Πάντειον Πανεπιστήμιο Panteion University

**Τμήμα Δημόσιας Διοίκησης**

*Department of Public Administration*

ΠΜΣ «Νομική και Διοικητική Επιστήμη»
Δίκαιο και Πολιτικές της Ε.Ε.

# Ηλεκτρονικό Εμπόριο

# &

# Ηλεκτρονική Απάτη

**Διπλωματική εργασία**

**Αθανασίας Η. ΚΕΛΓΙΩΡΓΗ**

Α.Μ. 7123Μ004

Επιβλέπων Καθηγητής: Άγγελος Μπώλος, Καθηγητής

Αθήνα, Νοέμβριος 2024

**Τριμελής Επιτροπή**

Άγγελος Μπώλος , Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)

Ευαγγελία Μπάλτα, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου

Χριστίνα Χριστοπούλου, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου

**ΕΥΧΑΡΙΣΤΗΡΙΟ ΣΗΜΕΙΩΜΑ**

Με το παρόν θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή της μεταπτυχιακής μου διατριβής κ. Μπώλο Άγγελο, Καθηγητή του Τμ. Δημόσιας Διοίκησης του Παντείου Πανεπιστημίου, για όλη την βοήθεια, την καθοδήγηση, την υποστήριξη αλλά και την κατανόηση του κατά την διάρκεια της διαδικασίας εκπόνησής της.

Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένεια μου για την υποστήριξη και την υπομονή τους καθ' όλη την διάρκεια των μεταπτυχιακών μου σπουδών, καθώς χωρίς αυτούς δεν θα ήταν δυνατόν να τις ολοκληρώσω. Ελπίζω να αποτελέσω παράδειγμα για τις δύο κόρες μου και να συνεχίσουν την διαδικασία μόρφωσής τους σε όλη τη διάρκεια της ζωής τους

**Περιεχόμενα**

**Συντομογραφίες**

| | |
|---|---|
| ΓΚΠΔ | Γενικός Κανονισμός Προστασίας Δεδομένων |
| ΕΕ | Ευρωπαϊκή Ένωση |
| κυα | κοινή υπουργική απόφαση |
| Μ.Μ.Ε. | Μέσα Μαζικής Ενημέρωσης |
| ν. | νόμος |
| παρ. | παράγραφος |
| τ. | τεύχος |
| ΦΕΚ | Φύλλο Εφημερίδας Κυβέρνησης |

**Περίληψη**

Το ηλεκτρονικό εμπόριο αποτελεί πλέον μία καθημερινότητα και έναν ισάξιο αντίπαλο της κλασικής μορφής εμπορίου. Βασιζόμενο ωστόσο στην εξέλιξη της τεχνολογίας και του διαδικτύου πέραν των πλεονεκτημάτων που παρουσιάζει έναντι του κλασικού εμπορίου είναι ιδιαίτερα ευάλωτο στην εκδήλωση εγκληματικών ενεργειών.

Η παρούσα διπλωματική εργασία εξετάζει το φαινόμενο της ηλεκτρονικής απάτης σε βάρος των καταναλωτών στο πλαίσιο του ηλεκτρονικού εμπορίου καθώς και τους τρόπους αντιμετώπισής του

Στο πρώτο μέρος γίνεται αρχικά αναφορά στον προσδιορισμό της έννοιας του ηλεκτρονικού εμπορίου, των χαρακτηριστικών και των κατηγοριών του καθώς και των πλεονεκτημάτων και των μειονεκτημάτων του. Ειδική αναφορά γίνεται στα ηλεκτρονικά καταστήματα και στις ηλεκτρονικές πλατφόρμες αγορών.

Επιπλέον στο πρώτο μέρος αναπτύσσεται η έννοια της ηλεκτρονικής απάτης στο ηλεκτρονικό εμπόριο, τα είδη και οι συνέπειές της για τους καταναλωτές.

Στο δεύτερο μέρος εστιάζει στην προστασία των καταναλωτών από την ηλεκτρονική απάτη. Γίνεται αναφορά στο θεσμικό πλαίσιο, ενωσιακό και εθνικό καθώς και στους θεσμικούς, ενωσιακούς και εθνικούς, φορείς για την αντιμετώπισή της. Το τελευταίο τμήμα της εργασίας εστιάζει στην πρόληψη του φαινομένου και τον ρόλο σε αυτή τόσο των καταναλωτών όσο και των επιχειρήσεων.

**Λέξεις κλειδιά**: Ηλεκτρονικό εμπόριο, Ηλεκτρονική Απάτη, Ηλεκτρονικό Κατάστημα, Ηλεκτρονική Πλατφόρμα Αγορών, Καταναλωτής, Επιχείρηση

**ABSTRACT**

E-commerce is now an everyday occurrence and an equal rival to the classic form of commerce. However, based on the development of technology and the internet, in addition to the advantages it presents over classic commerce, it is particularly vulnerable to the occurrence of criminal acts.

This thesis examines the phenomenon of electronic fraud against consumers in the context of e-commerce as well as ways to deal with it.

The first part initially refers to the definition of the concept of e-commerce, its characteristics and categories, as well as its advantages and disadvantages. Special reference is made to online stores and online shopping platforms.

In addition, the first part develops the concept of electronic fraud in e-commerce, its types and its consequences for consumers.

The second part focuses on the protection of consumers from electronic fraud. Reference is made to the institutional framework, EU and national, as well as to the institutional, EU and national, bodies for dealing with it. The last part of the work focuses on the prevention of the phenomenon and the role of both consumers and businesses in it.

**Keywords:** E-commerce, E-Fraud, E-Store, E-Shopping Platform, Consumer, Business

## Εισαγωγή

Το ηλεκτρονικό εμπόριο πλέον καταλαμβάνει μεγάλο μέρος της καταναλωτικής μας καθημερινότητας καθώς εκμεταλλευόμενο την ραγδαία εξάπλωση της τεχνολογίας και του διαδικτύου αναπτύσσεται με ιλιγγιώδεις ρυθμούς προσφέροντας ευκολία στις συναλλαγές των καταναλωτών. Η «έκρηξη» στις ηλεκτρονικές συναλλαγές πραγματοποιήθηκε την περίοδο της πανδημίας του κορονοϊού οπότε και οι καταναλωτές στράφηκαν στη χρήση του διαδικτυακού εμπορίου και στις ηλεκτρονικές αγορές, ωστόσο εξακολουθεί να αναπτύσσεται ραγδαία.

Εκ πρώτης όψεως θα μπορούσε να πει κάποιος ότι καταναλωτές και επιχειρήσεις μόνο να ωφεληθούν έχουν από την νέα αυτή πραγματικότητα στις εμπορικές συναλλαγές. Ωστόσο όπως κάθε νόμισμα έχει δύο όψεις, έτσι συμβαίνει και με την περίπτωση του ηλεκτρονικού εμπορίου. Στην πραγματικότητα μπορεί τα πλεονεκτήματα που προσφέρει να είναι πολλά και σημαντικά για όλους τους εμπλεκόμενους αλλά το ίδιο σημαντικά και πολλά είναι τα μειονεκτήματά του.

Η εξέλιξη της τεχνολογίας και του διαδικτύου όμως έχουν επίπτωση και στην αύξηση της εγκληματικής δραστηριότητας που παρατηρείται στον ψηφιακό κόσμο καθιστώντας την ηλεκτρονική απάτη ένα διαρκώς αυξανόμενο έγκλημα με τα περιστατικά σε βάρος των καταναλωτών να πολλαπλασιάζονται.

Οι καταναλωτές επομένως προκειμένου να προστατευθούν και να απολαύσουν τα πολλαπλά οφέλη του ηλεκτρονικού εμπορίου θα πρέπει να είναι ενήμεροι και προσεκτικοί με τους κινδύνους που ελλοχεύουν κατά την πραγματοποίηση ηλεκτρονικών αγορών. Επιπλέον τα κράτη θα πρέπει να διασφαλίσουν το ηλεκτρονικό εμπόριο εφαρμόζοντας το κατάλληλο θεσμικό πλαίσιο και ενεργοποιώντας φορείς, εθνικούς και διεθνείς, που θα αναλάβουν την πρόληψη και την αντιμετώπιση του φαινομένου της ηλεκτρονικής απάτης στο ηλεκτρονικό εμπόριο.

## Μέρος Α΄

## Ηλεκτρονικό εμπόριο & Μορφές Ηλεκτρονικής Απάτης

### Ι. Ηλεκτρονικό Εμπόριο

1. Ορισμός

Υπάρχει μία πληθώρα ορισμών για τον προσδιορισμό της έννοιας του ηλεκτρονικού εμπορίου βασιζόμενοι στα χαρακτηριστικά του και στον σκοπό του. Απλούστεροι ή πιο σύνθετοι χρησιμοποιούνται για να περιγράψουν μια έννοια που τα τελευταία χρόνια έχει κατακλύσει την ζωή μας.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή ως ηλεκτρονικό εμπόριο συνίσταται η πώληση ή η αγορά αγαθών ή υπηρεσιών, μεταξύ επιχειρήσεων, νοικοκυριών, ιδιωτών ή ιδιωτικών οργανισμών, μέσω ηλεκτρονικών συναλλαγών που πραγματοποιούνται μέσω διαδικτύου ή άλλων δικτύων με τη χρήση ηλεκτρονικού υπολογιστή. Ο όρος καλύπτει την παραγγελία αγαθών και υπηρεσιών που αποστέλλονται μέσω δικτύων υπολογιστών, αλλά η πληρωμή και η τελική παράδοση των αγαθών ή της υπηρεσίας μπορεί να πραγματοποιηθεί είτε on line είτε εκτός σύνδεσης[1].

Τον ορισμό του ηλεκτρονικού εμπορίου παραθέτει και η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στην ιστοσελίδα της όπου αναφέρει ότι με τον όρο ηλεκτρονικό εμπόριο εννοούμε κάθε ολοκληρωμένη συναλλαγή, η οποία εκτελείται αποκλειστικά σε ηλεκτρονικό επίπεδο, μέσω διαδικτύου, τηλεφώνου και φαξ, χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλόμενων μερών. Για την πραγματοποίηση μιας τέτοιας συναλλαγής χρησιμοποιούνται πολύπλοκοι προγραμματιστικοί μηχανισμοί και το κατάλληλο λογισμικό, το οποίο επιτρέπει την Ηλεκτρονική Ανταλλαγή Δεδομένων μεταξύ των δύο αντισυμβαλλόμενων μελών[2].

Η Επιτροπή Ανταγωνισμού στην Τελική Έκθεση της κλαδικής έρευνας στο Ηλεκτρονικό Εμπόριο ορίζει ότι «ως ηλεκτρονικό εμπόριο νοείται η δημιουργία εσόδων για την επιχείρηση, από την πώληση αγαθών, υπηρεσιών και πληροφοριών, μέσω της χρήσης του διαδικτύου ή άλλων δικτύων υπολογιστών. Το ηλεκτρονικό εμπόριο εντάσσεται στο ηλεκτρονικό επιχειρείν και αφορά επιχειρηματική δραστηριότητα που εμπεριέχει ανταλλαγή αξίας. Με άλλα λόγια, το ηλεκτρονικό εμπόριο είναι η έκφανση του ηλεκτρονικού επιχειρείν που αφορά σε ανταλλαγή

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Eζ`-commerce
[2] https://cyberalert.gr/ti-einai-to-ilektroniko-emporio/

αξίας ή, διαφορετικά, το ηλεκτρονικό επιχειρείν γίνεται ηλεκτρονικό εμπόριο τη στιγμή που πραγματοποιείται ανταλλαγή αξίας»[3] .

Πολλοί ορισμοί με παρεμφερές περιεχόμενο έχουν διατυπωθεί από μελετητές του ηλεκτρονικού εμπορίου προσπαθώντας να συλλάβουν την έννοιά του. Σύμφωνα με τους Σ. Βαλσαμίδη και Ι. Καζανίδη το ηλεκτρονικό εμπόριο επικεντρώνεται στις δραστηριότητες των αγορών, των πωλήσεων, των ανταλλαγών και της ενοικίασης προϊόντων, των υπηρεσιών και των πληροφοριών, οι οποίες (δραστηριότητες) υποστηρίζονται από τις νέες τεχνολογίες της πληροφορικής και των επικοινωνιών, με τη χρήση δικτύων υπολογιστικών συστημάτων[4].

Το ηλεκτρονικό εμπόριο πλέον αποτελεί αναγκαιότητα και όχι μία απλή πραγματικότητα ή μία αναβάθμιση για τις φυσικές επιχειρήσεις. Μετά την εποχή της πανδημίας του κορονοϊού, οπότε και αναγκαστικά στράφηκαν οι καταναλωτές στις ηλεκτρονικές αγορές, πλέον είναι καθημερινότητα καθώς οι καταναλωτές επιλέγουν να πραγματοποιούν τις αγορές τους ηλεκτρονικά για πολλούς και διάφορους λόγους με κυριότερους την ευκολία στις αγορές, την πρόσβαση σε ποικιλία προϊόντων και την εξοικονόμηση χρημάτων[5].

Η δημιουργία ηλεκτρονική ιστοσελίδα για την πραγματοποίηση αγορών στο παρελθόν αποτελούσε πολυτέλεια για τις φυσικές επιχειρήσεις. Σήμερα αποτελεί αναγκαίο εργαλείο βιωσιμότητας για τις επιχείρησης εφόσον θέλουν να συνεχίσουν να είναι ανταγωνιστικές και να διεκδικούν μερίδιο στις αγορές των καταναλωτών στο χώρο του ηλεκτρονικού εμπορίου.

## 2. Κατηγορίες ηλεκτρονικού εμπορίου[6].

Ο τρόπος λειτουργίας μιας επιχείρησης για την πώληση προϊόντων και αγαθών μέσω διαδικτύου αποτελεί συνιστά το επιχειρηματικό μοντέλο ηλεκτρονικού εμπορίου που ακολουθεί η επιχείρηση. Υπάρχουν διάφορα μοντέλα- κατηγορίες ηλεκτρονικού εμπορίου ανάλογα με τα κριτήρια που χρησιμοποιούνται. Με τη χρήση ως κριτηρίου τη φύση των συμμετεχόντων στις ηλεκτρονικές συναλλαγές προκύπτουν τρείς κατηγορίες: i) Επιχείρηση προς Καταναλωτή (Business to Consumer- B2C), ii) Επιχείρηση προς Επιχείρηση (Business

[3] Κλαδική Έρευνα στο Ηλεκτρονικό Εμπόριο, Τελική Έκθεση, Επιτροπή Ανταγωνισμού, Αθήνα, Νοέμβριος 2022, σελ. 22

[4] Ηλεκτρονικό Εμπόριο και εφαρμογές διαδικτύου, Σ. Βαλσαμίδης- Ι. Καζανίδης, Εκδόσεις Δίσιγμα, 2020, σελ. 53-54

[5] Lawyermagazine.gr: «E-commerce: Η επόμενη μέρα για το ελληνικό εμπόριο», Ιωάννα Γεωργίου, 30-11-2022, https://lawyermagazine.gr/e-commerce-η-επόμενη-μέρα-για-το-ηλεκτρονικό-εμ/, Παρομοίως: liberal.gr: «Οι 7 στους 10 χρήστες του διαδικτύου κάνουν τις αγορές τους online», 12-06-2023, https://www.liberal.gr/oikonomia/oi-7-stoys-10-hristes-toy-diadiktyoy-kanoyn-tis-agores-toys-online

[6] Ηλεκτρονικό Εμπόριο και εφαρμογές διαδικτύου, Σ. Βαλσαμίδης- Ι. Καζανίδης, Εκδόσεις Δίσιγμα, 2020, σελ. 61 κ.ε.

to Business- B2B) και iii) Καταναλωτής προς Καταναλωτή (Consumer to Consumer- C2C). Πέραν των προαναφερόμενων κατηγοριών που συνιστούν τις βασικές κατηγορίες, υπάρχουν και άλλες μορφές ηλεκτρονικού εμπορίου όπως: iv) Καταναλωτές προς Επιχειρήσεις (Consumer to Business- C2B), v) Ηλεκτρονικό Εμπόριο μεταξύ ομότιμων συστημάτων (Peer to Peer- P2P), vi) Επιχειρήσεις προς Εργαζομένους (Business to Employees- B2E), vii) Επιχειρήσεις προς Κυβερνήσεις (Business to Governments- B2G), viii) Κινητό Ηλεκτρονικό Εμπόριο (M-Commerce), ix) Κοινωνικό Ηλεκτρονικό Εμπόριο (Social E-Commerce), x) Επιχείρηση προς Επιχείρηση προς Καταναλωτή (Business to Business to Consumer- B2B2C), xi) Καταναλωτής προς Κυβέρνηση (Consumer to Governments- C2G) και xii) Απευθείας στον Καταναλωτή (Direct to Consumer- D2C).

Η ιδέα του «ηλεκτρονικού εμπορίου» εμφανίστηκε για πρώτη φορά το 1979 όταν ο Michael Aldrich[7] συνέδεσε μία τροποποιημένη οικιακή τηλεόραση σε έναν υπολογιστή επεξεργασίας συναλλαγών σε πραγματικό χρόνο μέσω μίας εγχώριας τηλεφωνικής γραμμής και χρησιμοποίησε το μοντέλο αυτό για να προσεγγίσει καταναλωτές για την πραγματοποίηση πωλήσεων. Με τον τρόπο αυτό εφηύρε τις ηλεκτρονικές αγορές που σήμερα ονομάζεται ηλεκτρονικό εμπόριο και είναι μία ταχέως αναπτυσσόμενη παγκόσμια επιχείρηση.

Η βασική και πιο δημοφιλής κατηγορία ηλεκτρονικού εμπορίου είναι η κατηγορία «Επιχείρηση προς Καταναλωτή (Business to Consumer- B2C)» που αποτελεί στην πραγματικότητα τον παραδοσιακό τρόπο εμπορίου με τη διαφορά ότι οι συναλλαγές γίνονται ηλεκτρονικά. Αναφέρεται δηλαδή στις λιανικές πωλήσεις προϊόντων από επιχειρήσεις σε απλούς καταναλωτές και πρόκειται για την πιο γνωστή και διαδεδομένη μορφή ηλεκτρονικού εμπορίου.

Το μοντέλο αυτό παραδοσιακά αναφερόταν σε αγορές σε εμπορικά κέντρα, φαγητό σε εστιατόρια, σε ταινίες με πληρωμή ανά θέαση και σε ενημερωτικές διαφημίσεις. Οι ιστότοποι στο παρελθόν αποτελούσαν την ηλεκτρονική «βιτρίνα» των φυσικών καταστημάτων που σκοπό είχαν να προσελκύσουν τους πελάτες στα φυσικά καταστήματα.

Η άνοδος του διαδικτύου δημιούργησε ένα νέο επιχειρηματικό κανάλι. Οι ιστότοποι έχουν πλέον έχουν αναβαθμιστεί και τις περισσότερες φορές αποτελούν οι ίδιοι τα καταστήματα χωρίς να συνδέονται με φυσικό κατάστημα. Μάλιστα μέσω ειδικών προγραμμάτων δίνουν τη δυνατότητα στους καταναλωτές να «δοκιμάζουν» τα προϊόντα, να συγκρίνουν τις τιμές πώλησής τους μεταξύ των διάφορων καταστημάτων και να συγκρίνουν τα χαρακτηριστικά του με άλλα παρόμοια πριν προβούν στην τελική αγορά.

[7] https://www.aldricharchive.co.uk/inventors-story

Σήμερα το μοντέλο αυτό αποτελεί το πιο διαδεδομένο και αναγνωρίσιμο μοντέλο ηλεκτρονικού εμπορίου που επιτρέπει στις επιχειρήσεις να συνδέονται άμεσα με τους τελικούς καταναλωτές. Διακρίνεται σε δύο υποκατηγορίες στηριζόμενες στον τρόπο διάθεσης των προϊόντων στους καταναλωτές. Η πρώτη κατηγορία είναι το καθαρό ή άμεσο ηλεκτρονικό εμπόριο και αφορά στα προϊόντα που παραδίδονται απευθείας στους καταναλωτές χωρίς την μεσολάβηση τρίτου, όπως βιβλία και μουσικά κομμάτια σε ψηφιακή μορφή. Η δεύτερη υποκατηγορία είναι το μερικό ή έμμεσο ηλεκτρονικό εμπόριο, στο οποίο για την παράδοση του προϊόντος από την επιχείρηση στον καταναλωτή πρέπει να μεσολαβήσει τρίτος, όπως είναι τα τρόφιμα (delivery).

Το άμεσο ηλεκτρονικό εμπόριο περιλαμβάνει την παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών όπως για παράδειγμα η αγορά ενός ηλεκτρονικού εισιτηρίου από ένα δικτυακό τόπο μιας αεροπορικής εταιρίας ή για μία θεατρική παράσταση ή για μία κινηματογραφική προβολή όταν η έρευνα αγοράς, η κράτηση, η πληρωμή και η παράδοση γίνονται εξ' ολοκλήρου ηλεκτρονικά. Το έμμεσο ηλεκτρονικό εμπόριο αφορά την ηλεκτρονική παραγγελία υλικών αγαθών που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους όπως είναι το ταχυδρομείο ή οι εταιρείες ταχυμεταφοράς. Τόσο το άμεσο όσο και το έμμεσο ηλεκτρονικό εμπόριο προσφέρουν συγκεκριμένες δυνατότητες. Το έμμεσο ηλεκτρονικό εμπόριο εξαρτάται όμως από εξωτερικούς παράγοντες, όπως από την αποτελεσματικότητα του συστήματος μεταφορών. Το άμεσο ωστόσο παρέχει δυνατότητα πραγματοποίησης απρόσκοπτων ηλεκτρονικών συναλλαγών πέρα από γεωγραφικά σύνορα εκμεταλλευόμενο όλες τις δυνατότητες των παγκόσμιων ηλεκτρονικών αγορών.

Η κατηγορία «Επιχείρηση προς Καταναλωτή» εμφανίζει διάφορους τύπους διαδικτυακών επιχειρηματικών μοντέλων όπως τους άμεσους πωλητές, τους διαδικτυακούς μεσάζοντες, το εμπόριο μέσω κοινοτήτων και το εμπόριο με συνδρομή. Ο πιο κοινός τύπος είναι ο πρώτος οπότε και οι καταναλωτές αγοράζουν αγαθά από διαδικτυακούς λιανοπωλητές. Μπορεί να πρόκειται για κατασκευαστές ή μικρές επιχειρήσεις ή διαδικτυακές εκδόσεις πολυκαταστημάτων που πωλούν προϊόντα από διάφορους κατασκευαστές. Ο τύπος των ηλεκτρονικών αγορών μέσω διαδικτυακών μεσαζόντων αφορά την πραγματοποίηση αγορών ηλεκτρονικά μέσω πωλητών που στην πραγματικότητα δεν κατέχουν προϊόντα ή υπηρεσίες αλλά ενώνουν πωλητές ή υπηρεσίες όπως για παράδειγμα ο ιστότοπος trivago. Άλλος τύπος αναπτύσσεται μέσω κοινοτήτων μέσων κοινωνικής δικτύωσης όπως το Facebook. Τα μέσα δημιουργούν διαδικτυακές κοινότητες με βάση κοινά ενδιαφέροντα και βοηθούν εμπόρους και διαφημιστές να προωθούν τα προϊόντα τους απευθείας στους

καταναλωτές. Τελευταίος τύπος είναι οι ιστότοποι που παρέχουν τα προϊόντα και τις υπηρεσίες τους κατόπιν συνδρομής όπως το Netflix ή οι διαδικτυακές ιστότοποι εφημερίδων.

Δεκαετίες μετά την έκρηξη του ηλεκτρονικού εμπορίου, ραγδαία ανάπτυξη γνωρίζει το κινητό ηλεκτρονικό εμπόριο (m-commerce). Η κατηγορία αυτή περιλαμβάνει τη χρήση ασύρματων φορητών συσκευών όπως κινητά τηλέφωνα και τάμπλετ για τη διεξαγωγή εμπορικών συναλλαγών στο διαδίκτυο, συμπεριλαμβανομένης της αγοράς και πώλησης προϊόντων, της ηλεκτρονικής τραπεζικής και της πληρωμής λογαριασμών. Οι χρήστες των συσκευών μπορούν να πραγματοποιούν συναλλαγές οπουδήποτε, υπό την προϋπόθεση ότι υπάρχει πάροχος ασύρματου διαδικτύου στην περιοχή. Μάλιστα με την αύξηση της χρήσης ασύρματων συσκευών, την επίλυση ζητημάτων ασφαλείας και τον πολλαπλασιασμό εφαρμογών m-commerce η κατηγορία αυτή εξελίσσεται ραγδαία ενώ εταιρείες όπως η Google και η Apple έχουν αναπτύξει δικές τους υπηρεσίες κινητού εμπορίου[8].

Από τα παραπάνω διαπιστώνουμε ότι το ηλεκτρονικό εμπόριο έχει τη δυνατότητα της συνεχούς εξέλιξης μέσω της προσαρμογής στις επιθυμίες και τις τάσεις των καταναλωτών εκμεταλλευόμενο τις τεχνολογικές εξελίξεις. Με αυτό τον τρόπο καταφέρνει διαρκώς όχι απλά να παραμένει επίκαιρο αλλά και να αποτελεί μία κερδοφόρα αγορά επιδιώκοντας να αφήσει στη δεύτερη θέση το παραδοσιακό εμπόριο.

## 3. Χαρακτηριστικά του ηλεκτρονικού εμπορίου.

Με την ραγδαία εξάπλωση του διαδικτύου και της τεχνολογίας το ηλεκτρονικό εμπόριο εξελίσσεται σε έναν από τους κύριους τρόπους διεξαγωγής του εμπορίου που επιλέγουν επιχειρήσεις και καταναλωτές. Σύμφωνα με την έρευνα που δημοσίευσε η Ελληνική Στατιστική Αρχή τον Δεκέμβριο του 2023 για τον βαθμό χρήσης των τεχνολογιών πληροφόρησης και επικοινωνίας από τα νοικοκυριά και τα μέλη τους[9], το 55,3% του πληθυσμού ηλικίας 16 - 74 ετών, που έχουν οποτεδήποτε χρησιμοποιήσει, έστω και μία φορά, το διαδίκτυο, πραγματοποίησαν, κατά το Α΄ τρίμηνο του 2023, κάποια ηλεκτρονική αγορά ή παραγγελία αγαθών ή υπηρεσιών μέσω του διαδικτύου, για προσωπική χρήση. Όπως φαίνεται και από το ακόλουθο γράφημα που δημοσιεύτηκε στην εν λόγω έρευνα, σε

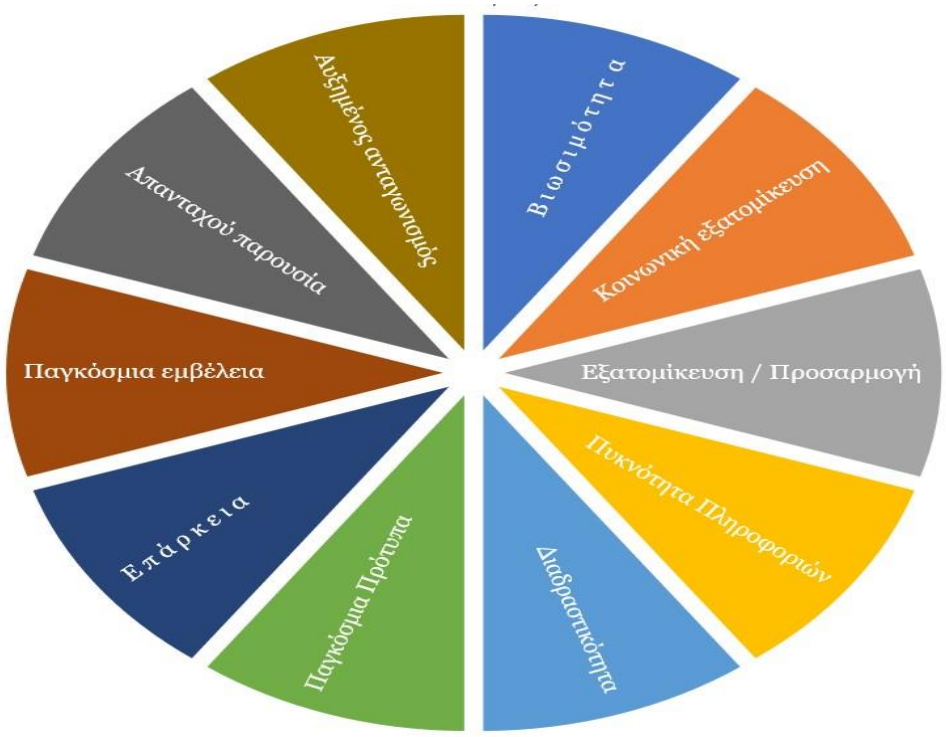
[8] Σύμφωνα με την "M-Commerce - Global Strategic Business Report" αναφορά του ResearchAndMarkets,com για το έτος 2025 η παγκόσμια αγορά για το m-commerce αποτιμήθηκε σε 678,2 δισεκατομμύρια δολάρια Η.Π.Α. και ως το 2030 προβλέπεται να φτάσει τα 2,4 τρισεκατομμύρια δολάρια Η.Π.Α.

[9]«ΕΡΕΥΝΑ ΧΡΗΣΗΣ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΠΟ ΝΟΙΚΟΚΥΡΙΑ ΚΑΙ ΑΤΟΜΑ: Έτος 2023», Ελληνική Στατιστική Εταιρεία, σελ. 6, https://www.statistics.gr/documents/20181/7add8452-9379-0e6d-6313-fb619174f96c

σύγκριση με το αντίστοιχο ποσοστό του έτους 2022 (53,2%) καταγράφεται αύξηση 4,0%, ενώ αύξηση 104,8% καταγράφεται σε σύγκριση με το 2013.


Τι είναι ωστόσο αυτό που ωθεί τους καταναλωτές να πραγματοποιούν αγορές με τη χρήση του ηλεκτρονικού εμπορίου όλο και περισσότερο; Ποια χαρακτηριστικά έχει το ηλεκτρονικό εμπόριο σε σχέση με το εμπόριο στην κλασική του μορφή που το διαφοροποιούν και κάνει τους καταναλωτές να το επιλέγουν;

Χαρακτηριστικά ηλεκτρονικού εμπορίου



α. Πανταχού παρουσία (Ubiquity)

Σύμφωνα με το λεξικό[10] ο όρος «ubiquity» είναι η ιδιότητα του να είναι κάποιος πανταχού παρών δηλαδή να βρίσκεται παντού ή να είναι ταυτόχρονα παρών σε πολλά μέρη. Αυτό λοιπόν που χαρακτηρίζει το ηλεκτρονικό εμπόριο είναι ότι είναι διαθέσιμο από οπουδήποτε, ανά πάσα στιγμή και από οποιαδήποτε συσκευή που είναι συνδεδεμένη είτε ενσύρματα είτε ασύρματα με κάποιον πάροχο ίντερνετ.

