η πρόσβασή σας δεν είναι ενεργή!

Το [redacted]gr

Eurobank

Αγαπητέ πελάτη

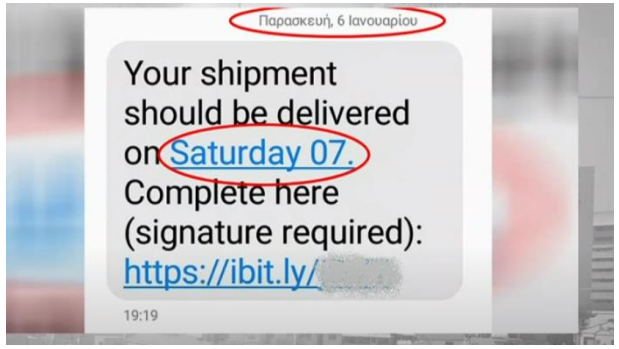
Έχουμε τοποθετήσει προσωρινά κλειδαριά στην κάρτα σας!

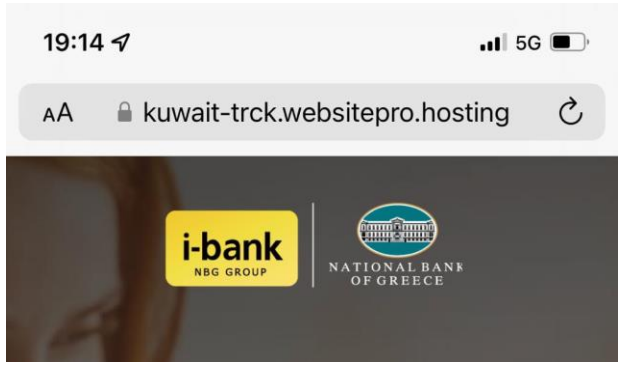
Οι διαδικτυακές πληρωμές και αναλήψεις μετρητών δεν μπορούν να γίνουν έως ότου επιλυθεί αυτό το ζήτημα. Επιβεβαιώστε την πρόσβασή σας εντός των επόμενων 48 ωρών.

Ενεργοποίηση τώρα

Απαντήστε σε αυτό το e-mail εάν έχετε περαιτέρω απορίες ή θέλετε να επικοινωνήσετε μαζί μας.

Θερμούς χαιρετισμούς,
EuroBank





From: Bank of America <crvdgi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Bank of America

Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

http://bit.do/ghsdfhgsd

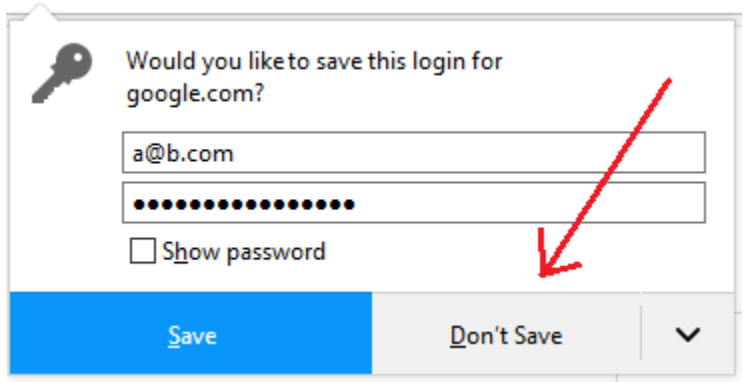
Grammatical Error

Το Πρόγραμμα Περιήγησης (Browser)

Τα προγράμματα περιήγησης ιστού χρησιμοποιούνται συχνά σε εταιρικές και οικιακές συσκευές και οι επιτιθέμενοι θα προσπαθήσουν να εκμεταλλευτούν τις ευπάθειες και κενά ασφαλείας σε αυτά για να πάρουν τον έλεγχο κάποιου λογαριασμού σας.

