Οδηγίες για ασφαλείς συναλλαγές Ηλεκτρονικού Εμπορίου (e-Commerce Gateway / Payment Link)

Διασφαλίστε ότι οι συναλλαγές ηλεκτρονικού εμπορίου της επιχείρησής σας διενεργούνται με ασφάλεια, ακολουθώντας ορισμένους βασικούς κανόνες:

1. **Αντιμετωπίστε με ιδιαίτερη προσοχή τις συναλλαγές που παρουσιάζουν ιδιαιτερότητες**, όπως:
   - Ασυνήθιστη χώρα προέλευσης. Ενεργοποιήστε τη δυνατότητα IP Address blocking, ώστε να αποκλείονται οι συναλλαγές με ασυνήθιστη προέλευση, όπου κρίνεται αναγκαίο.
   - Μεγάλο πλήθος, συχνότητα και αξία συναλλαγών ανά κάρτα ή πολλαπλές συναλλαγές ίδιου ποσού με διαφορετικές κάρτες.
   - Παραγγελία πολλών και ετερόκλητων προϊόντων.
   - Μη υπαρκτά ονόματα π.χ. μόνο με σύμφωνα /φωνήεντα ή επαναλαμβανόμενους χαρακτήρες στα πεδία των στοιχείων του πελάτη (ονοματεπώνυμο, cardholder's name, e-mail κ.λ.π).
   - Συναλλαγές στις οποίες δηλώνονται ασυνήθιστα ή μη αληθοφανή ονόματα στα πεδία των στοιχείων του πελάτη και η παραλαβή των εμπορευμάτων ζητείται να γίνει σε υποκαταστήματα εταιρειών courier ή σε περιοχές με υψηλή εγκληματικότητα.
   - Διαφορετικά στοιχεία πληρωτή και παραλήπτη (ονοματεπώνυμο, διευθύνσεις) σε συνδυασμό με κάποια από τις παραπάνω συνθήκες.

2. **Προβείτε σε ταυτοποίηση του παραλήπτη κατά την παράδοση των προϊόντων**, με βάση τα στοιχεία της παραγγελίας (ονοματεπώνυμο, διεύθυνση παράδοσης).

3. **Αναφέρετε στον ιστότοπο της επιχείρησής σας την επωνυμία ή το διακριτικό τίτλο της**, ώστε να αποφεύγονται τυχόν αμφισβητήσεις συναλλαγών, στην περίπτωση που η επωνυμία ή ο διακριτικός τίτλος δεν προκύπτει από την ηλεκτρονική διεύθυνση του ιστοτόπου (domain).

4. **Πραγματοποιήστε συναλλαγές** αποκλειστικά και μόνο για προϊόντα και υπηρεσίες, για τις οποίες **η επιχείρηση σας έχει συμβληθεί με την Worldline Greece**.

5. **Ακολουθήστε τις οδηγίες που τυχόν σας αποστέλλονται από την Worldline Greece ή/και τον προμηθευτή της πλατφόρμας e-Commerce Gateway**, για την ορθή λειτουργία της πλατφόρμας.

6. **Αποφύγετε τις πληκτρολογημένες συναλλαγές. Οι πληκτρολογημένες συναλλαγές (MOTO: Mail order /Telephone order) ενέχουν σημαντικό ρίσκο,** το οποίο αναλαμβάνει η εκάστοτε επιχείρηση υπογράφοντας τους σχετικούς όρους της Worldline Greece. Το ρίσκο απορρέει από το γεγονός ότι για τις συγκεκριμένες συναλλαγές δε μπορεί να αποδειχθεί η συναίνεση του κατόχου της κάρτας, όπως συμβαίνει για τις συναλλαγές που πραγματοποιεί ο κάτοχος με ισχυρή ταυτοποίηση και βαραίνει την επιχείρηση σε περίπτωση αμφισβήτησης.