Αυτή είναι η πρώτιστη διαφορά με το φυσικό εμπόριο. Στο φυσικό εμπόριο οι καταναλωτές πρέπει να επισκεφτούν το φυσικό κατάστημα τις ώρες λειτουργίας του για να πραγματοποιήσουν μία αγορά. Η μετάβασή τους στο φυσικό χώρο της επιχείρησης και το να πραγματοποιηθεί η επίσκεψη στις ώρες λειτουργίας της επιχείρησης είναι προϋποθέσεις της καθώς διαφορετικά ο καταναλωτής δεν μπορεί να προμηθευτεί το προϊόν.

Με τα ηλεκτρονικά καταστήματα όμως είναι δυνατή η εξυπηρέτηση των καταναλωτών και η πραγματοποίηση των αγορών ανεξάρτητα του τόπου όπου βρίσκονται και της ώρας που πραγματοποιούν την αγορά. Η μόνη προϋπόθεση είναι να είναι συνδεδεμένοι στο διαδίκτυο. Έτσι έχουν τη δυνατότητα να πραγματοποιούν αγορές όταν βρίσκονται στο σπίτι, στην εργασία τους ή στο αυτοκίνητο οποιαδήποτε ώρα της ημέρας είτε πολύ νωρίς το πρωί είτε πολύ αργά τη νύχτα.

Ο χώρος αγοράς του ηλεκτρονικού εμπορίου είναι πέρα από τα παραδοσιακά γεωγραφικά και χρονικά όρια προσφέροντας ευκολία στους καταναλωτές αφού δεν χρειάζεται να μετακινηθούν για να μεταβούν σε ένα συγκεκριμένο χώρο. Έτσι επωφελούνται σε χρόνο και σε κόστος ενώ οι αγορές δεν αποτελούν ταλαιπωρία αφού δεν χρειάζεται καν να κουραστούν σωματικά για να εντοπίσουν το προϊόν που χρειάζονται.

β. Παγκόσμια εμβέλεια (global reach)

Ένα άλλο βασικό χαρακτηριστικό του ηλεκτρονικού εμπορίου είναι η παγκόσμια εμβέλειά του, το πλήθος δηλαδή των ανθρώπων στο οποίο παρέχεται η δυνατότητα να πραγματοποιήσει μία εμπορική συναλλαγή. Με το ηλεκτρονικό εμπόριο ξεπερνιέται κάθε είδους σύνορο μετατρέποντας τις τοπικές αγορές σε παγκόσμιες αγορές αυξάνοντας κατακόρυφα των αριθμό πελατών μιας επιχείρησης. Ως αποτέλεσμα, πελάτες μίας ηλεκτρονικής επιχείρησης μπορούν να είναι όλοι οι άνθρωποι που είναι συνδεδεμένοι στο διαδίκτυο. Αν λάβουμε υπόψη ότι σύμφωνα με την έρευνα που δημοσιεύτηκε[11] τον Νοέμβριο του 2024 στην παγκόσμια πλατφόρμα δεδομένων και επιχειρηματικής ευφυίας Statista τον

[10] Oxford Advanced Learner's Dictionary
[11] https://www.statista.com/statistics/617136/digital-population-worldwide/

Οκτώβριο του 2024 οι χρήστες του διαδικτύου ανήλθαν στα 5,52 δισεκατομμύρια παγκοσμίως, αριθμός που αντιστοιχεί στο 67,5% του παγκόσμιου πληθυσμού, μπορούμε να αντιληφθούμε το μέγεθος του αριθμού των ανθρώπων στους οποίους δίνει πρόσβαση στην αγορά το ηλεκτρονικό εμπόριο.

Πριν από το ηλεκτρονικό εμπόριο, οι περισσότερες εταιρείες λειτουργούσαν σε τοπικό επίπεδο. Δυνατότητα πρόσβασης στην παγκόσμια αγορά υπό μία έννοια είχαν μόνο εταιρείες κολοσσοί που είχαν τη δυνατότητα να ανοίξουν καταστήματα και σε άλλες πόλεις ή/και χώρες από την επιχειρηματική έδρα τους ωστόσο και πάλι τα καταστήματα απευθύνονταν στον αριθμό των καταναλωτών που είχαν πρόσβαση στα φυσικά αυτά καταστήματα. Με το ηλεκτρονικό εμπόριο αυτή η δυνατότητα της παγκόσμιας εμβέλειας έχει δοθεί σε όλες τις επιχειρήσεις καθιστώντας την αγορά ισοδύναμη για όλες, μικρότερες και μεγαλύτερες επιχειρήσεις

.

γ. Παγκόσμια πρότυπα (Universal Standards)

Το επόμενο χαρακτηριστικό του ηλεκτρονικού εμπορίου το οποίο συνέβαλε για την καθολική εξάπλωσή του συμβάλλοντας στην παγκόσμια εμβέλεια που έχει είναι τα τεχνικά πρότυπα των τεχνολογιών στις οποίες στηρίζεται το ηλεκτρονικό εμπόριο είναι καθολικά τεχνικά πρότυπα. Το Διαδίκτυο είναι κοινό για όλους τους ανθρώπους παγκοσμίως και είναι δυνατό να συνδέονται υπολογιστές μεταξύ τους ανεξάρτητα από την τεχνολογία που χρησιμοποιούν, επιτρέποντας την ανταλλαγή αρχείων ανεξάρτητα από το σε ποιο μέρος του κόσμου βρίσκονται οι υπολογιστές αυτοί.

Αυτό είναι που κάνει το Διαδίκτυο πιο ευέλικτο σε σχέση με τις παραδοσιακές τεχνολογίες εμπορίου όπως η τηλεόραση ή το ραδιόφωνο, των οποίων τα τεχνικά πρότυπα διαφέρουν από χώρα σε χώρα ενώ δεν διαθέτουν την εμβέλεια που διαθέτει το διαδίκτυο. Χάρη στα κοινά αυτά πρότυπα διασφαλίζεται ότι τα διάφορα στοιχεία του ηλεκτρονικού εμπορίου όπως ιστότοποι, πύλες πληρωμών και συστήματα διαχείρισης αποθεμάτων μπορούν να συνεργαστούν αποτελεσματικά ανεξάρτητα την τοποθεσία της επιχείρησης και του καταναλωτή.

Ορισμένα παραδείγματα καθολικών προτύπων που εφαρμόζονται στο ηλεκτρονικό εμπόριο τα οποία διασφαλίζουν την ομαλή και συνεπή εμπειρία χρήστη στο ηλεκτρονικό εμπόριο είναι τα ακόλουθα:

- HTTP (Hypertext Transfer Protocol): Το HTTP είναι το θεμέλιο της επικοινωνίας στον Παγκόσμιο Ιστό. Επιτρέπει στα προγράμματα περιήγησης και στους διακομιστές Ιστού να ανταλλάσουν πληροφορίες όπως ιστοσελίδες και δεδομένα μέσω του Διαδικτύου.

- HTML (Hypertext Markup Language): Η HTML είναι η τυπική γλώσσα σήμανσης που χρησιμοποιείται για την δημιουργία ιστοσελίδων. Καθορίζει τη δομή και τη διάταξη του περιεχομένου των ιστοσελίδων, επιτρέποντας τη συνεπή απόδοσή τους σε διαφορετικά προγράμματα περιήγησης και συσκευές.
- Πύλες πληρωμών: Οι πύλες πληρωμών, όπως η PayPal, παρέχουν ένα καθολικό πρότυπο για την ασφαλή επεξεργασία των διαδικτυακών πληρωμών. Διαχειρίζονται την κρυπτογράφηση, την εξουσιοδότηση και τον διακανονισμό των συναλλαγών μεταξύ αγοραστών, πωλητών και χρηματοπιστωτικών ιδρυμάτων.
- APIs (Application Programming Interfaces): Τα API επιτρέπουν σε διαφορετικά συστήματα ηλεκτρονικού εμπορίου να αλληλεπιδρούν και να ανταλλάσσουν δεδομένα. Παρέχουν έναν τυποποιημένο τρόπο για τους προγραμματιστές να έχουν πρόσβαση και να χειρίζονται δεδομένα από εξωτερικά συστήματα, όπως η ανάκτηση πληροφοριών προϊόντος ή η ενημέρωση των επιπέδων αποθέματος.

δ. Επάρκεια των πληροφοριών (Information Richness)[12]

Η επάρκεια των πληροφοριών στο ηλεκτρονικό εμπόριο αναφέρεται στο βάθος, την ποιότητα και την ποικιλία των πληροφοριών που προσφέρει μία ιστοσελίδα ηλεκτρονικού εμπορίου στους καταναλωτές. Για να θεωρηθεί ότι μία ιστοσελίδα παρέχει επαρκή πληροφόρηση θα πρέπει να περιέχει όλες τις απαραίτητες πληροφορίες που επιτρέπουν στους καταναλωτές να λάβουν τεκμηριωμένες αποφάσεις αγοράς. Τέτοιες πληροφορίες σχετίζονται με λεπτομέρειες των προϊόντων, περιγραφές, εικόνες και βίντεο, πληροφορίες πληρωμής και παράδοσης/παραλαβής, εξατομικευμένες προτάσεις, κριτικές και αξιολογήσεις πελατών.

Η έννοια της επάρκειας των πληροφοριών είναι σημαντική στο ηλεκτρονικό εμπόριο καθώς σχετίζεται με την ικανοποίηση των πελατών αφού εξαιτίας της επάρκειας είναι σε θέση να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την αγορά ή προϊόντων. Ως αποτέλεσμα ενισχύεται η εμπιστοσύνη των καταναλωτών προς τις ιστοσελίδες ηλεκτρονικού εμπορίου που παρέχουν επαρκή πληροφόρηση, τις οποίες θα επισκεφτούν εκ νέου για την πραγματοποίηση νέων αγορών ή θα τις συστήσουν σε άλλους καταναλωτές. Με αυτό τον τρόπο βελτιώνεται η εμπειρία αγορών των καταναλωτών μέσω ηλεκτρονικού εμπορίου καθώς τους δίνει τη σιγουριά που έχουν όταν πραγματοποιούν αγορές ακολουθώντας τον παραδοσιακό τρόπο εμπορίου με φυσική παρουσία.

[12]https://www.researchgate.net/publication/313611404_Information_richness_and_trust_in_V-commerce_implications_for_services_marketing

ε. Διαδραστικότητα (Interactivity)

Οι τεχνολογίες ηλεκτρονικού εμπορίου είναι διαδραστικές καθώς στηρίζουν την αμφίδρομη σχέση επιχείρησης- καταναλωτή και επιτρέπουν την αλληλεπίδραση των δύο μερών κάνοντας τη σχέση έως ένα βαθμό να προσομοιάζει με αυτή του παραδοσιακού εμπορίου. Η επιχείρηση μέσω της διαδραστικότητας προσελκύει πελάτες παρέχοντας τους εμπειρία αγοράς ανάλογης της εμπειρίας αγοράς στα φυσικά καταστήματα όπου έμπορος και πελάτης συναλλάσσονται πρόσωπο με πρόσωπο αλλά σε παγκόσμια κλίμακα.

Ένας από τους πιο προφανής τρόπους για να αναπτυχθεί η διαδραστικότητα μεταξύ επιχείρησης και καταναλωτών είναι τα μέσα κοινωνικής δικτύωσης. Ωστόσο αυτό δεν σημαίνει ότι αρκεί ένας στατικός λογαριασμός όπου η επιχείρηση μοιράζεται μόνο περιεχόμενο και ενημερώσεις. Θα πρέπει μέσω αυτών των λογαριασμών η επιχείρηση να αλληλεπιδρά με τους καταναλωτές και τους πελάτες και να ανταποκρίνεται. Δηλαδή θα πρέπει να απαντά σε σχόλια, ερωτήσεις, παράπονα και αναφορές έγκαιρα με σοβαρότητα και ενσυναίσθηση. Η αλληλεπίδραση με έναν πελάτη αυτόματα μεταφέρει το μήνυμα ότι αυτή η οικειότητα και η προσβασιμότητα αφορά όλους τους πελάτες. Με αυτό τον τρόπο αλληλεπίδρασης ενισχύεται η αναγνωρισιμότητα της επιχείρησης και είναι δυνατή η προσέλκυση περισσότερων πελατών.

Η διαδραστικότητα της επιχείρησης όμως πρέπει να υπάρχει και στον ιστότοπο της επιχείρησης. Θα πρέπει το περιεχόμενο του ιστοτόπου να προκαλεί το ενδιαφέρον των καταναλωτών όπως άρθρα και αναρτήσεις ιστολογίου. Με αυτό τον τρόπο αυξάνεται η πιθανότητα οι καταναλωτές να παραμείνουν στην ιστοσελίδα και να αγοράσουν προϊόντα μέσω αυτής. Επίσης το να υπάρχει κάπου να πάει στη συνέχεια ο καταναλωτής θα τον κάνει να αλληλεπιδράσει περισσότερο με μία σελίδα. Για παράδειγμα μία ανάρτηση ιστολογίου μπορεί να οδηγήσει στη σελίδα ενός συγκεκριμένου προϊόντος. Από εκεί μπορεί να βρεθεί στις αξιολογήσεις και κριτικές του προϊόντος και μετά στη σελίδα με τις συχνές ερωτήσεις που το αφορούν. Η διαδραστικότητα ενός ιστοτόπου επιτυγχάνεται και με τις επιλογές εξατομίκευσης όπως επιλογή προτιμώμενης γλώσσας ή τα φίλτρα που εξατομικεύουν την αναζήτηση και την προσαρμόζουν στις επιθυμίες του καταναλωτή. Τέλος διαδραστικότητα στις ιστοσελίδες των επιχειρήσεων προσφέρουν εφαρμογές όπως τα chatbots που δίνουν την εντύπωση στον καταναλωτή της ζωντανής συνομιλίας ή εφαρμογές επαυξημένης πραγματικότητας μέσω των οποίων ο καταναλωτής μπορεί να δοκιμάσει τα προϊόντα πριν τα αγοράσει.

στ. Πυκνότητα πληροφοριών (Information density)[13]

Η πυκνότητα πληροφοριών είναι κάτι ευρύτερο από την επάρκεια των πληροφοριών. Όσον αφορά στο ηλεκτρονικό εμπόριο η πυκνότητα των πληροφοριών αναφέρεται στον όγκο, την επάρκεια, την ποιότητα και την πολυπλοκότητα των πληροφοριών που είναι διαθέσιμες στους καταναλωτές και τις επιχειρήσεις στην ηλεκτρονική αγορά και συμβάλλει σημαντικά στη διαμόρφωση της συμπεριφοράς των καταναλωτών και την λήψη της σχετικής απόφασης για την πραγματοποίηση ή μη της αγοράς, στη βελτίωση της λήψης αποφάσεων και στην ώθηση των μετατροπών. Μπορεί να έχει θετικές και αρνητικές επιπτώσεις στην εμπειρία του πελάτη.

Προκειμένου να εξηγήσουμε τη σημασία της έννοιας της πυκνότητας θα μπορούσαμε να επαναλάβουμε όσα περιγράφονται στο υποκεφάλαιο 5.4 για την επάρκεια των πληροφοριών καθώς οι δύο έννοιες προσομοιάζουν μέχρι ένα βαθμό. Βάθος στις πληροφορίες προσφέρουν οι αναλυτικές και λεπτομερείς περιγραφές των προϊόντων σχετικά με τα χαρακτηριστικά τους, τις προδιαγραφές τους, τις τιμές τους, την διαθεσιμότητά τους καθώς και ο,τιδήποτε μπορεί να συμβάλλει στην ενίσχυσή τους για να γίνουν κατανοητές από τους καταναλωτές όπως εικόνες, βίντεο, εγχειρίδια χρήσης κ.α.

Ποιότητα και όγκο στις πληροφορίες παρέχουν οι κριτικές και οι αξιολογήσεις των πελατών που έχουν ήδη αγοράσει και χρησιμοποιήσει το προϊόν, τόσο οι θετικές όσο και οι αρνητικές, αν και υπάρχει ο κίνδυνος οι τελευταίες να αποθαρρύνουν τους καταναλωτές από την πραγματοποίηση της αγορά. Η ποιότητα ενισχύεται από την τακτική οι πελάτες μαζί με την κριτική ή την αξιολόγηση να ανεβάζουν κι φωτογραφίες και βίντεο όπου να δείχνουν «ζωντανά» το προϊόν και να αναδείξουν την ποιότητά του (καλή ή κακή), τη λειτουργικότητά του και τη χρηστικότητά του.

«Βάθος» και όγκο στις πληροφορίες προσφέρουν εκτός από τις σχετικές με την ευδιάκριτη τιμολόγησή του και πληροφορίες που σχετίζονται με το επίπεδο της τιμής σε σύγκριση με τα υπόλοιπα ηλεκτρονικά καταστήματα. Υπάρχουν δηλαδή ιστοσελίδες που επισημαίνουν ότι η συγκεκριμένη τιμή στην οποία προσφέρει το προϊόν το κατάστημα είναι η χαμηλότερη ενός συγκεκριμένου διαστήματος π.χ. των τριάντα (30) τελευταίων ημερών.

Η πυκνότητα των πληροφοριών αυξάνει επίσης με τις λεπτομερείς και κατατοπιστικές πληροφορίες αποστολής, παραλαβής, επιστροφής ή αλλαγής των προϊόντων όπως και οι λεπτομερείς πληροφορίες σχετικά με την επικοινωνία και την υποστήριξη των πελατών.

[13] «The Concept of e-Commerce», Dr. Rohit Sublaik, 2022, WKRISHIND PUBLISHERS, σελ. 15

ζ. Εξατομίκευση/ Προσαρμογή (Personalization/ Customization)

Η εξατομίκευση και η προσαρμογή είναι δύο στρατηγικές που χρησιμοποιούνται στο ηλεκτρονικό εμπόριο για να προσαρμόσουν την εμπειρία αγορών ώστε να ανταποκρίνονται στις προτιμήσεις και τις ανάγκες κάθε πελάτη ξεχωριστά.

Η εξατομίκευση στο ηλεκτρονικό εμπόριο περιλαμβάνει τη χρήση δεδομένων τεχνολογίας για την παροχή εξατομικευμένου περιεχομένου, προτάσεων προϊόντων και προσφορών με βάση το ιστορικό περιήγησης, τα δημογραφικά στοιχεία, τις προηγούμενες αγορές και άλλα μοτίβα συμπεριφοράς. Οι πλατφόρμες ηλεκτρονικού εμπορίου μέσω της ανάλυσης και της κατανόησης των δεδομένων των πελατών μπορούν να παρέχουν εξατομικευμένες προτάσεις προϊόντων και υπηρεσιών, προσαρμοσμένα μηνύματα ηλεκτρονικού ταχυδρομείου και εξατομικευμένες ιστοσελίδες κάνοντας την διαδικασία αγορών μέσω ηλεκτρονικού εμπορίου μία ευχάριστη και ελκυστική εμπειρία.

Η τακτική της προσαρμογής από την άλλη πλευρά δίνει τη δυνατότητα στους πελάτες να εξατομικεύουν και να τροποποιούν ορισμένες πτυχές των προϊόντων και των υπηρεσιών που αγοράζουν. Με αυτό τον τρόπο οι πελάτες συμμετέχουν ενεργά στο σχεδιασμό και την εξατομίκευση των προϊόντων προσαρμόζοντάς τα στις επιθυμίες και τις ανάγκες τους. Οι επιλογές προσαρμογής μπορούν να περιλαμβάνουν επιλογές χρώματος, μεγέθους, υλικού καθώς και άλλα χαρακτηριστικά εξατομίκευσης. Με την προσαρμογή ο πελάτης έχει την αίσθηση της προσωποποίησης κατά την αγορά ενώ μπορεί να αγοράζει προϊόντα που συνάδουν απόλυτα στις επιθυμίες του και τις απαιτήσεις του.

η. Κοινωνική τεχνολογία (Social Technology)

Η κοινωνική τεχνολογία στο ηλεκτρονικό εμπόριο αναφέρεται στην ενσωμάτωση εργαλείων, πλατφορμών και λειτουργιών κοινωνικής δικτύωσης μέσα στο περιβάλλον του ηλεκτρονικού εμπορίου για τη βελτίωση της εμπειρίας αγορών στο διαδίκτυο. Αρχικά πρόκειται για τις απευθείας πωλήσεις που πραγματοποιούνται μέσω των πλατφορμών κοινωνικής δικτύωσης όπως το Facebook, Instagram, TikTok κ.α. Χαρακτηριστική περίπτωση είναι το Market Place του Facebook όπου κάποιος μπορεί να πουλήσει από ρούχα και αξεσουάρ μέχρι έπιπλα και σπίτια.

Άλλη μορφή κοινωνικής τεχνολογίας είναι η συνεργασία με τους λεγόμενους influencers (άτομα με μεγάλο αριθμό ακολούθων στους λογαριασμούς κοινωνικής δικτύωσης). Στο πλαίσιο του μάρκετινγκ οι επιχειρήσεις συνεργάζονται επ' αμοιβή με τα συγκεκριμένα άτομα προκειμένου να δημιουργήσουν περιεχόμενο (συνήθως βίντεο ή εικόνες) και να προωθήσουν το προϊόν στους ακολούθους τους.

Υπάρχει ωστόσο και η αντίστροφη σχέση μεταξύ των ιστοσελίδων ηλεκτρονικού εμπορίου και των πλατφορμών κοινωνικής δικτύωσης. Συγκεκριμένα οι ιστοσελίδες ηλεκτρονικού εμπορίου διαθέτουν συνδέσμους που παραπέμπουν στους λογαριασμούς που διατηρούν στα μέσα κοινωνικής δικτύωσης αυξάνοντας την αλληλεπίδραση με τους καταναλωτές ενώ πολλές φορές υπάρχει η δυνατότητα να δουν οι καταναλωτές τι αγόρασαν κοινοί φίλοι στα μέσα κοινωνικής δικτύωσης.

Οι πλατφόρμες κοινωνικής δικτύωσης μπορούν να χρησιμοποιηθούν από τις εταιρείες ως ένα επιπλέον κανάλι επικοινωνίας και υποστήριξης των πελατών. Χρησιμοποιούν δηλαδή την εφαρμογή μηνυμάτων που παρέχουν οι πλατφόρμες όπως π.χ. το Facebook Messenger για να απαντούν σε ερωτήματα των καταναλωτών άμεσα, γρήγορα και με πιο προσωπικό τρόπο. Οι απαντήσεις στα ερωτήματα δίνονται είτε από το προσωπικό της επιχείρησης είτε η επιχείρηση έχει ενσωματώσει τεχνολογία τεχνητής νοημοσύνης και οι απαντήσεις δίνονται μέσω chatbots.

θ. Βιωσιμότητα (Sustainability)

Το ηλεκτρονικό εμπόριο παίζει μεγάλο ρόλο στην προώθηση της βιωσιμότητας και στη μείωση του αποτυπώματος άνθρακα. Οι πελάτες μπορούν να αποφύγουν την μετάβαση σε φυσικά καταστήματα και να πραγματοποιήσουν τις αγορές τους μέσω ηλεκτρονικών καταστημάτων και έτσι να μειώσουν τις εκπομπές άνθρακα. Επιπλέον, οι επιχειρήσεις ηλεκτρονικού εμπορίου έχουν την δυνατότητα να χρησιμοποιούν πιο βιώσιμα υλικά και μεθόδους συσκευασίας σε σύγκριση με το παραδοσιακό λιανικό εμπόριο.

Επιπλέον, με την άνοδο του dropshipping (διαδικτυακός μεσάζων) και της παραγωγής κατ' απαίτηση, οι επιχειρήσεις μπορούν να διατηρήσουν χαμηλά τα επίπεδα αποθεμάτων και να παράγουν προϊόντα μόνο όταν υπάρχει ζήτηση για αυτά. Αυτό μειώνει την ποσότητα του πλεονάζοντος αποθέματος και των απορριμμάτων, καθιστώντας το ηλεκτρονικό εμπόριο μια πιο φιλική προς το περιβάλλον επιλογή.

ι. Αυξημένος Ανταγωνισμός (Increased Competition)

Ο αυξημένος ανταγωνισμός στο ηλεκτρονικό εμπόριο αναφέρεται στον αυξανόμενο αριθμό επιχειρήσεων και ηλεκτρονικών καταστημάτων που συναγωνίζονται για την προσέλκυση περισσότερων καταναλωτών και την αύξηση των πωλήσεων στην ψηφιακή αγορά. Καθώς το ηλεκτρονικό εμπόριο έχει επεκταθεί παγκοσμίως, έχει γίνει ευκολότερο για τις επιχειρήσεις —τόσο μεγάλες όσο και μικρές— να εισέλθουν στην αγορά και να ανταγωνίζονται μεταξύ τους. Ο αυξανόμενος ανταγωνισμός λειτουργεί προς όφελος των

καταναλωτών καθώς επωφελούνται από περισσότερες επιλογές προϊόντων, χαμηλότερες τιμές και καλύτερες υπηρεσίες. Ωστόσο δημιουργεί αυξανόμενες δυσκολίες και προκλήσεις για τις επιχειρήσεις που πρέπει διαρκώς να βελτιώνουν τις υπηρεσίες που παρέχουν, να βελτιώνουν την ποσότητα και την ποιότητα των προϊόντων που προσφέρουν σε συνάρτηση με τις καλύτερες τιμές είτε με τη λογική της χαμηλότερης τιμής είτε με τη λογική της καλύτερης τιμής σε συνάρτηση με την ποιότητα και την ποσότητα του προσφερόμενου προϊόντος.

## 4. Πλεονεκτήματα Ηλεκτρονικού Εμπορίου

Το ηλεκτρονικό εμπόριο σε όλες του τις μορφές αποτελεί μία εναλλακτική του κλασικού εμπορίου που πραγματοποιείται μέσω των φυσικών καταστημάτων όπου απευθύνονται οι καταναλωτές για την αγορά αγαθών και υπηρεσιών. Μάλιστα με την εξέλιξη του διαδικτύου πλέον καταλαμβάνει περίοπτη θέση στον τομέα των εμπορικών συναλλαγών προσφέροντας πληθώρα πλεονεκτημάτων τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές.

### α. Πλεονεκτήματα ηλεκτρονικού εμπορίου για τις επιχειρήσεις.

Ένα από τα μεγαλύτερα πλεονεκτήματα του ηλεκτρονικού εμπορίου είναι η δυνατότητα των επιχειρήσεων να προσεγγίσει πελάτες σε παγκόσμιο επίπεδο. Δεν είναι απαραίτητο να περιοριστούν σε πελάτες που βρίσκονται σε μία συγκεκριμένη περιοχή αλλά οπουδήποτε στον κόσμο.

Η μείωση των λειτουργικών εξόδων για τις επιχειρήσεις μειώνονται δεδομένου ότι η λειτουργία ενός ηλεκτρονικού καταστήματος είναι πολύ πιο οικονομική από τη λειτουργία ενός φυσικού καταστήματος. Δεν χρειάζεται η ενοικίαση ή η αγορά κάποιου χώρου όπου θα στεγαστεί το φυσικό κατάστημα αλλά αρκεί η αγορά χώρου φιλοξενίας ιστοσελίδας που είναι σαφώς οικονομικότερη. Για ένα κατάστημα ηλεκτρονικού εμπορίου το τυπικό κόστος περιλαμβάνει την κατοχύρωση της επωνυμίας, την κατασκευή και φιλοξενία της ιστοσελίδας και το απόθεμα εμπορεύματος.

Η δυνατότητα των επιχειρήσεων να ανταποκρίνονται γρηγορότερα στις τάσεις της αγοράς και στις απαιτήσεις των πελατών αξιοποιώντας την εξέλιξη στον τομέα των logistics είναι ένα τρίτο πολύ σοβαρό πλεονέκτημα. Μάλιστα οι επιχειρήσεις μπορούν τάχιστα να ξεκινήσουν καμπάνιες και προσφορές ώστε να προσελκύσουν συντομότερα περισσότερους πελάτες.

Σημαντική είναι επίσης η δυνατότητα των επιχειρήσεων να μπορούν πολύ γρήγορα να εμπορεύονται και να προωθούν τα προϊόντα τους με νέους τρόπους. Σε ελάχιστο χρόνο και με ελάχιστο κόπο μπορούν να ξεκινήσουν προγράμματα αφοσίωσης και επιβράβευσης, να ανακοινώσουν την κυκλοφορία νέων προϊόντων και να προχωρήσουν σε στοχευμένες διαφημίσεις στα κοινωνικά δίκτυα.

Το ηλεκτρονικό εμπόριο προσφέρει πολλαπλά κανάλια πωλήσεων, όπως για παράδειγμα τα μέσα κοινωνικής δικτύωσης, εφαρμογές για κινητά, ιστοσελίδες, ιστολόγια, διαφημίσεις με banner, διαφημίσεις στη Google κ.α. Εξίσου σημαντικό πλεονέκτημα είναι η δυνατότητα επέκτασης του φυσικού καταστήματος χωρίς στην πραγματικότητα να χρειαστεί το φυσικό κατάστημα να μετακινηθεί σε μεγαλύτερο χώρο ή χωρίς να απαιτείται το άνοιγμα νέων καταστημάτων με τη μορφή αλυσίδας και συνεπώς την επιβάρυνση επιπλέον κόστους για την επέκτασή του. Αρκεί να βελτιωθεί η υποδομή της πληροφορικής του ηλεκτρονικού καταστήματος, να αυξηθούν τα κανάλια επικοινωνίας με τους πελάτες, να αναβαθμιστούν τα προϊόντα και οι υπηρεσίες και να συμπεριληφθούν περισσότερες επιλογές πληρωμής.

Τέλος αν και όχι μικρότερης σημασίας είναι οι δυνατότητες που αποκτούν οι επιχειρήσεις από τη συλλογή δεδομένων των πελατών. Οι επιχειρήσεις αξιοποιώντας τις πληροφορίες για τις αγοραστικές συνήθειες των πελατών, τα δημογραφικά στοιχεία και τις προτιμήσεις τους μπορούν να προωθήσουν καλύτερα τα προϊόντα τους. Μπορούν να προβλέψουν πότε η ζήτηση ενός προϊόντος θα είναι υψηλότερη ή χαμηλότερη ώστε να προσαρμόσουν τη διαθεσιμότητα των προϊόντων και τις απαιτούμενες υπηρεσίες για να φτάσουν τα προϊόντα στους πελάτες. Επίσης με τις πληροφορίες αυτές μπορούν να κάνουν την εμπειρία αγορών μέσω ηλεκτρονικού καταστήματος ευκολότερη για τον πελάτη.

