*Μάρτιος 2022*

**ΔΕΛΤΙΟ ΤΥΠΟΥ**

**Συμβουλές για προστασία από διαδικτυακές απάτες**

Σε έξαρση βρίσκονται οι απάτες μέσω ηλεκτρονικών συναλλαγών οι οποίες μάλιστα μεταλλάσσονται διαρκώς, με συνέπεια καθημερινά πολίτες να χάνουν χρήματα. Είτε μέσω γνωστών επιχειρήσεων ή χρηματοπιστωτικών ιδρυμάτων, είτε μέσω ψεύτικων αγγελιών ή απατηλών email, επιτήδειοι αποκτούν πρόσβαση στα προσωπικά και περιουσιακά στοιχεία των θυμάτων τους.

Οι οικονομικές απάτες αποτέλεσαν κατά το 2021 το 28% των συνολικών καταγγελιών που έλαβε η Ανοιχτή γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο [SafeLine.gr](https://www.safeline.gr/). Από αυτές, το 40% των καταγγελιών αφορούσε κάτι που συνέβη στο Instagram και το 39% κάποια ενέργεια στο Facebook.



## **Θύμα οικονομικής απάτης πέφτουν πολύ συχνά και οι έφηβοι**

Σύμφωνα με τα αποτελέσματα πανελλήνιας έρευνας που πραγματοποιήθηκε το Νοέμβριο -Δεκέμβριο του 2021 σε ένα δείγμα 5000 μαθητών ηλικίας 12-18 ετών, το 10% των παιδιών δηλώνει ότι έχει πέσει θύμα απάτης στο διαδίκτυο. Συγκεκριμένα το 28% από τους εφήβους που δηλώνουν ότι έχουν πέσει θύματα απάτης, δηλώνει ότι έχει πέσει θύμα οικονομικής απάτης στο διαδίκτυο.





Το [Ελληνικό Κέντρο Ασφαλούς Διαδικτύου του ΙΤΕ](https://saferinternet4kids.gr/) συστήνει στους πολίτες να είναι ενημερωμένοι για τις απάτες που κυκλοφορούν, να επιδεικνύουν ιδιαίτερη προσοχή στην επικοινωνία μέσω ηλεκτρονικών μηνυμάτων, να μην παρέχουν προσωπικά στοιχεία σε τρίτους και να επιλέγουν ισχυρούς κωδικούς πρόσβασης.

**Απάτες phishing μέσω ηλεκτρονικού ταχυδρομείου, μέσων κοινωνικής δικτύωσης, τηλεφωνικής κλήσης ή μηνύματος κειμένου**

Ένας απατεώνας επικοινωνεί μαζί σας προσποιούμενος ότι προέρχεται από κάποια (συνήθως) γνωστή επιχείρηση, όπως μια τράπεζα, ένας πάροχος υπηρεσιών τηλεφώνου ή διαδικτύου.

* Ο επιτήδειος σας ζητά να δώσετε ή να επιβεβαιώσετε τα προσωπικά σας στοιχεία.
* Για παράδειγμα, μπορεί να ισχυριστεί ότι η τράπεζα ή ο οργανισμός επαληθεύει τα αρχεία πελατών λόγω τεχνικού σφάλματος.
* Ή, μπορεί να σας ζητήσουν να συμπληρώσετε μια έρευνα πελατών και να σας προσφέρουν ένα βραβείο για τη συμμετοχή.
* Εναλλακτικά, ο επιτήδειος μπορεί να σας ειδοποιήσει για «μη εξουσιοδοτημένη ή ύποπτη δραστηριότητα στον λογαριασμό σας».
* Μπορεί να σας πουν ότι έχει γίνει μια μεγάλη αγορά σε μια ξένη χώρα και να σας ρωτήσουν εάν εξουσιοδοτήσατε την πληρωμή.

