Τμήμα Οικονομικών Επιστημών

MSc law & economics
DEPARTMENT of ECONOMICS, UNIVERSITY of MACEDONIA and SCHOOL of LAW, ARISTOTLE UNIVERSITY of THESS.

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
Νομική Σχολή

ΔΙΪΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΚΑ

Διπλωματική Εργασία

ΗΛΕΚΤΡΟΝΙΚΑ-ΟΙΚΟΝΟΜΙΚΑ ΕΓΚΛΗΜΑΤΑ: ΝΟΜΙΚΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

Της

ΣΤΑΥΡΟΥΛΑΣ Ν. ΛΑΒΑΝΤΣΙΩΤΗ
(A.M.: mle22013)

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: ΑΝΑΣΤΑΣΙΑ ΛΙΤΙΝΑ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος Ειδίκευσης Δίκαιο και Οικονομικά
(Κατεύθυνση Δίκαιο και Οικονομικά στον Τομέα των Επιχειρήσεων)

ΦΕΒΡΟΥΑΡΙΟΣ 2023

ΑΦΙΕΡΩΣΗ

Η διπλωματική αυτή εργασία είναι αφιερωμένη στην οικογένειά μου, τη μητέρα μου Γεωργία, τον πατέρα μου Νίκο και την αδελφή μου Ευαγγελία. Πάντοτε με ενθάρρυναν να θέτω στόχους στη ζωή μου και να ακολουθώ τα όνειρά μου. Χωρίς την απεριόριστη αγάπη τους, την υπομονή και τη στήριξή τους τίποτα απ' όλα αυτά δεν θα είχε γίνει πραγματικότητα. Τους αγαπώ και τους ευχαριστώ μέσα από την καρδιά μου για όλες τις αξίες και τα αγαθά που μου έχουν προσφέρει, αλλά και για τους κόπους και τις θυσίες που έχουν κάνει ώστε να ολοκληρώσω τις σπουδές μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτριά μου κα. Αναστασία Λίτινα για την άψογη συνεργασία μας και τις πολύτιμες γνώσεις που μου μεταλαμπάδευσε τόσο κατά τη συγγραφή της διπλωματικής εργασίας όσο και κατά τη διάρκεια της φοίτησής μου στο μεταπτυχιακό. Η βοήθειά της ήταν ανεκτίμητη.

Επιπλέον, θα ήθελα να ευχαριστήσω θερμά και τους διδάσκοντες του διατμηματικού προγράμματος μεταπτυχιακών σπουδών «Δίκαιο και Οικονομικά», νομικούς και οικονομολόγους για την καθοδήγησή τους, αλλά και τις χρήσιμες γνώσεις που μας παρείχαν κατά τη διάρκεια των μαθημάτων στο πρόγραμμα σπουδών.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

α.	άρθρο
Α.Π.	Άρειος Πάγος
ΑΤΜ	Automated Teller Machine
Ε.Ε.	Ευρωπαϊκή Ένωση
Ε.Κ.	Ευρωπαϊκό Κοινοβούλιο
ΕΛΣΤΑΤ	Ελληνική Στατιστική Υπηρεσία
Η/Υ	Ηλεκτρονικός Υπολογιστής
Ν.Π.Δ.Δ.	Νομικό Πρόσωπο Δημοσίου Δικαίου
νΠ.Κ.	Νέος Ποινικός Κώδικας
Ο.Τ.Α.	Οργανισμός Τοπικής Αυτοδιοίκησης
P.C.	Penal Code
Π.Κ.	Ποινικός Κώδικας
P.O.S.	Point Of Sale
ΤΝΠ	Τράπεζα Νομικών Πληροφοριών
URL	Uniform Resource Locators

ΠΕΡΙΛΗΨΗ

Η τεχνολογία και το Διαδίκτυο αποτελούν αναπόσπαστο στοιχείο της καθημερινής ζωής του σύγχρονου ανθρώπου. Καθημερινά όλο και περισσότεροι άνθρωποι χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές, τα έξυπνα κινητά (smartphones) και άλλες ψηφιακές συσκευές με πρόσβαση στο Διαδίκτυο για πληροφόρηση, επικοινωνία, διασκέδαση και συναλλαγές. Αναμφίβολα, έχει επηρεάσει πολλούς παράγοντες της ζωής μας με θετικό τρόπο, καθιστώντας το Διαδίκτυο ένα από τα μεγαλύτερα και πιο χρήσιμα παγκόσμια εργαλεία. Ωστόσο, το Διαδίκτυο, παρουσιάζει κι ένα σημαντικό μειονέκτημα, την έλλειψη ασφάλειας κατά τη χρήση του, που ευνοεί μη εξουσιοδοτημένες ή παράνομες ενέργειες.

Στην παρούσα εργασία αναπτύσσεται η έννοια των ηλεκτρονικών- οικονομικών εγκλημάτων καθώς και το νομικό πλαίσιο που τα περιβάλλει τόσο σε εθνικό όσο και ευρωπαϊκό επίπεδο. Εξετάζονται αναλυτικά τα αδικήματα της απάτης με υπολογιστή 386^{A} ΠΚ και της απάτης μέσω υπολογιστή 386 ΠΚ, καθώς και τα κίνητρα και προφίλ των δραστών που τους ωθούν στην τέλεση ηλεκτρονικών οικονομικών εγκλημάτων. Ακολούθως, παρουσιάζεται η οικονομική προσέγγιση του φαινομένου και του κοινωνικού κόστους αυτού. Εν συνεχεία, για την καλύτερη κατανόηση της εξέλιξης του φαινομένου , αναλύονται στατιστικά στοιχεία σχετικά με τη συχνότητα και τα είδη κυβερνοεπιθέσεων στις ΗΠΑ, την Ευρώπη και την Ελλάδα πριν και μετά την περίοδο της πανδημίας του κορονοϊού. Τέλος, πραγματώνεται σύνοψη και συνολική αποτίμηση των ζητημάτων που αναπτύχθηκαν και εξάγονται συμπεράσματα επ'αυτών.