β. Πλεονεκτήματα για τους καταναλωτές.

Το δεύτερο μέρος μίας συναλλαγής, ο καταναλωτής, είναι εξίσου σημαντικό και καθοριστικό του εμπορίου αφού η ζήτηση του καταναλωτή είναι αυτή που καθορίζει την προσφορά, τα δε πλεονεκτήματα του ηλεκτρονικού εμπορίου για τον καταναλωτή είναι εξίσου σημαντικά.

Όπως προέκυψε και από την μεγάλη έρευνα που πραγματοποίησε η Επιτροπή Ανταγωνισμού, τα αποτελέσματα της οποίας περιγράφονται στην Τελική Έκθεση που δημοσιεύτηκε τον Νοέμβριο του 2022, τα οφέλη του ηλεκτρονικού εμπορίου για τους καταναλωτές όπως οι ίδιοι τα περιγράφουν είναι: i) η δυνατότητα αγοράς χωρίς μετακίνηση-ευκολία, ii) η δυνατότητα πραγματοποίησης αγοράς σε βραδινές ώρες/ σε ώρες που τα

φυσικά καταστήματα δεν λειτουργούν, iii) η πρόσβαση σε προϊόντα που δεν υπάρχουν σε φυσικά καταστήματα και iv) η υγιεινή- αποφυγή συγχρωτισμού[14].

Το ηλεκτρονικό εμπόριο παρέχει στους καταναλωτές ευκολία ως προς το χρόνο και τον τόπο που μπορούν να αγοράσουν οτιδήποτε χωρίς τους περιορισμούς των ωρών λειτουργίας των καταστημάτων ή των γεωγραφικών τοποθεσιών. Αυτή η προσβασιμότητα τους επιτρέπει οποιαδήποτε ώρα της ημέρας, οποιαδήποτε ημέρα της εβδομάδας από όπου και αν βρίσκονται, στην οικία τους, στην εργασία τους ή ακόμη και εν κινήσει στο αυτοκίνητό τους ή στα μέσα μαζικής μεταφοράς, να πραγματοποιήσουν αγορές. Επίσης οι καταναλωτές μπορούν να κάνουν τις αγορές τους μακριά από τον συγχρωτισμό καταναλωτών στα καταστήματα και της αναμονής «στην ουρά» για να ολοκληρώσουν την αγορά τους στο ταμείο. Επιπλέον με την ποικιλία επιλογών πληρωμής, paypal, χρεωστικές ή πιστωτικές κάρτες, κατάθεση σε λογαριασμό στην τράπεζα, ο κάθε καταναλωτής μπορεί να επιλέξει τον τρόπο που τον εξυπηρετεί.

Η ευρεία επιλογή προϊόντων και υπηρεσιών που παρέχει το ηλεκτρονικό εμπόριο είναι ένα ακόμη ουσιαστικό πλεονέκτημα. Οι ηλεκτρονικές αγορές δίνουν πρόσβαση σε μεγαλύτερη ποικιλία προϊόντων από ό,τι υπάρχει στα φυσικά καταστήματα. Οι ηλεκτρονικές αγορές επιτρέπουν τη σύγκριση πληροφοριών και τιμών μέσω ειδικών ιστοτόπων ή εφαρμογών που περιέχουν οι ιστοσελίδες ώστε ο καταναλωτής να εντοπίζει την καλύτερη προσφορά και να διασφαλίζει ότι αποκομίζει τη μεγαλύτερη αξία για τα χρήματά του.

Τα ηλεκτρονικά καταστήματα «παρακολουθούν» τις συνήθειες περιήγησης των καταναλωτών και τις παλαιότερες αγορές ώστε να προτείνουν εξατομικευμένα προϊόντα. Αυτό κάνει πιο ευχάριστη τη διαδικασία των αγορών και ενισχύει την εμπιστοσύνη των καταναλωτών με μία προσαρμοσμένη επάνω τους διαδικτυακή εμπειρία αγοράς. Η αγοραστική εμπειρία των καταναλωτών ενισχύεται και από τη δυνατότητα πριν την αγορά να μπορούν να διαβάζουν τις περιγραφές των προϊόντων, τις αξιολογήσεις και τις κριτικές τους από άλλους καταναλωτές που τα έχουν αγοράσει. Με αυτό τον τρόπο έχουν τη δυνατότητα να καταλήγουν στην καταλληλότερη για αυτούς αγορά.

5. Μειονεκτήματα ηλεκτρονικού εμπορίου.

Όπως κάθε νόμισμα έχει δύο όψεις έτσι και το ηλεκτρονικό εμπόριο πέρα από πλεονεκτήματα έχει και μειονεκτήματα για τα εμπλεκόμενα μέρη, τα οποία ουδόλως θα

[14] Τελική Έκθεση επί της κατ' άρθρο 40 του Ν. 3959/2011 Κλαδικής Έρευνας στο Ηλεκτρονικό Εμπόριο της Επιτροπής Ανταγωνισμού, Αθήνα, Νοέμβριος 2022, σελ. 255-256 https://www.epant.gr/enimerosi/dimosieyseis/kladikes/item/2472-teliki-ekthesi-kladikis-erevnas-sto-ilektroniko-emporio.html

μπορούσαν να χαρακτηριστούν ως ασήμαντα και αδιάφορα. Τα μειονεκτήματα αυτά έγκεινται στους κινδύνους που ελλοχεύουν στο πλαίσιο των ηλεκτρονικών αγορών, τους οποίους θα πρέπει τα μέρη να γνωρίζουν και να κατανοούν.

α. Μειονεκτήματα για τις επιχειρήσεις.

Η δημιουργία ενός ηλεκτρονικού καταστήματος μπορεί να είναι δύσκολη για άτομα που δεν διαθέτουν τεχνική εμπειρία. Σε πολλές περιπτώσεις απαιτείται τεχνική εξειδίκευση για να εξασφαλιστεί ότι ο ιστότοπος είναι βελτιωμένος για χρήση π.χ. από κινητές συσκευές ή για να διορθωθούν τεχνικά προβλήματα που πιθανόν να ανακύψουν.

Στο ηλεκτρονικό εμπόριο ο κίνδυνος ασφαλείας είναι υψηλός. Οι επιχειρήσεις χρειάζεται να αποθηκεύουν προσωπικά δεδομένα των καταναλωτών όπως διευθύνσεις κατοικίας ή στοιχεία των τραπεζικών καρτών. Προϋπόθεση επομένως αποτελεί η ύπαρξη μίας ασφαλούς ιστοσελίδας για τη διεξαγωγή του ηλεκτρονικού εμπορίου προστατευμένη από οποιαδήποτε απειλή.

Ο περιορισμός αποκλειστικά στη χρήση του ηλεκτρονικού εμπορίου μπορεί να οδηγήσει μία εταιρεία στην απώλεια καταναλωτών. Και αυτό συμβαίνει γιατί υπάρχει μερίδα καταναλωτών που προτιμούν την αγορά στα φυσικά καταστήματα ώστε να έχουν τη δυνατότητα να εκτιμήσουν δια ζώσης το προϊόν που πρόκειται να το αγοράσουν, να κρίνουν την ποιότητά του και να το δοκιμάσουν πριν προβούν σε αγορά.

Σημαντικός παράγοντας στο ηλεκτρονικό εμπόριο είναι το κόστος αποστολής των προϊόντων που σε κάποιες περιπτώσεις θα μπορούσε να επηρεάσει αρνητικά την διαδικασία αγοράς. Το κόστος αποστολής διαφοροποιείται ανάλογα την τοποθεσία του πελάτη, το χρόνο παράδοσης και το προϊόν. Τα έξοδα αποστολής προστίθενται στην τελική τιμή αγοράς του προϊόντος, η οποία αν είναι πολύ υψηλή θα αποθαρρύνει τους καταναλωτές από το να πραγματοποιήσουν μια αγορά.

Ζήτημα ανακύπτει και με τον υπολογισμό των φόρων στην περίπτωση των διαφορετικών γεωγραφικών τοποθεσιών. Οι χώρες εφαρμόζουν διαφορετική φορολογική ρύθμιση για τα διάφορα προϊόντα προκαλώντας δυσκολίες στις επιχειρήσεις να υπολογίζουν το φόρο και το επιπλέον κόστος που δημιουργείται για το προϊόν.

β. Μειονεκτήματα για τους καταναλωτές.

Σημαντικά μειονεκτήματα εμφανίζει το ηλεκτρονικό εμπόριο και για τους καταναλωτές. Αρχικά ενδέχεται να αντιμετωπίσουν ζητήματα ασφάλειας. Οι καταναλωτές προκειμένου να

ολοκληρώσουν μία αγορά χρειάζεται να παρέχουν στο ηλεκτρονικό κατάστημα προσωπικά τους δεδομένα όπως διεύθυνση κατοικίας και δεδομένα των τραπεζικών τους καρτών. Υπάρχει ο κίνδυνος πάντοτε οι ιστοσελίδες των ηλεκτρονικών καταστημάτων να αποτελέσουν θύματα ψηφιακής απάτης με αποτέλεσμα να υποκλαπούν/διαρρεύσουν τα στοιχεία των καταναλωτών.

Στο ηλεκτρονικό εμπόριο οι καταναλωτές δεν μπορούν να δούνε το προϊόν σε φυσική μορφή με αποτέλεσμα να μην μπορούν να εκτιμήσουν αν ανταποκρίνεται στην αξία του, να ελέγξουν την ποιότητά του ή να διαπιστώσουν αν τους ταιριάζει. Έτσι πάντοτε υπάρχει ο κίνδυνος να μην μείνουν ευχαριστημένοι, κάτι που θα οδηγούσε στην επιστροφή των προϊόντων με αντίστοιχη επιστροφή των χρημάτων και σε κακές κριτικές και αξιολογήσεις.

Σε αντίθεση με το φυσικό εμπόριο όπου τα προϊόντα λαμβάνονται αμέσως από τους καταναλωτές, στο ηλεκτρονικό εμπόριο οι χρόνοι αποστολής είναι ένα από τα μεγαλύτερα μειονεκτήματα. Ενώ σε αρκετές περιπτώσεις η αποστολή των προϊόντων μπορεί να γίνει αυθημερόν από το κατάστημα, οι πελάτες συνήθως λαμβάνουν τις παραγγελίες τους μετά από δύο ή και περισσότερες ημέρες όσον αφορά ηλεκτρονικά καταστήματα που εδρεύουν εντός των ορίων της χώρας διαμονής τους, ενώ στις περιπτώσεις διεθνών αγορών οι χρόνοι αποστολής μπορεί να ανέλθουν και σε τρεις με τέσσερις βδομάδες, αν όχι και περισσότερο.

Ένα επιπλέον δαπανηρό μειονέκτημα είναι το κόστος αποστολής, το οποίο εξαρτάται από τον τόπο διαμονής του πελάτη, το χρόνο παράδοσης του προϊόντος αλλά και από τη φύση και το μέγεθος του προϊόντος. Κάποιες φορές το κόστος αποστολής είναι αρκετά υψηλό και προστίθεται στο κόστος του προϊόντος ενώ τα καταστήματα δεν μπορούν πάντα να απορροφήσουν το εν λόγω κόστος και το μετατοπίζουν στον καταναλωτή.

Σε ένα φυσικό κατάστημα οι καταναλωτές εφόσον έχουν κάποια ερώτηση ή ένα πρόβλημα μπορούν να απευθυνθούν σε έναν υπάλληλο του καταστήματος για βοήθεια. Σε ένα ηλεκτρονικό κατάστημα εμπορίου η εξυπηρέτηση πελατών είναι περιορισμένη. Ο ιστότοπος μπορεί να παρέχει υποστήριξη μόνο κατά τη διάρκεια συγκεκριμένων ωρών ενώ το αυτοματοποιημένο σύστημα τεχνητής νοημοσύνης που πλέον υφίσταται σχεδόν σε όλα τα ηλεκτρονικά καταστήματα ενδεχομένως να μην είναι σε θέση να απαντήσει σε μία συγκεκριμένη ερώτηση ή να δώσει την κατάλληλη λύση.

Τέλος το ηλεκτρονικό εμπόριο προϋποθέτει γνώση χρήσης ηλεκτρονικών υπολογιστών ή κινητών συσκευών καθώς και γνώση χειρισμού ιστοσελίδων καθώς και πλοήγησης στο διαδίκτυο. Αυτονόητη προϋπόθεση είναι η σύνδεση με πάροχο διαδικτύου είτε ασύρματα είτε ενσύρματα ώστε ο καταναλωτής να μπορεί να περιηγηθεί στο διαδίκτυο για να κάνει τις ηλεκτρονικές του αγορές. Υπάρχει επομένως μία μεγάλη μερίδα καταναλωτών ιδίως

μεγαλύτερων σε ηλικία που δεν διαθέτουν γνώσεις χρήσης του διαδικτύου ή/και πρόσβαση σε ηλεκτρονικό υπολογιστή ή ασύρματη συσκευή με αποτέλεσμα να επιλέγουν το φυσικό εμπόριο για τις αγορές τους.

## 6. Ηλεκτρονικό κατάστημα (e-shop) και ηλεκτρονική πλατφόρμα αγορών (marketplace)

### α. Ηλεκτρονικό κατάστημα (e-shop)

Το ηλεκτρονικό εμπόριο αφορά το σύνολο των ενεργειών που περιλαμβάνει την μεταφορά χρημάτων και την ανταλλαγή δεδομένων για την εκτέλεση συναλλαγών μεταξύ μιας επιχείρησης και ενός καταναλωτή για την πραγματοποίηση αγοράς προϊόντων ή υπηρεσιών. Οι διεργασίες αυτές πραγματοποιούνται μέσω ιστοτόπων, των ηλεκτρονικών καταστημάτων, (e-shops) τα οποία συνδυάζουν τεχνολογίες, πληροφορίες και επικοινωνίες για την υποστήριξη όλων των απαιτούμενων εργασιών για την ολοκλήρωση μιας αγοραπωλησίας μέσω διαδικτύου χωρίς φυσική παρουσία των μερών κατά τη διάρκεια της συναλλαγής. Το ηλεκτρονικό κατάστημα επομένως είναι η ιστοσελίδα μέσω της οποίας οι καταναλωτές μπορούν να πραγματοποιούν αγορές προϊόντων μέσω του διαδικτύου. Μπορεί να αποτελεί τη «βιτρίνα» ενός φυσικού καταστήματος στο διαδίκτυο αλλά μπορεί να αποτελεί και το ίδιο κατάστημα χωρίς την ύπαρξη αντίστοιχου φυσικού. Εντάσσεται επομένως στην κατηγορία ηλεκτρονικού εμπορίου «Επιχείρηση προς καταναλωτή (Business to Consumer)».

Με την έξαρση του ηλεκτρονικού εμπορίου τα ηλεκτρονικά καταστήματα αυξάνονται τάχιστα εξαιτίας της ευκολίας που προσφέρουν για την διεξαγωγή εμπορικών συναλλαγών. Τα καταστήματα αυτά υπερτερούν των φυσικών καταστημάτων σε πολλά σημεία κάνοντας πιο ελκυστικά τα πρώτα.

Κυριότερο πλεονέκτημα των ηλεκτρονικών καταστημάτων θα μπορούσε να πει κάποιος ότι είναι η δυνατότητα συνεχούς λειτουργίας 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Δίνουν έτσι τη δυνατότητα στους καταναλωτές να πραγματοποιούν τις αγορές τους οποιαδήποτε ώρα της ημέρας χωρίς τους περιορισμούς του ωραρίου των φυσικών καταστημάτων.

Δεύτερο μεγάλο πλεονέκτημα είναι ο μη περιορισμός από γεωγραφικά όρια. Η πελατεία ενός ηλεκτρονικού καταστήματος θα μπορούσε εν δυνάμει να αντιστοιχεί με όλους τους συνδεδεμένους χρήστες στο διαδίκτυο ανεξάρτητα από την γεωγραφική τοποθεσία στην οποία βρίσκονται σε σχέση με ένα φυσικό κατάστημα που απευθύνεται σε πελάτες που

βρίσκονται σε περιορισμένο γεωγραφικό χώρο. Αυτόματα η πελατεία ενός ηλεκτρονικού καταστήματος είναι πολύ μεγαλύτερη από αυτή ενός φυσικού καταστήματος.

Στα σημεία που υπερτερεί το ηλεκτρονικό κατάστημα πρέπει να προστεθεί το γεγονός ότι δεν απαιτείται ιδιαίτερα μεγάλος φυσικός χώρος για τη λειτουργία του, καθώς αρκεί να υπάρχει μόνο χώρος αποθήκευσης του αποθέματος. Ειδικά στην περίπτωση αυτών που λειτουργούν με τη μορφή των διαδικτυακών μεσαζόντων, δεν χρειάζεται ούτε καν η ύπαρξη φυσικού χώρου όπου θα στεγάζεται το απόθεμα του καταστήματος. Αυτό σημαίνει ότι το κόστος συντήρησης ενός ηλεκτρονικού καταστήματος είναι πολύ μικρότερο από ένα φυσικό αφού το πρώτο είναι πολλές φορές απαλλαγμένο από καταβολή ενοικίων, πληρωμή λογαριασμών και λοιπών εξόδων. Τα λειτουργικά έξοδα τους μειώνονται ακόμη περισσότερο δεδομένου ότι το κόστος εξυπηρέτησης πελατών για τα ηλεκτρονικά καταστήματα είναι ακόμη μικρότερο από αυτό των φυσικών. Τα ηλεκτρονικά καταστήματα δεν χρειάζονται τόσους υπαλλήλους όσο τα φυσικά και επομένως οι ανάγκες για καταβολή μισθών, ασφαλιστικών εισφορών κ.α. είναι μικρότερες. Δεν είναι απαραίτητη η ύπαρξη μεγάλης ποσότητας αποθέματος, γεγονός που σημαίνει ότι μειώνεται και το κόστος του αποθέματος που δεν θα διατεθεί και συνεπώς η ζημία που προκαλείται από το γεγονός αυτό.

Τελευταίο αλλά επίσης σημαντικό πλεονέκτημα για το ηλεκτρονικό κατάστημα είναι η μεγαλύτερη ευκολία διαφήμισης που παρέχει το διαδίκτυο σε σχέση με το φυσικό κατάστημα. Αφενός η πρόσβαση στους καταναλωτές μέσω των διαδικτυακών διαφημίσεων είναι ευκολότερη σε σχέση με τους κλασικούς τρόπους διαφήμισης (έντυπα περιοδικά, διανομή φυλλαδίων, τηλεόραση, ραδιόφωνο), αφετέρου το αποτέλεσμα είναι αμεσότερο καθώς οι ηλεκτρονικές διαφημίσεις μπορούν να οδηγήσουν τους καταναλωτές απευθείας με διασύνδεση στον ιστότοπο του καταστήματος για να πραγματοποιήσουν τις αγορές τους.

Ωστόσο το ηλεκτρονικό κατάστημα εκτός από πλεονεκτήματα έχει και μειονεκτήματα. Όσο ευέλικτη και να είναι η διαδικασία των αγορών μέσω διαδικτύου δεν παύει να υστερεί σε σχέση με το φυσικό εμπόριο καθώς απουσιάζει η φυσική παρουσία και η φυσική επαφή με το προϊόν προς αγορά. Μπορεί τα ηλεκτρονικά καταστήματα με τη χρήση των τεχνολογιών τεχνητής νοημοσύνης και εικονικής πραγματικότητας να προσφέρουν στους καταναλωτές τη δυνατότητα να «δοκιμάσουν» ψηφιακά το προς αγορά προϊόν, δεν παύει να υστερεί σε σχέση με την δοκιμή του προϊόντος σε φυσική μορφή.

Επίσης η διαδικασία αγοράς μέσω διαδικτύου διαρκεί περισσότερο από την περίπτωση της αγοράς του προϊόντος με φυσική παρουσία δεδομένου ότι μεσολαβεί ο χρόνος αποστολής και παράδοσης του προϊόντος από το ηλεκτρονικό κατάστημα στον καταναλωτή. Αν στον ανωτέρω χρόνο προσθέσουμε και την πιθανότητα, που είναι αρκετά

σοβαρή το προϊόν να χρειάζεται αλλαγή γιατί για παράδειγμα ήταν λάθος το μέγεθος, γίνεται αντιληπτό ότι ο χρόνος της ολοκλήρωσης της αγοράς μεγαλώνει ακόμη περισσότερο μέχρι ο καταναλωτής να λάβει στα χέρια του το προϊόν που τελικά αγόρασε.

Τέλος το πιο σοβαρό μειονέκτημα των ηλεκτρονικών καταστημάτων για τους καταναλωτές είναι η ευκολία διάπραξης εγκληματικών ενεργειών σε βάρος τους με τη χρήση των προσωπικών τους δεδομένων κατόπιν υποκλοπής τους με διάφορες μεθόδους. Για την αντιμετώπιση τέτοιων φαινομένων είναι απαραίτητη η διαρκής εγρήγορση τόσο των καταστημάτων όσο και των καταναλωτών για την προστασία των ηλεκτρονικών συναλλαγών και την διασφάλισή τους. Στο επόμενο κεφάλαιο θα αναπτυχθεί διεξοδικότερα το πρόβλημα της ηλεκτρονικής απάτης σε βάρος των καταναλωτών στο πλαίσιο του ηλεκτρονικού εμπορίου.

β. Ηλεκτρονική πλατφόρμα αγορών (marketplace)

Αγορές προϊόντων εκτός από τα ηλεκτρονικά καταστήματα (e shops) μπορούν να πραγματοποιηθούν και μέσω ηλεκτρονικών πλατφορμών αγορών όπως για παράδειγμα το skroutz. Οι διαδικτυακές πλατφόρμες πωλήσεις προϊόντων και υπηρεσιών αποτελούν βασικό μέρος του ηλεκτρονικού εμπορίου[15]. Σύμφωνα με την Ευρωπαϊκή Επιτροπή πάνω από ένα εκατομμύριο επιχειρήσεις στην ΕΕ πωλούν αγαθά ή ψηφιακές υπηρεσίες μέσω τέτοιων πλατφορμών[16].

Οι διαδικτυακές πλατφόρμες πώλησης στην πραγματικότητα είναι ένα ηλεκτρονικό κατάστημα που φιλοξενεί πολλές επιχειρήσεις, οι οποίες τοποθετούν μόνες τους τα προϊόντα τους. Ο καταναλωτής έχει τη δυνατότητα μέσω της πλατφόρμας αυτής να επιλέξει πολλά προϊόντα από διαφορετικές επιχειρήσεις ταυτόχρονα με μία μόνο παραγγελία και πληρώνοντας μία φορά.

Οι πλατφόρμες αυτές παρέχουν αρκετά πλεονεκτήματα στους καταναλωτές σε σύγκριση με ένα απλό ηλεκτρονικό κατάστημα. Αρχικά οι καταναλωτές έχουν πρόσβαση σε μία τεράστια ποικιλία προϊόντων και υπηρεσιών από διαφορετικές επιχειρήσεις σε μία ενιαία πλατφόρμα. Αυτό σημαίνει ότι μπορούν να βρούν μία πληθώρα επιλογών σε διάφορες κατηγορίες προϊόντων καλύπτοντας ένα ευρύτερο φάσμα αναγκών και προτιμήσεων.

Ως αποτέλεσμα των προαναφερόμενων προκύπτει ένα ακόμη πλεονέκτημα αυτών των πλατφορμών. Ο καταναλωτής έχει τη δυνατότητα της άμεσης σύγκρισης τιμών και

[15] Ενδεικτικές αναφορές των Μέσων Μαζικής Ενημέρωσης για τη σημασία των marketplace: startupper.gr: «Marketplace: Το μέλλον του ηλεκτρονικού εμπορίου είναι εδώ». 10-12-2022, https://startupper.gr/news/98154/marketplace-to-mellon-tou-ilektronikou-eboriou-einai-edo/
[16] https://digital-strategy.ec.europa.eu/el/policies/online-platforms-and-e-commerce

χαρακτηριστικών ώστε να επιλέξει το καλύτερο προϊόν με βάση τις ανάγκες του, την τιμή και την ποιότητά του.

Μία επιπλέον δυνατότητα που παρέχουν αυτές οι πλατφόρμες στους καταναλωτές είναι η δυνατότητα να διαβάζουν τις αξιολογήσεις και τις κριτικές άλλων καταναλωτών σχετικά με την ποιότητα του προϊόντος και την αξιοπιστία της επιχείρησης. Οι ανατροφοδοτήσεις αυτές επιτρέπουν στους καταναλωτές να κατανοήσουν τα πραγματικά χαρακτηριστικά ενός προϊόντος και την απόδοσή του με αποτέλεσμα να αποφεύγουν λανθασμένες αγορές.

Οι πλατφόρμες αυτές έχουν διαισθητικά και εύχρηστα εργαλεία αναζήτησης που επιτρέπουν στον καταναλωτή να βρει γρήγορα και εύκολα αυτό που ψάχνει χωρίς να χρειάζεται να κάνει πολλαπλές αναζητήσεις στα επιμέρους ηλεκτρονικά καταστήματα των επιχειρήσεων.

Στα πλεονεκτήματα τους θα πρέπει να προστεθεί οι εγγυήσεις ασφαλείας και προστασίας του καταναλωτή που παρέχουν ειδικά σε περίπτωση που δεν παραληφθεί το προϊόν ή παρουσιαστεί πρόβλημα στην παραγγελία. Επίσης συχνά προσφέρουν ασφαλή συστήματα πληρωμών (π.χ. paypal, πιστωτικές κάρτες κ.α.) μειώνοντας τον κίνδυνο απάτης.

Οι διαδικτυακές πλατφόρμες πώλησης προϊόντων και υπηρεσιών παρουσιάζουν σημαντικά πλεονεκτήματα σε σχέση με τα μεμονωμένα ηλεκτρονικά καταστήματα βελτιώνοντας την εμπειρία των ηλεκτρονικών αγορών για τους καταναλωτές ωθώντας τους να ακολουθήσουν την διαδικασία του ηλεκτρονικού εμπορίου και στην επόμενη αγορά τους. Είναι χαρακτηριστικό ότι μεγάλες εταιρείες όπως π.χ. Skroutz, Public, Μασούτης κ.α. μεταμόρφωσαν τα ηλεκτρονικά καταστήματά τους (e-shops) σε διαδικτυακές πλατφόρμες πώλησης προϊόντων (marketplaces)[17]

## II. Ηλεκτρονική απάτη

Στο προηγούμενο κεφάλαιο αναπτύχθηκε η έννοια του ηλεκτρονικού εμπορίου, οι κατηγορίες του, οι τεχνολογίες του, τα χαρακτηριστικά του, τα πλεονεκτήματα και τα μειονεκτήματα του. Πρόκειται για έναν τρόπο συναλλαγών που αν και είναι ιδιαίτερα σημαντικός στον τομέα του εμπορίου, είναι ιδιαίτερα ευάλωτος στο να προσβληθεί με κάποιες

[17]blog.public.gr: «Τα Public δημιουργούν το 1ο ελληνικό marketplace», Δελτίο τύπου στις 14-05-2018, https://blog.public.gr/ta-public-dimiourgoun-1o-elliniko-marketplace.
Παρομοίως, businessnews.gr: «Πώς η Μασούτης μετατρέπει σταδιακά το e-shop της σε marketplace», 01-11-2022, https://www.businessnews.gr/epixeiriseis/item/250370-pos-i-masoytis-thelei-na-metatrepsei-to-e-shop-tis-se-marketplace.
Όσον αφορά το Skroutz, η εταιρεία λάνσαρε την υπηρεσία Marketplace από τον Νοέμβριο του 2019. https://startupper.gr/news/65359/skroutz-marketplace-enas-chronos-leitourgias-2500-engegrammena-katastimata/

φορές ασύμμετρα αποτελέσματα για τους εμπλεκόμενους που φτάνουν από την απλή υποκλοπή των προσωπικών δεδομένων μέχρι την υπερχρέωση τραπεζικών καρτών ή εμπλοκή των πραγματικών προσώπων εν αγνοία τους σε παράνομες ενέργειες.

Η ηλεκτρονική απάτη (e fraud) αναφέρεται σε κάθε είδος παράνομης δραστηριότητας που διεξάγεται με χρήση ηλεκτρονικών μέσων, ιδιαίτερα του Διαδικτύου και των ψηφιακών τεχνολογιών. Αυτό μπορεί να περιλαμβάνει ένα ευρύ φάσμα παράνομων ενεργειών με στόχο την κλοπή χρημάτων, δεδομένων ή πολύτιμων περιουσιακών στοιχείων. Με την άνοδο των ηλεκτρονικών συναλλαγών, των ψηφιακών υπηρεσιών και των διασυνδεδεμένων συστημάτων, η ηλεκτρονική απάτη αποτελεί σοβαρή απειλή για άτομα, επιχειρήσεις και κυβερνήσεις παγκοσμίως. Μπορεί να λάβει χώρα σε διάφορες ψηφιακές πλατφόρμες, συμπεριλαμβανομένων ιστοτόπων ηλεκτρονικού εμπορίου, μέσων κοινωνικής δικτύωσης, τραπεζικών εφαρμογών, email, ακόμη και στην ψηφιακή υποδομή εταιρειών. Μπορεί να πραγματοποιηθεί από άτομα ή οργανωμένες ομάδες με σκοπό την εξαπάτηση ή τη χειραγώγηση των θυμάτων ώστε να παρέχουν οικονομικές ή προσωπικές πληροφορίες.

Πρόκειται για ένα πολύ μεγάλο κεφάλαιο στον τομέα του διαδικτύου, ωστόσο στην παρούσα θα περιοριστούμε στην ηλεκτρονική απάτη που συμβαίνει στο πλαίσιο του ηλεκτρονικού εμπορίου (e commerce fraud) σε βάρος των καταναλωτών.