 Εάν απαντήσετε ότι δεν το κάνατε, θα σας ζητηθεί να επιβεβαιώσετε τα στοιχεία της πιστωτικής σας κάρτας ή της τράπεζας, ώστε η δήθεν «τράπεζα» να μπορέσει να διερευνήσει. Σε ορισμένες περιπτώσεις, ο απατεώνας μπορεί να έχει ήδη τον αριθμό της πιστωτικής σας κάρτας και να σας ζητήσει να επιβεβαιώσετε την ταυτότητά σας αναφέροντας τον 3 ή 4ψήφιο κωδικό ασφαλείας που είναι τυπωμένος στην κάρτα.

Τα μηνύματα **ηλεκτρονικού ψαρέματος** έχουν σχεδιαστεί για να φαίνονται γνήσια και συχνά αντιγράφουν τη μορφή που χρησιμοποιείται από τον οργανισμό που o επιτήδειος προσποιείται ότι αντιπροσωπεύει, συμπεριλαμβανομένης της επωνυμίας και του λογότυπου.

 Θα σας μεταφέρουν σε έναν ψεύτικο ιστότοπο που μοιάζει με τον πραγματικό ιστότοπο του οργανισμού, αλλά έχει μια ελαφρώς διαφορετική διεύθυνση. Για παράδειγμα, εάν ο νόμιμος ιστότοπος είναι "https://www.winbank.gr", ο απατεώνας μπορεί να χρησιμοποιήσει μια διεύθυνση όπως "http://www.winbanks.com".

Εάν παρέχετε στον απατεώνα τα στοιχεία σας στο διαδίκτυο ή μέσω τηλεφώνου, θα τα χρησιμοποιήσει για να προβεί σε δόλιες δραστηριότητες, όπως η χρήση των πιστωτικών καρτών σας και η κλοπή των χρημάτων σας.

**Ύποπτα σημάδια**

* Λαμβάνετε ένα email, ένα μήνυμα κειμένου ή ένα τηλεφώνημα που ισχυρίζεται ότι προέρχεται από τράπεζα, πάροχο τηλεπικοινωνιών ή άλλη επιχείρηση με την οποία συναλλάσσεστε τακτικά, ζητώντας σας να ενημερώσετε ή να επαληθεύσετε τα στοιχεία σας.
* Το email ή το μήνυμα κειμένου δεν εμπεριέχει ολόκληρο το όνομά σας και ενδέχεται να περιέχει ορθογραφικά ή άλλα γραμματικά λάθη.
* Η διεύθυνση του ιστότοπου δεν μοιάζει με τη διεύθυνση που χρησιμοποιείτε συνήθως και ζητά λεπτομέρειες που συνήθως δεν ζητά ο νόμιμος ιστότοπος.

**Πώς να προστατευτείτε**

* Μην κάνετε κλικ σε συνδέσμους ή μην ανοίξετε συνημμένα από μηνύματα ηλεκτρονικού ταχυδρομείου ή SMS που ισχυρίζονται ότι προέρχονται από την τράπεζά σας ή άλλον αξιόπιστο οργανισμό και σας ζητούν να ενημερώσετε ή να επαληθεύσετε τα στοιχεία σας – απλώς διαγράψτε τα .
* Κάντε μια αναζήτηση στο Διαδίκτυο χρησιμοποιώντας τα ονόματα ή την ακριβή διατύπωση του email ή του μηνύματος για να ελέγξετε για τυχόν αναφορές σε απάτη – πολλές απάτες μπορούν να εντοπιστούν με αυτόν τον τρόπο.
* Αναζητήστε το σύμβολο ασφαλείας. Οι ασφαλείς ιστότοποι μπορούν να αναγνωριστούν με τη χρήση του 'https:' αντί του 'http:' στην αρχή της διεύθυνσης Διαδικτύου ή ενός κλειστού λουκέτου ή ενός εικονιδίου χωρίς σπασίματα στην κάτω δεξιά γωνία του παραθύρου του προγράμματος περιήγησής σας. Οι νόμιμοι ιστότοποι που σας ζητούν να καταχωρίσετε εμπιστευτικές πληροφορίες είναι γενικά κρυπτογραφημένοι για την προστασία των στοιχείων σας.
* Ποτέ μην παρέχετε τα προσωπικά σας στοιχεία, τα στοιχεία της πιστωτικής κάρτας ή του λογαριασμού σας στο διαδίκτυο, εάν λάβετε κλήση που ισχυρίζεστε ότι προέρχεται από την τράπεζά σας ή οποιονδήποτε άλλο οργανισμό. Αντίθετα, ζητήστε το όνομά τους και τον αριθμό επικοινωνίας τους και κάντε έναν ανεξάρτητο έλεγχο με τον εν λόγω οργανισμό πριν καλέσετε ξανά.