Λέξεις κλειδιά: Απάτη με υπολογιστή, απάτη μέσω υπολογιστή, α.386 ΠΚ, α.386^{A} ΠΚ, ηλεκτρονικά οικονομικά εγκλήματα, κυβερνοασφάλεια, phishing

ABSTRACT

Technology and the Internet have become an integral part of contemporary human's daily life. Every day, more people use computers, smartphones, and several other digital devices with internet access to satisfy their needs for information, communication, entertainment, and transactions. Undoubtedly, the Internet has affected in a positive way many aspects of human life, making it one of the biggest and most useful global utilities. However, there is an important disadvantage in it, the lack of the needed security during its usage, which leads to many unauthorized or illegal actions.

In this thesis, we are analyzing the concept of cyber economic crimes, as well as, the legal framework applied on them at a national and European level. The crimes of computer fraud 386A P.C. and fraud via computer 386 P.C. are analyzed in detail, so do the motives and the criminal profile of the perpetrators that lead them to commit this type of crimes. Next, there is presented an economic approach of this type of criminality and its social cost. Then, for a better comprehension of the development of the phenomenon, there are analyzed statistics regarding to the frequency and types of cyber economics crimes in the USA, Europe, and Greece for the period before and after the Covid-19 pandemic. Finally, we end up with a summary and overall assessment of the issues mentioned at this thesis and their conclusions.

Keywords: Computer fraud, fraud via computer, a.386 P.C., a.386A P.C., cyber economic crimes, cyber security, phishing

ΕΙΣΑΓΩΓΗ

Η σύγχρονη τεχνολογία με την εξέλιξη των ηλεκτρονικών υπολογιστών και του Διαδικτύου έχουν δημιουργήσει μία νέα καθημερινότητα, παρέχοντας μια πληθώρα δυνατοτήτων στους χρήστες τους και διευκολύνοντας δραστικά τη ζωή τους. Εκτός από ένα γιγάντιο αποθετήριο πληροφοριών, το Διαδίκτυο αποτελεί και μέσο επικοινωνίας, ψυχαγωγίας αλλά και εξ αποστάσεως αγορών και οικονομικών συναλλαγών με τη χρήση πλαστικού χρήματος. Η ευκολία στη χρήση του αλλά και η ταχύτητα στη διεκπεραίωση των υποχρεώσεων που αυτό προσφέρει, το καθιστούν πόλο έλξης για όλο και περισσότερους χρήστες όλων των ηλικιών. Μέρα με τη μέρα όλο και περισσότεροι τομείς δραστηριοποίησης του ανθρώπου εκσυγχρονίζονται και εισέρχονται στον κόσμο της ψηφιοποίησης. Παρά την απλοποίηση ορισμένων εργασιών και την ταχεία οργάνωση και διαχείριση τεράστιου όγκου δεδομένων και πληροφοριών, η εκτεταμένη χρήση του Διαδικτύου και των ηλεκτρονικών συστημάτων από εκατομμύρια χρήστες, εκτός από τις ωφέλειες που παρέχει, δημιουργεί ευνοϊκές συνθήκες για την εμφάνιση νέων μορφών εγκλημάτων. Το ηλεκτρονικό έγκλημα αποτελεί φαινόμενο που εξελίσσεται με ραγδαίους ρυθμούς και ακολουθεί την ανάπτυξη της τεχνολογίας σε κάθε της βήμα. Λόγω της μαζικής και ταυτόχρονης ανταλλαγής τεράστιου όγκου πληροφοριών και δεδομένων μεταξύ εκατομμυρίων χρηστών του Διαδικτύου, παρατηρούνται φαινόμενα παράκαμψης της ασφάλειας με αποτέλεσμα να εμφανίζονται περιστατικά εξαπάτησης των χρηστών και υποκλοπής στοιχείων ταυτότητας. Τα περιστατικά αυτά αυξάνονται ολοένα και περισσότερο, με την πληθώρα αυτών να καταλήγουν σε περιουσιακή βλάβη των θυμάτων

ή τρίτων. Χαρακτηριστικά παραδείγματα αποτελούν η απάτη με υπολογιστή και η απάτη μέσω υπολογιστή, στις οποίες συγκαταλέγονται τα φαινόμενα Phishing, Pharming, η χρήση μαγνητικής κάρτας ανάληψης χρημάτων από ΑΤΜ χωρίς άδεια, η χρήση κωδικών πρόσβασης σε υπηρεσία ebanking χωρίς άδεια κ.ά.

Στόχος της παρούσας μελέτης είναι να παρουσιαστούν οι εκφάνσεις του ηλεκτρονικού-οικονομικού εγκλήματος, ποιες συμπεριφορές ποινικοποιούνται τόσο κατά την ευρωπαϊκή όσο και την ελληνική νομοθεσία και τι ποινές προβλέπονται για εκάστη των περιπτώσεων. Πιο συγκεκριμένα θα αναλυθούν τα αδικήματα της απάτης με υπολογιστή και της απάτης μέσω υπολογιστή όπως αυτά προβλέπονται στο νέο Ποινικό Κώδικα με ιδιαίτερη μνεία στα περιστατικά phishing, pharming και χρήση μαγνητικής κάρτας ανάληψης χρημάτων από ΑΤΜ χωρίς άδεια. Παράλληλα θα αναπτυχθεί το περιεχόμενο ευρωπαϊκών κειμένων σχετικών με την κυβερνοασφάλεια και ειδικότερα η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Σύμβαση της Βουδαπέστης 23/11/2001), οι ευρωπαϊκές οδηγίες 2013/40/ΕΕ και 2019/713/ΕΕ καθώς και ο ελληνικός νόμος 4411/2016. Αυτά τα κείμενα νομοθετικού περιεχομένου πλαισιώνουν το νομικό κορμό της παρούσας μελέτης.

