ΤΡΑΠΕΖΑ EUROBANK Α.Ε.
Όθωνος 8, 105 57 Αθήνα
Αρ. Γ.Ε.ΜΗ. 154558160000
eurobank.gr

ΟΔΗΓΙΕΣ ΠΡΟΛΗΨΗΣ ΑΠΑΤΗΣ ΓΙΑ ΣΥΝΑΛΛΑΓΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Αγαπητοί συνεργάτες,

Ικανοποιώντας την ανάγκη για εκπαίδευση σε θέματα που αφορούν τις συναλλαγές ηλεκτρονικού εμπορίου και έχοντας σαν στόχο τη διασφάλιση των συναλλαγών από πιθανή απάτη αλλά και την καλύτερη δυνατή ενημέρωσή σας, σας μεταφέρουμε μερικές χρήσιμες οδηγίες και επισημάνσεις σχετικά με τον τρόπο που θα πρέπει να πραγματοποιούνται οι συγκεκριμένες συναλλαγές:

- Ενεργοποιήστε τη δυνατότητα IP Address blocking, ώστε να αποκλείονται, εάν κριθεί αναγκαίο, οι συναλλαγές με «ύποπτη» ή ασυνήθιστη προέλευση (π.χ. συναλλαγές από χώρες της Αφρικής και της Νοτιοανατολικής Ασίας).

- Επιβεβαιώνετε, εάν είναι δυνατόν, τα στοιχεία ταυτότητας του πελάτη – κατόχου πιστωτικής κάρτας (π.χ. με την αποστολή φωτοαντίγραφου της ταυτότητας ή του διαβατηρίου).

- Αντιμετωπίζετε με ιδιαίτερη προσοχή τις συναλλαγές που παρουσιάζουν ιδιαιτερότητες, όπως π.χ.:
  - ✓ ασυνήθιστη χώρα προέλευσης.
  - ✓ μεγάλο πλήθος και αξία συναλλαγών ανά πιστωτική κάρτα.
  - ✓ παραγγελία πολλών και ετερόκλητων προϊόντων.
  - ✓ μεγάλη συχνότητα συναλλαγών με την ίδια κάρτα.
  - ✓ διαφορετική διεύθυνση παραλαβής από τη διεύθυνση του πελάτη.
  - ✓ πελάτες με ξενικά ονόματα που επιθυμούν να παραλάβουν τα εμπορεύματα σε καταστήματα εταιρειών courier ή σε περιοχές του κέντρου της Αθήνας (π.χ. Ομόνοια , Κυψέλη , Εξάρχεια κ.λπ.).
  - ✓ χώρα προέλευσης (Client IP Address) διαφορετική από αυτή που καταχωρείται από τον πελάτη.

- Προβαίνετε σε ταυτοποίηση του παραλήπτη κατά την παράδοση των προϊόντων και αρχειοθετείτε τα σχετικά παραστατικά.

- Αναφέρετε στο site την επωνυμία της επιχείρησης, ώστε να αποφεύγονται τυχόν αμφισβητήσεις συναλλαγών στην περίπτωση που η επωνυμία δεν προκύπτει από το url address.

- Πραγματοποιείτε συναλλαγές που αφορούν αποκλειστικά και μόνον προϊόντα και υπηρεσίες που προσφέρει η επιχείρηση.

- Πιστοποιήστε την επιχείρησή σας βάσει του προτύπου ασφαλείας PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS), το οποίο έχει δημιουργηθεί από τους Διεθνείς Οργανισμούς Πληρωμών (Visa, MasterCard κ.ά.). Επισκεφθείτε για περισσότερες πληροφορίες τον δικτυακό τόπο www.pcisecuritystandards.org. Ενδεικτικά μέτρα ασφαλείας με τα οποία θα πρέπει να συμμορφώνεστε παρατίθενται στο **Παράρτημα 2**.

- Μη διστάζετε να απευθύνεστε στην Τράπεζα πριν από κάθε συναλλαγή που κρίνετε σαν «ύποπτη» γιατί έτσι προφυλάσσονται και τα δύο μέρη από πιθανή απάτη (τηλ. επικοινωνίας **214-4059040, FTV@eurobank-cards.gr**). Για αναλυτικότερες οδηγίες, βλ. **Παράρτημα 1**.

Σε περίπτωση που λάβετε ενημέρωση από την τεχνική σας εταιρεία για την ύπαρξη κώδικα στην ιστοσελίδα σας και υποψία υποκλοπής στοιχείων καρτών, παρακαλούμε όπως επικοινωνήσετε ΑΜΕΣΑ με την Τράπεζα.

Τμήμα Ελέγχου Συναλλαγών: Τηλ. 214-4059040, Email: FTV@eurobank-cards.gr

Σας Ευχαριστούμε,

Τμήμα Ηλεκτρονικού Εμπορίου

Στη διάθεσή σας για κάθε διευκρίνιση.

ΠΑΡΑΡΤΗΜΑ 1

Σε περίπτωση που σας δημιουργηθούν υποψίες αναφορικά με την αυθεντικότητα κάποιας συναλλαγής και επιθυμείτε να αποστείλετε αίτημα για επιβεβαίωση στοιχείων του πελάτη προς το Τμήμα Ελέγχου Συναλλαγών, παρακαλούμε να συμπληρώνετε την παρακάτω φόρμα για κάθε συναλλαγή ξεχωριστά και να την αποστέλλετε στην ηλεκτρονική διεύθυνση **FTV@eurobank-cards.gr** με subject: ΕΠΙΒΕΒΑΙΩΣΗ ΣΤΟΙΧΕΩΝ ΣΥΝΑΛΛΑΓΗΣ / MERCHANT TITLE_ TRANS ID.

