«ΠΩΣ ΝΑ ΠΑΡΑΜΕΙΝΕΤΕ ΑΣΦΑΛΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

«ΨΗΦΙΑΚΗ ΕΚΠΑΙΔΕΥΣΗ: ΕΞΕΛΙΞΕΙΣ ΚΑΙ ΠΑΙΔΑΓΩΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ»
ΠΕΜΠΤΗ 8 ΙΟΥΝΙΟΥ 2023

ΔΙΟΡΓΑΝΩΣΗ ΗΜΕΡΙΔΑΣ: ΠΑΙΔΑΓΩΓΙΚΟ ΙΝΣΤΙΤΟΥΤΟ ΚΥΠΡΟΥ

ΚΑΘΗΓΗΤΕΣ: ΧΑΤΖΗΣΟΦΟΚΛΕΟΥΣ ΑΡΙΣΤΟΣ, ΕΥΘΥΜΙΟΥ ΣΤΕΦΑΝΟΣ, ΜΙΧΑΗΛΙΔΗΣ ΧΡΙΣΤΟΣ

28 Μαρτίου 2023, 10:25

philenews

Κυβερνοεπίθεση δέχθηκε χθες το Ανοικτό Πανεπιστήμιο Κύπρου.

Σε ανακοίνωση του αναφέρει πως «ο ιστοχώρος, η πλατφόρμα τηλεκπαίδευσης, οι διαδικτυακές πύλες και το σύστημα υποβολής αιτήσεων υποψηφίων φοιτητών/τριών ΔΕΝ λειτουργούν μέχρι νεοτέρας λόγω περιστατικού κυβερνοεπίθεσης».

Άρπαξαν €23 εκατ. με ηλεκτρονικές απάτες

Πρωτοφανή ποσά έχασαν Κύπριοι από ηλεκτρονικές απάτες εντός του 2022, παρά τις συστάσεις της Αστυνομίας και άλλων οργανισμών, να μην ανταποκρίνονται σε ύποπτα μηνύματα με τα οποία στόχος είναι το «ψάρεμα» ανυποψίαστων πολιτών.

Σοβαρή κυβερνοεπίθεση: Οι χάκερ έριξαν μαύρο στο Πανεπιστήμιο Κύπρου

ΓΙΩΡΓΟΣ ΠΥΡΙΣΙΗΣ Δημοσιεύθηκε 3.3.2023

Νέα διαδικτυακή απάτη - Απέσπασαν 156 χιλιάδες δολάρια από εταιρεία στη Λεμεσό

Από εξετάσεις που έγιναν, διαπιστώθηκε ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου ήταν παραποιημένη

Σοβαρό το ζήτημα – Δεν κινείται φύλλο λόγω της κυβερνοεπίθεσης

ΓΡΑΦΕΙ Ο ΧΑΡΑΛΑΜΠΟΣ ΖΑΚΟΣ

«Κτύπησαν τον πνεύμονα της Οικονομίας». Αυτό ήταν το σχόλιο του **Διευθυντή του Τμήματος Κτηματολογίου, Ελίκκου Ηλία**, στην **Brief**, το οποίο περιγράφει πλήρως τη σοβαρότητα του **προβλήματος** συνεπεία της **κυβερνοεπίθεσης** στο Κτηματολόγιο.

Είναι Γεγονός ότι ....

- Η επανάσταση του Διαδικτύου έχει μεταμορφώσει τον τρόπο με τον οποίο επικοινωνεί και συναλλάσσεται ο κόσμος.
- Το Διαδίκτυο αποτελεί πολύτιμο εργαλείο στη σημερινή μας κοινωνία.
- Γενικά, <u>όσο πιο ισχυρό είναι ένα εργαλείο, τόσο πιο επικίνδυνο μπορεί να γίνει</u>. Ένα βενζινοκίνητο αλυσοπρίονο μπορεί να κάνει πολύ περισσότερα από ένα χειροπρίονο, ωστόσο πρέπει να χρησιμοποιείται προσεκτικά. Παρόμοια, το Διαδίκτυο είναι εξαιρετικά ισχυρό και χρήσιμο, αλλά πρέπει να ενεργούμε με σύνεση όταν το χρησιμοποιούμε, καθώς εγκυμονεί σοβαρούς κινδύνους.