Ο οικονομικός κορμός της μελέτης πλαισιώνεται από την οικονομική ανάλυση του εγκλήματος. Πιο συγκεκριμένα θα αναπτυχθούν τα κίνητρα που ωθούν τους υποψήφιους δράστες στην επιλογή τέλεσης των ηλεκτρονικών οικονομικών εγκλημάτων και ποιο είναι κοινωνικό κόστος που αυτά επιφέρουν. Για την καλύτερη κατανόηση της εξέλιξης των ηλεκτρονικών οικονομικών εγκλημάτων θα αναλυθούν στατιστικά στοιχεία προερχόμενα από τις ΗΠΑ, την Ευρώπη και την Ελλάδα σχετικά με τα ποσοστά εμφάνισης του φαινομένου, τις μορφές που λαμβάνει, τα ηλικιακά γκρουπ των θυμάτων στα οποία στοχεύει καθώς και τον οικονομικό αντίκτυπο που επιφέρει στα θύματα. Η ανάλυση θα αφορά σε δύο χρονικές περιόδους, την προ και μετά Covid-19 χρονική περίοδο, δεδομένου ότι οι νέες συνθήκες που δημιουργήθηκαν εξαιτίας των πολύμηνων lockdowns κατά τη διάρκεια της πανδημίας του Covid-19 κατέστησαν απαραίτητη τη χρήση του Διαδικτύου και των ηλεκτρονικών υπολογιστών από άτομα όλων των ηλικιών. Κατ' αυτόν τον τρόπο θα εξαχθούν συμπεράσματα σχετικά με το κατά πόσο η αύξηση στη χρήση του Διαδικτύου επηρεάζει και με κατά ποιον τρόπο την εμφάνιση ηλεκτρονικών οικονομικών εγκλημάτων.

ΚΕΦΑΛΑΙΟ Α'
1. ΗΛΕΚΤΡΟΝΙΚΟ-ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

1.1 Ορισμός και βασικά χαρακτηριστικά

Τι θεωρείται οικονομικό έγκλημα; Το οικονομικό έγκλημα αποτελεί μια πολυδιάστατη έννοια, καθώς περιλαμβάνει μια πληθώρα παράνομων πράξεων. Η διατύπωση ενός μοναδικού ορισμού για τα οικονομικά εγκλήματα αποτέλεσε μια εξαιρετικά δύσκολη διεργασία. Η πρώτη απόπειρα έγινε από το Γρηγόρη Λάζο, όπου σύμφωνα με την προσέγγιση του, ως οικονομικό έγκλημα θεωρείται μια κατηγορία πράξεων, οι οποίες λαμβάνουν χώρα στο πλαίσιο της αγοράς, θίγουν έννομα αγαθά που έχουν σχέση με το οικονομικό σύστημα και αποτελούν παραβιάσεις νόμων που ρυθμίζουν τις εσωτερικές λειτουργίες της αγοράς και τις σχέσεις γενικότερα με την ευρύτερη κοινωνία.

Κατά τον Μανωλεδάκη, ως οικονομικό έγκλημα ορίζεται « η τυποποιημένη από το νόμο αξιόποινη πράξη που τελείται με εκμετάλλευση των δυνατοτήτων του οικονομικού συστήματος και αποσκοπεί στην επαύξηση της περιουσίας του δράστη.»[1]

Τα εγκλήματα αυτά δεν είναι πρωτόγνωρα στην κοινωνία. Έκαναν την εμφάνισή τους αρκετά πριν την ανάπτυξη του διαδικτύου και των νέων τεχνολογιών. Η πρώτη αναφορά στα οικονομικά εγκλήματα εν γένει έγινε από τον Edwin Sutherland, κατά τον οποίο επρόκειτο για μια κατηγορία εγκλημάτων που γίνεται στα πλαίσια της επαγγελματικής δραστηριότητας και από έναν δράστη με υψηλό κοινωνικό προφίλ.[2] Κατά την προσέγγισή του , τα οικονομικά εγκλήματα αποτελούν ειδικό τομέα ενδιαφέροντος και φέρουν τα εξής χαρακτηριστικά:

α)Προκαλούν ζημιά σε έναν μεγάλο, και ορισμένες φορές απροσδιόριστο, αριθμό ατόμων
β)Βλάπτουν την εθνική οικονομία
γ)Προκαλούν απώλεια εμπιστοσύνης στο οικονομικό σύστημα του κράτους.

Επιπλέον, υποστήριξε πως το οικονομικό έγκλημα βρίσκεται σε άμεση συσχέτιση με τις δραστηριότητες του οργανωμένου εγκλήματος.

[1] Στέργιος Αλεξιάδης, Τα οικονομικά του εγκλήματος, Σάκκουλας, 2010, σελ.78
[2] Λάζος Γρηγόρης (2013), σελ.34

Στην κατηγορία των οικονομικών εγκλημάτων, ωστόσο, δεν εντάσσεται κάθε πράξη που αποβλέπει σε οικονομικό όφελος. Το οικονομικό έγκλημα προκύπτει από τη χρήση των μηχανισμών που ανήκουν στο οικονομικό σύστημα, η οποία γίνεται προς όφελος του δράστη, συμπαρασύροντας παράλληλα με την ομαλή λειτουργία του οικονομικού συστήματος και άλλες πτυχές του, όπως το ασφαλιστικό και το χρηματοπιστωτικό σύστημα, προκαλώντας σημαντικές ζημίες οικονομικής και όχι μόνο φύσεως. Κατά συνέπεια, οι βλαπτόμενοι από το οικονομικό έγκλημα δεν είναι μόνο φυσικά πρόσωπα, αλλά αντιθέτως προσβάλλονται κι άλλοι φορείς κι έννομα αγαθά.

Τα τελευταία χρόνια, η ανάπτυξη της τεχνολογίας και των ηλεκτρονικών υπολογιστών, ειδικά από την δεκαετία του 1980 κι έπειτα, έχει ευνοήσει την εμφάνιση νέων μορφών οικονομικής εγκληματικότητας. Τα ηλεκτρονικά- οικονομικά εγκλήματα, όπως αυτά ονομάζονται, πραγματοποιούνται με τη χρήση ηλεκτρονικών υπολογιστών, Smartphones ή/και άλλων σύγχρονων τεχνολογικών μέσων με σύνδεση στο Διαδίκτυο κι έχουν ως αποτέλεσμα την προσβολή έννομων αγαθών οικονομικής φύσης. Χαρακτηριστικά παραδείγματα ηλεκτρονικών οικονομικών εγκλημάτων αποτελούν οι διαδικτυακές απάτες και κλοπές, οι τραπεζικές απάτες, το ηλεκτρονικό ψάρεμα (Phising) κτλ.