## 1. Ηλεκτρονική απάτη στο ηλεκτρονικό εμπόριο.

Η ηλεκτρονική απάτη στο ηλεκτρονικό εμπόριο αναφέρεται σε παράνομες δραστηριότητες που στοχεύουν ειδικά διαδικτυακές επιχειρήσεις και καταναλωτές που συμμετέχουν σε ηλεκτρονικές συναλλαγές. Με την ταχεία ανάπτυξη του ηλεκτρονικού εμπορίου, οι εγκληματίες έχουν γίνει ολοένα και πιο ικανοί να εκμεταλλεύονται τις αδυναμίες στις ψηφιακές πλατφόρμες για να διαπράττουν διάφορους τύπους απάτης, όπως κλοπή πληροφοριών πληρωμής, χειραγώγηση συναλλαγών ή εξαπάτηση πελατών για να πληρώσουν για ανύπαρκτα αγαθά ή υπηρεσίες. Οι συνέπειές της είναι αρκετά επώδυνες για τα θύματα, επιχειρήσεις και καταναλωτές, αφού μπορεί να επιφέρει τεράστιες οικονομικές απώλειες τόσο στις επιχειρήσεις όσο και στους καταναλωτές αλλά και ζημία στη φύση των επιχειρήσεων. Τα περιστατικά ηλεκτρονικής απάτης είναι καθημερινά όπως μπορεί να διαπιστώσει κάποιος με μία απλή αναζήτηση του όρου στο διαδίκτυο[18] δείχνοντας πόσο

[18] Σύμφωνα με δημοσίευμα στην kathimerini.gr τα θύματα ηλεκτρονικής απάτης το 2023 άγγιζαν τα 10 την ημέρα, «Ηλεκτρονικές απάτες: Δέκα θύματα την ημέρα το 2023- Τους «χρέωναν» ακόμη και δάνεια», https://www.kathimerini.gr/society/562973545/ilektronikes-apates-deka-thymata-tin-imera-to-2023-toys-chreonan-akomi-kai-daneia/

δύσκολο είναι να προστατευτούν καταναλωτές και επιχειρήσεις από αυτό το εγκληματικό φαινόμενο[19].

Η ηλεκτρονική απάτη δεν πραγματοποιείται με έναν μόνο τρόπο κάθε φορά ούτε υπάρχει μόνο ένα είδος. Προκειμένου να μπορούν να διαπράττουν κάθε φορά μία «επιτυχημένη» απάτη, οι επίδοξοι εγκληματίες πρέπει να εξελίσσουν τις τακτικές που ακολουθούν και να εφευρίσκουν τρόπους ώστε να διαπερνούν τα συστήματα ασφαλείας που επιχειρήσεις και καταναλωτές εφαρμόζουν ώστε να προστατεύσουν τις ηλεκτρονικές συναλλαγές τους. Επίσης πολλές φορές θα δούμε ότι χρησιμοποιούν τις ίδιες τακτικές ή συνδυασμούς αυτών για να διαπράξουν τα διάφορα είδη απάτης. Ο στόχος της απάτης σχεδόν σε όλες τις περιπτώσεις είναι τα διακινούμενα προσωπικά δεδομένα των μερών σε μία ηλεκτρονική εμπορική συναλλαγή, συμπεριλαμβανομένων των στοιχείων ταυτότητας, των στοιχείων διεύθυνσης και των οικονομικών στοιχείων τόσο των καταναλωτών όσο και των επιχειρήσεων.

Οι ηλεκτρονικές συναλλαγές στηρίζονται στην διακίνηση, συλλογή, επεξεργασία και αποθήκευση των προσωπικών δεδομένων των καταναλωτών και των επιχειρήσεων που είναι απαραίτητα για την ολοκλήρωση μίας οικονομικής συναλλαγής και την αποστολή και παράδοση του προϊόντος.

Η έννοια των προσωπικών δεδομένων είναι λίγο πολύ γνωστή πλέον σε όλους. Ο όρος «προσωπικά δεδομένα» αναφέρεται σε κάθε πληροφορία που αφορά ορισμένο φυσικό πρόσωπο. Ειδικότερα σύμφωνα με το άρθρο 4 παρ. 1 του Γενικού Κανονισμού Προσωπικών Δεδομένων[20], *«δεδομένα προσωπικού χαρακτήρα»* νοείται *κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.*

[19] Ενδεικτικά, kathimerini.gr, «Θεσσαλονίκη: Εξιχνιάστηκαν ηλεκτρονικές απάτες με λεία 15.000 ευρώ https://www.kathimerini.gr/society/563159812/thessaloniki-exichniastikan-ilektronikes-apates-me-leia-15-000-eyro/
Παρομοίως: moneyreview.gr: «Βιτρίνες ηλεκτρονικής απάτης- Λουκέτο σε 50 e-shops σε 10 μήνες», Δημήτρης Δελεβέγκος, 16-07-2024, https://www.moneyreview.gr/business-and-finance/150698/vitrines-ilektronikis-apatis-loyketo-se-50-e-shops-se-10-mines/. Επίσης, tanea.gr: «Κινέζικο δίκτυο πίσω από μία τεράστια διαδικτυακή απάτη», Γιώργος Κανελλόπουλος, 10-05-2024, https://www.tanea.gr/2024/05/10/economy/kineziko-diktyo-piso-apo-crmia-terastia-diadiktyaki-apati-online/

[20] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ

Στην παρ. 12 του ίδιου άρθρου του Γενικού Κανονισμού Προσωπικών Δεδομένων περιγράφεται η έννοια της παραβίασης των προσωπικών δεδομένων, σύμφωνα με την οποία παραβίαση των προσωπικών δεδομένων είναι *η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ΄ άλλο τρόπο σε επεξεργασία*[21].

Η διακίνηση των προσωπικών δεδομένων για την πραγματοποίηση ηλεκτρονικών εμπορικών συναλλαγών, τα καθιστά πιο ευάλωτα σε παραβίαση σε σύγκριση με τις φυσικές αγορές. Οι εγκληματίες αναζητούν τις αδυναμίες των διαδικτυακών καναλιών ανταλλαγής δεδομένων για να καταφέρουν να τα παραβιάσουν ώστε να υποκλέψουν τα προσωπικά δεδομένα των χρηστών ή επινοούν τρόπους εξαπάτησης των χρηστών του διαδικτύου ώστε να τους αποκαλύψουν οι ίδιοι τα προσωπικά τους δεδομένα. Στη συνέχεια τα χρησιμοποιούν είτε για να διαπράξουν οι ίδιοι παράνομες πράξεις χρησιμοποιώντας τα παράνομα αποκτηθέντα προσωπικά δεδομένα είτε τα πωλούν στο διαδίκτυο σε άλλους εγκληματίες ώστε να τα χρησιμοποιήσουν οι τελευταίοι.

## 2. Είδη ηλεκτρονικής απάτης

Θύματα της ηλεκτρονικής απάτης μπορούν να είναι όλα τα μέρη μιας ηλεκτρονικής συναλλαγής, τόσο δηλαδή οι καταναλωτές όσο και οι επιχειρήσεις. Μάλιστα τα περιστατικά ηλεκτρονικής απάτης στο πλαίσιο του ηλεκτρονικού εμπορίου παρουσιάζουν δραματική αύξηση τα τελευταία χρόνια, γεγονός που μπορεί κάποιος εύκολα να διαπιστώσει από τις επαναλαμβανόμενες αναφορές στα Μέσα Μαζικής Ενημέρωσης[22]. Στη συνέχεια θα αναπτυχθούν τα είδη της ηλεκτρονικής απάτης που πραγματοποιούνται σε βάρος των καταναλωτών, αν και με παρόμοιο τρόπο λειτουργούν οι εγκληματίες όταν οι πράξεις τους στρέφονται κατά των επιχειρήσεων.

### α. Το ηλεκτρονικό ψάρεμα (phising)

Το ηλεκτρονικό ψάρεμα (phising) είναι μία πρακτική εξαπάτησης με την οποία ο δράστης προσποιείται ότι είναι μία αξιόπιστη οντότητα ή πρόσωπο, μέσω μηνύματος

[21] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ

[22] Ενδεικτικά: kathimerini.gr: «Έκρηξη στις απάτες με κάρτες – Ξεπέρασαν τις 400.000 το 2023», 26-04-2024, Παρομοίως, iefimerida.gr, «Έκρηξη στις απάτες με πλαστικό χρήμα- Πως δρουν τα κυκλωματα, τι δείχνουν τα στοιχεία», 25-04-2024. Παρομοίως: dealnews.gr: «ΤτΕ: Έκρηξη στις συναλλαγές με πλαστικό χρήμα – Οι ηλεκτρονικές απάτες συνεχίζονται», 24-10-2024.

ηλεκτρονικού ταχυδρομείου ή μέσω κάποιας άλλη μορφή επικοινωνίας, προκειμένου να διανείμει κακόπιστους συνδέσμους μέσω των οποίων μπορεί να αποκτήσει πρόσβαση στα προσωπικά στοιχεία ταυτότητας του θύματος, στους λογαριασμούς του και στα στοιχεία σύνδεσης.

Πρόκειται για μία αρκετά δημοφιλή πρακτική ηλεκτρονικής απάτης καθώς είναι πιο εύκολο να εξαπατήσεις κάποιον ώστε να συνδεθεί σε κάποιον κακόβουλο σύνδεσμο που περιλαμβάνεται σε ένα φαινομενικά νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου παρά να παραβιάσεις το λογισμικό ασφαλείας που διαθέτει ένας υπολογιστής. Οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) αυξάνονται και εξελίσσονται συνεχώς καθώς οι δράστες αξιοποιούν προς όφελός τους την ανάπτυξη της τεχνολογίας όπως για παράδειγμα την ραγδαία αύξηση στη χρήση των εργαλείων τεχνητής νοημοσύνης[23].

Οι επιθέσεις ηλεκτρονικού ψαρέματος γίνονται συνήθως με τη μορφή πλαστών μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων που φέρονται να προέρχονται από αξιόπιστη πηγή όπως τράπεζα, εμπορικό κατάστημα ή πλατφόρμα μέσων κοινωνικής δικτύωσης. Το μήνυμα μπορεί να ζητήσει από τον παραλήπτη του να παράσχει πληροφορίες προσωπικές ή οικονομικές όπως τα στοιχεία σύνδεσης σε ένα λογαριασμό ή τα στοιχεία της πιστωτικής κάρτας, πατώντας πάνω σε έναν σύνδεσμο ή κάνοντας λήψη ενός συνημμένου αρχείου.

Οι δράστες για να μπορέσουν να δημιουργήσουν ένα «αξιόπιστο» μήνυμα ηλεκτρονικού ταχυδρομείου μπορούν να χρησιμοποιούν τα στοιχεία που είναι δημοσιευμένα σε πλατφόρμες όπως το Linkedin, το Facebook, το Twitter, το TikTok κ.α. Μέσω αυτών των πλατφόρμων συγκεντρώνουν στοιχεία που αφορούν προσωπικά δεδομένα, ιστορικό εργασίας, ιστορικό μετακινήσεων, ενδιαφέροντα και δραστηριότητες του θύματος. Χρησιμοποιούν τις πληροφορίες αυτές ώστε το μήνυμα- «δόλωμα» που πρόκειται να αποστείλουν να είναι πιο πειστικό, προκειμένου να παρασύρει το θύμα να συνδεθεί στο σύνδεσμο που τυχόν περιέχει ή να πραγματοποιήσει τις ενέργειες που περιγράφει.

Ο στόχος των επιθέσεων ηλεκτρονικού ψαρέματος είναι η εξαπάτηση των θυμάτων για να τους αποκαλύψουν προσωπικά δεδομένα και οικονομικές πληροφορίες που θα επιτρέψει στους δράστες να πραγματοποιήσουν με τα κλεμμένα στοιχεία παράνομες εμπορικές οικονομικές συναλλαγές προκειμένου να αποκτήσουν παράνομο κέρδος. Ως εκ τούτου οι δράστες στοχεύουν συνήθως επιχειρήσεις που αποθηκεύουν δεδομένα πιστωτικών καρτών ή έχουν τα κεφάλαια για να πραγματοποιήσουν μεγάλες οικονομικές συναλλαγές. Στόχοι

[23] Liberal.gr: «Phishing: Αύξηση των επιθέσεων το 2024, λόγω εργαλείων Τεχνητής Νοημοσύνης και τακτικών πολλαπλών καναλιών», 10-11-2024, Παρομοίως, sepe.gr: «Το τοπίο των κυβερνοεπιθέσεων το 2025, οι επιθέσεις με AI θα αυξηθούν», 29-11-2024

τέτοιων επιθέσεων είναι τα ηλεκτρονικά εμπορικά καταστήματα όπως οι τράπεζες, τα χρηματοπιστωτικά ιδρύματα, οι εταιρείες πληροφορικής και τηλεπικοινωνιών και τα μέσα κοινωνικής δικτύωσης.

Πως λειτουργεί το ηλεκτρονικό ψάρεμα; Το θύμα λαμβάνει ένα μήνυμα που φαίνεται να έχει σταλεί από κάποια γνωστή επαφή ή οργανισμό. Η επίθεση πραγματοποιείται όταν το θύμα ανοίξει κάποιο κακόβουλο συνημμένο αρχείο που περιέχεται στο μήνυμα ή συνδεθεί σε κάποιον σύνδεσμο που τον μεταφέρει σε κακόβουλο ιστότοπο. Και στις δύο περιπτώσεις ο δράστης επιδιώκει να εγκαταστήσει κακόβουλο λογισμικό στη συσκευή του χρήστη ή να τον κατευθύνει σε ένα ψεύτικο ιστότοπο ώστε να αποκαλύψουν προσωπικές και οικονομικές πληροφορίες, όπως κωδικούς πρόσβασης, αναγνωριστικά λογαριασμού (όνομα χρήστη και κωδικός σύνδεσης) ή στοιχεία πιστωτικών καρτών.

Οι πιο συνηθισμένοι τύποι επιθέσεων ηλεκτρονικού ψαρέματος είναι οι ακόλουθοι:

- Ηλεκτρονικό ψάρεμα μέσω ηλεκτρονικού ταχυδρομείου (Email Phishing).
  Ένας από τους πρωταρχικούς αλλά και πιο συνηθισμένους τρόπους ηλεκτρονικού ψαρέματος είναι η αποστολή μηνύματος μέσω ηλεκτρονικού ταχυδρομείου. Με τα μηνύματα ηλεκτρονικού ταχυδρομείου οι δράστες στοχεύουν τα θύματα προσποιούμενοι ότι προέρχονται από αξιόπιστο αποστολέα. Για να ενισχύσουν την αξιοπιστία του μηνύματος οι δράστες αντιγράφουν την ηλεκτρονική διεύθυνση από μία νόμιμη εταιρεία ή τραπεζικό ίδρυμα[24] ακόμη και από δημόσια υπηρεσία[25] και συμπεριλαμβάνουν ένα κακόβουλο αρχείο όπως σύνδεσμο, εικόνα ή έγγραφο ώστε το θύμα να εξαπατηθεί και να επιβεβαιώσει τα προσωπικά του στοιχεία ή να κατεβάσει στη συσκευή του το κακόβουλο λογισμικό.
- Φωνητικό ηλεκτρονικό ψάρεμα (Voice fishing-vishing)
  Στην περίπτωση του φωνητικού ηλεκτρονικού ψαρέματος ο δράστης καλεί τηλεφωνικά το θύμα και προσπαθεί να κλέψει χρήματα ή πληροφορίες. Ο δράστης που καλεί προσπαθεί να δημιουργήσει την αίσθηση επείγουσας κατάστασης ώστε να περιέλθει το θύμα σε κατάσταση άγχους και να μην μπορεί να σκεφτεί ψύχραιμα και καθαρά. Οι πιο γνωστές τακτικές αυτής της μορφής ηλεκτρονικού ψαρέματος είναι ότι ένα μέλος της οικογένειας

[24] Ενδεικτικές αναφορές από Μέσα Μαζικής Ενημέρωσης: theopinion.gr: «Νέα απάτη phishing για πελάτες τράπεζας- Δείτε το μήνυμα ηλεκτρονικής αλληλογραφίας» 29-09-2024 https://www.theopinion.gr/texnologia/nea-apati-phishing-gia-pelates-trapezas-deite-to-minyma-ilektronikis-allilografias/
Παρομοίως, ertnews.gr: «Απατεώνες υποδύονται την Εθνική Τράπεζα και επιχειρούν να αδειάσουν λογαριασμούς πολιτών», 25-05-2023, https://www.ertnews.gr/eidiseis/ellada/apateones-ypodyontai-tin-ethniki-trapeza-kai-epixeiroun-na-adeiasoun-logariasmous-politon/

[25] Χαρακτηριστική το από 29-10-2024 δελτίο τύπου- ανακοίνωση του Υπουργείου Ψηφιακής Διακυβέρνησης για αποστολή παραπλανητικών μηνυμάτων τύπου phishing μέσω ηλεκτρονικού ταχυδρομείου, https://mindigital.gr/archives/6725

ενεπλάκη σε τροχαίο ατύχημα και χρειάζεται μεγάλο χρηματικό ποσό για να διευθετήσει τα ζητήματα που προέκυψαν από αυτό. Μία άλλη τακτική είναι να προσποιούνται το λογιστή ή το βοηθό λογιστή και να ζητούν τα στοιχεία σύνδεσης στις ηλεκτρονικές φορολογικές εφαρμογές ώστε να τακτοποιήσουν φορολογικές εκκρεμότητες ή να ζητούν τον αριθμό τραπεζικού λογαριασμού και τους κωδικούς σύνδεσης στην τράπεζα για να ολοκληρωθεί η διαδικασία είσπραξης κάποιου επιδόματος. Οι δράστες που χρησιμοποιούν αυτή την τακτική απάτης έχουν τη «βοήθεια» των εργαλείων τεχνητής νοημοσύνης και τις τεχνολογίες τεχνητής μάθησης τα οποία εξελίσσονται ταχύτατα[26].

- Ηλεκτρονικό ψάρεμα με κλωνοποίηση (Clone Phishing)

  Σε αυτή τη μορφή της επίθεσης ο δράστης αντιγράφει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που έχει λάβει κάποιος και δημιουργεί έναν κλώνο του, στον οποίο όμως αντικαθιστά με κακόβουλο λογισμικό τα πραγματικά συνημμένα του μηνύματος ή αντικαθιστά τον πραγματικό σύνδεσμο που περιέχει το αρχικό μήνυμα με έναν κακόβουλο σύνδεσμο. Με τον τρόπο αυτό επιχειρείται να εξαπατηθεί ο λήπτης του μηνύματος- θύμα ώστε να κατεβάσει και να εκτελέσει το κακόβουλο λογισμικό ή να επισκεφτεί έναν κακόβουλο ιστότοπο.

- Ηλεκτρονικό ψάρεμα μέσω μηνυμάτων (SMS phishing- smishing)

  Αυτή η μορφή επίθεσης στοχεύει στις κινητές συσκευές και χρησιμοποιεί μηνύματα κειμένου για να πείσει τα θύματα να αποκαλύψουν τα στοιχεία ενός λογαριασμού ή να εγκαταστήσουν ένα κακόβουλο λογισμικό. Συνήθως ζητείται από το θύμα να συνδεθεί σε κάποιον σύνδεσμο ή να καλέσει έναν αριθμό τηλεφώνου ή να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου και να παράσχει προσωπικά του δεδομένα. Οι δράστες χρησιμοποιούν αξιόπιστες πηγές όπως δημόσιες αρχές ή νόμιμες εταιρείες[27], οι οποίες εμφανίζονται ως αποστολείς των μηνυμάτων ώστε να πείσουν και να εξαπατήσουν ευκολότερα τα θύματά τους.

- Αναδυόμενο ηλεκτρονικό ψάρεμα (Pop up phishing)

  Με την τακτική αυτή οι δράστες μπορούν και ενσωματώνουν κακόβουλα λογισμικά σε ιστότοπους. Στη συνέχεια εμφανίζονται ως ειδοποιήσεις ή αναδυόμενες διαφημίσεις, ακόμη

[26] Είναι χαρακτηριστικό ότι τρία δευτερόλεπτα ομιλίας αρκούν για μία εφαρμογή τεχνητής νοημοσύνης για να κλωνοποιήσει τη φωνή κάποιου, theopinion.gr: «Voice phishing: Η νέα μορφή απάτης με την βοήθεια της AI που «σαρώνει», 21-10-2024, https://www.theopinion.gr/texnologia/voice-phishing-h-nea-morfi-apatis-me-ti-voitheia-ai-poy-saronei-video/

[27] Χαρακτηριστικό το από 15-02-2024 δελτίο τύπου της Ανεξάρτητης Αρχής Δημοσίων Εσόδων για παραπλανητικά μηνύματα SMS υποκλοπής στοιχείων σε βάρος των πολιτών, σύμφωνα με το οποίο τα παραπλανητικά μηνύματα εμφάνιζαν ως αποστολέα την Αρχή, είχαν ως θέμα τη λήψη αποζημίωσης ή επιδόματος και παρότρυνα τους πολίτες να συνδεθούν μέσω υπερσυνδέσμου (link) σε πλαστή ιστοσελίδα, που τους ενημερώνει ότι δικαιούνται επίδομα και πρέπει να υποβάλουν αίτημα συμπληρώνοντας τα προσωπικά τους στοιχεία (Ονοματεπώνυμο, ΑΦΜ, κωδικούς Taxis, Στοιχεία Τραπεζών, κ.λπ.). https://www.aade.gr/sites/default/files/2024-02/dt_15.02.2024.pdf

και αν τα θύματα έχουν εγκαταστήσει πρόγραμμα αποκλεισμού αναδυόμενων παραθύρων ή διαφημίσεων. Ως αποτέλεσμα εάν τα θύματα ανοίξουν τα αναδυόμενα παράθυρα ή τις διαφημίσεις, η συσκευή τους να μολυνθεί από κακόβουλο λογισμικό.

β. Κοινωνική μηχανική (Social Engineering)[28]

Η κοινωνική μηχανική είναι μια τεχνική χειραγώγησης που χρησιμοποιούν οι δράστες για να εξαπατήσουν άτομα ώστε να αποκαλύψουν εμπιστευτικές ή προσωπικές πληροφορίες. Στο πλαίσιο της απάτης στο ηλεκτρονικό εμπόριο, η κοινωνική μηχανική περιλαμβάνει την εκμετάλλευση της ανθρώπινης συμπεριφοράς και δεν βασίζεται σε τεχνικές ευπάθειες για την πραγματοποίηση απάτης. Με το χειρισμό των συναισθημάτων, της εμπιστοσύνης και της επιθυμίας για επείγουσα ανάγκη ή ασφάλεια, οι δράστες μπορούν να εξαπατήσουν άτομα -είτε πελάτες είτε υπαλλήλους-, να κλέψουν τα προσωπικά τους δεδομένα, να πραγματοποιήσουν παράνομες συναλλαγές ή να παραχωρήσουν μη εξουσιοδοτημένη πρόσβαση σε πλατφόρμες ηλεκτρονικού εμπορίου.

Στο ηλεκτρονικό εμπόριο, οι επιθέσεις κοινωνικής μηχανικής μπορούν να στοχεύουν τόσο καταναλωτές όσο και σε επιχειρήσεις και μπορούν να λάβουν ποικίλες μορφές. Αυτές οι επιθέσεις αξιοποιούν ψυχολογικές τακτικές, δημιουργώντας μια αίσθηση επείγοντος, εμπιστοσύνης ή φόβου, για να χειραγωγήσουν τα άτομα ώστε να ενεργήσουν με τρόπους που δεν θα έκαναν υπό κανονικές συνθήκες. Οι τακτικές social engineering περιλαμβάνουν μία σειρά από τακτικές που στοχεύουν στην οικοδόμηση μίας σχέσης με το θύμα, ώστε να μπορέσει ο δράστης να αποκτήσει πρόσβαση στα προσωπικά του δεδομένα για να τα χρησιμοποιήσει στη συνέχεια για την διενέργεια παράνομων δραστηριοτήτων ή μη εξουσιοδοτημένων αγορών. Πρόκειται για μία τακτική απάτης που καταλαμβάνει διαρκώς μεγαλύτερο ποσοστό στις περιπτώσεις ηλεκτρονικής απάτης με την πάροδο των ετών[29].

Οι πιο συνηθισμένες τακτικές εξαπάτησης στην κοινωνική μηχανική στο πλαίσιο του ηλεκτρονικού εμπορίου είναι οι επιθέσεις phishing και οι διάφορες υποκατηγορίες του που περιγράφονται στην προηγούμενη ενότητα. Άλλες τακτικές είναι οι εξής:

[28] Πάνω από το 77% των ηλεκτρονικών απατών για το έτος 2023, δηλαδή περισσότερα από τρία στα τέσσερα περιστατικά ξεκίνησαν από πλατφόρμες κοινωνικής δικτύωσης , όπως το Facebook, το Instagram, το WhatsApp και το Messenger, kathimerini.gr: «Κερκόπορτα τα social media για τις ηλεκτρονικές απάτες», 24-05-2024, https://www.kathimerini.gr/economy/563040541/kerkoporta-ta-social-media-gia-ilektronikes-apates/

[29] Securityreport.gr, «Το 92% των οργανισμών πλήττεται από παραβίαση διαπιστευτηρίων από επιθέσεις social engineering», 20-06-2024

- Δόλωμα (Baiting)

  Με την τακτική αυτή χρησιμοποιείται μία ελκυστική προσφορά ως «δόλωμα» για να δελεάσει το θύματος προκειμένου να παράσχει ευαίσθητες προσωπικές ή/και οικονομικές πληροφορίες ή να εγκαταστήσει κακόβουλο λογισμικό που μπορεί να χρησιμοποιηθεί για πρόσβαση σε λογαριασμούς ή για παράνομες συναλλαγές.

  Συνήθως «δόλωμα» αποτελεί κάτι ιδιαίτερα ελκυστικό όπως δωρεάν προϊόντα, ειδική έκπτωση ή αποκλειστική πρόσβαση σε αντάλλαγμα για ευαίσθητες πληροφορίες ή ενέργειες που θα θέσουν σε κίνδυνο την ασφάλεια ή κάτι που προκαλεί τον συναισθηματικό κόσμο των θυμάτων. Για την τακτική αυτή μπορούν να χρησιμοποιηθούν ψεύτικες διαφημίσεις, αναδυόμενα παράθυρα ή άλλες φαινομενικά νόμιμες διαδικτυακές προσφορές ή δημοσιεύσεις.
- Απάτη στα μέσα κοινωνικής δικτύωσης

  Οι δράστες χρησιμοποιούν τις πλατφόρμες μέσων κοινωνικής δικτύωσης για να δημιουργήσουν πλαστά προφίλ ή αναρτήσεις που εξαπατούν άτομα να παρέχουν ευαίσθητες πληροφορίες ή να κάνουν μια παράνομη συναλλαγή. Αυτό μπορεί να περιλαμβάνει τη δημιουργία ψεύτικων προωθήσεων ή εκπτώσεων για ιστότοπους ηλεκτρονικού εμπορίου που δεν υπάρχουν μέσω διαφημίσεων. Τα θύματα που επιλέγουν τις διαφημίσεις μπορεί να κληθούν να παράσχουν προσωπικά στοιχεία ή να πληρώσουν για ανύπαρκτα προϊόντα[30].

γ. Κλοπή ταυτότητας (Identity theft)[31]

Η κλοπή ταυτότητας μέσω του ηλεκτρονικού εμπορίου αναφέρεται στις διάφορες μεθόδους με τις οποίες κάποιος κλέβει προσωπικές και οικονομικές πληροφορίες ή

[30] Οι δράστες πολλές φορές χρησιμοποιούν το όνομα δημόσιων αρχών ή νόμιμων εταιριών για να εξαπατήσουν τα θύματα. Για παράδειγμα τον Αύγουστο του 2024 ο Δήμος Αθηναίων ενημέρωσε του πολίτες για απάτη που πραγματοποιούνταν μέσω του facebook σύμφωνα με την οποία ο δήμος Αθηναίων πρόσφερε δωρεάν μετακινήσεις στα μέσα μαζικής μεταφοράς ως νέο μέτρο που εφαρμόζει η δημοτική αρχή. athenstransport.com: «Δήμος Αθηναίων: Προειδοποίηση για απάτη μέσω facebook με δωρεάν κάρτες μετακίνησης στις συγκοινωνίες», 19-08-2024, https://www.athenstransport.com/2024/08/dimos-athinaion-facebook-apati.
Άλλη παρόμοια περίπτωση απάτης μέσω facebook αφορούσε το Αστικό Κτελ Βόλου. Οι δράστες χρησιμοποιώντας σελίδα στο facebook που προσομοίαζε στην πραγματική σελίδα του Αστικού Κτελ Βόλου προσέφεραν μέσω διαγωνισμού δωρεάν ή σε πολύ οικονομική τιμή ετήσια κάρτα μετακίνησης με σκοπό να αποκτήσουν πρόσβαση στους τραπεζικούς λογαριασμούς των θυμάτων και να αποσπάσουν χρηματικά ποσά. thenewspaper.gr: ««Πώς έστησαν απάτη με το Αστικό Κτελ Βόλου- Τι πρέπει να προσέξετε», 20-11-2024, https://www.thenewspaper.gr/2024/11/20/pos-estisan-apati-me-to-astiko-ktel-volou-ti-prepei-na-prosexete/

[31] Χαρακτηριστικό παράδειγμα είναι η πρόσφατη δημοσίευση στο protothema.gr: «Απατεώνας παρίστανε τον πρίγκιπα Παύλο για να πάρει χρήματα από ηλικιωμένους», 26-11-2024, https://www.protothema.gr/greece/article/1567238/apateonas-paristane-ton-prigipa-paulo-gia-na-parei-hrimata-apo-ilikiomenous/

πληροφορίες λογαριασμών από τους καταναλωτές κατά τη διάρκεια εμπορικών διαδικτυακών συναλλαγών.

Οι δράστες χρησιμοποιούν διάφορα μέσα όπως παραβίαση προσωπικών δεδομένων, ηλεκτρονικό ψάρεμα (phishing) ή κοινωνική μηχανική (social engineering) για να αποκτήσουν τα προσωπικά δεδομένα τρίτων. Τα δημόσια προφίλ σε κοινωνικά δίκτυα ή άλλες δημοφιλείς διαδικτυακές υπηρεσίες μπορούν να χρησιμοποιηθούν ως πηγές άντλησης πληροφοριών. Στη συνέχεια χρησιμοποιούν τα στοιχεία αυτά για να προσποιηθούν το θύμα και να πραγματοποιήσουν αγορές, να ανοίξουν λογαριασμούς στο όνομά του, να αναλάβουν τους διαδικτυακούς του λογαριασμούς ή να κινηθούν νομικά στο όνομά τους. Για να μπορέσουν να ολοκληρώσουν αυτό το είδος της απάτης οι δράστες δεν χρειάζονται απαραίτητα τα στοιχεία των τραπεζικών καρτών αλλά λογαριασμούς ηλεκτρονικού ταχυδρομείου, λογαριασμούς χρηστών, ονοματεπωνυμικά στοιχεία, διευθύνσεις κατοικίας, διευθύνσεις IP ώστε να προσποιηθούν το θύμα.