Λογικό κανείς να αναρωτιέται ....

- Γιατί υπάρχει τόσο πολλή ανησυχία;
- Ποιοι 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;

Σήμερα θα Δούμε …

- **Δράσεις** από τη Συμμετοχή της ΤΕΣΕΚ Πάφου στο πρόγραμμα «Ασφαλές Σχολείο για το Διαδίκτυο».
- **Αποτελέσματα** από Έρευνα ανάμεσα στους μαθητές του σχολείου.
- Ποιοι είναι μερικοί από τους κινδύνους τους οποίους πρέπει να προσέξει ένας χρήστης του Διαδικτύου; Πως μπορεί κανείς να παραμείνει Ασφαλής καθώς χρησιμοποιεί τις υπηρεσίες του Διαδικτύου;
- **Στόχοι και Επιδιώξεις** για τη Συνέχεια.

Πρόγραμμα: Ασφαλές Σχολείο για το Διαδίκτυο

- Στόχος του Προγράμματος Ασφαλές σχολείο για το Διαδίκτυο (Οκτώβριος 2022 – Μάιος 2023) είναι να εισαγάγει τα σχολεία σε διαδικασία ανάληψης δράσης για την προώθηση της ασφαλούς χρήσης του διαδικτύου στο περιβάλλον του σχολείου.

- Στόχος, επίσης, του Προγράμματος είναι να βοηθήσει το σχολείο να αξιοποιήσει τις δυνατότητες του διαδικτύου αλλά και να προλάβει ή και να αντιμετωπίσει προβλήματα που μπορούν να προκύψουν και αφορούν στη χρήση των σύγχρονων τεχνολογιών.

Το σχολείο μας, επιλέγοντας να συμμετάσχει στο Πρόγραμμα «Ασφαλές σχολείο για το διαδίκτυο», διεκδικεί ***πιστοποίησή ως Ασφαλές Σχολείο για το Διαδίκτυο***.

Μερικές Από τις Δράσεις του Προγράμματος

- **Συμμετοχή σε Διαδικτυακές Επιμορφώσεις** Συντονιστών Προγράμματος
- **Αποτίμηση Αναγκών**: Διεξαγωγή Έρευνας για τη Χρήση του Διαδικτύου από τους μαθητές
- **Μαθησιακές Παρεμβάσεις** σε όλους τους μαθητές του σχολείου στα πλαίσια σχετικών Επιμορφώσεων
- **Επιμορφώσεις Μαθητών και Εκπαιδευτικών** από Επίσημους Φορείς
  - 23 Δεκεμβρίου 2022 – Αρχή Ψηφιακής Ασφάλειας
  - 23 Μαρτίου 2023 – ΑΤΗΚ
- **Δημιουργία Πολιτικής Ορθής Χρήσης (ΠΟΧ)** για την ΤΕΣΕΚ Πάφου
- **Συμμετοχή σε Ενδοτμηματικές Εκδηλώσεις** την Ημέρα Ασφαλούς Διαδικτύου [07/02/2023]
- **Ενημερωτικό Υλικό σε Εκπαιδευτικούς και Γονείς / Κηδεμόνες**

Με μια ματιά …

7 Μήνες Δραστηριοτήτων (Πλάνο Δράσεων – Διάρκεια Προγράμματος)

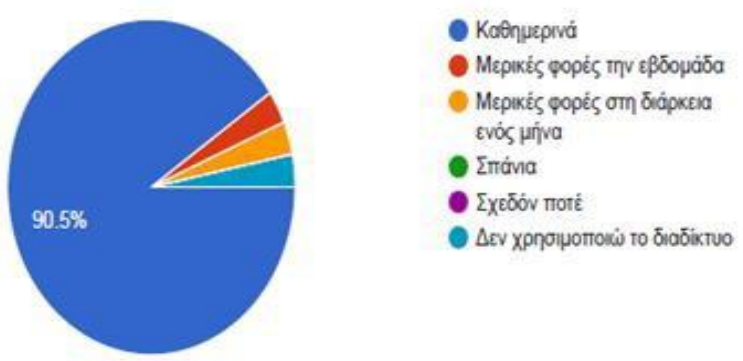
2 Εξειδικευμένα Επιμορφωτικά Σεμινάρια (ΑΨΑ, ΑΤΗΚ)

