

ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΓΟΡΕΣ



Προστατέψτε τις κάρτες σου, όπως θα προστάτευες τα μετρητά σου.

Μην αποθηκεύεις ή σημειώνεις τον κωδικό σου PIN.

Ποτέ μην αποκαλύπτεις το PIN σου σε οποιονδήποτε.

Αποθήκευσε τον αριθμό επικοινωνίας της Υπηρεσίας αποκλεισμού καρτών (της τράπεζάς σου).

Εξοικειώσου με τους γενικούς όρους και προϋποθέσεις της κάρτας σου.

Πάντα να διατηρείς την κάρτα σου στην κατοχή σου.

Όρισε όρια ανάληψης και αγορών στην κάρτα σου που ανταποκρίνονται στις ανάγκες σου.

Οι κάρτες που έχουν λήξει πρέπει να ακυρώνονται με κοπή σε πολλά κομμάτια, ώστε η μαγνητική λωρίδα και το chip να καταστρέφονται.

Μόνο εγκληματίες θα ζητήσουν τους κωδικούς της ηλεκτρονικής τραπεζικής σου ή τα στοιχεία της κάρτας σου μέσω ηλεκτρονικού ταχυδρομείου ή τηλεφώνου. Ούτε η τράπεζά σου ούτε οι αστυνομικές αρχές θα σου ζητήσουν ποτέ κάτι τέτοιο.

Αν έχεις αποκαλύψει τους κωδικούς της ηλεκτρονικής τραπεζικής σου ή τα στοιχεία της κάρτας σου σε άγνωστο άτομο, ακύρωσε την κάρτα και επικοινωνήσε αμέσως με την τράπεζά σου.

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΣΦΑΛΗΣ ONLINE ΣΥΝΑΛΛΑΓΕΣ

Αγόρασε από αξιόπιστες πηγές.

Πραγματοποίησε αγορές από εταιρείες και καταστήματα που γνωρίζεις ή που έχεις αγοράσει ξανά και έλεγξε τις αξιολογήσεις κάθε πωλητή σε ιστοσελίδες όπως Amazon και eBay.

Έλεγξε τις επαναλαμβανόμενες χρεώσεις.

Πριν δώσεις τα στοιχεία της κάρτας σου για την πληρωμή μιας επαναλαμβανόμενης υπηρεσίας μέσω διαδικτύου, ψάξε τον τρόπο διακοπής αυτής.

Πολλά διαδικτυακά καταστήματα ζητούν την αποθήκευση των στοιχείων πληρωμής.

Σκέψου διπλά πριν αποφασίσεις και βεβαιώσου ότι κατανοείς τους κινδύνους που ελλοχεύουν.

Χρησιμοποίησε κάρτες κατά τις διαδικτυακές αγορές.

Οι περισσότερες κάρτες διαθέτουν ισχυρή πολιτική προστασίας πελάτη. Εάν δεν λάβεις το προϊόν που έχεις παραγγείλει, ο εκδότης της κάρτας θα σε αποζημιώσει.

Βεβαιώσου για την ασφαλή διαδικασία μεταφοράς δεδομένων.

Αναζήτησε το σύμβολο του λουκέτου στη γραμμή URL και τη χρήση των πρωτοκόλλων HTTPS και SSL κατά την περιήγηση στο διαδίκτυο.

ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΓΟΡΕΣ



Αποθήκευε πάντα όλα τα παραστατικά (έγγραφα) που σχετίζονται με διαδικτυακές αγορές.

Ενδέχεται να χρειαστούν για τον καθορισμό των όρων και προϋποθέσεων της αγοράς ή για την απόδειξη της πληρωμής των προϊόντων.

Εάν δεν αγοράζεις συγκεκριμένο προϊόν ή υπηρεσία, μην υποβάλλεις τα στοιχεία της κάρτας σου.

Όταν αγοράζεις μέσω διαδικτύου από ιδιώτη, μη στέλνεις χρήματα προκαταβολικά στον πωλητή. Εάν είναι δυνατό, διατήρησε το δικαίωμα της πρότερης παραλαβής των προϊόντων (διαδικασία αντικαταβολής).

Μην στέλνεις χρήματα σε κάποιον που δε γνωρίζεις.

Εάν κάποιος σε προσεγγίσει μέσω διαδικτύου και σου ζητήσει χρήματα σκέψου εάν θα έδινες μετρητά σε άγνωστο πρόσωπο στο δρόμο.