Τα θύματα μπορούν να υποστούν μεγάλη οικονομική ζημία και να υποστούν αλλαγές στην πιστωτική τους κατάσταση. Υπάρχει ακόμη η πιθανότητα να θεωρηθούν υπεύθυνα για τις παράνομες ενέργειες των δραστών και να βρεθούν αντιμέτωποι με τη δικαιοσύνη αντιμετωπίζοντας νομικές κατηγορίες. Στη συνέχεια περιγράφονται κάποιες βασικές τακτικές με τις οποίες επιτυγχάνεται η κλοπή ταυτότητας. Αυτό που διαπιστώνουμε είναι ότι οι τακτικές επαναλαμβάνονται στις διάφορες μορφές ηλεκτρονικής απάτης και πολλές φορές οι δράστες τις χρησιμοποιούν συνδυαστικά για να επιτύχουν το σκοπό τους.

- Ανάληψη λογαριασμού (Account takeover)

  Οι δράστες αποκτούν πρόσβαση στον διαδικτυακό λογαριασμό ενός ατόμου π.χ. στον λογαριασμό επεξεργασίας πληρωμών ενός ατόμου. Για να το πετύχουν αυτό χρησιμοποιούν στοιχεία σύνδεσης που αποκτούν από παραβιάσεις δεδομένων με τακτικές όπως το ηλεκτρονικό ψάρεμα (phishing) ή επιθέσεις ωμής βίας (brute force attack). Στη συνέχεια χρησιμοποιούν τους λογαριασμούς για να κάνουν παράνομες αγορές ή να αποσύρουν χρήματα προς όφελός τους. Στην επίθεση ωμής βίας ο δράστης προσπαθεί να μαντέψει τις πληροφορίες σύνδεσης δοκιμάζοντας όλους τους πιθανούς συνδυασμούς.
- Κλοπή ταυτότητας μέσω παραβιάσεων δεδομένων (Identity theft via Data Breaches).

  Οι παραβιάσεις δεδομένων είναι σοβαρές παραβιάσεις ασφαλείας πλατφορμών ηλεκτρονικού εμπορίου ή διαδικτυακών υπηρεσιών με τις οποίες οι δράστες αποκτούν πρόσβαση στις προσωπικές και οικονομικές πληροφορίες των συναλλασσομένων με τις πλατφόρμες αυτές. Τα στοιχεία αυτά αφορούν σε ονοματεπωνυμικά στοιχεία, διευθύνσεις κατοικίας ή αποστολής, τηλεφωνικοί αριθμοί, στοιχεία πιστωτικών καρτών, στοιχεία

πρόσβασης και πληροφορίες για τραπεζικούς λογαριασμούς και ιστορικό αγορών. Στη συνέχεια οι δράστες χρησιμοποιούν τα στοιχεία αυτά είτε για να πραγματοποιήσουν παράνομες συναλλαγές προς όφελός τους ή να πουλήσουν τα στοιχεία σε άλλους εγκληματίες.

- Χρήση στοιχείων πρόσβασης (Crecedial Stuffing)

  Είναι γεγονός πως οι χρήστες του διαδικτύου για την πρόσβασή τους σε λογαριασμούς που διατηρούν σε διάφορους ιστότοπους και εφαρμογές χρησιμοποιούν τους ίδιους κωδικούς σύνδεσης προς διευκόλυνσή τους. Οι δράστες αυτής της τακτικής εκμεταλλεύονται αυτή την αδυναμία των χρηστών και χρησιμοποιούν τα στοιχεία σύνδεσης που έχουν ήδη κλέψει και μέσω αυτοματοποιημένων εργαλείων χρησιμοποιούν συνδυασμούς αυτών για να αποκτήσουν πρόσβαση και σε άλλους λογαριασμούς των θυμάτων. Οι δράστες επομένως χρησιμοποιούν τα στοιχεία σύνδεσης που έκλεψαν από προηγούμενη παραβίαση δεδομένων για να αποκτήσουν πρόσβαση στους λογαριασμούς ηλεκτρονικού εμπορίου των χρηστών.

- Απάτη ανταλλαγής SIM (Swim Swap Fraud)[32]

  Με αυτή την τακτική οι δράστες εξαπατούν τους παρόχους κινητής τηλεφωνίας ώστε να τους χορηγήσουν μία νέα κάρτα SIM δίνοντάς τους τη δυνατότητα να κλέψουν τους κωδικούς 2FA που χρησιμοποιούνται για τον έλεγχο ταυτότητας δύο παραγόντων. Η διαδικασία αυτή απαιτεί δύο μορφές ταυτοποίησης για την πρόσβαση σε πόρους και δεδομένα. Με τον τρόπο αυτό ο δράστης υποκλέπτει τους κωδικούς σύνδεσης του θύματος και αποκτά πρόσβαση στους λογαριασμούς ηλεκτρονικού εμπορίου που διαθέτει και πραγματοποιεί παράνομες αγορές.

Η κλοπή ταυτότητας μέσω ηλεκτρονικού εμπορίου αποτελεί μία αυξανόμενη απειλή καθώς περισσότερα άτομα και επιχειρήσεις επιλέγουν να πραγματοποιήσουν τις εμπορικές τους συναλλαγές μέσω του διαδικτύου. Οι δράστες εκμεταλλεύονται την εμπιστοσύνη των χρηστών προς τις διαδικτυακές υπηρεσίες και πλατφόρμες για να εξαπατήσουν τους χρήστες, να παραβιάσουν τα μέτρα ασφαλείας και να πραγματοποιήσουν παράνομες συναλλαγές χρησιμοποιώντας τις κλεμμένες προσωπικές και οικονομικές πληροφορίες των χρηστών.

[32] Σωρεία δημοσιευμάτων στα Μ.Μ.Ε. δείχνουν ότι αυτή η μορφή απάτης χρησιμοποιείται από τους δράστες πολλαπλώς για να επιτύχουν το στόχο τους και να αποκτήσουν πρόσβαση στους λογαριασμούς των θυμάτων τους. Ενδεικτικά: newsbeast.gr: «Sim Swapping: Η απάτη μέσω κινητού- Πώς αδειάζουν τραπεζικούς λογαριασμούς "ανταλλάσσοντας" κάρτες», 30-10-2021, https://www.newsbeast.gr/technology/arthro/7954393/sim-swapping-i-apati-meso-kinitou-pos-adeiazoun-trapezikous-logariasmous-antallassontas-kartes,
Παρομοίως: enikos.gr: «Τρεις αναπάντητες κλήσεις και τα χρήματά σας κάνουν φτερά- Πώς λειτουργεί η απάτη Sim Swap Scam», 02-11-2023 https://www.enikos.gr/timeout/treis-anapantites-kliseis-kai-ta-chrimata-sas-kanoun-ftera-pos-leitourgei-i-apati-sim-swap-scam/2054082/

δ. Απάτη με πιστωτικές κάρτες[33] (E commerce credit fraud)

Η απάτη με πιστωτικές κάρτες στο ηλεκτρονικό εμπόριο αναφέρεται στη μη εξουσιοδοτημένη χρήση στοιχείων πιστωτικής κάρτας για την πραγματοποίηση παράνομων συναλλαγών μέσω διαδικτυακών πληρωμών. Αυτή η μορφή απάτης μπορεί να αφορά από απλή κλοπή δεδομένων πιστωτικών καρτών έως πιο εξελιγμένες τακτικές που εκμεταλλεύονται τις ευπάθειες των διαδικτυακών συστημάτων πληρωμής.

Παραδοσιακά η απάτη αυτή συμβαίνει όταν μία φυσική κάρτα κλαπεί από τον κάτοχό της και ο δράστης τη χρησιμοποιεί για να πραγματοποιήσει αγορές προς όφελός του ή να αφαιρέσει χρήματα. Ωστόσο στη σύγχρονη εποχή ο δράστης το πιθανότερο είναι να υποκλέψει τα στοιχεία της πιστωτικής κάρτας και όχι τη φυσική κάρτα και να τη χρησιμοποιήσει για την πραγματοποίηση αγορών ή για να αφαιρέσει χρήματα. Οι πιο συνηθισμένοι τρόποι απάτης με πιστωτικές κάρτες είναι η κλοπή πιστωτικής κάρτας, η απάτη χωρίς την φυσική παρουσία κάρτας, η απάτη με φυσική παρουσία κάρτας και η δοκιμή πιστωτικών καρτών. Συμφώνα με την Έκθεση Χρηματοπιστωτικής Σταθερότητας της Ελλάδας που δημοσιεύτηκε τον Οκτώβριο του 2024[34] προκύπτει ότι μπορεί το υψηλότερο ποσοστό απάτης να εξακολουθεί να αφορά τις εξ αποστάσεως συναλλαγές με πιστωτική κάρτα, ωστόσο και οι άλλες περιπτώσεις απάτης εμφανίζουν σημαντικό αριθμό περιστατικών οδηγώντας στην απώλεια σημαντικών χρηματικών ποσών για τα θύματα.

- Κλοπή πιστωτικής κάρτας.

  Στην περίπτωση αυτή οι δράστες κλέβουν τον αριθμό της πιστωτικής κάρτας, το ονοματεπώνυμο του κατόχου και τα αλλά σχετικά στοιχεία που είναι απαραίτητα για την πραγματοποίηση διαδικτυακών συναλλαγών όπως ημερομηνία λήξης και κωδικός αριθμός ασφαλείας (Card Verification Value- CVV) και τα χρησιμοποιούν για να πραγματοποιήσουν παράνομες αγορές στο διαδίκτυο. Οι δράστες για να αποκτήσουν πρόσβαση στις πληροφορίες των πιστωτικών καρτών χρησιμοποιούν διάφορες μεθόδους όπως ηλεκτρονικό ψάρεμα, παραβίαση βάσεων δεδομένων, τακτικές κοινωνικής μηχανικής κ.α.

- Απάτη χωρίς την φυσική παρουσία κάρτας (Card Not Present Fraud)

[33] imerisia.gr: «Έκρηξη στις ηλεκτρονικές επιθέσεις σε τραπεζικές κάρτες πληρωμών - 202.000 απάτες με αξία 12,5 εκατ. ευρώ σε ένα 6μηνο», 09-11-2023 https://www.imerisia.gr/oikonomia/83238_ekrixi-stis-ilektronikes-epitheseis-se-trapezikes-kartes-pliromon-202000-apates-me,
Επίσης: newmoney.gr: «Έξαρση στα περιστατικά απάτης με κάρτες – Έκαναν… φτερά 24 εκατ. ευρώ το 2023 – Ποιες συναλλαγές είναι πιο ευάλωτες», 26-04-2024, https://www.newmoney.gr/roh/palmos-oikonomias/trapezes/exarsi-sta-peristatika-apatis-me-kartes-ekanan-ftera-24-ekat-evro-to-2023-pies-sinallages-ine-pio-epirrepis/ κ.α.

[34] https://www.bankofgreece.gr/Publications/FINANCIAL_STABILITY_REVIEW_OCTOBER_2024_EL.pdf

Ο δράστης χρησιμοποιεί πλαστά ή κλεμμένα στοιχεία πιστωτικής κάρτας χωρίς να την έχει στην κατοχή του για την πραγματοποίηση συναλλαγών σε ιστότοπους ηλεκτρονικού εμπορίου που δεν απαιτούν επαλήθευση φυσικής κάρτας.

- Απάτη με φυσική παρουσία της κάρτας (Card Present Fraud)
  Η απάτη με φυσική παρουσία της κάρτας γίνεται όλο και λιγότερο συνηθισμένη εξαιτίας της ύπαρξης του chip και του PIN. Σε αυτή την περίπτωση απάτης ο δράστης θα πρέπει να έχει στην κατοχή του την κλεμμένη πιστωτική κάρτα ή να έχει μία πλαστή πιστωτική κάρτα με κλεμμένα στοιχεία. Ωστόσο λόγω της μεγαλύτερης «ευκολίας» που παρουσιάζει η απάτη χωρίς την παρουσία της κάρτας για τους δράστες αφού είναι δυσκολότερο να εντοπιστούν και να τιμωρηθούν, η απάτη με φυσική παρουσία της κάρτας εμφανίζεται όλο και λιγότερο συχνά.
- Δοκιμή πιστωτικών καρτών (Card Testing Fraud)
  Με την τακτική αυτή οι δράστες χρησιμοποιούν τα κλεμμένα στοιχεία της πιστωτικής κάρτας και αρχικά κάνουν μικρές αγορές χαμηλού κόστους για να ελέγξουν την εγκυρότητα της κάρτας πριν την χρησιμοποιήσουν για μεγαλύτερες συναλλαγές. Συνήθως οι δράστες διαθέτουν λίστες με στοιχεία κλεμμένων πιστωτικών καρτών. Για να εντοπίσουν ποιες από αυτές είναι έγκυρες και μπορούν να χρησιμοποιηθούν για αγορές επιχειρούν μικρές συναλλαγές σε διάφορους ιστότοπους ηλεκτρονικού εμπορίου. Όταν εντοπίσουν ποιες από αυτές τις πιστωτικές κάρτες της λίστας είναι έγκυρες προχωρούν σε μεγαλύτερες και ακριβότερες συναλλαγές.

Η απάτη με τη χρήση πιστωτικών καρτών μέσω του ηλεκτρονικού εμπορίου είναι δυναμική καθώς οι επίδοξοι εγκληματίες εξελίσσουν διαρκώς τις μεθόδους τους για να εκμεταλλευτούν τα τρωτά στοιχεία των ψηφιακών συναλλαγών. Αυτό σημαίνει ότι όσο αναβαθμίζονται τα επίπεδα ασφαλείας των πλατφορμών μέσω των οποίων πραγματοποιείται το ηλεκτρονικό εμπόριο, αναβαθμίζονται και οι μέθοδοι που χρησιμοποιούν οι εγκληματίες για να επιτύχουν το σκοπό τους.

ε. Απάτη εξαγοράς λογαριασμού (Account takeover fraud- ATO)

Πρόκειται για μία σοβαρή απάτη που αποτελεί αυξανόμενη απειλή στον τομέα του ηλεκτρονικού εμπορίου, όπου οι εγκληματίες του κυβερνοχώρου αποκτούν μη εξουσιοδοτημένη πρόσβαση στον λογαριασμό του θύματος για να πραγματοποιήσουν παράνομες δραστηριότητες. Στο ηλεκτρονικό εμπόριο οι δράστες έχουν πρόσβαση στον λογαριασμό του θύματος στην ιστοσελίδα κάποιου ηλεκτρονικού καταστήματος, στα στοιχεία

πληρωμής ή σε άλλες ευαίσθητες πληροφορίες και στη συνέχεια τα χρησιμοποιούν για να κάνουν αγορές ή να κλέψουν προσωπικά δεδομένα.

Η απάτη εξαγοράς λογαριασμού είναι μία ιδιαίτερα ανησυχητική μορφή απάτης στο ηλεκτρονικό εμπόριο, επειδή περιλαμβάνει παραβίαση της ασφάλειας του λογαριασμού ενός υπάρχοντος πελάτη και τη χρήση του για παράνομες δραστηριότητες ή συναλλαγές. Ειδικότερα οι δράστες χρησιμοποιούν τεχνικές ηλεκτρονικού ψαρέματος, παραβιάσεις δεδομένων, χρήση στοιχείων πρόσβασης άλλου λογαριασμού ή κοινωνικής μηχανικής για να αποκτήσουν τα στοιχεία σύνδεσης σε έναν λογαριασμό (όνομα χρήστη και κωδικό πρόσβασης)[35]. Μόλις αποκτήσουν τα στοιχεία σύνδεσης, μπορούν να συνδεθούν στο λογαριασμό του νόμιμου χρήστη στην ιστοσελίδα ηλεκτρονικού εμπορίου. Εάν δεν υπάρχει επιπλέον έλεγχος ταυτότητας π.χ. με τη χρήση δύο παραγόντων (2FA), η διαδικασία μπορεί να είναι ακόμα πιο εύκολη, καθώς ο δράστης χρειάζεται μόνο το όνομα χρήστη και τον κωδικό πρόσβασης για να αποκτήσει πλήρη πρόσβαση.

Στη συνέχεια οι δράστες μπορούν να προβούν σε διάφορες παράνομες ενέργειες. Αρχικά αλλάζουν τα στοιχεία του λογαριασμού του θύματος, όπως τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον κωδικό πρόσβασης, για να κλειδώσουν τον αρχικό κάτοχο λογαριασμού από τον λογαριασμό. Στη συνέχεια χρησιμοποιούν τις αποθηκευμένες πληροφορίες πληρωμής (πιστωτικές κάρτες, χρεωστικές κάρτες ή άλλους τρόπους πληρωμής) για να πραγματοποιήσουν αγορές για λογαριασμό του νόμιμου κατόχου του λογαριασμού, ο οποίος μπορεί να μην το αντιληφθεί άμεσα. Μάλιστα για να το καθυστερήσουν μπορούν να προσθέσουν τους δικούς τους τρόπους πληρωμής ώστε να δυσκολέψουν τον κάτοχο του λογαριασμού να εντοπίσει τις παράνομες δραστηριότητες.

Σε ορισμένες περιπτώσεις, ο δράστης μπορεί να κλέψει τα προσωπικά δεδομένα του πραγματικού κατόχου και να τα πουλήσει στον σκοτεινό ιστό (dark web) ή να τα χρησιμοποιήσει για περαιτέρω παράνομες δραστηριότητες όπως κλοπή ταυτότητας, άνοιγμα νέων τραπεζικών λογαριασμών, έκδοση νέων πιστωτικών καρτών κ.α.

## 3. Συνέπειες της ηλεκτρονικής απάτης για τους καταναλωτές.

Η απάτη στο ηλεκτρονικό εμπόριο έχει σοβαρές συνέπειες για τους καταναλωτές, που κυμαίνονται από οικονομικές απώλειες έως συναισθηματική δυσφορία. Οι συνέπειες αυτές

[35] Πολλές φορές δεν διστάζουν να χρησιμοποιήσουν ως προκάλυμμα δημόσιες υπηρεσίες για να επιτύχουν την πρόσβαση στους λογαριασμούς του θύματος, protothema.gr, «Απάτη με δόλωμα την δήθεν επικαιροποίηση στοιχείων στο Gov.gr.- Δείτε τις απάτες των επιτήδειων», 04-02-2024, https://www.protothema.gr/greece/article/1462812/apati-me-doloma-tin-dithen-epikairopoiisi-stoiheion-sto-govgr-deite-tis-pagides-ton-epitideion/

είναι ιδιαίτερα σημαντικές αφού επηρεάζουν την συμπεριφορά των καταναλωτών απέναντι στο ηλεκτρονικό εμπόριο και καθορίζουν ακόμη και την ύπαρξη και τη λειτουργία των ίδιων των ηλεκτρονικών καταστημάτων. Ο χρυσός κανόνας της ζήτησης και της προσφοράς ισχύει και στην περίπτωση του ηλεκτρονικού εμπορίου και συνεπώς εάν οι καταναλωτές δεν επιλέγουν το ηλεκτρονικό εμπόριο, υπάρχει ο κίνδυνος αυτό να ατονήσει. Ποιες όμως είναι οι συνέπειες για τους καταναλωτές;

- Οικονομική Ζημιά

Η πρωταρχική συνέπεια και για τους καταναλωτές είναι η οικονομική ζημία που υπόκεινται. Οι παράνομες συναλλαγές, όπως η απάτη με πιστωτική κάρτα ή η κλοπή ταυτότητας, μπορεί να οδηγήσουν σε μη εξουσιοδοτημένες χρεώσεις στον λογαριασμό ενός πελάτη ενώ ο δράστης μπορεί να πραγματοποιήσει αγορές ή να αποσύρει χρήματα, αφήνοντας τον πελάτη με σημαντικές οικονομικές απώλειες. Δυστυχώς στην περίπτωση που οι καταναλωτές πέφτουν θύματα απάτης ηλεκτρονικού ψαρέματος ή εξαγοράς λογαριασμού και διαπιστώσουν ότι ο τραπεζικός τους λογαριασμός ή το ψηφιακό πορτοφόλι τους έχει αδειάσει δεν υπάρχει άμεσος τρόπος ανάκτησης των κλεμμένων χρημάτων.

Ακόμη και στην περίπτωση που πέσουν θύματα μιας παράνομης συναλλαγής ή μη εξουσιοδοτημένης αγοράς, το πιο πιθανό είναι να αντιμετωπίσουν καθυστερήσεις στην επιστροφή των χρημάτων από τις επιχειρήσεις. Αφενός και οι επιχειρήσεις θα πρέπει να διερευνήσουν την περίπτωση απάτης ώστε να διαπιστώσουν ότι ο καταναλωτής είναι όντως το θύμα και όχι ο δράστης ενώ ενδέχεται να αμφισβητήσουν την αξίωση ή να κάνουν δύσκολη τη διαδικασία επιστροφής χρημάτων, δημιουργώντας επιπλέον οικονομική πίεση στον πελάτη.

- Κλοπή Ταυτότητας

Η δεύτερη σημαντική συνέπεια για τους καταναλωτές είναι η κλοπή της ταυτότητάς τους. Ευαίσθητες προσωπικές και οικονομικές τους πληροφορίες (ονοματεπωνυμικά στοιχεία, διευθύνσεις κατοικίας, διευθύνσεις αποστολής, αριθμοί ταυτότητας ή διαβατηρίου, αριθμοί φορολογικού μητρώου, αριθμοί μητρώου κοινωνικής ασφάλισης) μετά την κλοπή βρίσκονται στη διάθεση εγκληματιών που μπορούν να τα χρησιμοποιήσουν για τη πραγματοποίηση παράνομων συναλλαγών και δραστηριοτήτων υποδυόμενοι τα θύματα.

- Μείωση της πιστοληπτικής ικανότητας

Σε συνέχεια της κλοπής της ταυτότητας του θύματος μια τρίτη συνέπεια με την οποία είναι αλληλένδετη είναι αυτή της μείωσης της πιστοληπτικής ικανότητας του θύματος. Οι δράστες χρησιμοποιώντας τα στοιχεία του θύματος πραγματοποιούν μεγάλες αγορές ή λαμβάνουν δάνεια τα οποία και φυσικά δεν αποπληρώνουν με το οικονομικό χρέος να

βαραίνει το πραγματικού θύματος, το οποίο στο μέλλον μπορεί να αντιμετωπίσει πρόβλημα στις συναλλαγές του με τα χρηματοπιστωτικά ιδρύματα όπως λήψη δανείου ή έκδοση τραπεζικής κάρτας.

- Παραβίαση προσωπικών δεδομένων

Εκτός της κλοπής των στοιχείων ταυτότητας που μπορεί κάποιος να αντιμετωπίσει, μπορεί να υποστεί και παραβίαση των προσωπικών του δεδομένων όπως αριθμοί τηλεφώνου, διευθύνσεις ηλεκτρονικού ταχυδρομείου, στοιχεία σύνδεσης στους λογαριασμούς κοινωνικής δικτύωσης ή σε λογαριασμού που διατηρούν σε διάφορες ιστοσελίδες κ.α. Στην περίπτωση αυτή οι πληροφορίες τους είναι διαθέσιμες στους εγκληματίες οι οποίοι μπορούν να τα χρησιμοποιήσουν στο μέλλον για την πραγματοποίηση παράνομων δραστηριοτήτων.

- Κίνδυνος συνεχιζόμενης απάτης ή απάτης που θα επαναληφθεί στο μέλλον.

Αυτό μας οδηγεί στην επόμενη συνέπεια που προκύπτει εξαιτίας της «διαθεσιμότητας» των στοιχείων ταυτότητας και των άλλων προσωπικών και οικονομικών πληροφοριών των θυμάτων που κλάπηκαν σε εγκληματίες. Υπάρχει ο κίνδυνος της διάπραξης συνεχιζόμενων απατών με τη χρήση των κλεμμένων στοιχείων των θυμάτων, με την έννοια της αλυσιδωτής εκδήλωσης περιπτώσεων απάτης που η επόμενη στηρίζεται στην προηγούμενη. Επίσης υπάρχει μεγάλος κίνδυνος τα θύματα να γίνουν συχνός στόχος μελλοντικών προσπαθειών απάτης, με τη διαρκή χρήση των κλεμμένων στοιχείων.

- Απώλεια της εμπιστοσύνης στις ηλεκτρονικές αγορές

Η εμπειρία της απάτης στο ηλεκτρονικό εμπόριο μπορεί να οδηγήσει πολλούς καταναλωτές να χάσουν την εμπιστοσύνη στις διαδικτυακές πλατφόρμες αγορών. Η έλλειψη εμπιστοσύνης αυτόματα οδηγεί και σε αλλαγή της αγοραστικής τους συμπεριφορά αφού στο μέλλον γίνονται πιο επιφυλακτικοί με τις ηλεκτρονικές αγορές προϊόντων ή τις αποφεύγουν εντελώς επιλέγοντας τον παραδοσιακό τρόπο εμπορίου.

- Επιπτώσεις στους πιστωτικούς και τραπεζικούς λογαριασμούς

Το χρηματοπιστωτικό ίδρυμα εάν εντοπιστεί απάτη στον τραπεζικό λογαριασμό ή στον λογαριασμό πιστωτικής κάρτας ενός πελάτη, η τράπεζα μπορεί να δεσμεύσει τον λογαριασμό ή να ακυρώσει την κάρτα ως προληπτικό μέτρο. Αν και αυτό γίνεται για να αποτραπούν περαιτέρω μη εξουσιοδοτημένες συναλλαγές, ωστόσο μπορεί να προκαλέσει δυσλειτουργία στην καθημερινότητα του καταναλωτή ιδίως αν βασίζεται σε αυτό τον λογαριασμό ή αυτή την κάρτα για τις καθημερινές συναλλαγές.

- Απώλεια απορρήτου

Οι περισσότερες μορφές ηλεκτρονικής απάτης έχουν ως στόχο την παραβίαση ή των κλοπή των στοιχείων ταυτότητας, των προσωπικών και οικονομικών πληροφοριών του

θύματος. Με τον τρόπο αυτό το θύμα χάνει το δικαίωμά του στην προστασία του απόρρητου των δεδομένων του που κλάπηκαν αφού αυτά μετά την απάτη είναι διαθέσιμα στο δίκτυο των εγκληματιών που δραστηριοποιούνται στην ηλεκτρονική απάτη. Και μπορεί το θύμα να αλλάξει τα στοιχεία σύνδεσής του σε λογαριασμούς, να εκδώσει νέες τραπεζικές κάρτες ακυρώνοντας τις παλιές, ωστόσο ένα μέρος των στοιχείων του (στοιχεία ταυτότητας, αριθμός φορολογικού μητρώου, αριθμός μητρώου κοινωνικής ασφάλισης) δεν είναι δυνατόν να αντικατασταθούν με άλλα. Αυτή η παραβίαση των προσωπικών δεδομένων του θύματος μπορεί να έχει μακροχρόνιες επιπτώσεις, ειδικά όταν οδηγεί σε περαιτέρω εγκληματική δραστηριότητα.

- Δυσκολία στην ανάκαμψη από την απάτη

Ένας καταναλωτής που έπεσε θέμα ηλεκτρονικής απάτης και έχασε ένα σημαντικό χρηματικό ποσό εξαιτίας αυτής, δεν είναι εύκολο να ανακτήσει τα κεφάλαια αυτά ενώ σε ορισμένες περιπτώσεις μπορεί να μην καταφέρει να τα ανακτήσει ποτέ. Σε αυτή την οικονομική ζημία που έχει υποστεί εξαιτίας της απάτης, θα πρέπει να προσθέσουμε και την οικονομική επιβάρυνση του θύματος που υφίσταται για να μπορέσει να επιλύσει την σε βάρος του απάτη. Ως αποτέλεσμα οδηγείται σε συνεχόμενες οικονομικές δυσκολίες που κάποιες φορές μπορούν να επηρεάσουν ακόμη και την ποιότητα της ζωής του.

- Κίνδυνοι προσωπικής ασφάλειας και νομικές επιπτώσεις

Στις ακραίες περιπτώσεις απάτης, ειδικά στην περίπτωση κλοπής της ταυτότητας και της σύναψης δανειακών συμβάσεων από την πλευρά του δράστη στο όνομα του θύματος, το θύμα υπάρχει περίπτωση να βρεθεί αντιμέτωπο με εισπρακτικές εταιρείες και εταιρείες παροχής πιστώσεων που θα ζητούν από το θύμα να αποπληρώσει το δάνειο. Στην περίπτωση δε που τα στοιχεία ταυτότητάς του χρησιμοποιηθούν για την πραγματοποίηση παράνομων ενεργειών που συνιστούν αδικήματα είναι πιθανόν να βρεθεί κατηγορούμενο διάπραξης ποινικών αδικημάτων και να έχουν νομικές συνέπειες.

- Συναισθηματική Δυσφορία και Στρες

Τελευταία συνέπεια αν και εξίσου σημαντική είναι η συναισθηματική δυσφορία και το στρες που βιώνουν τα θύματα που έρχονται αντιμέτωπα με την εμπειρία της απάτης στο ηλεκτρονικό εμπόριο. Η αβεβαιότητα επίλυσης μιας υπόθεσης απάτης, ειδικά εάν πρόκειται για μεγάλο χρηματικό ποσό, ο χρόνος και οι πόροι που απαιτούνται μπορεί να προκαλέσουν επιπλέον άγχος στο θύμα. Αυτό περιλαμβάνει συναισθήματα ευπάθειας, θυμού, απογοήτευσης και δυσπιστίας στο ηλεκτρονικό εμπόριο και σε ό,τι αυτό περιλαμβάνει.

Η απάτη στο ηλεκτρονικό εμπόριο όπως διαπιστώνουμε έχει σοβαρές και εκτεταμένες συνέπειες για τους καταναλωτές. Μπορούν να επηρεαστούν βαθιά από απάτη στο

ηλεκτρονικό εμπόριο, με τις επιπτώσεις να εκτείνονται από την οικονομική απώλεια, την κλοπή ταυτότητας μέχρι το συναισθηματικό στρες και μακροπρόθεσμες επιπτώσεις στην προστασία της ιδιωτικής τους ζωής. Είναι σημαντικό να λάβουν μέτρα για την ελαχιστοποίηση αυτών των κινδύνων. Οι καταναλωτές πρέπει να βρίσκονται σε επαγρύπνηση και να ενημερώνονται σχετικά με την εξέλιξη των τρόπων απάτης στο ηλεκτρονικό εμπόριο ώστε να προστατεύουν όσο γίνεται τους εαυτούς τους. Μεγάλο μέρος της πρόληψης αλλά και της προστασίας των καταναλωτών και κατ΄ επέκταση του ηλεκτρονικού εμπορίου ωστόσο βαραίνει και τις επιχειρήσεις, οι οποίες θα πρέπει να εφαρμόζουν ισχυρά μέτρα πρόληψης της απάτης και ισχυρά μετρά προστασίας των ηλεκτρονικών τους καταστημάτων.