1.2. Νομική προσέγγιση

Η εμφάνιση αυτών των νέων μορφών εγκληματικότητας και η ραγδαία εξάπλωσή τους, έχουν προκαλέσει διχογνωμία στη νομική κοινότητα. Αρκετοί υποστηρίζουν πως το ηλεκτρονικό έγκλημα δεν αποτελεί τίποτα άλλο παρά μια νέα έκφανση του παραδοσιακού εγκλήματος, προσαρμοσμένη στην τεχνολογική εποχή. Μία άλλη μερίδα νομικών υποστηρίζει πως αποτελεί μια διακριτή νεοφανή κατηγορία εγκλημάτων, στην οποία θα υπάγονται αμιγώς τεχνολογικής φύσεως εγκλήματα. Βέβαια, σε αυτή την περίπτωση θα απαιτείται και η θέσπιση ανάλογου νομοθετικού πλαισίου. Κατά την ορθότερη ερμηνεία, ωστόσο, στην κατηγορία των ηλεκτρονικών εγκλημάτων θα πρέπει να υπάγονται τόσο οι νέες εκφάνσεις των παραδοσιακών εγκλημάτων, όσο και τα αμιγώς νέα ψηφιακά εγκλήματα.

1.3. Επιδιωκόμενο αποτέλεσμα και προφίλ δραστών

Ένα κρίσιμο ερώτημα που συχνά τίθεται από την κοινωνία είναι *για ποιον λόγο επιλέγουν την εγκληματικότητα και γιατί το συγκεκριμένο έγκλημα;* Διαχρονικά, έχουν διατυπωθεί ποικίλες θεωρίες, βάσει των οποίων οι άνθρωποι αποφασίζουν να διαπράξουν κάποιο έγκλημα και να ακολουθήσουν παραβατική συμπεριφορά. Η ύπαρξη πληθώρας θεωριών έγκειται στο γεγονός ότι, η ανθρώπινη συμπεριφορά είναι απρόβλεπτη και δεν μπορούν να προσδιοριστούν εκ των προτέρων όλες οι πιθανές αντιδράσεις του ατόμου σε κάθε περιστατικό ή κατάσταση.

Οι σημαντικότερες θεωρίες που έχουν διατυπωθεί για την εγκληματική συμπεριφορά είναι οι εξής:

1)**Κλασσική εγκληματολογία**: Βάση της αποτελεί η αρχή του ωφελιμισμού, κατά την οποία οι άνθρωποι είναι ορθολογικά σκεπτόμενα όντα κι ενεργούν με τέτοιον τρόπο, ώστε να αποφύγουν τον πόνο και τον κόπο και να πετύχουν τη μέγιστη ικανοποίηση για τον εαυτό τους. Υπό αυτό το σκεπτικό, τα άτομα βρίσκονται σε θέση να επιλέξουν αν θα ακολουθήσουν μια εγκληματική συμπεριφορά μόνο όταν τα προσδοκώμενα οφέλη είναι μεγαλύτερα από τις προσδοκώμενες απώλειες.
Ο ωφελιμισμός παραμένει η πιο δημοφιλής ερμηνεία της εγκληματικής συμπεριφοράς, υπό την προϋπόθεση ότι το άτομο που θα διαπράξει το έγκλημα έχει «ζυγίσει» προηγουμένως τα οφέλη και τις απώλειες απ' αυτήν την ενέργεια και η «η ζυγαριά» κλίνει προς τα οφέλη.

2) **Θεωρία Δραστηριοτήτων Ρουτίνας**: Η θεωρία αυτή υποστηρίζει ότι κινητήρια δύναμη του εγκλήματος είναι η απληστία και η ηδονή του ανθρώπου, καθώς και η έμφυτη επιθυμία να ικανοποιήσει το «εγώ» του. Αποτελεί μια εναλλακτική προσέγγιση των αιτιών που οδηγούν ένα άτομο στην παράβαση του νόμου.

3) Τέλος, η **Θεωρία της Ανομίας** φαίνεται πως κερδίζει έδαφος ως η επικρατέστερη των θεωριών της εγκληματικότητας. Υποστηρίζει, πως τα άτομα επειδή αισθάνονται θυμό και απογοήτευση που αδυνατούν να πετύχουν τους οικονομικούς και κοινωνικούς στόχους που έχουν θέσει, οδηγούνται στην εγκληματικότητα. Κατά τον κοινωνιολόγο Robert Merton, η αιτία που οδηγεί σε εγκληματική συμπεριφορά είναι οι διαφοροποιήσεις και αποκλίσεις

μεταξύ των επιθυμιών των ανθρώπων, όπως αυτές επιβάλλονται από την κοινωνία, και των πραγματικών επιτευγμάτων των ανθρώπων.[3]

Ο βασικός στόχος των δραστών, για την τέλεση ηλεκτρονικών οικονομικών εγκλημάτων, είναι να αποσπάσουν από τα θύματά τους μεγάλα χρηματικά ποσά, γεγονός που διευκολύνεται πλέον από την εξέλιξη των τεχνολογικών μέσων συνδυαστικά με την ψηφιοποίηση του χρήματος. Ο λόγος για τον οποίο οι δράστες προτιμούν τη διάπραξη των συγκεκριμένων εγκλημάτων, έγκειται στο γεγονός πως το Διαδίκτυο είναι προσβάσιμο σε οποιονδήποτε δυνητικά δράστη και ο αναγκαίος εξοπλισμός αρκετά οικονομικός και διαθέσιμος στην αγορά. Το ηλεκτρονικό έγκλημα είναι ταχύτατο, καθώς λαμβάνει χώρα σε πραγματικό χρόνο, με αποτέλεσμα τα θύματα πολλές φορές να μην το αντιλαμβάνονται άμεσα. Επιπλέον, η εξιχνίαση του ηλεκτρονικού-οικονομικού εγκλήματος μπορεί να καταστεί χρονοβόρα όταν τα ίχνη που αφήνονται δεν επαρκούν για τον εντοπισμό του δράστη ή όταν υπάρχει το διασυνοριακό στοιχείο όπου απαιτείται συνεργασία και συντονισμός περισσότερων κρατών για τη διαλεύκανση του εγκλήματος. Παράλληλα, η αύξηση αυτού του είδους εγκλημάτων ευνοείται ιδιαίτερα από την ανωνυμία που προσφέρει το Διαδίκτυο και ως εκ τούτου τη δυσκολία στην ταυτοποίηση και τον εντοπισμό του δράστη.