7. **Ενημερωθείτε και εφόσον χρειάζεται πιστοποιήστε την επιχείρησή σας** βάσει του προτύπου ασφαλείας **PCI DSS** (Payment Card Industry Data Security Standards), το οποίο έχει

δημιουργηθεί από τους Διεθνείς Οργανισμούς Καρτών (π.χ. Visa, Mastercard). Ενδεικτικά μέτρα ασφαλείας δίνονται στο Παράρτημα στο τέλος του παρόντος. Για περισσότερες πληροφορίες επισκεφθείτε τον δικτυακό τόπο pcisecuritystandards.org.

8. **Επικοινωνήστε άμεσα με το Τμήμα Ελέγχου Συναλλαγών της Worldline Greece** στο email dl-ftv.acquiring.gr@worldline.com σε περίπτωση που:
   - λάβετε ενημέρωση από την τεχνική σας εταιρεία ή από πελάτη σας για πιθανή **ύπαρξη κακόβουλου λογισμικού ή υποψία υποκλοπής στοιχείων καρτών** στον ιστότοπο της επιχείρησής σας.
   - εντοπίσετε **συναλλαγή που ενδέχεται να είναι ύποπτη** για να προφυλαχθείτε από πιθανή απάτη, γνωστοποιώντας μας τα παρακάτω στοιχεία της:

Στοιχεία Συναλλαγής
Ημερομηνία Συναλλαγής
Ποσό Συναλλαγής
Trans id (transaction id)
Αριθμός Κάρτας (masked card)
Στοιχεία τιμολόγησης / κατόχου κάρτας (Billing details)
Στοιχεία παράδοσης εμπορευμάτων /παροχής υπηρεσιών (Shipping details)

Συχνές Ερωτήσεις:

- **Είναι απαραίτητο να είναι αναρτημένη στο ηλεκτρονικό κατάστημα (e-shop) της επιχείρησης η πολιτική ακύρωσης/ επιστροφής και υπαναχώρησης;**

  Ναι, σε περίπτωση που έχετε ηλεκτρονικό κατάστημα (e-shop) η πολιτική ακύρωσης /επιστροφής και υπαναχώρησης θα πρέπει να είναι αναρτημένη στο e-shop σας. Ειδικότερα, εάν η επιχείρησή σας προσφέρει υπηρεσίες, τότε στη σελίδα πληρωμής του e-shop σας είναι απαραίτητο να υπάρχει ειδικό πεδίο για την επιλογή της αποδοχής της πολιτικής ακύρωσης /επιστροφής (cancellation policy) από τους πελάτες σας.

- **Πως γνωστοποιείται η πολιτική ακύρωσης /επιστροφής και υπαναχώρησης σε πελάτες που λαμβάνουν Payment Link από την επιχείρηση;**

  Σε περίπτωση που χρησιμοποιείτε την υπηρεσία Payment Link, χρειάζεται να γνωστοποιείτε στον πελάτη σας την πολιτική ακύρωσης /επιστροφής και υπαναχώρησης μέσω ηλεκτρονικού ταχυδρομείου, πριν την εκτέλεση της πληρωμής. Διατηρείτε την σχετική ηλεκτρονική αλληλογραφία

που αποστείλατε στον πελάτη σας, για την περίπτωση που σας ζητηθεί η επιβεβαίωση της γνωστοποίησης (στοιχεία αποστολέα, παραλήπτη, ημερομηνίας, ώρας και πολιτικής).

- **Ποια διαδικασία ακολουθείται σε περίπτωση αμφισβήτησης;**

  Σε κάθε περίπτωση αμφισβήτησης η Worldline Greece ακολουθεί πιστά την διαδικασία που εφαρμόζεται στις περιπτώσεις των αμφισβητήσεων, εντός του πλαισίου που οριοθετείται από τα διεθνή συστήματα πληρωμών και τους κανονισμούς που διέπουν τους Διεθνείς Οργανισμούς Καρτών Visa & Mastercard.

- **Μπορεί ένας πελάτης να αμφισβητήσει μια 3D συναλλαγή;**

  Ναι, ο πελάτης διατηρεί αυτό το δικαίωμα. Η αμφισβήτηση 3D συναλλαγής συναντάται κυρίως λόγω μη παράδοσης εμπορευμάτων ή μη παροχής υπηρεσιών, διπλής χρέωσης, ελαττωματικού προϊόντος κ.λ.π.