## ΜΕΡΟΣ Β΄

## Προστασία από την απάτη στο ηλεκτρονικό εμπόριο

### Ι. Θεσμικό Πλαίσιο

Η προστασία των καταναλωτών στο πλαίσιο του ηλεκτρονικού εμπορίου είναι ένα μείζον ζήτημα στον τομέα αυτό, ώστε το διαδίκτυο να είναι ένα ασφαλές και αξιόπιστο μέσο για να πραγματοποιούν τις αγορές τους οποιαδήποτε στιγμή από οποιοδήποτε μέρος βρίσκονται και να διασφαλιστεί η δυναμική και η εξέλιξη των ηλεκτρονικού εμπορίου. Η Ευρωπαϊκή Ένωση αλλά και η Ελλάδα έχουν ψηλά στην ατζέντα τους την προστασία των δικαιωμάτων των καταναλωτών και τη διασφάλισή τους από παράνομες ενέργειες κατά τη διάρκεια εμπορικών ηλεκτρονικών συναλλαγών.

Η θέσπιση του απαραίτητου νομοθετικού πλαίσιο ήταν στόχος και σκοπός για την προστασία των καταναλωτών και των προσωπικών τους δεδομένων, την επίλυση διαφορών που προκύπτουν από ηλεκτρονικές εμπορικές συναλλαγές και την ασφάλεια των συναλλαγών για διαδικτυακές αγορές γενικά. Θα διαπιστώσουμε παρακάτω ότι η ΕΕ έχει θεσπίσει μία πληθώρα νομοθετημάτων θέλοντας να προστατεύσει τις διαδικτυακές συναλλαγές και το ηλεκτρονικό εμπόριο καθώς αποτελεί βασικό εργαλείο για την επίτευξη της ενιαίας αγοράς.

1. Ενωσιακή Νομοθεσία

α. Ο Χάρτης των Θεμελιωδών Δικαιωμάτων

Το κύριο στοιχείο των καταναλωτών που πρέπει να προστατευτεί σε μία εμπορική συναλλαγή είναι τα προσωπικά τους δεδομένα. Η Ευρωπαϊκή Ένωση έκρινε ότι η προστασία των προσωπικών δεδομένων των πολιτών της θα πρέπει να ενισχυθεί υπό το πρίσμα των κοινωνικών αλλαγών, της κοινωνικής προόδου και των επιστημονικών και τεχνολογικών εξελίξεων. Για να το επιτύχει αυτό προέβλεψε ρητά την προστασία τους στο άρθρο 8 παρ. 1 και 2 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ[36] σύμφωνα με το οποίο, «*1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των προσωπικών δεδομένων που το αφορούν. 2 Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.*»

[36] https://www.europarl.europa.eu/charter/pdf/text_el.pdf

β. Η Οδηγία για το Ηλεκτρονικό Εμπόριο

Σκοπός της Ευρωπαϊκής Ένωσης ήταν η δημιουργία στενότερων δεσμών μεταξύ των ευρωπαϊκών κρατών και λαών και η εξασφάλιση της οικονομικής και κοινωνικής προόδου. Στόχος είναι η εσωτερική αγορά που αποτελεί έναν χώρο χωρίς εσωτερικά σύνορα μέσα στον οποίο διασφαλίζεται η ελεύθερη κυκλοφορία των εμπορευμάτων και των υπηρεσιών, καθώς και η ελευθερία εγκατάστασης. Ζωτικής σημασίας μέσο για την κατάργηση των φραγμών που χωρίζουν τους ευρωπαϊκούς λαούς είναι η ανάπτυξη των υπηρεσιών της κοινωνίας της πληροφορίας στο χώρο χωρίς εσωτερικά σύνορα. Η ανάπτυξη του ηλεκτρονικού εμπορίου στο πλαίσιο της κοινωνίας της πληροφορίας προσφέρει σημαντικές ευκαιρίες απασχόλησης στην Κοινότητα, ιδίως στις μικρομεσαίες επιχειρήσεις, και διευκολύνει την ανάπτυξη των ευρωπαϊκών επιχειρήσεων, καθώς και τις επενδύσεις στην καινοτομία, και μπορεί να αυξήσει την ανταγωνιστικότητα της ευρωπαϊκής βιομηχανίας, υπό την προϋπόθεση ότι ο καθένας θα έχει πρόσβαση στο Internet[37].

Για να επιτευχθούν οι προαναφερόμενοι σκοποί η Ευρωπαϊκή Ένωση εξέδωσε την Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»). Με την Οδηγία η ΕΕ θέλει να επιτύχει την ομαλή λειτουργία της εσωτερικής αγοράς εξασφαλίζοντας την ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ των κρατών μελών[38].

Στην ελληνική νομοθεσία η Οδηγία ενσωματώθηκε με το Προεδρικό Διάταγμα 131/2003 με καθυστέρηση δεκαέξι μηνών. Αποτελεί τον θεμέλιο λίθο του ηλεκτρονικού εμπορίου και επιβάλλει μία σειρά υποχρεώσεων στους παρόχους υπηρεσιών της Κοινωνίας της Πληροφορίας. Ο ορισμός της έννοιας αυτών των υπηρεσιών δίνεται στο άρθρο 1 του π.δ. 131/2003 όπου ορίζεται ότι, *υπηρεσία της Κοινωνίας της Πληροφορίας θεωρείται οποιαδήποτε υπηρεσία της κοινωνίας της πληροφορίας, ήτοι κάθε υπηρεσία που συνήθως παρέχεται έναντι αμοιβής, με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν προσωπικής επιλογής ενός αποδέκτη υπηρεσιών κατά την έννοιαν της παραγράφου 2 του άρθρου 2 του Π.Δ. 39/2001 (Α' 28).*

Αρχικά, ο φορέας παροχής υπηρεσιών οφείλει να προσφέρει στους αποδέκτες του και στις αρμόδιες αρχές, εύκολη, άμεση και συνεχή πρόσβαση, στις πληροφορίες όπως

[37] Σκέψεις 1 και 2 της Οδηγίας 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»)

[38] Άρθρο 1 της προαναφερόμενης οδηγίας

επωνυμία, γεωγραφική διεύθυνση, στοιχεία που επιτρέπουν ταχεία, άμεση και ουσιαστική επικοινωνία, τον αριθμό εγγραφής σε εμπορικό ή δημόσιο μητρώο (εάν είναι εγγεγραμμένος), τα στοιχεία της εποπτικής αρχής που χορήγησε έγκριση δραστηριότητας (εάν απαιτείται έγκριση), τον αριθμό αναγνώρισης που προβλέπεται από το κοινό σύστημα Φ.Π.Α. εφόσον η δραστηριότητα υπόκειται σε ΦΠΑ.. Επίσης οι τιμές πρέπει να αναγράφονται σαφώς και επακριβώς και να διευκρινίζεται αν περιλαμβάνουν φόρο και έξοδα αποστολής. Οι εμπορικές επικοινωνίες πρέπει να είναι σαφώς αναγνωρίσιμες, να είναι κατανοητό από ποιον γίνεται η εμπορική επικοινωνία, να είναι αναγνωρίσιμες οι προσφορές, εκπτώσεις, κ.α. Οι συμβάσεις θα πρέπει να είναι δυνατόν να καταρτιστούν με ηλεκτρονικά μέσα ενώ ο πάροχος των υπηρεσιών θα πρέπει να δίνει την δυνατότητα στον παραγγέλοντα να επιβεβαιώσει και να διορθώσει εάν χρειάζεται την παραγγελία του πριν την οριστική ανάθεσή της.

Οι πάροχοι υπηρεσιών φιλοξενίας δεν ευθύνονται για τις πληροφορίες που αποθηκεύουν τρίτοι, εφόσον δεν γνωρίζουν ότι πρόκειται για παράνομη δραστηριότητα ή πληροφορία. Όμως μόλις το αντιληφθούν πρέπει να αποσύρουν τις πληροφορίες, ή να καταστήσουν την πρόσβαση σε αυτές αδύνατη. Επίσης, έχουν υποχρέωση να ενημερώνουν πάραυτα τις αρμόδιες κρατικές αρχές, για τυχόν υπόνοιες περί χορηγούμενων παράνομων πληροφοριών, ή δραστηριοτήτων, που επιχειρούν αποδέκτες των υπηρεσιών τους και να διευκολύνουν τον εντοπισμό των αποδεκτών υπηρεσιών τους, με τους οποίους έχουν συμφωνίες αποθήκευσης.

γ. Η Οδηγία για τα δικαιώματα των καταναλωτών για τις εξ' αποστάσεως αγορές

Δεύτερο βασικό νομοθέτημα για το ηλεκτρονικό εμπόριο είναι η Οδηγία 2011/83/ΕΕ[39] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2011 σχετικά με τα δικαιώματα των καταναλωτών, την τροποποίηση της οδηγίας 93/13/ΕΟΚ του Συμβουλίου και της οδηγίας 1999/44/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της οδηγίας 85/577/ΕΟΚ του Συμβουλίου και της οδηγίας 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Η εσωτερική αγορά οφείλει να αποτελεί χώρο χωρίς εσωτερικά σύνορα στον οποίο εξασφαλίζονται η ελεύθερη κυκλοφορία των εμπορευμάτων και των υπηρεσιών και η ελευθερία εγκατάστασης. Η εναρμόνιση ορισμένων πτυχών των εξ αποστάσεως και εκτός καταστήματος συναπτόμενων συμβάσεων ήταν αναγκαία για την προαγωγή μιας πραγματικής εσωτερικής αγοράς των καταναλωτών που επιτυγχάνει τη σωστή ισορροπία

[39] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32011L0083#ntr1-L_2011304EL.01006401-E0001

μεταξύ υψηλού επιπέδου προστασίας των καταναλωτών και ανταγωνιστικότητας των επιχειρήσεων, εξασφαλίζοντας παράλληλα την τήρηση της αρχής της επικουρικότητας. Πριν την ψήφιση της οδηγίας το διασυνοριακό δυναμικό της εξ αποστάσεως πώλησης, το οποίο θα έπρεπε να αποτελεί ένα από τα κύρια απτά αποτελέσματα της εσωτερικής αγοράς, δεν αξιοποιείτο πλήρως. Σε σύγκριση με τη σημαντική ανάπτυξη των εγχώριων εξ αποστάσεως πωλήσεων, η ανάπτυξη των διασυνοριακών εξ αποστάσεως πωλήσεων ήταν περιορισμένη. Το διασυνοριακό δυναμικό συμβάσεων που αποτελούσε αντικείμενο διαπραγμάτευσης εκτός εμπορικών καταστημάτων (άμεση πώληση) περιοριζόταν από ορισμένους παράγοντες, συμπεριλαμβανομένων των διαφορετικών εθνικών κανόνων προστασίας των καταναλωτών που επιβάλλονται στη βιομηχανία.

Η Οδηγία για τα δικαιώματα των καταναλωτών για τις εξ' αποστάσεως αγορές έχει ως σκοπό, μέσω της επίτευξης ενός υψηλού επιπέδου προστασίας των καταναλωτών, να συμβάλει στην ομαλή λειτουργία της εσωτερικής αγοράς με την προσέγγιση ορισμένων πτυχών των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών για τις συμβάσεις που συνάπτονται μεταξύ καταναλωτών και εμπόρων. Στην ελληνική νομοθεσία μεταφέρθηκε με την ΚΥΑ Ζ1-891 (ΦΕΚ 2144/30-08-2013, τ. Β΄).

Η εν λόγω Οδηγία πρόσφατα τροποποιήθηκε με την Οδηγία (ΕΕ) 2023/2673[40] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 22ας Νοεμβρίου 2023 για την τροποποίηση της οδηγίας 2011/83/ΕΕ όσον αφορά τις συμβάσεις χρηματοοικονομικών υπηρεσιών που συνάπτονται εξ αποστάσεως και για την κατάργηση της οδηγίας 2002/65/ΕΚ.

δ. Η Οδηγία για την εναλλακτική επίλυση διαφορών

Η Οδηγία 2013/11/ΕΕ[41] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013, για την εναλλακτική επίλυση καταναλωτικών διαφορών και για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2006/2004 και της οδηγίας 2009/22/ΕΚ (οδηγία ΕΕΚΔ) στοχεύει στη διασφάλιση της εύρυθμης λειτουργίας της ενιαίας αγοράς της ΕΕ. Οι χώρες της ΕΕ πρέπει να διασφαλίζουν ότι όλες οι συμβατικές διαφορές που προκύπτουν από την πώληση αγαθών ή την παροχή υπηρεσιών —μεταξύ καταναλωτών που κατοικούν και εμπόρων που είναι εγκατεστημένοι στην ΕΕ — μπορούν να υποβάλλονται σε φορέα εναλλακτικής επίλυσης διαφορών. Με τον τρόπο αυτό οι καταναλωτές διαθέτουν έναν οικονομικά προσιτό, απλό και γρήγορο τρόπο επίλυσης διαφορών, όπως σε περιπτώσεις κατά τις οποίες ένας έμπορος αρνείται να επισκευάσει ένα προϊόν ή να προβεί σε επιστροφή χρημάτων την οποία ο

[40] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L_202302673
[41] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32013L0011

καταναλωτής δικαιούται. Οι φορείς εναλλακτικής επίλυσης διαφορών περιλαμβάνουν ένα ουδέτερο μέρος, όπως ο διαμεσολαβητής, ο συνήγορος του πολίτη ή ένα όργανο εκδίκασης προσφυγών, που αναλαμβάνουν ρόλο επίλυσης διαφορών μέσω διαδικασιών εναλλακτικής επίλυσης διαφορών. Ανάλογα με τη μορφή της διαδικασίας που ένας συγκεκριμένος φορέας εφαρμόζει, το ουδέτερο μέρος μπορεί να προτείνει ή να επιβάλλει μια λύση ή να φέρει τα μέρη σε επαφή προκειμένου να τα βοηθούν στην εξεύρεση λύσης.

Στη Ελλάδα οι απαραίτητες ρυθμίσεις για την προσαρμογή της ελληνικής νομοθεσίας στην προαναφερόμενη οδηγία λήφθηκαν με την Κοινή Υπουργική Απόφαση 70330οικ./2015 από 30-06-3015 (ΦΕΚ 1421, τ. Β΄). Σύμφωνα με την Οδηγία κάθε χώρα της ΕΕ θα πρέπει να ορίσει μία ή περισσότερες αρμόδιες αρχές, οι οποίες θα έχουν την εποπτεία των φορέων εναλλακτικής επίλυσης διαφορών σε εθνικό επίπεδο και διασφαλίζουν τη συμμόρφωσή τους με τις απαιτήσεις ποιότητας. Οι αρμόδιες αρχές συντάσσουν κατάλογο των φορέων σε εθνικό επίπεδο στον οποίο συμπεριλαμβάνονται μόνο φορείς επίλυσης διαφορών που συμμορφώνονται με τις απαιτήσεις ποιότητας. Για την Ελλάδα σύμφωνα με την ως άνω κυα ως «αρμόδια αρχή»[42] ορίστηκε η Γενική Διεύθυνση Προστασίας Καταναλωτή και Εποπτείας της Αγοράς της Γενικής Γραμματείας Εμπορίου και Προστασίας Καταναλωτή. Όσον αφορά τους φορείς εναλλακτικής επίλυσης διαφορών στην Ελλάδα που είναι καταχωρημένοι στο σχετικό Μητρώο[43] είναι: i) ο Συνήγορος του Καταναλωτή που αποτελεί ανεξάρτητη αρχή με στόχο την εξωδικαστική και φιλική διευθέτηση διαφορών καταναλωτών κατά προμηθευτών, ii) ο Ελληνικός Χρηματοοικονομικός Μεσολαβητής που ασχολείται με τις διαφορές καταναλωτών που προκύπτουν κατά τις συναλλαγές με τράπεζες σε εθνικό επίπεδο, iii) το Κέντρο Εναλλακτικής Επίλυσης Διαφορών- ADR POINT ΙΚΕ που επιλαμβάνεται διαφορών καταναλωτή κατά προμηθευτή σε μία ευρεία γκάμα συναλλαγών, iv) το Ινστιτούτο Εναλλακτικής Επίλυσης Διαφορών (startADR) που επιλαμβάνεται εγχώριων και διασυνοριακών διαφορών καταναλωτή κατά προμηθευτή σε μια ευρεία γκάμα συναλλαγών και v) η Ρυθμιστική Αρχή Αποβλήτων, Ενέργειας και Υδάτων που επιλαμβάνεται διαφορών που απορρέουν από τη συμβατική σχέση ενός πελάτη με τον προμηθευτή του και αφορούν όλες τις πτυχές της προμήθειας ηλεκτρικής ενέργειας ή και φυσικού αερίου.

[42] Άρθρο 5 εδ. α Κοινής Υπουργικής Απόφασης 70330οικ./2015 από 30-06-3015 (ΦΕΚ 1421, τ.Β΄).

[43] https://kataggelies.mindev.gov.gr/%ce%b5%ce%bd%ce%b7%ce%bc%ce%ad%cf%81%cf%89%cf%83%ce%b7-%ce%ba%ce%b1%cf%84%ce%b1%ce%bd%ce%b1%ce%bb%cf%89%cf%84%cf%8e%ce%bd/%ce%bc%ce%b7%cf%84%cf%81%cf%8e%ce%b1-%cf%85%cf%80%ce%b7%cf%81%ce%b5%cf%83%ce%af%ce%b1%cf%82/

ε. Ο Κανονισμός (ΕΕ) αριθ. 524/2013 για την ηλεκτρονική επίλυση καταναλωτικών διαφορών

Η εσωτερική αγορά που όπως έχουμε επαναλάβει αρκετές φορές είναι ο στόχος της ΕΕ, αποτελεί πραγματικότητα για τους καταναλωτές στην καθημερινή ζωή τους, όταν ταξιδεύουν, αγοράζουν και πραγματοποιούν πληρωμές. Οι καταναλωτές είναι βασικοί παράγοντες στην εσωτερική αγορά και συνεπώς βρίσκονται στο επίκεντρό της. Πλέον πραγματοποιούν όλο και περισσότερες αγορές μέσω του διαδικτύου, ενώ όλο και περισσότεροι έμποροι πωλούν τα προϊόντα τους ηλεκτρονικά. Και οι δύο πλευρές θα πρέπει να αισθάνονται εμπιστοσύνη κατά τη διενέργεια ηλεκτρονικών συναλλαγών[44]. Η δυνατότητα να έχουν οι καταναλωτές πρόσβαση σε απλούς, αποτελεσματικούς, γρήγορους και χαμηλού κόστους τρόπους επίλυσης των διαφορών που ανακύπτουν από την ηλεκτρονική πώληση αγαθών ή παροχή υπηρεσιών ενισχύει την εμπιστοσύνη τους στην εσωτερική αγορά και τους ωθεί να προβαίνουν σε διασυνοριακές αγορές επωφελούμενοι από την ψηφιακή της διάσταση[45].

Με τον Κανονισμό (ΕΕ) αριθ. 524/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013 για την ηλεκτρονική επίλυση καταναλωτικών διαφορών και για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2006/2004 και της οδηγίας 2009/22/ΕΚ (κανονισμός για την ΗΕΚΔ) η ΕΕ επιδιώκει να επιτύχει υψηλού επιπέδου προστασία των καταναλωτών, στην ορθή λειτουργία της εσωτερικής αγοράς, ιδίως στην ψηφιακή της διάσταση, καθιερώνοντας την ευρωπαϊκή πλατφόρμα ΗΕΔ («πλατφόρμα ΗΕΔ») για τη διευκόλυνση της ανεξάρτητης, αμερόληπτης, διαφανούς, αποτελεσματικής, γρήγορης και δίκαιης εξωδικαστικής επίλυσης των διαφορών μεταξύ καταναλωτών και εμπόρων ηλεκτρονικά[46]. Με το άρθρο 5 του Κανονισμού καθορίζεται η λειτουργία της πλατφόρμας ΗΕΔ η οποία αποτελεί ενιαίο σημείο εξυπηρέτησης για τους καταναλωτές και εμπόρους που επιδιώκουν την εξωδικαστική επίλυση διαφορών που καλύπτονται από τον παρόντα κανονισμό. Πρόκειται για έναν διαδραστικό ιστότοπο στον οποίο υπάρχει δυνατότητα δωρεάν ηλεκτρονικής πρόσβασης σε όλες τις επίσημες γλώσσες των θεσμικών οργάνων της Ένωσης.

Κάθε κράτος μέλος είναι υποχρεωμένο να ορίσει ένα σημείο επαφής ηλεκτρονικής επίλυσης διαφορών, το οποίο παρέχει υποστήριξη για την επίλυση διαφορών που αφορούν

[44] Σκέψη 6 Κανονισμού (ΕΕ) αριθ. 524/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013 για την ηλεκτρονική επίλυση καταναλωτικών διαφορών και για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2006/2004 και της οδηγίας 2009/22/ΕΚ (κανονισμός για την ΗΕΚΔ)

[45] Σκέψη 2 προαναφερόμενου Κανονισμού

[46] Άρθρο 1 προαναφερόμενου Κανονισμού

καταγγελίες οι οποίες υποβάλλονται μέσω της πλατφόρμας ΗΕΔ[47]. Για την Ελλάδα ως σημείο επαφής Ηλεκτρονικής Επίλυσης Διαφορών ορίζεται ο Συνήγορος του Καταναλωτή - Ευρωπαϊκό Κέντρο Καταναλωτή Ελλάδας[48].

στ. Η Οδηγία (ΕΕ) 2015/2366 για τις πανευρωπαϊκές υπηρεσίες πληρωμών

Η Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2015 σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ, (γνωστή ως η αναθεωρημένη οδηγία για τις υπηρεσίες πληρωμών ή PSD2) παρέχει τη νομική βάση για την περαιτέρω ανάπτυξη μιας καλύτερα ενοποιημένης εσωτερικής αγοράς για τις ηλεκτρονικές πληρωμές εντός της Ευρωπαϊκής Ένωσης (ΕΕ). Θεσπίζονται γενικοί κανόνες για τις υπηρεσίες πληρωμών, με στόχο τη διασφάλιση εναρμονισμένων κανόνων για την παροχή υπηρεσιών πληρωμών στην ΕΕ και υψηλού επιπέδου προστασίας των καταναλωτών. Η οδηγία θεσπίζει μια σαφή και ολοκληρωμένη δέσμη κανόνων που ισχύει για υφιστάμενους και νέους παρόχους καινοτόμων υπηρεσιών πληρωμών. Οι εν λόγω κανόνες επιδιώκουν να διασφαλίσουν ότι οι πάροχοι αυτοί είναι σε θέση να ανταγωνίζονται επί ίσοις όροις, οδηγώντας έτσι σε μεγαλύτερη αποτελεσματικότητα, περισσότερες επιλογές και μεγαλύτερη διαφάνεια των υπηρεσιών πληρωμών, ενισχύοντας παράλληλα την εμπιστοσύνη των καταναλωτών προς μια εναρμονισμένη αγορά πληρωμών.

Η προαναφερόμενη Οδηγία ενσωματώθηκε στην ελληνική νομοθεσία με τον ν. 4537/2018 (ΦΕΚ 84, τ. Α΄). Ο νόμος αυτός αποτελεί μέρος της εναρμόνισης της Ελλάδας με τις ευρωπαϊκές απαιτήσεις για τη διευκόλυνση των πληρωμών και την διασφάλιση των χρηματοοικονομικών συναλλαγών. Με τον νόμο αυτό: i) επιτρέπεται η δημιουργία νέου τύπου χρηματοοικονομικών υπηρεσιών όπως οι υπηρεσίες πληρωμών από τρίτους παρόχους, επιτρέποντας στους χρήστες να συνδέονται στον τραπεζικό τους λογαριασμό μέσω εξωτερικών πλατφορμών ώστε να εκτελούν πληρωμές ή να αποκτούν πληροφορίες για τον λογαριασμό τους, ii) εφαρμόζονται αυστηρές διαδικασίες ελέγχου για την προστασία των πληρωμών και την μείωση των κινδύνων απάτης και iii) εξασφαλίζεται διαφάνεια στις χρεώσεις και δυνατότητα ακύρωσης πληρωμών και επιστροφής ποσών σε περίπτωση μη εξουσιοδοτημένων πληρωμών. Με την ενσωμάτωση της Οδηγίας πραγματοποιείται ένα

[47] Άρθρο 7 προαναφερόμενου Κανονισμού
[48] Άρθρο 5 εδ. β Κοινής Υπουργικής Απόφασης 70330οικ./2015 από 30-06-3015 (ΦΕΚ 1421, τ.Β΄).

σημαντικό βήμα στην εξέλιξη των χρηματοοικονομικών υπηρεσιών παρέχοντας περισσότερες επιλογές, διαφάνεια στις ηλεκτρονικές συναλλαγές και ασφάλεια στους καταναλωτές.

ζ. Η Οδηγία για το Έγκλημα στον Κυβερνοχώρο

Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου μπορεί να μην έχει άμεση σχέση με το ηλεκτρονικό εμπόριο, αλλά έχει άμεση σχέση με την καταπολέμηση των εγκλημάτων που διαπράττονται στον κυβερνοχώρο μεταξύ άλλων και στο πλαίσιο του ηλεκτρονικού εμπορίου. Η Οδηγία αποσκοπεί στην καταπολέμηση του ηλεκτρονικού εγκλήματος και την προώθηση της ασφάλειας των πληροφοριών μέσω ισχυρότερων εθνικών νόμων, αυστηρότερων ποινικών κυρώσεων και περισσότερης συνεργασίας μεταξύ των αρμόδιων αρχών. Προβλέπει νέους κανόνες που εναρμονίζουν την ποινικοποίηση και τις ποινές για σειρά αδικημάτων που στρέφονται κατά των συστημάτων πληροφοριών. Τα κύρια είδη ποινικών αδικημάτων που καλύπτονται από την παρούσα οδηγία είναι οι επιθέσεις κατά των συστημάτων πληροφοριών, που περιλαμβάνουν επιθέσεις άρνησης υπηρεσιών με σκοπό να τεθεί εκτός λειτουργίας ένας εξυπηρετητής, αλλά και υποκλοπή δεδομένων και επιθέσεις «botnet».

Στην ελληνική νομοθεσία ενσωματώθηκε με τον ν. 4411/2016 (ΦΕΚ 142, τ. Α΄), με τον οποίο κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών[49]. Η Σύμβαση αποσκοπεί στην καταπολέμηση των εγκλημάτων που μπορούν να γίνουν μόνο με τη χρήση τεχνολογίας, όπου οι συσκευές είναι το εργαλείο τέλεσης όσο και ο στόχος του εγκλήματος, καθώς και η αντιμετώπιση εγκλημάτων όπου η τεχνολογία έχει χρησιμοποιηθεί για τη διευκόλυνση άλλου εγκλήματος, για παράδειγμα απάτης. Παρέχει κατευθυντήριες γραμμές για κάθε χώρα που καταρτίζει εθνική νομοθεσία για το έγκλημα στον κυβερνοχώρο και λειτουργεί ως βάση για τη διεθνή συνεργασία μεταξύ των μερών της σύμβασης[50].

η. Η Οδηγία (ΕΕ) 2019/713

Η Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής

[49] https://rm.coe.int/1680081561
[50] https://eur-lex.europa.eu/EL/legal-content/summary/convention-on-cybercrime.html

πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου αποτελεί το όπλο της ΕΕ κατά της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών οι οποίες συνιστούν απειλές για την ασφάλεια, καθώς αντιπροσωπεύουν πηγή εισοδήματος για το οργανωμένο έγκλημα και συνεπώς επιτρέπουν την ανάπτυξη άλλων εγκληματικών δραστηριοτήτων, όπως η τρομοκρατία, η παράνομη διακίνηση ναρκωτικών ουσιών και η εμπορία ανθρώπων[51]. Οι δυο αυτές παράνομες δραστηριότητες αποτελούν τροχοπέδη στην ψηφιακή ενιαία αγορά αφού διαβρώνουν την εμπιστοσύνη των καταναλωτών. Με την Οδηγία θεσπίζονται στοιχειώδεις κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και κυρώσεων στους τομείς της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και διευκολύνεται η πρόληψη των αδικημάτων αυτών και η παροχή συνδρομής και στήριξης των θυμάτων.

Με τον ν. 4947/2022 (ΦΕΚ 124, τ. Α΄) ενσωματώθηκε η Οδηγία στην ελληνική έννομη τάξη με σκοπό την αντιμετώπιση της απάτης, της πλαστογραφίας, της παραχάραξης και άλλων αξιόποινων πράξεων, που αφορούν στα μέσα πληρωμής πλην των μετρητών, προκειμένου να αναπτυχθεί ανεμπόδιστα η ψηφιακή οικονομία και να διευκολυνθεί η διάδοση της καινοτομίας στον τομέα των τεχνολογιών ή ψηφιακών πληρωμών.

θ. Η Οδηγία (ΕΕ) 2022/2555 (Οδηγία NIS 2)

Η Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS) αποτελεί μέρος της γενικότερης στρατηγικής της ΕΕ για την ενίσχυση της κυβερνοασφάλειας και την προστασία κρίσιμων υποδομών από τις ψηφιακές απειλές. Αποτελεί συνέχεια της καταργούμενης Οδηγίας NIS (2016/1148/ΕΕ) η οποία ήταν η πρώτη νομική πράξη της ΕΕ για τη διαχείριση της κυβερνοασφάλειας. Η Οδηγία στοχεύει σε «υπηρεσίες ψηφιακής υποδομής» που είναι κρίσιμες για τη λειτουργία της οικονομίας και της κοινωνίας όπως το cloud computing[52], την υποδομή διαχείρισης δεδομένων, τα δίκτυα επικοινωνίας και τις

[51] Σκέψη 1 της Οδηγίας (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου

[52] Υπολογιστικό νέφος. Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την εύκολη, κατ' απαίτηση πρόσβαση στο δίκτυο σε μια κοινόχρηστη ομάδα διαμορφώσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, χώρο αποθήκευσης, εφαρμογές και υπηρεσίες) που μπορεί να παρασχεθεί και να κυκλοφορήσει γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο υπηρεσιών, https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

υπηρεσίες ψηφιακής πληρωμής. Οι οργανισμοί που παρέχουν αυτές τις υπηρεσίες είναι υποχρεωμένοι να αναπτύξουν στρατηγικές και διαδικασίες για την πρόληψη, ανίχνευση και αντίδραση σε κυβερνοεπιθέσεις, εφαρμόζοντας μέτρα ασφαλείας σύμφωνα με τα διεθνή πρότυπα. Με την ενίσχυση των απαιτήσεων ασφαλείας για κρίσιμες ψηφιακές υποδομές, η ΕΕ επιδιώκει να μειώσει τον κίνδυνο μεγάλων και καταστροφικών κυβερνοεπιθέσεων που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια, την οικονομία και την κοινωνία.