Η εξέλιξη της τεχνολογίας και οι δυνατότητες που παρέχει, δίνουν την ευκαιρία στο δράστη να διαπράξει με ανωνυμία το έγκλημά του και να καλύψει με ιδιαίτερη ευκολία τα ίχνη του. Δράστης δεν μπορεί να είναι ο οποιοσδήποτε αλλά (θα πρέπει να είναι) ένα άτομο που να διαθέτει τις απαιτούμενες ειδικές γνώσεις σχετικά με τη λειτουργία και χρήση των πληροφοριακών συστημάτων. Ανάλογα με το μέγεθος των γνώσεων και των ικανοτήτων που διαθέτουν, οι ηλεκτρονικοί εγκληματίες διακρίνονται στις εξής κατηγορίες:[4]

α) Ερασιτέχνες, οι οποίοι διαθέτουν πολύ βασικές γνώσεις στη χρήση και λειτουργία των Η/Υ και κάνουν επιθέσεις σε άλλα ηλεκτρονικά συστήματα ως μια μορφή «χόμπι».

[3] Σπυρίδων Ρεπούσης, Χρηματοοικονομική απάτη και διαφθορά, Σάκκουλας, 2010, σελ.3
[4]Anderson R, Security Engineering: A guide to building dependable distributed systems, John Wiley & Son Inc.,New York. σελ.175

β)Οι hackers, οι οποίοι διαθέτουν εξειδικευμένες γνώσεις και τεχνικές στη χρήση Η/Υ και οι επιθέσεις σε άλλα ηλεκτρονικά συστήματα γίνονται προκειμένου να επιδιώξουν προσωπικές φιλοδοξίες.

γ) Οι crackers, οι οποίοι προβαίνουν σε επιθέσεις προκειμένου να αποκομίσουν περιουσιακό όφελος

δ)Και τέλος, οι επαγγελματίες, οι οποίοι κάνουν αυτές τις επιθέσεις ως επάγγελμα για το βιοπορισμό τους.

Παλαιότερα, οι hackers, χαρακτηρίζονταν ως άτομα που θεωρούσαν τον εαυτό τους πνευματικά ανώτερο από τους άλλους ανθρώπους. Εκλαμβάνονταν ως «πνευματικά» προικισμένοι , ιδιαίτερα ευφυείς και ως άτομα ικανά να επιλύσουν ιδιαίτερης σοβαρότητας και δυσκολίας προβλήματα. Πλέον, όμως, η επιλογή ενός ατόμου να συγκαταλεγεί στην ομάδα των hackers δεν του προσδίδει απαραίτητα και τα χαρακτηριστικά που προαναφέραμε. Οι δράστες των επιθέσεων μπορεί να προέρχονται από διάφορα κοινωνικά στρώματα , αρκεί να διαθέτουν τις γνώσεις που προαναφέραμε και πρόσβαση σε Η/Υ ή κάποιο smartphone. Άτομα με επιμονή και υπομονή, που επιθυμούν να εκμεταλλευτούν «δημιουργικά» τον ελεύθερό τους χρόνο, αποκτούν πληθώρα γνώσεων στην προσβολή και παράκαμψη πληροφοριακών συστημάτων και με ιδιαίτερη τεχνική κάνουν επιθέσεις σε πληροφοριακά συστήματα και ηλεκτρονικούς υπολογιστές, με αποτέλεσμα την πρόκληση περιουσιακής βλάβης στα θύματα της επίθεσης ή σε τρίτους.[5]Λόγω της ευρύτατης ανάπτυξης και διάδοσης του Διαδικτύου κατά την τελευταία κυρίως δεκαπενταετία, αλλά και της εξοικείωσης που αποκτούν από μικρή ηλικία πλέον με τους Η/Υ, το ηλικιακό προφίλ των δραστών είναι σχετικά νέο, με δράστες ακόμα και 12-24 ετών.

1.4. Κίνητρα των δραστών

Ως κίνητρα, νοούνται οι λόγοι που ωθούν το άτομο στη λήψη ορισμένης απόφασης , ώστε να προχωρήσει σε συγκεκριμένη βουλητική δραστηριότητα. Τα κίνητρα, συνεπώς,

5 Φ.Σπυρόπουλος, Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking), Σάκκουλα Ε.Ε.,2016

αποτελούν καθοριστικούς παράγοντες διαμόρφωσης της ανθρώπινης συμπεριφοράς. Διαμορφώνουν σε μεγάλο βαθμό τις κοινωνικές σχέσεις και την κοινωνική ζωή του ατόμου και ανάλογα με το είδος των κινήτρων που επικρατεί, το άτομο επιδεικνύει κοινωνική ή αντικοινωνική συμπεριφορά αναλόγως.[6]

Ο λόγος που παρακινεί τους δράστες να προκαλέσουν περιουσιακή βλάβη στα θύματα που επιτίθενται είναι διαφορετικός για τον καθένα. Μια ομάδα hackers με το σύνδρομο "Robin Hood" επιτίθεται για ιδεολογικούς λόγους σε μεγάλες επιχειρήσεις, υπουργεία ή και σε άτομα με ιδιαίτερη οικονομική επιφάνεια, ώστε μέσα από την πρόκληση περιουσιακής βλάβης σε αυτές τις οντότητες να καταπολεμήσουν την κοινωνική ανισότητα και να επιτύχουν δίκαιη αναδιανομή του πλούτου μεταξύ των διαφόρων κοινωνικών στρωμάτων.

Από την άλλη πλευρά βρίσκεται και η ομάδα των crackers που δεν υπηρετεί τόσο ανιδιοτελείς σκοπούς. Αυτοί προβαίνουν σε επιθέσεις προκειμένου να αποκομίσουν περιουσιακό όφελος για τον εαυτό τους. Κατ' αυτόν τον τρόπο, αξιοποιούν το ταλέντο τους στην παραβίαση πληροφοριακών συστημάτων, ώστε να πλουτίσουν παρανόμως από την περιουσιακή βλάβη των θυμάτων τους, όπου οι τελευταίοι μπορεί να ανήκουν σε οποιοδήποτε κοινωνικό στρώμα.[7] Φαίνεται, λοιπόν, πως εφαρμόζεται εδώ η κλασσική εγκληματολογική θεωρία που αναλύθηκε ανωτέρω, καθώς τα άτομα προσπαθούν να επιτύχουν το στόχο τους (που είναι η απόκτηση χρημάτων) χωρίς κόπο. Άλλωστε, σύμφωνα με μελέτη που εκπονήθηκε από το γερμανικό πανεπιστήμιο Martin Luther University Halle-Wittenberg (MLU), διαπιστώθηκε πως το βασικό κίνητρο που οδηγεί το άτομο στο ηλεκτρονικό-οικονομικό έγκλημα είναι οικονομικό.