**Εχετε πέσει θύμα;**

Εάν πιστεύετε ότι έχετε πέσει θύμα τέτοιας απάτης  επικοινωνήστε αμέσως με τον νόμιμο οργανισμό για να τον ενημερώστε για την απάτη, ώστε να προβεί στις απαραίτητα βήματα μπλοκαρίσματος καρτών ή και άλλων ενεργειών. Επίσης μπορείτε να κάνετε καταγγελία στην Δίωξη Ηλεκτρονικού Εγκλήματος.

Σας προτρέπουμε επίσης να αναφέρετε τις απάτες στην Γραμμή καταγγελιών παράνομου περιεχομένου στο διαδίκτυο [**www.safeline.gr**](https://www.safeline.gr) μέσω της σελίδας αναφοράς απάτης. Αυτό μας βοηθά να προειδοποιούμε τους ανθρώπους για τρέχουσες απάτες, να παρακολουθούμε τις τάσεις και να διακόπτουμε τις απάτες όπου είναι δυνατόν. H [**SafeLine**](https://www.safeline.gr) παρέχει επίσης οδηγίες για την προστασία σας από απάτες και πού να λάβετε βοήθεια.

Σε μια [ειδικά διαμορφωμένη σελίδα στο site του SaferInternet4Kids.gr](https://saferinternet4kids.gr/scams/) παρέχεται ενημέρωση για τις συχνότερες απαντώμενες απάτες στον κυβερνοχώρο αλλά για τους τρόπους αναγνώρισης και πρόληψης τους.



Επίσης μέσα από δυο ευφάνταστα βίντεο, με χιούμορ, απλό και κατανοητό λόγο που δημιούργησε το Ελληνικό κέντρο Ασφαλούς διαδικτύου και η Αρχή κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης επιχειρείται η επιμόρφωση των πολιτών σε θέματα δημιουργίας και σωστής χρήσης ισχυρών κωδικών πρόσβασης καθώς και η εκπαίδευση τους στο να αναγνωρίζουν το phishing στο διαδίκτυο και το smishing (διαδικτυακές απάτες μέσω sms).

Μπορείτε να δείτε τα βίντεο [εδώ](https://youtu.be/dS-R8J7t5-w) και [εδώ](https://youtu.be/LRnUDB6PTiI).

*Σας υπενθυμίζουμε ότι το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, είναι επίσημος εκπρόσωπος στην Ελλάδα των Πανευρωπαϊκών Οργανισμών INSAFE / INHOPE που χαράσσουν την ευρωπαϊκή στρατηγική για ένα ασφαλές και ποιοτικό διαδίκτυο και παρέχει ενημέρωση, βοήθεια και υποστήριξη στους μικρούς και μεγάλους χρήστες του διαδικτύου με την ανάπτυξη τριών διακριτών δράσεων:*