Η Οδηγία (ΕΕ) 2022/2555 ενσωματώθηκε στην ελληνική έννομη τάξη με τον ν. 5160/2024 (ΦΕΚ 195, τ. Α. ). Ο νόμος αυτός αποτελεί τη δέσμευση της χώρας μας να συμμορφωθεί στις απαιτήσεις που απορρέουν από την Οδηγία και εντάσσεται στην Ευρωπαϊκή Στρατηγική Κυβερνοασφάλειας[53]. Επιδιώκει να ενισχύσει τις ελληνικές και ευρωπαϊκές ψηφιακές υποδομές, προχωρά στη δημιουργία ή ενίσχυση των αρμόδιων αρχών που είναι υπεύθυνες για την εποπτεία και τη διασφάλιση της κυβερνοασφάλειας όπως η Εθνική Αρχή Κυβερνοασφάλειας[54], προβλέπει σαφείς υποχρεώσεις για τους φορείς που διαχειρίζονται κρίσιμες ψηφιακές υποδομές, όπως η υποχρέωση να αναπτύξουν σχέδια κυβερνοασφάλειας και να υλοποιούν τα απαραίτητα μέτρα προστασίας.

ι. Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) προστατεύει τα φυσικά πρόσωπα όταν τα δεδομένα τους υπόκεινται σε επεξεργασία από τον ιδιωτικό τομέα και από το μεγαλύτερο μέρος του δημοσίου τομέα και επιτρέπει στα άτομα να ελέγχουν καλύτερα τα δεδομένα προσωπικού χαρακτήρα τους.

Με τον ΓΚΠΔ ενισχύονται τα υπάρχοντα δικαιώματα, προβλέπονται νέα δικαιώματα και παρέχεται στα φυσικά πρόσωπα μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων. Ειδικότερα τα πρόσωπα αποκτούν ευκολότερη πρόσβαση στα ατομικά δεδομένα ώστε να τους παρέχονται περισσότερες πληροφορίες σχετικά με τον τρόπο επεξεργασίας των δεδομένων και τη διασφάλιση ότι οι πληροφορίες αυτές είναι διαθέσιμες με τρόπο σαφή και

[53] Η στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο αποσκοπεί στην ενίσχυση της ανθεκτικότητας στις απειλές στον κυβερνοχώρο και στη διασφάλιση ότι οι πολίτες και οι επιχειρήσεις επωφελούνται από αξιόπιστες ψηφιακές τεχνολογίες, https://digital-strategy.ec.europa.eu/el/policies/cybersecurity-strategy

54 https://mindigital.gr/dioikisi/kyvernoasfaleia: Η Εθνική Αρχή Κυβερνοασφάλειας αποτελεί τον βασικό φορέα διαμόρφωσης και εφαρμογής των πολιτικών κυβερνοασφάλειας στη χώρα. Οι αρμοδιότητες και ο ρόλος λειτουργίας της καθορίζονται κυρίως από τον ν. 5086/2024 (ΦΕΚ 23, τ. Α )και τον ν. 5160/2024 (ΦΕΚ 196, τ. Α΄) ο οποίος ενσωματώνει την Οδηγία NIS 2 (2022/2555).

κατανοητό. Επίσης δίνεται στα πρόσωπα σαφέστερο δικαίωμα διαγραφής. Συγκεκριμένα όταν ένα άτομο δεν επιθυμεί πλέον την επεξεργασία των δεδομένων του και δεν υπάρχει θεμιτός λόγος για τη διατήρησή τους, τα δεδομένα θα διαγράφονται. Τέλος δίνεται στα πρόσωπα το δικαίωμα να γνωρίζουν πότε παραβιάστηκαν τα δεδομένα προσωπικού χαρακτήρα τους καθώς οι εταιρείες και οι οργανισμοί πρέπει να ενημερώνουν την αρμόδια εποπτική αρχή προστασίας δεδομένων αλλά και τα φυσικά πρόσωπα που επηρεάζονται στην περίπτωση σοβαρών παραβιάσεων δεδομένων προσωπικού χαρακτήρα.

Η ελληνική νομοθεσία προσαρμόστηκε στον ΓΚΠΔ με τον ν. 4624/2019 (ΦΕΚ 137, τ. Α΄). Ο νόμος έθεσε τις διαδικασίες και τις υποχρεώσεις των υπεύθυνων επεξεργασίας δεδομένων και των υπεύθυνων προστασίας δεδομένων, ενίσχυσε το ρόλο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και διασφάλισε τα δικαιώματα των φυσικών προσώπων σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων.

## 2. Εθνική Νομοθεσία

Η εθνική νομοθεσία για την προστασία των καταναλωτών από παράνομες ενέργειες σε βάρος τους είναι κυρίως εναρμονισμένη με την ευρωπαϊκή νομοθεσία, οδηγίες και κανονισμούς, καθώς το ηλεκτρονικό εμπόριο διασχίζει τα σύνορα της χώρας αλλά και της ΕΕ και απαιτούνται κοινοί κανόνες και κοινές αρχές για να εξασφαλιστεί η προστασία των καταναλωτών και η ομαλή λειτουργία των διαδικτυακών αγορών.

### α. Ποινικός Κώδικας

Κάποιες επιπλέον διατάξεις πέραν των όσων έχουν αναφερθεί ήδη στην υποενότητα «Ενωσιακή Νομοθεσία» περιλαμβάνονται στον Ποινικό Κώδικα. Δεν πρόκειται για ειδικές διατάξεις που αφορούν αποκλειστικά το ηλεκτρονικό εμπόριο αλλά είναι πιο γενικές που αφορούν εγκλήματα που εμφανίζονται και στο πλαίσιο του ηλεκτρονικού εμπορίου όπως η παράνομη πρόσβαση σε σύστημα πληροφοριών ή δεδομένα, η παράνομη πρόσβαση σε δεδομένα υπολογιστών και η απάτη με υπολογιστή.

Με το άρθρο 370Β ποινικοποιείται η πρόσβαση σε σύστημα σε σύστημα πληροφοριών ή ηλεκτρονικά δεδομένα, ανεξάρτητα από την επέλευση ζημίας. Η διάταξη αυτή προέκυψε από την ανάγκη για αυξημένη προστασία από την ραγδαία εξέλιξη της τεχνολογίας και την αυξημένη ανάγκη προστασίας των προσωπικών δεδομένων ώστε αυτά να μην είναι εύκολα προσβάσιμα.

Με το άρθρο 370Γ προστατεύονται τα διάφορα απόρρητα στοιχεία ή προγράμματα Η/Υ, τα οποία συνιστούν κρατικά, επιστημονικά, επαγγελματικά ή απόρρητα επιχειρήσεων του δημοσίου ή ιδιωτικού τομέα και με το άρθρο 370Δ ποινικοποιείται η αθέμιτη αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη σε τρίτο ή παραβίαση στοιχείων ή προγράμματος.

Η απάτη με υπολογιστή προβλέπεται στο άρθρο 386 Α του Ποινικού Κώδικα. Το άρθρο θεσμοθετήθηκε για πρώτη φορά το 1988 με το άρθρο 5 του ν. 1805/1988 (ΦΕΚ 199, τ. Α΄). Ο νομοθέτης με το άρθρο ήθελε να προστατεύσει την περιουσία από προσβολές που συνδεόταν με την ανάπτυξη της τεχνολογίας και εκδηλωνόταν μέσω των ηλεκτρονικών υπολογιστών.[55] Με την τροποποίηση που επέφερε ο ν. 4619/2019 (ΦΕΚ 95, τ. Α΄) προσδιορίζεται ως αξιόποινο αποτέλεσμα η βλάβη της ξένης περιουσίας, απαριθμεί τους τρόπους τέλεσης του εγκλήματος της απάτης με τη χρήση υπολογιστή, ποινικοποιεί τις προπαρασκευαστικές πράξεις του εγκλήματος και θέτει τις προϋποθέσεις χαρακτηρισμού του ως κακούργημα.

β. Κώδικας καταναλωτικής δεοντολογίας για το ηλεκτρονικό εμπόριο

Με την Υπουργική Απόφαση 31619οικ./2017 από 14-03-2017 (ΦΕΚ 969, τ. Β΄) καθιερώθηκε ο Κώδικας Καταναλωτικής Δεοντολογίας για το ηλεκτρονικό εμπόριο. Ο Κώδικας αφορά σε κανόνες αυτορρύθμισης των επιχειρήσεων που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο, θέτει τις γενικές αρχές και ορίζει τους ελάχιστους κανόνες επαγγελματικής δεοντολογίας και ηθικής συμπεριφοράς που πρέπει να τηρούν οι επιχειρήσεις απέναντι στους καταναλωτές. Ο Κώδικας εφαρμόζεται στις συναλλαγές στο πλαίσιο των συμβάσεων πώλησης αγαθών ή παροχής υπηρεσιών που συνάπτονται μεταξύ καταναλωτών και προμηθευτών έναντι αμοιβής εξ ολοκλήρου διαδικτυακά, δηλαδή με ηλεκτρονικά μέσα εξ αποστάσεως χωρίς να είναι απαραίτητη η ταυτόχρονη φυσική παρουσία των δύο μερών (συναλλαγές επιχείρηση προς καταναλωτή)[56]. Διέπεται από τις αρχές της προστασίας του καταναλωτή, της διαφάνειας, της αμεροληψίας, της τεχνολογικής ουδετερότητας, της επαγγελματικής δεοντολογίας, της ηθικής συμπεριφοράς και του σεβασμού στην ιδιωτική ζωή, της προστασίας των προσωπικών δεδομένων και της προστασίας των ευάλωτων ομάδων πληθυσμού[57].

[55] Αδάμ Παπαδαμάκης, Τα περιουσιακά εγκλήματα, Β' Έκδοση, Εκδόσεις Σάκκουλα, 2016 , σελ. 162

[56] Άρθρο 1 Κώδικα Καταναλωτικής Δεοντολογίας για το ηλεκτρονικό εμπόριο, https://gge.mindev.gov.gr/tomeas-emporiou/kodikas-katanalotikis-deontologias-ilektroniko-emporio/

[57] Άρθρο 2 Κώδικα Καταναλωτικής Δεοντολογίας για το ηλεκτρονικό εμπόριο

## ΙΙ. Θεσμικοί φορείς για την αντιμετώπιση της απάτης στο ηλεκτρονικό έγκλημα

Η αντιμετώπιση της απάτης στο ηλεκτρονικό εμπόριο απαιτεί τη συνεργασία πολλών θεσμικών φορέων σε εθνικό και σε ευρωπαϊκό επίπεδο. Οι φορείς αυτοί διαδραματίζουν σημαντικό ρόλο στην πρόληψη, την ανίχνευση, την καταπολέμηση και την καταστολή της ηλεκτρονική απάτης μέσω νομοθετικών, οργανωτικών και τεχνολογικών μέτρων.

### 1. Θεσμικοί φορείς Ευρωπαϊκής Ένωσης

Όπως είδαμε και στον τομέα του νομοθετικού πλαισίου, η Ευρωπαϊκή Ένωση αντιμετωπίζει το ζήτημα της απάτης στον τομέα του ηλεκτρονικού εμπορίου πάρα πολύ σοβαρά. Τα εγκλήματα απάτης σε βάρος των καταναλωτών μπορούν να κλονίσουν την εμπιστοσύνη τους στο οικοδόμημα του ηλεκτρονικού εμπορίου το οποίο αποτελεί ένα από τα κύρια μέσα της ΕΕ για την ενιαία εσωτερική αγορά. Επομένως εκτός από ένα πολύ ισχυρό νομοθετικό πλέγμα η ΕΕ διαθέτει αρκετούς φορείς για την αντιμετώπιση εγκλημάτων ηλεκτρονικής απάτης.

#### α. EUROPOL (European Union Agency for Law Inforcement Cooperation)[58]

Η Europol αποτελεί τον ευρωπαϊκό οργανισμό αστυνομικής συνεργασίας που είναι υπεύθυνος για την υποστήριξη των εθνικών αστυνομικών αρχών στην καταπολέμηση του εγκλήματος στην ΕΕ. Παρέχει πλατφόρμες για τη συνεργασία και τον συντονισμό σε διακρατικές υποθέσεις και είναι κρίσιμος για την αντιμετώπιση της ηλεκτρονικής απάτης.

Διαθέτει το Ευρωπαϊκό Κέντρο Κυβερνοεγκλήματος (EC3) το οποίο εξειδικεύεται στην δίωξη ηλεκτρονικών εγκλημάτων που σχετίζονται με ηλεκτρονικές απάτες, phishing, κακόβουλο λογισμικό και άλλες μορφές ηλεκτρονικών εγκλημάτων. Το κέντρο παρέχει τεχνική υποστήριξη στις εθνικές αστυνομικές αρχές, οργανώνει εκπαιδευτικά προγράμματα και βοηθά στην ανάλυση ψηφιακών στοιχείων για να εντοπιστούν οι δράστες.

#### β. ENISA (European Union Agency for Cybersecurity)[59]

Η ENISA είναι η Ευρωπαϊκή Υπηρεσία για την Κυβερνοασφάλεια, η οποία ενισχύει την ασφάλεια του κυβερνοχώρου στην ΕΕ. Αν και ο κύριος στόχος της είναι η γενική προστασία

[58] https://www.europol.europa.eu/
[59] https://www.enisa.europa.eu/

των δικτύων και των πληροφοριών στην ΕΕ, έχει σημαντικό ρόλο στην πρόληψη της ηλεκτρονικής απάτης μέσω στρατηγικών και εργαλείων που αφορούν την κυβερνοασφάλεια.

Παρέχει τεχνική υποστήριξη για την αντιμετώπιση κυβερνοεπιθέσεων και ευαισθητοποιεί για τις απειλές που σχετίζονται με την ηλεκτρονική απάτη όπως το phishing και τις επιθέσεις κακόβουλου λογισμικού. Επίσης παρέχει καθοδήγηση και εκπαίδευση στους φορείς του δημόσιου και ιδιωτικού τομέα για να ενισχύσουν τα μέτρα ασφαλείας τους και να προλαμβάνουν τα εγκλήματα στον κυβερνοχώρο

.

γ. EUROJUST (European Union Agency for Criminal Justice Cooperation)[60]

Η Eurojust είναι η Ευρωπαϊκή Υπηρεσία για τη συνεργασία στον τομέα της δικαιοσύνης και ενισχύει τη συνεργασία μεταξύ των δικαστικών αρχών των κρατών μελών της ΕΕ για την καταπολέμηση του εγκλήματος. Ο ρόλος της είναι κρίσιμος για την ολοκλήρωση των δικαστικών διαδικασιών και την ενίσχυση της δικαστικής συνεργασίας σε υποθέσεις ηλεκτρονικής απάτης που διαπράττονται σε διακρατικό επίπεδο.

Συνεργάζεται με τις εθνικές δικαστικές αρχές και τις αστυνομικές υπηρεσίες για τη δίωξη των εγκλημάτων που σχετίζονται με την ηλεκτρονική απάτη και την κυβερνοεγκληματικότητα και παρέχει υποστήριξη σε διεθνείς έρευνες ενώ συντονίζει τις διακρατικές διαδικασίες δίωξης.

δ. European Central Bank (ECB)[61]

Η Ευρωπαϊκή Κεντρική Τράπεζα και άλλες ρυθμιστικές αρχές της ΕΕ, όπως η Ευρωπαϊκή Τραπεζική Αρχή (EBA) αναλαμβάνουν την εποπτεία και την εφαρμογή κανόνων και οδηγιών για την προστασία των οικονομικών συναλλαγών και την ασφάλεια των ηλεκτρονικών πληρωμών.

Συνεργάζεται με τις εθνικές κεντρικές τράπεζες για να αναπτύξει μέτρα ασφαλείας για τις ηλεκτρονικές πληρωμές και την προστασία των τραπεζικών συστημάτων από ηλεκτρονικές απάτες. Επίσης αναπτύσσει τις κατευθυντήριες γραμμές για την ασφάλεια των χρηματοπιστωτικών υπηρεσιών και την πρόληψη της ηλεκτρονικής απάτης.

[60] https://www.eurojust.europa.eu/
[61] https://www.ecb.europa.eu/home/html/index.en.html

ε. Eurydice (European Union's Information and Communication Technologies Agency)[62]

Η Eurydice είναι η υπηρεσία της Ευρωπαϊκής Ένωσης για την προώθηση των πληροφοριών και των επικοινωνιακών τεχνολογιών στην ΕΕ και την προστασία των πολιτών από κινδύνους που προκύπτουν από την κακή χρήση αυτών των τεχνολογιών. Αναπτύσσει πλατφόρμες πληροφόρησης για τους πολίτες και τις επιχειρήσεις σχετικά με τους κινδύνους που συνδέονται με την ηλεκτρονική απάτη και τις ψηφιακές απειλές.

στ. European Data Protection Supervisor (EDPS)[63]

Ο Ευρωπαίος Επόπτης για την Προστασία Δεδομένων είναι υπεύθυνος για την παρακολούθηση της προστασίας των προσωπικών δεδομένων στο πλαίσιο των θεσμικών οργάνων της ΕΕ και τη διασφάλιση της συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Έχει κρίσιμο ρόλο στην προστασία των προσωπικών δεδομένων των πολιτών από τις ηλεκτρονικές απάτες που σχετίζονται με την παράνομη χρήση η τη διαρροή των προσωπικών δεδομένων μέσω διαδικτύου. Παράλληλα παρέχει καθοδήγηση και υποστήριξη στους φορείς ΕΕ για την ασφάλεια των δεδομένων και την πρόληψη της ηλεκτρονικής απάτης.

ζ. European Court of Justice[64]

Το Δικαστήριο της Ευρωπαϊκής Ένωσης έχει το δικαίωμα να επιλύει νομικές διαφορές που αφορούν την νομοθεσία της ΕΕ και να αποφασίζει για υποθέσεις ηλεκτρονικής απάτης που συνδέονται με διακρατικές συναλλαγές και την ερμηνεία του δικαίου της ΕΕ. Ειδικότερα μπορεί να εκδίδει αποφάσεις για διεθνείς απάτες στον κυβερνοχώρο ερμηνεύοντας την εφαρμογή των κανόνων της ΕΕ για την προστασία των δεδομένων και την ασφάλεια στο διαδίκτυο.

[62] https://eurydice.eacea.ec.europa.eu/
[63] https://www.edps.europa.eu/_en
[64] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en

2. Εθνικοί Θεσμικοί Φορείς

Όπως κάθε μέλος της ΕΕ έτσι και η Ελλάδα διαθέτει και τους δικούς της εθνικούς φορείς για την αντιμετώπιση της ηλεκτρονικής απάτης. Πρόκειται για φορείς με αρμοδιότητες σε διάφορους τομείς όπως η ασφάλεια του διαδικτύου, η προστασία των καταναλωτών, η ρύθμιση των τηλεπικοινωνιών και η προστασία των προσωπικών δεδομένων. Η συνεργασία τους τόσο σε εθνικό επίπεδο όσο και με τους προαναφερόμενους ευρωπαϊκούς φορείς είναι απαραίτητη για την ανάπτυξη μίας εθνικής στρατηγικής πρόληψης και αντίδρασης στις ηλεκτρονικές απάτες.

α. Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Ελληνικής Αστυνομίας[65]

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας είναι ο κύριος φορέας που είναι υπεύθυνος για την καταπολέμηση των εγκλημάτων που διαπράττονται μέσω του διαδικτύου. Ασχολείται με διάφορα είδη απάτης, όπως απάτη με χρήση πιστωτικών καρτών, phishing και κλοπή προσωπικών δεομένων, απάτες που αφορούν τις ηλεκτρονικές συναλλαγές και αγορές, κακόβουλο λογισμικό κ.α. Για την αντιμετώπιση των εγκλημάτων ηλεκτρονικής απάτης συνεργάζεται με διεθνείς οργανισμούς αλλά και φορείς άλλων χωρών.

β. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[66]

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα πρόκειται για συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή που έχει ως αποστολή την εφαρμογή των νομοθετημάτων που αφορούν στην προστασία των προσωπικών δεδομένων του ατόμου και διασφαλίζει ότι τα δεδομένα που συλλέγονται και επεξεργάζονται από τους οργανισμούς είναι ασφαλή. Όταν διαπράττεται ηλεκτρονική απάτη που περιλαμβάνει παραβίαση προσωπικών δεδομένων έχει τη δυνατότητα να ερευνήσει την υπόθεση και να επιβάλλει ποινές σε περίπτωση παραβίασης του κανονιστικού πλαισίου περί προστασίας δεδομένων.

[65] https://cyberalert.gr/
[66] https://www.dpa.gr/

γ. Συνήγορος του Καταναλωτή[67]

Ο Συνήγορος του Καταναλωτή είναι Ανεξάρτητη Αρχή που έχει ως αποστολή την προστασία και προώθηση των δικαιωμάτων των καταναλωτών. Σε σχέση με το ηλεκτρονικό εμπόριο παρέχει καθοδήγηση και υποστήριξη στους πολίτες που αντιμετωπίζουν προβλήματα στις συναλλαγές τους μέσω διαδικτύου καθώς και συμβουλές για την ασφάλεια των διαδικτυακών αγορών. Οι καταναλωτές μπορούν να υποβάλλουν καταγγελία για μία παράνομη ή αθέμιτη σε βάρος τους συμπεριφορά στο πλαίσιο μιας διαδικτυακής αγοράς. Ο Συνήγορος αν και δεν έχει δικαιοδοσία για τη λήψη νομικών αποφάσεων, προσφέρει διαμεσολάβηση μεταξύ καταναλωτή και επιχείρησης για επίλυση της διαφοράς.

δ. Γενική Διεύθυνση Αγοράς και Προστασίας Καταναλωτή[68]

Η Γενική Διεύθυνση Αγοράς και Προστασίας Καταναλωτή αποτελεί υπηρεσία της Γενικής Γραμματείας Εμπορίου του Υπουργείου Ανάπτυξης που έχει αποστολή την προάσπιση των οικονομικών συμφερόντων των καταναλωτών και της ασφάλειάς τους, τη διαμόρφωση υγιούς καταναλωτικής συνείδησης και προτύπων ορθής καταναλωτικής συμπεριφοράς καθώς και την ομαλή λειτουργία της αγοράς και τη διασφάλιση του υγιούς ανταγωνισμού των επιχειρήσεων.

ε. Επιτροπή Κεφαλαιαγοράς[69]

Η Επιτροπή Κεφαλαιαγοράς είναι Ν.Π.Δ.Δ. που είναι υπεύθυνο για την εποπτεία των χρηματοπιστωτικών αγορών στην Ελλάδα και η αρμοδιότητά της επεκτείνεται σε περιπτώσεις που αφορούν το ηλεκτρονικό εμπόριο στις χρηματοοικονομικές αγορές. Επιβλέπει τη συμμόρφωση των χρηματοπιστωτικών υπηρεσιών και πλατφορμών που δραστηριοποιούνται στο διαδίκτυο (π.χ. συναλλαγές με κρυπτονομίσματα) και παρεμβαίνει στην περίπτωση εξαπάτησης των καταναλωτών μέσω διαδικτυακών επενδύσεων ή παραπλανητικών διαδικτυακών προσφορών.

[67] https://www.synigoroskatanaloti.gr/el
[68] https://gge.mindev.gov.gr/home/γενικη-διευθυνση-αγορας-και-προστασι/
[69] http://www.hcmc.gr/el_GR/web/portal/home

στ. Υπουργείο Ψηφιακής Διακυβέρνησης[70]

Το Υπουργείο Ψηφιακής Διακυβέρνησης είναι υπεύθυνο για την ανάπτυξη πολιτικών και στρατηγικών στον τομέα των ψηφιακών υπηρεσιών και της κυβερνοασφάλειας. Σχετικά με το ηλεκτρονικό εμπόριο, το Υπουργείο προωθεί την εφαρμογή της ψηφιακής υπογραφής και των ασφαλών ηλεκτρονικών πληρωμών, υλοποιεί έργα για την ενίσχυση της ψηφιακής ασφάλειας των δημόσιων και ιδιωτικών υπηρεσιών και διασφαλίζει τη συμμόρφωση με την ευρωπαϊκή νομοθεσία για το ηλεκτρονικό εμπόριο και την ηλεκτρονική ασφάλεια.

## III. Πρόληψη ηλεκτρονικής απάτης στο ηλεκτρονικό εμπόριο

Το ηλεκτρονικό εμπόριο με την διαρκή εξέλιξη της τεχνολογίας θα καταλαμβάνει όλο και μεγαλύτερο μέρος της ενιαίας εσωτερικής αγοράς. Η Ευρωπαϊκή Ένωση προωθεί τις διαδικτυακές αγορές καθώς δεν γνωρίζουν σύνορα και συμβάλλουν στην ενίσχυση της ενιαίας αγοράς. Τόσο η ΕΕ όσο και τα κράτη μέλη έχουν αντιληφθεί τη σημασία του και έχουν δημιουργήσει ένα αρκετά ασφυκτικό νομοθετικό πλέγμα για την προστασία του από παράνομες ενέργειες αλλά και ένα δίκτυο φορέων που δραστηριοποιούνται σε διάφορους τομείς του διαδικτύου και συνεργάζονται μεταξύ τους για την πρόληψη και την αντιμετώπιση της ηλεκτρονικής απάτης. Αν και είναι πολύ σημαντική η ύπαρξη τόσο του νομοθετικού πλαισίου όσο και των φορέων που μεριμνούν για την εφαρμογή τους, ακόμη σημαντικότερη είναι η πρόληψη της για την οποία θα πρέπει να εργαστούν τα εμπλεκόμενα μέρη μιας διαδικτυακής συναλλαγής, επιχείρηση και καταναλωτής.

### 1. Ο ρόλος των καταναλωτών στην πρόληψη της ηλεκτρονικής απάτης

Οι καταναλωτές παίζουν καθοριστικό ρόλο στην πρόληψη της ηλεκτρονικής απάτης. Η ενημέρωση, η σωστή εκπαίδευση και η αυξημένη προσοχή στις διαδικτυακές συναλλαγές μπορούν να μειώσουν σημαντικά τον κίνδυνο εξαπάτησης. Ορισμένοι τρόποι με τους οποίους οι καταναλωτές μπορούν να προστατεύσουν τους εαυτούς τους είναι οι ακόλουθοι:
i) Επιλογή αξιόπιστων ιστοσελίδων και υπηρεσιών: Οι καταναλωτές θα πρέπει να επιλέγουν μόνο αξιόπιστα και αναγνωρισμένα ηλεκτρονικά καταστήματα για τις ηλεκτρονικές τους αγορές. Η εμφάνιση του ασφαλούς συνδέσμου https και των πιστοποιητικών ασφαλείας είναι καθοριστική για την αξιοπιστία της ιστοσελίδας.

[70] https://mindigital.gr/

ii) Αναγνώριση και αποφυγή ύποπτων μηνυμάτων: Οι καταναλωτές πρέπει να είναι προσεκτικοί όταν λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου ή γραπτά μηνύματα από άγνωστους αποστολείς που ζητούν προσωπικά δεδομένα ή τραπεζικές πληροφορίες. Θα πρέπει να επιβεβαιώνουν την γνησιότητα των αιτημάτων, αποφεύγοντας το άνοιγμα συνδέσμων ή την παροχή προσωπικών στοιχείων μέσω τέτοιων μηνυμάτων.

iii) Ενημέρωση και εκπαίδευση: Η συνεχής ενημέρωση και εκπαίδευση των καταναλωτών για τις πιο πρόσφατες απάτες και τις μεθόδους που χρησιμοποιούν οι εγκληματίες είναι καθοριστική. Αυτό περιλαμβάνει την αναγνώριση παραπλανητικών προσφορών ή εξαιρετικά χαμηλών τιμών που φαίνονται «πολύ καλές για να είναι αληθινές».[71]

iv) Χρήση ασφαλών μεθόδων πληρωμής: Οι καταναλωτές θα πρέπει να χρησιμοποιούν αξιόπιστους και ασφαλείς τρόπους πληρωμής για τις διαδικτυακές τους συναλλαγές, όπως πιστωτικές κάρτες, Paypal ή άλλες υπηρεσίες που προσφέρουν επιπλέον επίπεδα προστασίας και διευκολύνουν την αμφισβήτηση μιας συναλλαγής σε περίπτωση απάτης.

v) Ενημέρωση των αρχών σε περίπτωση απάτης: Σε περίπτωση που ένας καταναλωτής πέσει θύμα ηλεκτρονικής απάτης πρέπει να ενημερώσει άμεσα τις αρχές (όπως τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος) και τη χρηματοπιστωτική του υπηρεσία ώστε να δράσουν ώστε να μειωθούν οι συνέπειες της απάτης.

Η επιτυχής πρόληψη της ηλεκτρονικής απάτης εξαρτάται από τη συνεχιζόμενη ευαισθητοποίηση και τη συνεργασία των καταναλωτών. Οι τελευταίοι πρέπει να γνωρίζουν ότι είναι υπεύθυνοι για την προσωπική τους ασφάλεια και την προστασία των δεδομένων τους στις ηλεκτρονικές συναλλαγές. Αυτό απαιτεί όχι μόνο τη λήψη των κατάλληλων μέτρων ασφαλείας, αλλά και την ενεργεί συμμετοχή τους στην καταπολέμηση των εγκλημάτων αυτών μέσω της αναφοράς ύποπτων δραστηριοτήτων και της βοήθεια καταγραφής νέων μεθόδων απάτης.