Η άνθιση της ψηφιοποίησης και του αυτοματισμού των οικονομικών και μη συστημάτων έχουν ευνοήσει την αύξηση των εγκλημάτων που σχετίζονται με αυτά. Η κατηγορία των ηλεκτρονικών οικονομικών εγκλημάτων περιλαμβάνει μια πληθώρα επιμέρους εγκλημάτων, η οποία ολοένα και διευρύνεται, ωστόσο εμφανίζονται συνηθέστερα τα εξής : απάτη με Η/Υ, hacking τραπεζικού λογαριασμού, χρήση χωρίς άδεια χρεωστικής/ πιστωτικής κάρτας σε ATM ή POS κτλ.

[6] Στέργιος Αλεξιάδης, Τα οικονομικά του εγκλήματος, Σάκκουλας,2010, σελ.416
[7] Σπυρίδων Ρεπούσης, Χρηματοοικονομική απάτη και διαφθορά, Σάκκουλας, 2010, σελ.101.

ΚΕΦΑΛΑΙΟ Β’

2)ΑΝΑΛΥΣΗ ΕΠΙΜΕΡΟΥΣ ΗΛΕΚΤΡΟΝΙΚΩΝ-ΟΙΚΟΝΟΜΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

2.1. Απάτη με υπολογιστή 386Α ΠΚ

Άρθρο 386^{Α} ΠΚ

1. Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή:

α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή,

β) με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα,

γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας,

δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας, ή

ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή.

Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.

2. Όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή πληροφοριακό σύστημα που προορίζεται για τη διάπραξη του εγκλήματος της παρ. 1 τιμωρείται με φυλάκιση έως δύο (2) έτη και χρηματική ποινή. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του

θέληση το παραπάνω πρόγραμμα ή πληροφοριακό σύστημα πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παρ. 1.

3. Αν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου του Ελληνικού Δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι (20) έτη.

Το έγκλημα της απάτης με υπολογιστή 386Α ΠΚ, όπως και το έγκλημα της κοινής απάτης(απάτη μέσω υπολογιστή 386 ΠΚ), αποτελούν εγκλήματα κατά της περιουσίας στο σύνολό της. Τι χαρακτηρίζεται όμως ως περιουσία; Έχουν υποστηριχθεί ποικίλες θεωρίες σχετικά με τη φύση και τον ορισμό της περιουσίας. Κατά την οικονομική θεωρία, ως περιουσία θεωρείται *το σύνολο των οικονομικών αγαθών του προσώπου που έχουν χρηματική αξία (ΑΠ 404/2019 ΠΟΙΝ. ΤΝΠ ΝΟΜΟΣ).* Στον αντίποδα, η νομική θεωρία υποστηρίζει πως *η περιουσία αποτελεί ένα σύνολο περιουσιακών δικαιωμάτων και υποχρεώσεων ενός προσώπου ανεξάρτητα από την οικονομική τους αξία.* Μεταξύ των δύο αυτών θεωριών μεσολαβεί και μία τρίτη θεωρία, η νομικο-οικονομική, κατά την οποία η έννοια της περιουσίας *περιλαμβάνει μόνο τα αγαθά που δεν είναι αποδοκιμαστέα από την έννομη τάξη.* Στην έννοια αυτή συμπεριλαμβάνονται τόσο το λογιστικό όσο και το ηλεκτρονικό χρήμα αλλά και τυχόν δικαιώματα που απορρέουν από την επεξεργασία δεδομένων του υπολογιστή. Αυτή αποτελεί και την κρατούσα στην νομολογία θεωρία.

<u>Αντικειμενική υπόσταση του εγκλήματος</u>

Η απάτη με υπολογιστή 386Α ΠΚ. είναι κοινό έγκλημα, διότι δύναται να τελεστεί από οποιονδήποτε δράστη (“όποιος”). Αποτελεί πολύτροπο, υπαλλακτικώς μεικτό έγκλημα, καθώς μπορεί να λάβει χώρα με περισσότερους τρόπους. Στη διάταξη του νόμου αναφέρονται περιοριστικά πέντε (5) τρόποι τέλεσης του εγκλήματος, οι οποίοι οδηγούν σε τροποποίηση του αποτελέσματος που προκύπτει κατά την επεξεργασία των στοιχείων του υπολογιστή. Πιο συγκεκριμένα μπορεί να τελεστεί με τους εξής τρόπους:

1. **Μη ορθή διαμόρφωση προγράμματος υπολογιστή**

Η μη ορθή διαμόρφωση προγράμματος υπολογιστή συνιστά την πρώτη μορφή με την οποία λαμβάνει χώρα η απάτη με υπολογιστή. Η μη ορθή χρήση του προγράμματος υπολογιστή υφίσταται όταν αυτό χρησιμοποιείται ως το μέσο για την επέλευση μη νόμιμης περιουσιακής βλάβης, η οποία δεν εντάσσεται στα κοινωνικώς αποδεκτά όρια λειτουργίας και σκοπιμότητας του εν λόγω προγράμματος. Σε κάθε περίπτωση, η ορθή ή μη χρήση του προγράμματος εξαρτάται από τη βούληση του χρήστη του ηλεκτρονικού υπολογιστή αλλά και από το νομοθετικό πλαίσιο, που τυχόν διέπει τον τρόπο και τα όρια λειτουργίας του εκάστοτε προγράμματος. Στο σημείο αυτό , όμως, είναι κρίσιμο να αποσαφηνιστεί η έννοια του ”προγράμματος”. Ως πρόγραμμα, λοιπόν, νοείται το σύνολο των δεδομένων με τα οποία δίδονται εντολές στον υπολογιστή για την διενέργεια κάποιας εργασίας. Το αδίκημα τελείται με την αλλοίωση του προγράμματος , η οποία συντελείται με την παράνομη αφαίρεση ή προσθήκη εντολών σε αυτό που κατατείνουν σε περιουσιακή βλάβη. Χαρακτηριστικό παράδειγμα της εν λόγω μορφής απάτης με υπολογιστή αποτελεί η προσθήκη εντολών στο πρόγραμμα με τις οποίες δεσμεύεται μεγαλύτερο χρηματικό ποσό από αυτό που νομίμως είχε προβλεφθεί στο ορθό πρόγραμμα πχ θεωρείται ως μη ορθό το πρόγραμμα Τράπεζας το οποίο παρακρατεί 3 ευρώ παραπάνω στον κάθε πελάτη απ’ ότι θα συνέβαινε με το ορθό πρόγραμμα κατά την παροχή υπηρεσιών.[8]