Η συμπλήρωση των πεδίων με αστερίσκο (*) είναι υποχρεωτική.

ΦΟΡΜΑ ΕΠΙΒΕΒΑΙΩΣΗΣ ΣΤΟΙΧΕΩΝ ΠΕΛΑΤΗ

Παρακαλώ όπως προβείτε σε επιβεβαίωση των στοιχείων του κατόχου της κάρτας για την παρακάτω συναλλαγή που πραγματοποιήθηκε στο ηλεκτρονικό κατάστημα της εταιρείας μας **mid: xxxxxxxxxx.**

Στοιχεία Συναλλαγής:	
Ημερομηνία Συναλλαγής*:	
Ποσό Συναλλαγής*:	
Trans id*:	
Αριθμός κάρτας (masked card):	

Στοιχεία τιμολόγησης / κατόχου κάρτας (BILLING ADDRESS):	
Ονομ/μο κατόχου κάρτας*:	
Διεύθυνση κατόχου κάρτας*:	

Τα στοιχεία παράδοσης είναι διαφορετικά από τα στοιχεία τιμολόγησης / κατόχου κάρτας*:

☐ **ΝΑΙ** ☐ **ΟΧΙ**

(Σε περίπτωση που τα στοιχεία τιμολόγησης είναι διαφορετικά από τα στοιχεία παράδοσης)

Στοιχεία παράδοσης εμπορευμάτων / παροχής υπηρεσιών (SHIPPING ADDRESS):	
Ονομ/μο παραλήπτη*:	
Διεύθυνση παραλήπτη*:	

Προϊόν ή υπηρεσία:
(Συνοπτική περιγραφή του προϊόντος αγοράς ή της παρεχομένης υπηρεσίας)

Όνομα Εκπροσώπου επικοινωνίας

Τηλέφωνο επικοινωνίας

ΠΑΡΑΡΤΗΜΑ 2

Ενδεικτικά μέτρα ασφαλείας του προτύπου ασφαλείας PCI DSS, με τα οποία θα πρέπει να συμμορφώνονται οι εμπορικές επιχειρήσεις που δέχονται, επεξεργάζονται, αποθηκεύουν ή μεταδίδουν δεδομένα καρτών πληρωμής:

- Οι υποδομές του συγκεκριμένου ηλεκτρονικού καταστήματος θα πρέπει να προστατεύονται από network firewall τελευταίας τεχνολογίας.

- Όλες οι συνδέσεις προς το ηλεκτρονικό κατάστημα πρέπει να είναι secure (HTTPS) και να είναι ενεργοποιημένο το πρωτόκολλο TLSv1.2 μόνο.

- Τα διάφορα συστήματα της υποδομής του ηλεκτρονικού καταστήματος θα πρέπει να έχουν εγκατεστημένο και ενημερωμένο λογισμικό anti-virus στην τελευταία έκδοση (όπου υποστηρίζεται).

- Θα πρέπει να είναι ενημερωμένα τα συστήματα της υποδομής του ηλεκτρονικού καταστήματος με όλα τα διαθέσιμα security updates από τον αντίστοιχο κατασκευαστή / προμηθευτή.

- Θα πρέπει να δημιουργηθεί σχετική διαδικασία είτε για χειροκίνητη είτε για αυτόματη εγκατάσταση των security updates μέσα σε έναν μήνα από την ανακοίνωσή τους από τον αντίστοιχο κατασκευαστή / προμηθευτή.

- Θα πρέπει να εκτελείται μία φορά τον χρόνο τουλάχιστον – ή οποτεδήποτε άλλοτε χρειάζεται λόγω σημαντικών αλλαγών ή αναβαθμίσεων των συστημάτων – συνολικός έλεγχος ασφαλείας (vulnerability security assessment) από σχετική εξειδικευμένη εταιρεία.

- Η πρόσβαση στα συστήματα της υποδομής του ηλεκτρονικού καταστήματος θα πρέπει να γίνεται με μοναδικό κωδικό χρήστη και κωδικό πρόσβασης (username και password) για κάθε υπάλληλο.

- Οι κωδικοί πρόσβασης (password) θα πρέπει να είναι τουλάχιστον 8 χαρακτήρες σε μήκος και να περιέχουν γράμματα, αριθμούς και σύμβολα. Οι παραπάνω ρυθμίσεις θα πρέπει να είναι υποχρεωτικές.

- Οι υπάλληλοι που έχουν πρόσβαση στα συστήματα της υποδομής του ηλεκτρονικού καταστήματος θα πρέπει να είναι οι ελάχιστοι απαραίτητοι. Οι διαχειριστές, αντίστοιχα, θα πρέπει να είναι οι ελάχιστοι απαραίτητοι.

- Όλοι οι φάκελοι και τα αρχεία στα συστήματα της υποδομής του ηλεκτρονικού καταστήματος θα πρέπει να έχουν περιορισμούς στην πρόσβαση από τους χρήστες (access rights), με δικαιώματα ορισμένα στα απολύτως ελάχιστα για να λειτουργούν τα συστήματα.