18 Εκπαιδευτικοί συμμετείχαν στις Μαθησιακές Παρεμβάσεις

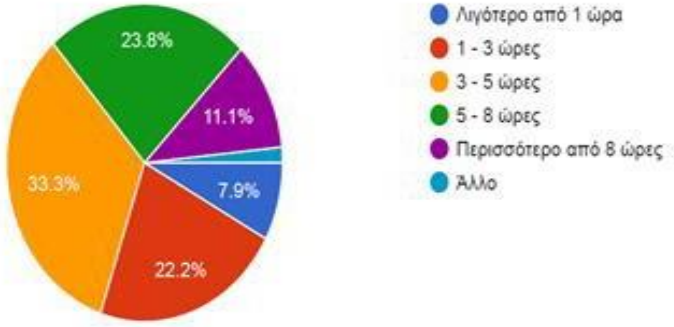
46 Τμήματα Μαθητών συμμετείχαν στις Μαθησιακές Παρεμβάσεις

600+ Μαθητές έτυχαν επιμόρφωσης

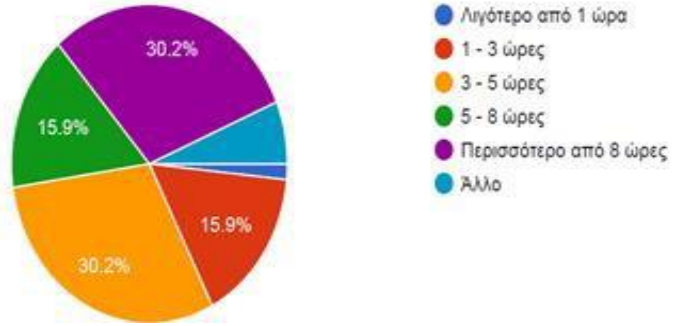
Πόσο συχνά χρησιμοποιώ το διαδίκτυο;



Κατά μέσο όρο αφιερώνω καθημερινά στη χρήση του διαδικτύου:

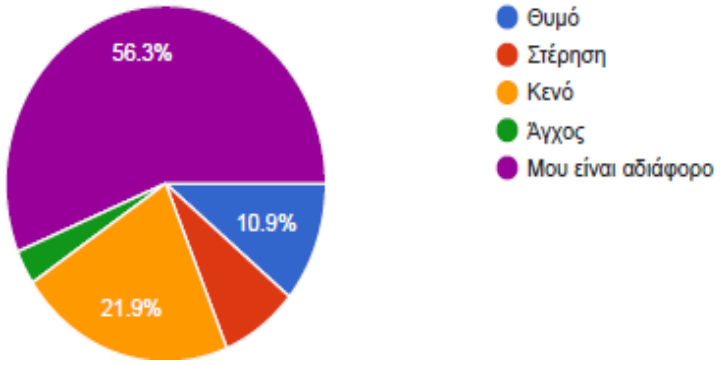


Κατά μέσο όρο αφιερώνω στη χρήση του διαδικτύου σε μέρες που δεν έχω σχολείο όπως π.χ Σαββατοκύριακα και αργίες:

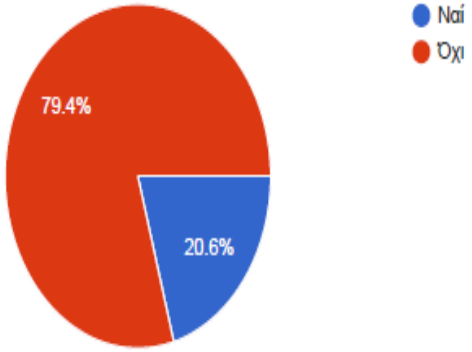


Αποτελέσματα Έρευνας [Νοέμβριος – Δεκέμβριος 2022]