- **Πώς ξεχωρίζω ότι μία συναλλαγή είναι 3D;**

  Μπορείτε να διακρίνετε αν μια συναλλαγή είναι 3D στην πλατφόρμα του ePOS, από την τιμή που εμφανίζεται στο πεδίο MOTO/ EFlag στην αρχική οθόνη της πλατφόρμας.

  Αναλυτικά, οι τιμές που ενδέχεται να λάβει το συγκεκριμένο πεδίο, είναι οι εξής:

  5: 3D συναλλαγή
  6: 3D συναλλαγή
  1: non 3D συναλλαγή (MO/TO: Mail Order/Telephone Order)
  7: non 3D συναλλαγή

Παραδείγματα εμφάνισης συναλλαγών στην πλατφόρμα του ePOS:

Date /Time	Type	TX id / Order id	Payment method	Merchant	PAN masked	Order Amount	Total Amount	Status	MOTO/ EFlag
Date / Time	Payment	xxxxxxx/ xxxxxxx	Visa	mid-Merchant title	479273## ######12	€ 200,0	€ 200,0	CAPTURED	N/5
Date / Time	Payment	xxxxxxx/ xxxxxxx	Visa	mid-Merchant title	479273## ######12	€ 200,0	€ 200,0	CAPTURED	N/6
Date / Time	Payment	xxxxxxx/ xxxxxxx	Visa	mid-Merchant title	479273## ######12	€ 200,0	€ 200,0	CAPTURED	N/7
Date / Time	Payment	xxxxxxx/ xxxxxxx	Visa	mid-Merchant title	479273## ######12	€ 200,0	€ 200,0	CAPTURED	Y/1

Παράρτημα

Ενδεικτικά μέτρα σύμφωνα με το πρότυπο 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 ηλεκτρονικού καταστήματος της επιχείρησης 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 μόνο το πρωτόκολλο TLSv1.2.

- Τα συστήματα υποδομής του ηλεκτρονικού καταστήματος θα πρέπει:
  - να έχουν εγκατεστημένο και ενημερωμένο λογισμικό anti-virus στην τελευταία έκδοση (όπου υποστηρίζεται).
  - να είναι ενημερωμένα με όλα τα διαθέσιμα security updates από τον αντίστοιχο κατασκευαστή / προμηθευτή.

- Θα πρέπει να δημιουργηθεί διαδικασία είτε για χειροκίνητη, είτε για αυτόματη εγκατάσταση των security updates μέσα σε έναν (1) μήνα από την ανακοίνωσή τους από τον αντίστοιχο κατασκευαστή / προμηθευτή.

- Είναι απαραίτητο να εκτελείται συνολικός έλεγχος ασφαλείας (vulnerability security assessment) από εξειδικευμένη εταιρεία, τουλάχιστον μία (1) φορά τον χρόνο ή οποτεδήποτε χρειάζεται λόγω σημαντικών αλλαγών ή αναβαθμίσεων των συστημάτων.

- Η πρόσβαση στα συστήματα 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 αποτελούνται υποχρεωτικά από τουλάχιστον οχτώ (8) χαρακτήρες και να περιέχουν γράμματα, αριθμούς και σύμβολα.

- Πρόσβαση στα συστήματα υποδομής του ηλεκτρονικού καταστήματος θα πρέπει να έχουν οι ελάχιστοι απαραίτητοι υπάλληλοι. Το ίδιο ισχύει αντίστοιχα για την πρόσβαση των διαχειριστών.

- Όλοι οι φάκελοι και τα αρχεία των συστημάτων υποδομής του ηλεκτρονικού καταστήματος θα πρέπει να έχουν περιορισμούς πρόσβασης από τους χρήστες (access rights) με περιορισμένα, στο ελάχιστο για τη λειτουργία των συστημάτων, δικαιώματα.