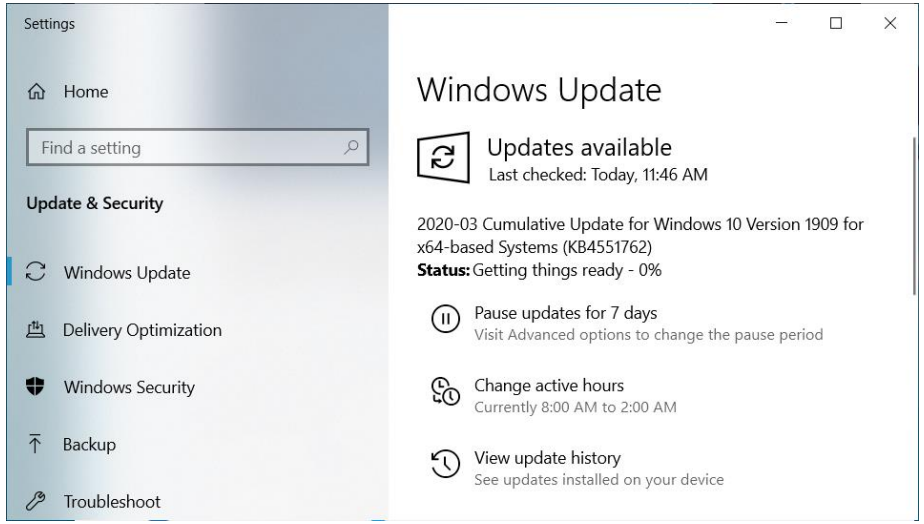
<u>Ο καλύτερος τρόπος για να ασφαλίσετε το πρόγραμμα περιήγησής σας στον ιστό είναι</u>:

1. Να διαμορφώσετε τις **αυτόματες ενημερώσεις**.
2. Να **αποφύγετε την αποθήκευση κωδικών πρόσβασης** στο πρόγραμμα περιήγησής σας.
3. Να **περιορίσετε τις ρυθμίσεις ασφαλείας και δεδομένων** που ανταλλάσσονται με παρόχους προγράμματος περιήγησης.

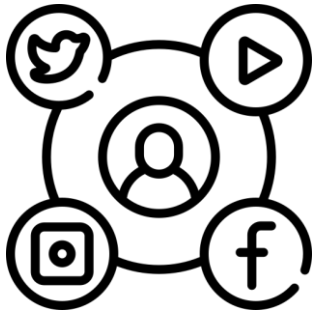


Ενημερώσεις Συσκευών (**Security Updates**)

Για να αποτρέψετε τους εισβολείς να επωφεληθούν από ευπάθειες στις έξυπνες συσκευές σας, **ενημερώστε τηλέφωνα, tablet, τηλεοράσεις, ηχεία κ.λπ. με το πιο πρόσφατο διαθέσιμο λογισμικό**. Εάν είναι διαθέσιμη μια λειτουργία αυτόματης ενημέρωσης, ενεργοποιήστε την. Αυτές οι συσκευές μπορεί ενδεχομένως να αποτελέσουν πηγή μόλυνσης όπως και κάθε άλλος υπολογιστής.



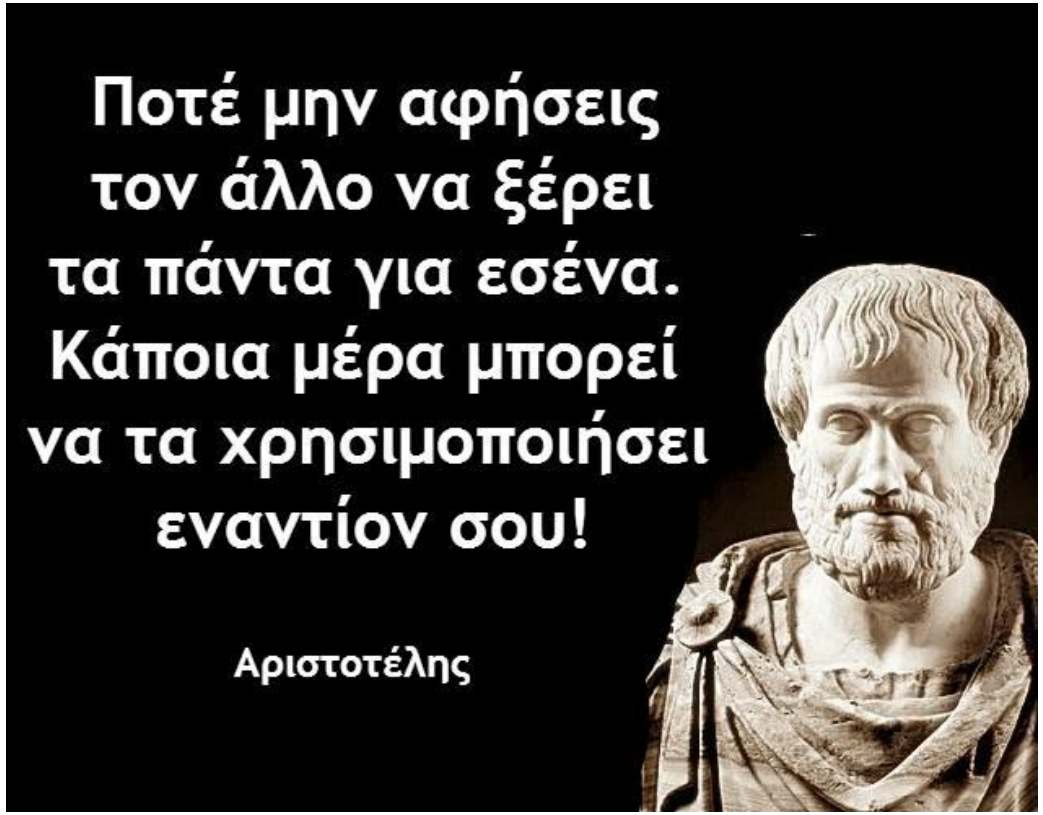
Προσοχή στα Μέσα Κοινωνικής Δικτύωσης!