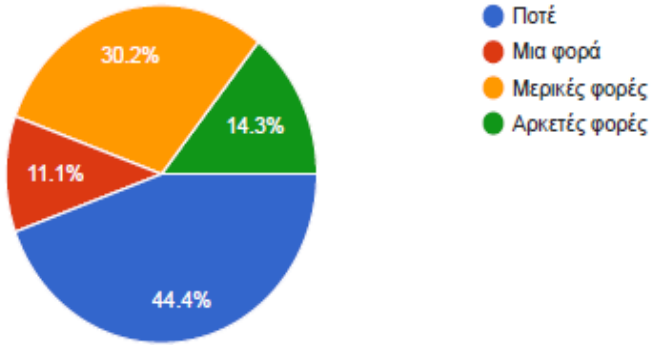
Όταν δεν έχω πρόσβαση στο διαδίκτυο αισθάνομαι:



Οι γονείς/κηδεμόνες μου ελέγχουν τις δραστηριότητες μου στο διαδίκτυο:

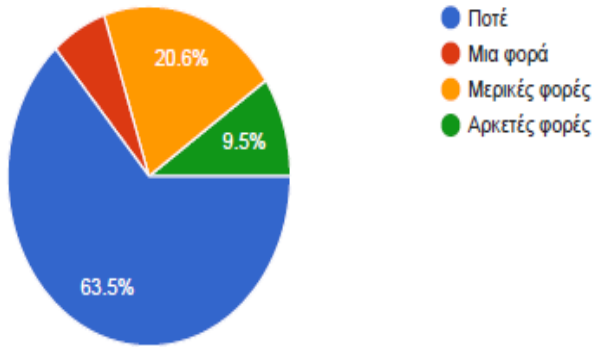


Εχω συναντήσει για γνωριμία άγνωστα άτομα με τα οποία συνομιλούσα στο διαδίκτυο

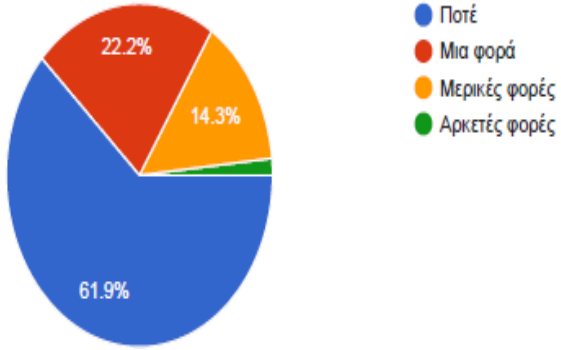


Αποτελέσματα Έρευνας [Νοέμβριος – Δεκέμβριος 2022]

Έχω ανταλλάξει προσωπικές μου φωτογραφίες με άγνωστα άτομα τα οποία γνώρισα στο διαδίκτυο



Έχω αντιμετωπίσει προβλήματα με ηλεκτρονικές συναλλαγές (π.χ εξαπατήθηκα, με ξεγέλασαν).



Απαντώντας ειλικρινά θα έλεγα ότι:

Αποτελέσματα Έρευνας [Νοέμβριος – Δεκέμβριος 2022]

~ 30% των Μαθητών Παραδέχεται Εθισμό στο Διαδίκτυο

Βασικοί Κίνδυνοι Διαδικτύου

- ✓ Εθισμός
- ✓ Υποκλοπή προσωπικών δεδομένων
- ✓ Παραπληροφόρηση
- ✓ Συνομιλίες με αγνώστους
- ✓ Εκφοβισμός
- ✓ Ανεπιθύμητα μηνύματα
- ✓ Αποξένωση από τον πραγματικό κόσμο
- ✓ Παραβίαση πνευματικών δικαιωμάτων
- ✓ Αποπλάνηση
- ✓ Ακατάλληλο περιεχόμενο
- ✓ Παρακίνηση σε επιβλαβείς συμπεριφορές
- ✓ Παραβίαση ιδιωτικότητας
- ✓ Ιοί
- ✓ Φυσικές παθήσεις

Πως να Παραμείνετε Ασφαλείς στο Διαδίκτυο

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. Να Διατηρείτε Εφεδρικά Αρχεία Ασφαλείας