Ποτέ μη δίνεις τον αριθμό της κάρτας σου, το PIN ή οποιαδήποτε άλλη πληροφορία για την κάρτα, μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Απόφυγε διαδικτυακές αγορές σε ιστοσελίδες που δεν χρησιμοποιούν πλήρη αυθεντικοποίηση (Verified by Visa/Mastercard Secure Code).

Ποτέ μη στέλνεις στοιχεία της κάρτας σου, με μη κρυπτογραφημένο ηλεκτρονικό ταχυδρομείο (e-mail).

Μερικά διαδικτυακά καταστήματα εκτός Ευρώπης, ίσως αιτηθούν την αποστολή μέσω fax, αντιγράφου της κάρτας ή του διαβατηρίου σου, ως εγγύηση.



ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Τ.Κ. 115 22, Αθήνα
e-mail: ccu@cybercrimeunit.gov.gr / Τηλ.: **11188** / Fax: **2131527471**

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Τ.Κ. 54 121, Θεσσαλονίκη
e-mail: ydheve@cybercrimeunit.gov.gr / Τηλ.: **11188** / Fax: **2131527666**

www.cyberkid.gov.gr / www.cyberalert.gr
<https://www.facebook.com/cyberkid.gov.gr/> / <https://www.facebook.com/CyberAlertGR/>
<https://www.instagram.com/cyberalert.gr/> / <https://twitter.com/CyberAlertGR>
<https://www.youtube.com/channel/UCSEctiscTH8tkxzBzX8gVcQ>

ΑΠΑΤΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ



Όπως συμβαίνει στον πραγματικό κόσμο έτσι και στο Διαδίκτυο, υπάρχουν απατεώνες που έχουν σκοπό να κλέψουν τα προσωπικά σας στοιχεία (όνομα, τηλέφωνο, διεύθυνση κ.λπ.), τα χρήματά σας, ή και τα δύο. Γι' αυτό απαιτείται μεγάλη προσοχή όταν surfάρουμε στο Διαδίκτυο.

Η απάτη στο συμβατικό κόσμο είναι ένα από τα πιο συνηθισμένα εγκλήματα. Η εμφάνιση, όμως, και ανάπτυξη του Διαδικτύου, μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης.

ΟΙ ΚΥΡΙΟΤΕΡΕΣ ΜΟΡΦΕΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΑΠΑΤΗΣ ΕΙΝΑΙ ΟΙ ΑΚΟΛΟΥΘΕΣ

Ισπανικό Λόττο

«Νιγηριανή» απάτη

Spamming

Phishing προσωπικών στοιχείων

Απάτες με ψευδείς διαγωνισμούς για δωροεπιταγές από γνωστές αλυσίδες καταστημάτων - σούπερ μάρκετ

Διαδικτυακή απάτη που υπόσχεται δωρεάν αεροπορικά εισιτήρια

Απάτη με ταξιδιωτικά πακέτα διακοπών.

Απάτες με δήμεν αγορές - πωλήσεις αυτοκινήτων

Απάτες με αγγελίες ενοικίασης σπιτιών μέσω διαδικτύου

Απάτες με προγνωστικά αθλητικών αγώνων

Απάτες με πρόφαση τις διαδικτυακές γνωριμίες

Απάτες με χορήγηση δανείων από μη αδειοδοτημένους φορείς

Απάτες με τη μέθοδο του «ενδιάμεσου» - εξαπάτηση επαγγελματιών στο διαδίκτυο (Business e-mail Compromise-BEC)

Απάτες με Θέσεις εργασίας



ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Τ.Κ. 115 22, Αθήνα
e-mail: ccu@cybercrimeunit.gov.gr / Τηλ.: **11188** / Fax: **2131527471**

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Τ.Κ. 54 121, Θεσσαλονίκη
e-mail: ydheve@cybercrimeunit.gov.gr / Τηλ.: **11188** / Fax: **2131527666**

www.cyberkid.gov.gr / www.cyberalert.gr
<https://www.facebook.com/cyberkid.gov.gr/> / <https://www.facebook.com/CyberAlertGR/>
<https://www.instagram.com/cyberalert.gr/> / <https://twitter.com/CyberAlertGR>
<https://www.youtube.com/channel/UCSEctiscTH8tkxzBzX8gVcQ>