2. **Χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή**

Αυτός ο τρόπος τέλεσης του αδικήματος απαιτεί την παρουσία συστήματος ηλεκτρονικού υπολογιστή. Το αδίκημα τελείται κατά τη χρήση του υπολογιστή, όταν ο δράστης προβαίνει σε παράβαση χωρίς δικαίωμα ή συγκατάθεση του πληροφοριακού συστήματος. Χαρακτηριστικό παράδειγμα αποτελεί το “hacking” του συστήματος υπολογιστή. Η έννοια του συστήματος υπολογιστή, ωστόσο, δεν είναι γενική και αόριστη. Σύμφωνα με το άρθρο 2 παρ. Α της Οδηγίας 2013/40/ΕΕ, το “σύστημα υπολογιστή” ταυτίζεται με το “πληροφοριακό σύστημα” και ορίζεται ως *“συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται αποτελούν αντικείμενο επεξεργασίας , ανακτώνται ή διαβιβάζονται από*

[8]Α. Χαραλαμπάκης, Ποινικός Κώδικας, Ερμηνεία Κατ’ άρθρο, Τόμος Δεύτερος, 2020

την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών."

3. **Χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας**

Ο εν λόγω τρόπος τέλεσης του αδικήματος εμφανίζει πολλά κοινά στοιχεία με την κοινή απάτη του α.386 ΠΚ. Πιο συγκεκριμένα, ως μη ορθά δεδομένα χαρακτηρίζονται αυτά που δεν ανταποκρίνονται στην πραγματικότητα και είναι ψευδή, ενώ ελλιπή είναι αυτά από τα οποία γίνεται σκόπιμη παρασιώπηση κάποιου στοιχείου τους. Σε αναλογία με την κοινή απάτη μέσω υπολογιστή, η χρησιμοποίηση μη ορθών δεδομένων φαίνεται πως αντιστοιχεί στην απόκρυψη ή παρασιώπηση γεγονότων, ενώ η χρησιμοποίηση ελλιπών δεδομένων στην παρασιώπηση αληθινών γεγονότων. Και στις δύο περιπτώσεις τα γεγονότα αφορούν σε περιστατικά του εξωτερικού κόσμου, που ανάγονται στο παρελθόν ή το παρόν και μπορούν να αποδειχθούν. [9]

Με το νέο Ποινικό Κώδικα προστέθηκε κι ένα νέο στοιχείο στη διάταξη, το οποίο χρήζει ανάλυσης. Πιο συγκεκριμένα, ως "δεδομένα ταυτότητας", νοείται κάθε πληροφορία σχετική με φυσικό πρόσωπο που έχει ή μπορεί να ταυτοποιηθεί. Για να τυποποιηθεί το έγκλημα της απάτης με υπολογιστή στην προκειμένη περίπτωση, θα πρέπει να μεσολαβήσει παρέμβαση κάποιου τρίτου φυσικού προσώπου, όπου και αυτό θα παραλάβει απλώς τα δεδομένα της ταυτότητας και θα προβεί εν συνεχεία σε παράνομη περιουσιακή διάθεση. Ένα από τα πιο χαρακτηριστικά παραδείγματα αυτού του τρόπου τέλεσης αποτελεί η καταχώρηση ψευδούς εισοδήματος προκειμένου το φυσικό πρόσωπο να λάβει οικονομική ενίσχυση ή να επωφεληθεί επιεικέστερης φορολογικής μεταχείρισης.

4. **Χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας**

[9] Α. Χαραλαμπάκης, Ποινικός Κώδικας, Ερμηνεία Κατ' άρθρο, Τόμος Δεύτερος, 2020

Η απάτη με υπολογιστή τελείται σε αυτή την περίπτωση με αλλοίωση ή εξάλειψη δεδομένων μέσω μόλυνσης από κάποιο κακόβουλο λογισμικό, το οποίο με απόκρυψη ή παρασιώπηση γεγονότων, οδηγεί σε άμεση απόκτηση παράνομης περιουσιακής ωφέλειας . Ως κακόβουλο λογισμικό θεωρούνται οι "ιοί", οι "δούρειοι ίπποι", τα "σκουλήκια" κτλ. , τα οποία προσβάλλουν τον ηλεκτρονικό υπολογιστή, με σκοπό την προσθήκη, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων αυτού.[10] Οι ενέργειες αυτές πραγματοποιούνται από το δράστη αθέμιτα ή χωρίς την εξουσιοδότηση του νόμιμου κατόχου του υπολογιστή. Και σε αυτόν τον τρόπο τέλεσης τα δεδομένα αναγνώρισης ταυτότητας αναφέρονται σε κάθε πληροφορία η οποία μπορεί να οδηγήσει σε ταυτοποίηση φυσικού προσώπου. Κρίσιμη κρίθηκε η απόφαση 1716/2019 του Αρείου Πάγου βάσει της οποίας έγινε δεκτό ότι τελείται το έγκλημα της απάτης με υπολογιστή όταν η εισαγωγή κάρτας ανάληψης και καταχώρηση του PINγίνεται χωρίς εξουσιοδότηση του νόμιμου κατόχου της και αφού έχει προηγηθεί παράνομη αφαίρεση της κάρτας από την κατοχή του θύματος. Το παραπάνω αδίκημα τελείται και όταν γίνεται παράνομη χρήση των κωδικών πρόσβασης της Ηλεκτρονικής Τραπεζικής (e-banking), χωρίς να έχει προηγηθεί εξουσιοδότηση γι' αυτήν την πράξη από το νόμιμο κάτοχο.[11]