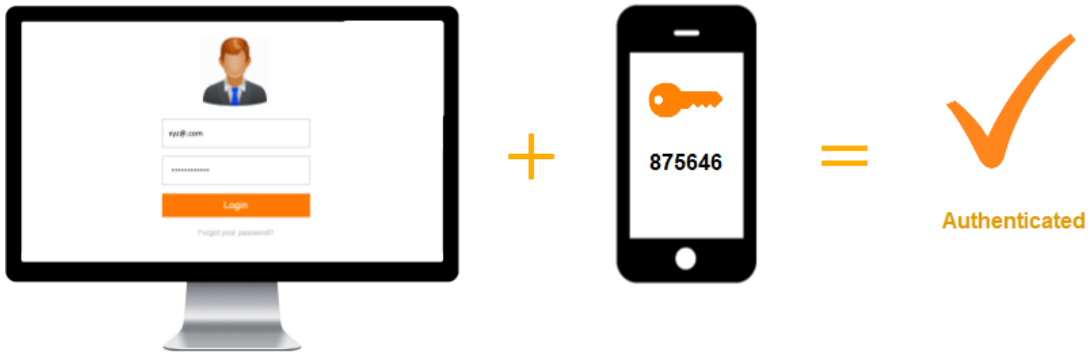
Κωδικοί Πρόσβασης

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.
- Αποφύγετε να χρησιμοποιείτε λέξεις, ειδικά ουσιαστικά.
- Μην συμπεριλάβετε ποτέ στοιχεία προσωπικής ταυτοποίησης.
- Να μην επαναχρησιμοποιούνται.

Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων

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.

Το Πρόγραμμα Περιήγησης (Browser)

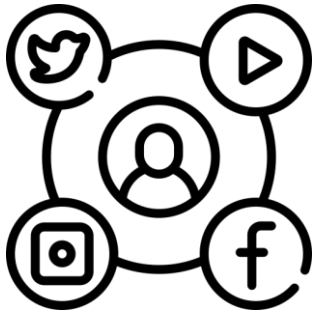
Τα προγράμματα περιήγησης ιστού χρησιμοποιούνται συχνά σε εταιρικές και οικιακές συσκευές και οι επιτιθέμενοι θα προσπαθήσουν να εκμεταλλευτούν τις ευπάθειες και κενά ασφαλείας σε αυτά για να πάρουν τον έλεγχο κάποιου λογαριασμού σας. Ο καλύτερος τρόπος για να ασφαλίσετε το πρόγραμμα περιήγησής σας στον ιστό είναι να διαμορφώσετε τις αυτόματες ενημερώσεις, να αποφύγετε την αποθήκευση κωδικών πρόσβασης στο πρόγραμμα περιήγησής σας και να περιορίσετε τις ρυθμίσεις ασφαλείας και δεδομένων που ανταλλάσσονται με παρόχους προγράμματος περιήγησης.

"Φροντίστε να έχετε πάντα τη τελευταία έκδοση του browser που χρησιμοποιείτε, αποφεύγετε την αποθήκευση των κωδικών σας & ενισχύστε τα privacy setting (ρυθμίσεις ιδιωτικότητας).

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. Όπως δεν υπάρχει και το «για πάντα»…Προσοχή λοιπόν, μην κάνετε αναρτήσεις που δεν θα θέλατε να δουν οι γονείς ή ένας μελλοντικός εργοδότης σας. Το ψηφιακό αποτύπωμα διαρκεί πολύ περισσότερο απ ’όσο πιστεύετε.

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

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. Δε δίνουμε ποτέ τους κωδικούς μας σε κανέναν. Μη δίνετε τα στοιχεία σας σε κάποιον που δεν γνωρίζετε!