*Μέσω της ιστοσελίδας* [*SaferInternet4Kids.gr*](file:///C%3A%5CUsers%5Ckpsaroudak%5CDownloads%5CSaferInternet4Kids.gr) *μπορεί κανείς να ενημερωθεί και να αντλήσει υλικό σχετικό με την ασφαλή χρήση του Ίντερνετ και τη χρήση των κοινωνικών δικτύων με το οποίο μπορεί με τη σειρά του να ενημερώσει διαδραστικά παιδιά και νέους κάθε ηλικίας. Το ενημερωτικό αυτό portal απευθύνεται τόσο σε γονείς και εκπαιδευτικούς όσο και σε εφήβους και παιδιά και περιλαμβάνει κατάλληλο πολυμεσικό υλικό.*

*Μέσω της συμβουλευτικής γραμμής Βοήθειας Ηelp-line (διαθέσιμη τηλεφωνικά στο 210-6007686 και μέσω του ιστοχώρου* [*www.help-line.gr*](file:///C%3A%5CUsers%5Ckpsaroudak%5CDownloads%5Cwww.help-line.gr)*), εξειδικευμένοι ψυχολόγοι παρέχουν υποστήριξη και συμβουλές για εξειδικευμένα θέματα που σχετίζονται με τη υπερβολική ενασχόληση στο διαδίκτυο, τον διαδικτυακό εκφοβισμό, την έκθεση σε ακατάλληλο περιεχόμενο και άλλους προβληματισμούς σχετικά με τη χρήση του διαδικτύου, του κινητού τηλεφώνου και των διαδικτυακών παιχνιδιών.*

*Και μέσω της Ανοιχτής Γραμμής Καταγγελιών για το παράνομο περιεχόμενο του διαδικτύου SafeLine (*[*http://www.safeline.gr*](http://www.safeline.gr)*), δέχεται καταγγελίες για παιδική κακοποίηση και παράνομη χρήση του διαδικτύου και συνεργάζεται τόσο με την Ελληνική αστυνομία όσο και με την INTERPOL μέσω του Ευρωπαϊκού οργανισμού INHOPE. H SafeLine είναι δηλαδή ένα κομμάτι ενός μεγάλου παζλ, μιας και η καταπολέμηση του παράνομου περιεχομένου του Ίντερνετ είναι υπόθεση παγκόσμιας κλίμακας και δεν περιορίζεται από εθνικά σύνορα.*

*Μάθετε νέα και άλλες ενδιαφέρουσες πληροφορίες από τη σελίδα μας στο Facebook* [*(https://www.facebook.com/SaferInternet4Kids-233337290392828)*](file:///C%3A%5CUsers%5Ckpsaroudak%5CDownloads%5C%28https%3A%5Cwww.facebook.com%5CSaferInternet4Kids-233337290392828%29)*, στο Instagram (*[*https://instagram.com/saferinternet4kids\_gr?utm\_medium=copy\_link*](https://l.facebook.com/l.php?u=https%3A%2F%2Finstagram.com%2Fsaferinternet4kids_gr%3Futm_medium%3Dcopy_link%26fbclid%3DIwAR2AQp1lwKvK6tOOHGBeeXIFgye7ieaEfQTHMd-7Q7TAZtu0Z_VwLQCxDg0&h=AT0D4BdKh7CdSuDUBpS9b5CrXzgCHzTqUO0I7mT3ZgCbMKZQq9JWRet57Z3yLBkgV24DVCbcccN3De9lYgBU2pMlQBgSdm9L_jt_2VDJaaWuXSdcONwDjuM2i8-bbdkXq-Pzrac6sL5ZE1h-Uog)*) και ακολουθήστε μας στο Twitter (*[*https://twitter.com/SaferInt4Kids*](https://twitter.com/SaferInt4Kids)*).*

**Την αποκλειστική ευθύνη της παρούσας έκδοσης φέρει ο συγγραφέας της. Η Ευρωπαϊκή Ένωση δεν φέρει καμία ευθύνη για οποιαδήποτε χρήση των περιεχομένων σ' αυτήν πληροφοριών.**