[71] Οι καταναλωτές έχουν τη δυνατότητα να ενημερώνονται και μέσα από τις ιστοσελίδες των αρμόδιων αρχών σχετικά με τους τρόπους προστασίας τους από περιπτώσεις ηλεκτρονικής απάτης αλλά και μέσα από τις πολλαπλές αναφορές στα μέσα μαζικής ενημέρωσης. Π.χ. Στην ιστοσελίδα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, cyberalert.gr, υπάρχει ειδικός «χώρος» που παρέχει οδηγίες στους πολίτες για την προστασία του, https://cyberalert.gr/syxnes-erotiseis/
Επίσης ανάλογες αναφορές: capital.gr: «Καμπάνια ενημέρωσης και ευαισθητοποίησης για την ηλεκτρονική απάτη από ΕΕΤ και Mastercard», 12-02-2024, https://www.capital.gr/epikairotita/3770909/kampania-enimerosis-kai-euaisthitopoiisis-gia-tin-ilektroniki-apati-apo-eet-kai-mastercard/,
Παρομοίως, tanea.gr: «Απάτη: Προσπαθούν να σας εξαπατήσουν με μηνύματα δήθεν από το gov.gr – Τι να προσέξετε» 29-10-2024, https://www.tanea.gr/2024/10/29/greece/apati-prospathoun-na-sas-eksapatisoun-me-minymata-dithen-apo-to-gov-gr-ti-na-proseksete/ κ.α.

2. Ο ρόλος των επιχειρήσεων στην πρόληψη της ηλεκτρονικής απάτης

Κρίσιμος στην πρόληψη της ηλεκτρονικής απάτης είναι ο ρόλος του έτερου μέρους μιας διαδικτυακής συναλλαγής, της επιχείρησης. Οι επιχειρήσεις όχι μόνο παρέχουν τα μέσα για τις ηλεκτρονικές συναλλαγές αλλά επίσης φέρουν την ευθύνη για την προστασία των δεδομένων των πελατών και τη διασφάλιση της εμπιστοσύνης των καταναλωτών στο ηλεκτρονικό εμπόριο. Εξαιτίας των αυξανόμενων απειλών στον κυβερνοχώρο οι επιχειρήσεις πρέπει να αναλάβουν μια ενεργή και προληπτική προσέγγιση για την αποτροπή της ηλεκτρονικής απάτης και της διατήρησης της ασφάλειας των συναλλαγών και των δεδομένων. Ορισμένα από τα μέτρα που μπορούν να λάβουν οι επιχειρήσεις στο πλαίσιο της πρόληψης είναι:

i) Εφαρμογή συστήματος Ασφαλούς Συναλλαγής: Θα πρέπει η επιχείρηση να εξασφαλίσει ότι οι διαδικτυακές συναλλαγές είναι ασφαλείς και προστατεύονται από απάτες. Για να το επιτύχει αυτό είναι αναγκαία η χρήση κρυπτογράφησης SSL (Secure Sockets Layer) ή TLS (Transport Layer Security) για την προστασία των δεδομένων που ανταλλάσσονται κατά τις συναλλαγές (π.χ. προσωπικά και οικονομικά στοιχεία πελατών). Με την κρυπτογράφηση αυτή διασφαλίζεται ότι οι πληροφορίες που διακινούνται μέσω της ιστοσελίδας είναι ασφαλείς από τρίτους. Επιπλέον η επιχείρηση θα πρέπει να επιλέξει ασφαλείς μεθόδους πληρωμής, όπως πιστωτικές κάρτες, paypal, σύγχρονα συστήματα πληρωμών και να συνεργάζεται με ασφαλείς και αξιόπιστους παρόχους πληρωμών που έχουν αποδεδειγμένο ιστορικό στην ασφάλεια.

ii) Πολυπαραγοντική Αυθεντικοποίηση (2FA): Η πολυπαραγοντική αυθεντικοποίηση είναι ένας αποτελεσματικός τρόπος για να προστατευτούν οι λογαριασμοί των χρηστών και οι συναλλαγές από μη εξουσιοδοτημένη πρόσβαση. Με τον διπλό έλεγχο ταυτότητας ο χρήστης πρέπει να εισάγει έναν επιπλέον κωδικό, τον οποίο μπορεί να λάβει μέσω e mail ή μέσω κινητού τηλεφώνου. Με τον τρόπο αυτό η επιχείρηση προσφέρει επιπλέον επίπεδο ασφαλείας, κάνοντας την είσοδο των χρηστών στους λογαριασμούς τους πιο ασφαλή.

iii) Εφαρμογή τεχνολογιών ανίχνευσης και πρόληψης απάτης: Η επιχείρηση μπορεί να χρησιμοποιήσει τεχνολογίες ανίχνευσης απάτης για να εντοπίσει ύποπτες ή ανώμαλες συναλλαγές σε πραγματικό χρόνο. Η χρήση αλγορίθμων που βασίζονται στην τεχνητή νοημοσύνη και την μηχανική μάθηση μπορεί να βοηθήσει στην ανίχνευση ύποπτων μοτίβων συναλλαγών όπως ασυνήθιστο μέγεθος συναλλαγών, γεωγραφική τοποθεσία ή επανειλημμένες αποτυχημένες προσπάθειες πληρωμής. Ένας άλλος τρόπος είναι η

βαθμολόγηση των συναλλαγών (αναγνώριση απάτης μέσω συστήματος scoring) χρησιμοποιώντας ιστορικά δεδομένα για να εντοπιστούν πιθανές κακόβουλες ενέργειες.

iv) Εκπαίδευση και ευαισθητοποίηση καταναλωτών: Η συνεχής ενημέρωση και εκπαίδευση των καταναλωτών είναι καθοριστική για την πρόληψη της ηλεκτρονικής απάτης. Οι επιχειρήσεις θα πρέπει να διασφαλίσουν ότι οι πελάτες τους είναι ενήμεροι για τους κινδύνους και τις προφυλάξεις που πρέπει να ληφθούν κατά τη διάρκεια των ηλεκτρονικών συναλλαγών. Μπορούν να διεξάγουν ενημερωτικές καμπάνιες σχετικά με τους κινδύνους ηλεκτρονικής απάτης, τη σημασία του ισχυρού κωδικού πρόσβασης και τα χαρακτηριστικά των ύποπτων μηνυμάτων ή email. Θα πρέπει επιπλέον να παρέχουν σαφείς οδηγίες στους πελάτες τους σχετικά με την ασφαλή πλοήγηση στην ιστοσελίδα τους και τη χρήση των ηλεκτρονικών πληρωμών.

v) Συμμόρφωση με τους κανονισμούς και τη νομοθεσία: Οι επιχειρήσεις πρέπει να τηρούν όλους τους νομικούς κανονισμούς και τις βέλτιστες πρακτικές ασφαλείας που ισχύουν για το ηλεκτρονικό εμπόριο και την προστασία των προσωπικών δεδομένων. Σύμφωνα με τον Γενικό Κανονισμό Προσωπικών Δεδομένων θα πρέπει να προστατεύουν τα προσωπικά δεδομένα των πελατών τους και να λαμβάνουν κάθε μέτρο για την διασφάλισή τους από παραβιάσεις. Επίσης όσες επιχειρήσεις επεξεργάζονται πληρωμές με πιστωτικές ή χρεωστικές κάρτες πρέπει να συμμορφώνονται με το πρότυπο PCI DSS[72] για την προστασία των δεδομένων των καρτών των πελατών.

vi) Συνεργασία με τις αρμόδιες αρχές και υπηρεσίες ασφαλείας: Η επιχείρηση πρέπει να συνεργάζεται με τις αρμόδιες αρχές όπως η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος για την αντιμετώπιση και πρόληψη ηλεκτρονικής απάτης. Κάθε επιχείρηση θα πρέπει να έχει μία διαδικασία για να αναφέρει τα περιστατικά απάτης στις αρμόδιες αρχές και να συνεργάζεται με αυτές για τη διερεύνηση των εγκλημάτων.

Οι επιχειρήσεις έχουν καθοριστικό ρόλο στην πρόληψη της απάτης στο ηλεκτρονικό εμπόριο. Θα πρέπει να εφαρμόζουν μία ολοκληρωμένη στρατηγική ασφαλείας που θα περιλαμβάνει τεχνολογικά μέτρα, εκπαίδευση χρηστών, συμμόρφωση με τους κανονισμούς και ενεργή συνεργασία με τις αρμόδιες αρχές. Θα πρέπει να επενδύσουν σε τεχνολογίες και διαδικασίες που ενισχύουν την ασφάλεια των ηλεκτρονικών συναλλαγών και παράλληλα ενημερώνουν και εκπαιδεύουν τους πελάτες τους για την αποφυγή κινδύνων απάτης.

[72]Το Payment Card Industry Data Security Standard (PCI DSS) αποτελεί ένα διεθνές πρότυπο ασφαλείας, που απευθύνεται σε όλες τις επιχειρήσεις και τους οργανισμούς που δέχονται, επεξεργάζονται, αποθηκεύουν ή μεταδίδουν δεδομένα καρτών πληρωμής, https://www.pcisecuritystandards.org/

**Συμπέρασμα**

Το ηλεκτρονικό εμπόριο και η ηλεκτρονική απάτη είναι δύο έννοιες άρρηκτα συνδεδεμένες μεταξύ τους. Το ηλεκτρονικό εμπόριο εμφανίζει έναν εντυπωσιακό ρυθμό ανάπτυξης, προσφέροντας σε επιχειρήσεις και καταναλωτές νέες δυνατότητες και ευκολίες στις συναλλαγές τους. Ωστόσο η ευκολία αυτή που παρέχει η εξέλιξη της τεχνολογίας συνδέεται με αυξανόμενους κινδύνους όπως η ηλεκτρονική απάτη που επηρεάζει επιχειρήσεις και καταναλωτές.

Οι καταναλωτές έχουν τη δυνατότητα να πραγματοποιούν συναλλαγές γρήγορα, εύκολα, χωρίς γεωγραφικούς περιορισμούς. Αξιοποιώντας όλες τις τεχνολογίες του ηλεκτρονικού εμπορίου μπορούν να πραγματοποιήσουν συγκρίσεις τιμών, χαρακτηριστικών, προϊόντων για να πραγματοποιήσουν την καταλληλότερη γι' αυτούς αγορά.

Η Ευρωπαϊκή Ένωση πολύ νωρίς κατάλαβε ότι το ηλεκτρονικό εμπόριο είναι ένα από τα σημαντικά μέσα που θα βοηθήσουν στην επίτευξη του στόχου της, μια ενιαία εσωτερική αγορά, χωρίς σύνορα και περιορισμούς. Εντόπισε όμως και τους μεγάλους κινδύνους που ελλοχεύουν από αυτό καθώς η ηλεκτρονική απάτη αποτελεί σοβαρή απειλή. Η αύξηση των ηλεκτρονικών πληρωμών και των ψηφιακών συναλλαγών σε συνδυασμό με την «ανωνυμία» που προσφέρει το διαδίκτυο έχει δημιουργήσει ένα ευνοϊκό περιβάλλον για εγκληματίες που χρησιμοποιούν διάφορες τεχνικές όπως το phishing, την κλοπή στοιχείων πληρωμής, την κοινωνική μηχανική κ.α. για να εξαπατήσουν τους καταναλωτές.

Για την προστασία τους και την προστασία του ηλεκτρονικού εμπορίου γενικά έχει δημιουργήσει ένα ισχυρό νομοθετικό πλέγμα θέλοντας να προστατεύσει κάθε πτυχή του ηλεκτρονικού εμπορίου. Παράλληλα δημιούργησε ένα σημαντικό δίκτυο φορέων στους οποίους ανέθεσε την προστασία των ηλεκτρονικών συναλλαγών. Συμμάχους της έχει τα κράτη μέλη τα οποία φροντίζουν με την εθνική τους νομοθεσία να ενισχύουν ακόμη περισσότερο την προστασία του ηλεκτρονικού εμπορίου ενώ αναθέτουν στις εθνικές τους αρχές να συνεργάζονται αποτελεσματικά με τος ευρωπαϊκούς φορείς για την πρόληψη και την αντιμετώπιση των εγκλημάτων ηλεκτρονικής απάτης στο ηλεκτρονικό εμπόριο.

Είναι όμως γεγονός ότι πέρα από τη νομοθεσία και τους φορείς καθοριστικός είναι ο ρόλος των καταναλωτών και των επιχειρήσεων στον τομέα της πρόληψης της ηλεκτρονικής απάτης. Οι επιχειρήσεις οφείλουν να παρέχουν ασφαλή περιβάλλοντα συναλλαγών και να προστατεύουν τα προσωπικά δεδομένα των πελατών τους. Οι καταναλωτές από την πλευρά τους πρέπει να είναι προσεχτικοί και να αναγνωρίζουν τα σημάδια ύποπτων δραστηριοτήτων.

Το ηλεκτρονικό εμπόριο θα συνεχίσει να αναπτύσσεται προσφέροντας μοναδικές δυνατότητες αγορών σε καταναλωτές και επιχειρήσεις. Η ηλεκτρονική απάτη θα αποτελεί και αυτή μία διαρκή απειλή αφού στηρίζεται στον ίδιο πυλώνα με το ηλεκτρονικό εμπόριο, στην εξέλιξη της τεχνολογίας απαιτώντας την διαρκή ανάπτυξη και εφαρμογή συστημάτων ασφαλείας και την ευαισθητοποίηση όλων των εμπλεκομένων για την προστασία των συναλλαγών. Μόνο με τη σωστή προστασία και την ενίσχυση των δικτύων ασφαλείας, το ηλεκτρονικό εμπόριο θα συνεχίσει να αναπτύσσεται με βιώσιμο και ασφαλή τρόπο.

## Βιβλιογραφία

### 1. Ελληνόγλωση


- Ηλεκτρονικό Εμπόριο και εφαρμογές διαδικτύου, Σ. Βαλσαμίδης- Ι. Καζανίδης, Εκδόσεις Δίσιγμα, 2020
- Ηλεκτρονικό Εμπόριο και Εφαρμογές Διαδικτύου (2η έκδοση), Σ. Βασλαμίδης- Ι. Καζανίδης, Εκδόσεις Δίσιγμα, 2024
- Ηλεκτρονικό Εμπόριο: Επιχειρήσεις, Τεχνολογία, Κοινωνία, 16η έκδοση, Laudon Kenneth, Carol Guercio Traver, Εκδόσεις Παπασωτηρίου, 2022
- Αδάμ Παπαδαμάκης, Τα περιουσιακά εγκλήματα, Β' Έκδοση, Εκδόσεις Σάκκουλα, 2016


### 2. Ξενόγλωσση


- The Palgrave Handbook of international Cybercrime and Cyberdeviance, Thomas J. Holt, Adam M. Bossler, palgrave macmillan, 2020
- Oxford Advanced Learner's Dictionary
- «The Concept of e-Commerce», Dr. Rohit Sublaik, 2022, WKRISHIND PUBLISHERS


### 3. Νομοθεσία


- **Ενωσιακή**
- Χάρτης των Θεμελιωδών Δικαιωμάτων
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ
- Κανονισμός (ΕΕ) αριθ. 524/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013 για την ηλεκτρονική επίλυση καταναλωτικών διαφορών και για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2006/2004 και της οδηγίας 2009/22/ΕΚ (κανονισμός για την ΗΕΚΔ)
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)
- Ο.δηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της

πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»)

- Οδηγία 2011/83/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2011 σχετικά με τα δικαιώματα των καταναλωτών, την τροποποίηση της οδηγίας 93/13/ΕΟΚ του Συμβουλίου και της οδηγίας 1999/44/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της οδηγίας 85/577/ΕΟΚ του Συμβουλίου και της οδηγίας 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου
- Οδηγία (ΕΕ) 2023/2673 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 22ας Νοεμβρίου 2023 για την τροποποίηση της οδηγίας 2011/83/ΕΕ όσον αφορά τις συμβάσεις χρηματοοικονομικών υπηρεσιών που συνάπτονται εξ αποστάσεως και για την κατάργηση της οδηγίας 2002/65/ΕΚ.
- Οδηγία 2013/11/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013, για την εναλλακτική επίλυση καταναλωτικών διαφορών και για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2006/2004 και της οδηγίας 2009/22/ΕΚ (οδηγία ΕΕΚΔ).
- Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2015 σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ, (γνωστή ως η αναθεωρημένη οδηγία για τις υπηρεσίες πληρωμών ή PSD2)
- Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου
- Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου
- Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)

➢ **Εθνική**

- Ποινικός Κώδικας
- Νόμος 2251/1994 (ΦΕΚ 191, τ. Α' ) «Προστασία των Καταναλωτών».
- Νόμος 4537/2018 (ΦΕΚ 84, τ. Α΄) «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2015/2366/ΕΕ για τις υπηρεσίες πληρωμών και άλλες διατάξεις.
- Νόμος 4947/2022 (ΦΕΚ 124, τ. Α΄) «Ενσωμάτωση της Οδηγίας (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των

μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου (L 123) και λοιπές επείγουσες διατάξεις».

- Προεδρικό Διάταγμα 131/2003, (ΦΕΚ 116, τ. Α΄) «Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο)».
- Κοινή Υπουργική Απόφαση 70330οικ./2015 από 30-06-3015 (ΦΕΚ 1421, τ. Β΄) «Ρυθμίσεις σχετικά με την προσαρμογή της ελληνικής νομοθεσίας, σε συμμόρφωση με την Οδηγία 2013/11/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013, για την εναλλακτική επίλυση καταναλωτικών διαφορών και για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2006/2004 και της οδηγίας 2009/22/ΕΚ (οδηγία ΕΕΚΔ) και την λήψη συμπληρωματικών εθνικών μέτρων εφαρμογής του Κανονισμού 524/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Μαΐου 2013 για την ηλεκτρονική επίλυση καταναλωτικών διαφορών».
- Υπουργική Απόφαση 31619οικ./2017 από 14-03-2017 (ΦΕΚ 969, τ. Β΄) «Κώδικας Καταναλωτικής Δεοντολογίας για το Ηλεκτρονικό Εμπόριο».

## 4. Εκθέσεις- Έρευνες

- Κλαδική Έρευνα στο Ηλεκτρονικό Εμπόριο, Τελική Έκθεση, Επιτροπή Ανταγωνισμού, Αθήνα, Νοέμβριος 2022
- «ΕΡΕΥΝΑ ΧΡΗΣΗΣ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΠΟ ΝΟΙΚΟΚΥΡΙΑ ΚΑΙ ΑΤΟΜΑ: Έτος 2023», Ελληνική Στατιστική Εταιρεία, https://www.statistics.gr/documents/20181/7add8452-9379-0e6d-6313-fb619174f96c
- Έκθεση Χρηματοπιστωτικής Σταθερότητας της Ελλάδας που δημοσιεύτηκε τον Οκτώβριο του 2024 https://www.bankofgreece.gr/Publications/FINANCIAL_STABILITY_REVIEW_OCTOBER_2024_EL.pdf

## 5. Δελτία τύπου- Ανακοινώσεις

- Το από 29-10-2024 δελτίο τύπου- ανακοίνωση του Υπουργείου Ψηφιακής Διακυβέρνησης για αποστολή παραπλανητικών μηνυμάτων τύπου phishing μέσω ηλεκτρονικού ταχυδρομείου. https://mindigital.gr/archives/6725
- Το από 15-02-2024 δελτίο τύπου της Ανεξάρτητης Αρχής Δημοσίων Εσόδων για παραπλανητικά μηνύματα SMS υποκλοπής στοιχείων σε βάρος των πολιτών. https://www.aade.gr/sites/default/files/2024-02/dt_15.02.2024.pdf

## 6. Ηλεκτρονικές πηγές

- https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Εζ`-commerce
- https://cyberalert.gr/ti-einai-to-ilektroniko-emporio/

- https://www.aldricharchive.co.uk/inventors-story
- https://www.statista.com/statistics/617136/digital-population-worldwide/
- https://www.researchgate.net/publication/313611404_Information_richness_and_trust_in_V-commerce_implications_for_services_marketing
- https://digital-strategy.ec.europa.eu/el/policies/online-platforms-and-e-commerce


**7. Ιστοσελίδες**


- https://www.europol.europa.eu/
- https://www.enisa.europa.eu/
- https://www.eurojust.europa.eu/
- https://www.ecb.europa.eu/home/html/index.en.html
- https://eurydice.eacea.ec.europa.eu/
- https://www.edps.europa.eu/_en
- https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en
- https://cyberalert.gr/
- https://www.dpa.gr/
- https:/www.synigoroskatanaloti.gr/el
- https://gge.mindev.gov.gr/home/γενικη-διευθυνση-αγορας-και-προστασι/
- http://www.hcmc.gr/el_GR/web/portal/home
- https://mindigital.gr/
- https://www.pcisecuritystandards.org/


**8. Αρθρογραφία**


- «Ηλεκτρονική Τραπεζική απάτη- Κατανομή κινδύνου και βάρος απόδειξης», Άγγελος Π. Μπώλος, Χρονικά Ιδιωτικού Δικαίου, Τόμος ΚΓ΄(2023), τεύχος 2ο


**9. Αρθογραφία στα ηλεκτρονικά Μέσα Μαζικής Ενημέρωσης**


- Lawyermagazine.gr: «E-commerce: Η επόμενη μέρα για το ελληνικό εμπόριο», Ιωάννα Γεωργίου, 30-11-2022 https://lawyermagazine.gr/e-commerce-η-επόμενη-μέρα-για-το-ηλεκτρονικό-εμ/
- liberal.gr: «Οι 7 στους 10 χρήστες του διαδικτύου κάνουν τις αγορές τους online», 12-06-2023 https://www.liberal.gr/oikonomia/oi-7-stoys-10-hristes-toy-diadiktyoy-kanoyn-tis-agores-toys-online
- startupper.gr: «Marketplace: Το μέλλον του ηλεκτρονικού εμπορίου είναι εδώ». 10-12-2022 https://startupper.gr/news/98154/marketplace-to-mellon-tou-ilektronikou-eboriou-einai-edo/
- blog.public.gr: «Τα Public δημιουργούν το 1ο ελληνικό marketplace», Δελτίο τύπου στις 14-05-2018

https://blog.public.gr/ta-public-dimiourgoun-1o-elliniko-marketplace.
- businessnews.gr: «Πώς η Μασούτης μετατρέπει σταδιακά το e-shop της σε marketplace», 01-11-2022 https://www.businessnews.gr/epixeiriseis/item/250370-pos-i-masoytis-thelei-na-metatrepsei-to-e-shop-tis-se-marketplace.
- Startupper.gr : «Skroutz Marketplace: Ένας χρόνος λειτουργίας, 2500 εγγεγραμμένα καταστήματα», 16-11-2020 https://startupper.gr/news/65359/skroutz-marketplace-enas-chronos-leitourgias-2500-engegrammena-katastimata/
- Kathimerini.gr: «Ηλεκτρονικές απάτες: Δέκα θύματα την ημέρα το 2023- Τους «χρέωναν» ακόμη και δάνεια» https://www.kathimerini.gr/society/562973545/ilektronikes-apates-deka-thymata-tin-imera-to-2023-toys-chreonan-akomi-kai-daneia/
- kathimerini.gr, «Θεσσαλονίκη: Εξιχνιάστηκαν ηλεκτρονικές απάτες με λεία 15.000 ευρώ https://www.kathimerini.gr/society/563159812/thessaloniki-exichniastikan-ilektronikes-apates-me-leia-15-000-eyro/
- kathimerini.gr: «Κερκόπορτα τα social media για τις ηλεκτρονικές απάτες», 24-05-2024 https://www.kathimerini.gr/economy/563040541/kerkoporta-ta-social-media-gia-ilektronikes-apates/
- moneyreview.gr: «Βιτρίνες ηλεκτρονικής απάτης- Λουκέτο σε 50 e-shops σε 10 μήνες», Δημήτρης Δελεβέγκος, 16-07-2024 https://www.moneyreview.gr/business-and-finance/150698/vitrines-ilektronikis-apatis-loyketo-se-50-e-shops-se-10-mines/.
- tanea.gr: «Κινέζικο δίκτυο πίσω από μία τεράστια διαδικτυακή απάτη», Γιώργος Κανελλόπουλος, 10-05-2024 https://www.tanea.gr/2024/05/10/economy/kineziko-diktyo-piso-apo-crmia-terastia-diadiktyaki-apati-online/
- kathimerini.gr: «Έκρηξη στις απάτες με κάρτες – Ξεπέρασαν τις 400.000 το 2023», 26-04-2024 https://www.kathimerini.gr/economy/562999567/ekrixi-stis-apates-me-kartes-xeperasan-tis-400-000-to-2023/
- iefimerida.gr, «Έκρηξη στις απάτες με πλαστικό χρήμα- Πως δρουν τα κυκλώματα, τι δείχνουν τα στοιχεία», 25-04-2024. https://www.iefimerida.gr/oikonomia/apates-me-plastiko-hrima-stoiheia-kyklomata
- dealnews.gr: «ΤτΕ: Έκρηξη στις συναλλαγές με πλαστικό χρήμα – Οι ηλεκτρονικές απάτες συνεχίζονται», 24-10-2024 https://www.dealnews.gr/ellada/1117683/tte-ekrixi-stis-synallages-me-plastiko-chrima/
- Liberal.gr: «Phishing: Αύξηση των επιθέσεων το 2024, λόγω εργαλείων Τεχνητής Νοημοσύνης και τακτικών πολλαπλών καναλιών», 10-11-2024. https://www.liberal.gr/tehnologia/phishing-ayxisi-ton-epitheseon-2024-logo-ergaleion-tehnitis-noimosynis-kai-taktikon
- sepe.gr: «Το τοπίο των κυβερνοεπιθέσεων το 2025, οι επιθέσεις με AI θα αυξηθούν», 29-11-2024

https://www.sepe.gr/tehnologia-pliroforiki/kuvernoasfaleia/22507088/to-topio-ton-kuvernoapeilon-to-2025-oi-epitheseis-me-ai-tha-auxithoun/

- theopinion.gr: «Νέα απάτη phishing για πελάτες τράπεζας- Δείτε το μήνυμα ηλεκτρονικής αλληλογραφίας» 29-09-2024 https://www.theopinion.gr/texnologia/nea-apati-phishing-gia-pelates-trapezas-deite-to-minyma-ilektronikis-allilografias/
- ertnews.gr: «Απατεώνες υποδύονται την Εθνική Τράπεζα και επιχειρούν να αδειάσουν λογαριασμούς πολιτών», 25-05-2023. https://www.ertnews.gr/eidiseis/ellada/apateones-ypodyontai-tin-ethniki-trapeza-kai-epixeiroun-na-adeiasoun-logariasmous-politon/
- theopinion.gr: «Voice phishing: Η νέα μορφή απάτης με την βοήθεια της AI που «σαρώνει», 21-10-2024 https://www.theopinion.gr/texnologia/voice-phishing-h-nea-morfi-apatis-me-ti-voitheia-ai-poy-saronei-video/
- Securityreport.gr, «Το 92% των οργανισμών πλήττεται από παραβίαση διαπιστευτηρίων από επιθέσεις social engineering», 20-06-2024 https://securityreport.gr/eidiseis/security-news/to-92-ton-organismon-plittetai-apo-paraviasi-diapisteytirion-apo-epitheseis-social-engineering/
- athenstransport.com: «Δήμος Αθηναίων: Προειδοποίηση για απάτη μέσω facebook με δωρεάν κάρτες μετακίνησης στις συγκοινωνίες», 19-08-2024 https://www.athenstransport.com/2024/08/dimos-athinaion-facebook-apati
- thenewspaper.gr: «»Πώς έστησαν απάτη με το Αστικό Κτελ Βόλου- Τι πρέπει να προσέξετε», 20-11-2024. https://www.thenewspaper.gr/2024/11/20/pos-estisan-apati-me-to-astiko-ktel-volou-ti-prepei-na-prosexete/
- protothema.gr: «Απατεώνας παρίστανε τον πρίγκιπα Παύλο για να πάρει χρήματα από ηλικιωμένους», 26-11-2024. https://www.protothema.gr/greece/article/1567238/apateonas-paristane-ton-prigipa-paulo-gia-na-parei-hrimata-apo-ilikiomenous/
- newsbeast.gr: «Sim Swapping: Η απάτη μέσω κινητού- Πώς αδειάζουν τραπεζικούς λογαριασμούς "ανταλλάσσοντας" κάρτες», 30-10-2021, https://www.newsbeast.gr/technology/arthro/7954393/sim-swapping-i-apati-meso-kinitou-pos-adeiazoun-trapezikous-logariasmous-antallassontas-kartes
- enikos.gr: «Τρεις αναπάντητες κλήσεις και τα χρήματά σας κάνουν φτερά- Πώς λειτουργεί η απάτη Sim Swap Scam», 02-11-2023. https://www.enikos.gr/timeout/treis-anapantites-kliseis-kai-ta-chrimata-sas-kanoun-ftera-pos-leitourgei-i-apati-sim-swap-scam/2054082/
- imerisia.gr: «Έκρηξη στις ηλεκτρονικές επιθέσεις σε τραπεζικές κάρτες πληρωμών - 202.000 απάτες με αξία 12,5 εκατ. ευρώ σε ένα 6μηνο», 09-11-2023 https://www.imerisia.gr/oikonomia/83238_ekrixi-stis-ilektronikes-epitheseis-se-trapezikes-kartes-pliromon-202000-apates-me
- newmoney.gr: «Έξαρση στα περιστατικά απάτης με κάρτες – Έκαναν… φτερά 24 εκατ. ευρώ το 2023 – Ποιες συναλλαγές είναι πιο ευάλωτες», 26-04-2024. https://www.newmoney.gr/roh/palmos-oikonomias/trapezes/exarsi-sta-peristatika-apatis-me-kartes-ekanan-ftera-24-ekat-evro-to-2023-pies-sinallages-ine-pio-epirrepis/

- protothema.gr, «Απάτη με δόλωμα την δήθεν επικαιροποίηση στοιχείων στο Gov.gr.- Δείτε τις απάτες των επιτήδειων», 04-02-2024. https://www.protothema.gr/greece/article/1462812/apati-me-doloma-tin-dithen-epikairopoiisi-stoiheion-sto-govgr-deite-tis-pagides-ton-epitideion/
- capital.gr: «Καμπάνια ενημέρωσης και ευαισθητοποίησης για την ηλεκτρονική απάτη από ΕΕΤ και Mastercard», 12-02-2024 https://www.capital.gr/epikairotita/3770909/kampania-enimerosis-kai-euaisthitopoiisis-gia-tin-ilektroniki-apati-apo-eet-kai-mastercard/
- tanea.gr: «Απάτη: Προσπαθούν να σας εξαπατήσουν με μηνύματα δήθεν από το gov.gr – Τι να προσέξετε» 29-10-2024. https://www.tanea.gr/2024/10/29/greece/apati-prospathoun-na-sas-eksapatisoun-me-minymata-dithen-apo-to-gov-gr-ti-na-proseksete/