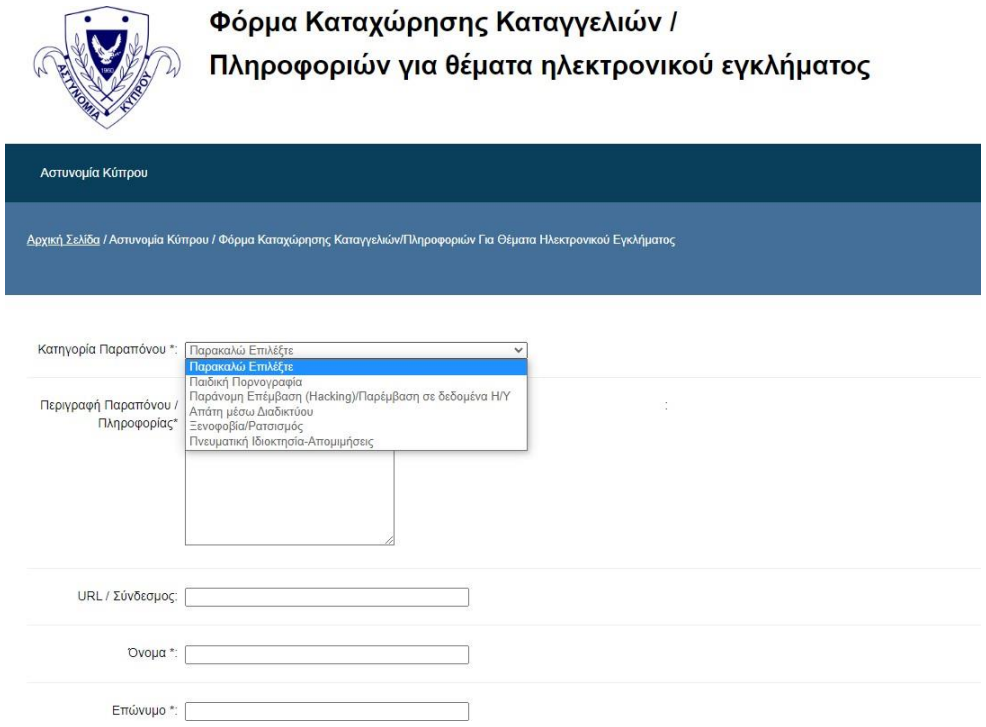
Πως να Παραμείνετε Ασφαλείς στο Διαδίκτυο

Μην παραλείπετε την τακτική λήψη αντιγράφων ασφαλείας των δεδομένων σας.

Τα αντίγραφα μπορούν να αποθηκευτούν σε σκληρούς δίσκους ή σε κάποιο Cloud πάροχο. Έτσι διασφαλίζετε ότι ακόμα κι αν «μπει» κάποιος στο σπίτι σας, δεν θα χάσετε την αξία των πραγμάτων του.

Δεν είστε Μόνοι …

https://cybercrime.police.gov.cy



Στόχοι και Επιδιώξεις

1. **Καθιέρωση** Επιμορφωτικών Προγραμμάτων για Μαθητές και Εκπαιδευτικούς σε θέματα Πρόληψης και Λήψης Μέτρων Αντιμετώπισης σε Περίπτωση Διαδικτυακής Απάτης.
2. **Υιοθέτηση** Έξυπνων Μαθησιακών Παρεμβάσεων για συναφή θέματα Ασφαλούς Χρήσης του Διαδικτύου.
3. **Πρόληψη και Καταπολέμηση** του φαινομένου του Εθισμού στο Διαδίκτυο.
4. **Εγκαθίδρυση Αμφίδρομης Επικοινωνίας** μεταξύ Γονέων/Κηδεμόνων και Εκπαιδευτικών αναφορικά με θέματα που αφορούν τους μαθητές σχετικά με τη χρήση του Διαδικτύου.
5. **Ανάπτυξη Δεξιοτήτων** για Αναγνώριση και Αντιμετώπιση πιθανών Κινδύνων και Απειλών στο Διαδίκτυο, από Μαθητές και Εκπαιδευτικούς.
6. **Καλλιέργεια Κουλτούρας** για την Ορθή Χρήση των υπηρεσιών του Διαδικτύου από όλα τα μέλη της Σχολικής Κοινότητας.

Πρόληψη ή Θεραπεία;

➔*Αναγνωρίζοντας και προλαμβάνοντας τους κινδύνους στο διαδίκτυο μπορούμε να αποφύγουμε πολλά προβλήματα και να Παραμείνουμε Ασφαλείς καθώς απολαμβάνουμε τις υπηρεσίες του!*

Ευχαριστούμε για την Προσοχή σας!
Συζήτηση - Ερωτήσεις