- Να γνωρίζετε **ποιες πληροφορίες μοιράζεστε** στα μέσα κοινωνικής δικτύωσης.
- Τα μέσα κοινωνικής δικτύωσης μπορεί να είναι ένας πολύ καλός τρόπος για να μοιράζεστε πληροφορίες με την οικογένεια και τους φίλους σας, αλλά **μοιράζεστε και πληροφορίες με τους εισβολείς**;
- **Ελέγξτε τις ρυθμίσεις απορρήτου σας σε επαναλαμβανόμενη βάση**, **διαγράψτε παλιούς και αχρησιμοποίητους λογαριασμούς** και **ελέγξτε τις φωτογραφίες και τα βίντεο σας στο προσκήνιο και στο παρασκήνιο πριν δημοσιεύσετε**, για να βεβαιωθείτε ότι δεν μοιράζεστε τίποτα που θα μπορούσε να αποκαλύψει βασικά στοιχεία προσωπικής ταυτοποίησης.
- Γι' αυτό προσοχή στο τι είδους αναρτήσεις κάνετε. Δεν υπάρχει τρόπος να σβήσουν για πάντα σχόλια και φωτογραφίες που μοιραστήκατε ή ανεβάσατε και τώρα το μετανιώσατε.

*Πριν πάτε να δημοσιεύσετε στα μέσα κοινωνικής δικτύωσης, αναρωτηθείτε – **θα μπορούσαν αυτές οι πληροφορίες που πρόκειται να δημοσιεύσετε να χρησιμοποιηθούν εναντίον σας**;*

Προσοχή στα Μέσα Κοινωνικής Δικτύωσης!



ΠΡΟΣΟΧΗ!!

- **Αποφύγετε** συνομιλίες με αγνώστους.
- Ακόμα και αν είναι φίλος γνωστού σας εμείς σας προτείνουμε να αποφύγετε την επαφή και συνομιλία με άτομα που δεν γνωρίζετε στις πλατφόρμες κοινωνικής δικτύωσης.
- **Ποτέ μην δίνετε τα προσωπικά σας στοιχεία**.
- **Αποφύγετε την δημοσιοποίηση προσωπικών σας στοιχείων** όπως οι ταυτότητα σας, η διεύθυνση σας ή τον αριθμό του τηλεφώνου σας.
- **Δεν δίνουμε ποτέ τους κωδικούς μας σε κανέναν.**
- Μη δίνετε τα στοιχεία σας σε κάποιον που δεν γνωρίζετε!

Παραμείνετε Ενημερωμένοι

- Τόσο οι γονείς όσο και τα παιδιά θα πρέπει να δίνουν **προτεραιότητα στην ψηφιακή παιδεία**.
- Η **κατανόηση του τρόπου λειτουργίας της τεχνητής νοημοσύνης, των πιθανών κινδύνων της, και η αναγνώριση των ευρύτερων διαδικτυακών απειλών** βοηθάει στο να λαμβάνονται ενημερωμένες αποφάσεις και να παραμένουν ασφαλείς.
- **Οι γονείς θα πρέπει να παραμένουν ενήμεροι σχετικά με τις εξελίξεις της τεχνητής νοημοσύνης και τους πιθανούς κινδύνους**. Η κατανόηση του πώς χρησιμοποιείται η ΤΝ σε διάφορες πλατφόρμες μπορεί να βοηθήσει στο να καθοδηγούν τα παιδιά για υπεύθυνη χρήση του διαδικτύου.

ΠΑΙΔΑΓΩΓΙΚΟ ΙΝΣΤΙΤΟΥΤΟ ΚΥΠΡΟΥ

Να Επικοινωνείτε!

- Δημιουργήστε μια **ανοιχτή και ειλικρινή γραμμή επικοινωνίας** μεταξύ γονέων και παιδιών.
- **Ενθαρρύνετε τα παιδιά να μοιράζονται τις online εμπειρίες τους** και εκπαιδεύστε τα για τους πιθανούς κινδύνους χωρίς να προκαλείτε φόβο.
- **Ζητήστε ΒΟΗΘΕΙΑ!**

https://cybercrime.police.gov.cy