5. **Χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων**

Ο τελευταίος αυτός τρόπος τέλεσης του εγκλήματος προστέθηκε με το νέο Ποινικό Κώδικα με σκοπό να συμπεριλάβει με ευρύτερο τρόπο την έννοια της αξιοποίησης λογισμικού. Η τεχνολογία μεταβάλλεται με ραγδαίους ρυθμούς, με αποτέλεσμα να προστίθενται συνεχώς νέες μορφές επηρεασμού του λογισμικού του υπολογιστή με απώτερο σκοπό την παράνομη περιουσιακή μετακίνηση. Η έννοια του χρήματος δεν βρίσκεται στα στενά όρια του παρελθόντος. Με την Οδηγία 2007/64/ΕΚ συνδυαστικά με την Οδηγία 2000/46/ΕΚ στα "χρηματικά ποσά" περιλαμβάνονται τα χαρτονομίσματα, τα κέρματα, το λογιστικό και ηλεκτρονικό χρήμα, το "ηλεκτρονικό χρήμα" που χαρακτηρίζεται κάθε νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη, η οποία α) είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα, β) έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού τουλάχιστον ίσου με την εκδοθείσα νομισματική αξία , γ)

[10] Μιχαήλ Μαργαρίτης, Ποινικός Κώδικας, ερμηνεία-εφαρμογή 2η έκδοση, ΣΑΚΚΟΥΛΑΣ Π.Ν., 2009, σελ.1193
[11] ΑΠ.1726/2019, ΤΝΠ ΝΟΜΟΣ

γίνεται δεκτή ως μέσο πληρωμής από άλλες επιχειρήσεις πέραν της εκδότριας. Παράλληλα και με τη νεότερη Οδηγία 2009/110/ΕΚ , ως "ηλεκτρονικό χρήμα" νοείται οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό απόθεμα νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για το σκοπό της πραγματοποίησης πράξεων πληρωμών και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη. Έτσι, με τη νέα προσθήκη της Οδηγίας 2009/110/ΕΚ καθώς και του Ν. 4021/2011, μπορεί να ενταχθεί και το κρυπτονόμισμα "bitcoin" στην έννοια του χρήματος.

Υποκειμενική υπόσταση του εγκλήματος

Η απάτη με υπολογιστή τελείται σε κάθε περίπτωση με δόλο (πρόθεση). Για όλα τα στοιχεία της αντικειμενικής υπόστασης αρκεί ο ενδεχόμενος δόλος, χωρίς να απαιτείται, όπως συμβαίνει στο αδίκημα της κοινής απάτης, δόλος β' βαθμού (γνώση του δράστη) για την αναλήθεια των στοιχείων. Τούτο σημαίνει πως ο δράστης προβλέπει την πρόκληση περιουσιακής ζημίας στο θύμα ως ενδεχόμενο και το αποδέχεται. Επιπλέον, πρέπει να σημειωθεί πως το έγκλημα της απάτης με υπολογιστή περιλαμβάνει στην υποκειμενική του υπόσταση και ένα πρόσθετο στοιχείο, αυτό του προσπορισμού παράνομου περιουσιακού οφέλους για τον ίδιο το δράστη ή για κάποιον άλλον. Γι' αυτό το λόγο, μιλάμε για έγκλημα «υπερχειλούς υποκειμενικής υπόστασης». Επομένως, ο δράστης έχει άμεσο δόλο α' βαθμού για τον προσπορισμό παράνομου περιουσιακού οφέλους, δηλαδή θα πρέπει να αποσκοπεί στην αύξηση της περιουσίας του ίδιου ή τρίτου.

Απόπειρα

Κατά το νέο Ποινικό Κώδικα το έγκλημα της απάτης με υπολογιστή θεωρείται τετελεσμένο όταν ο δράστης έχει αποκομίσει το παράνομο περιουσιακό όφελος στο οποίο αποσκοπούσε η πράξη του. Αν για οποιονδήποτε λόγο το περιουσιακό αυτό όφελος δεν αποκτήθηκε, ενώ συντελέστηκε αρχή εκτέλεσης του αδικήματος, δηλαδή ξεκίνησε η διαδικασία επηρεασμού των δεδομένων και στοιχείων του ηλεκτρονικού υπολογιστή, τότε υπάρχει απόπειρα του εγκλήματος κι όχι τετελεσμένο έγκλημα. Τέλος, στην περίπτωση που η μη χρήση ορθών ή ελλιπών στοιχείων δεν έλαβε καν τη μορφή της αρχής εκτέλεσης του αδικήματος, τότε δεν υφίσταται ούτε απόπειρα του αδικήματος.

2.2. Απάτη μέσω υπολογιστή 386ΠΚ

1. Όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόνείκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.

2. Αν η απάτη στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημιά που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι (20) έτη.

Η απάτη μέσω υπολογιστή εντοπίζεται στη διάταξη του Ποινικού Κώδικα για την κοινή απάτη (386 ΠΚ). Σε αυτή την περίπτωση, ο υπολογιστής αποτελεί απλά το μέσον για την τέλεση της απάτης, όπου η πλάνη προκαλείται σε φυσικό πρόσωπο κι όχι σε τεχνολογικό μέσο. Ο δράστης επιχειρεί να πείσει το θύμα (πλάνη), το οποίο είναι φυσικό πρόσωπο και όχι υπολογιστής ή κάποιο άλλο τεχνολογικό, μέσο να προβεί σε παράνομη περιουσιακή διάθεση. Επομένως, η περιουσιακή διάθεση δεν επέρχεται με επηρεασμό μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή αλλά αντιθέτως προκύπτει έπειτα από ενέργειες στις οποίες προβαίνει τρίτο φυσικό πρόσωπο, το οποίο έχει εσφαλμένη αντίληψη της πραγματικότητας (πλάνη). Σε κάθε περίπτωση, για να στοιχειοθετηθεί το αδίκημα της απάτης μέσω υπολογιστή θα πρέπει η περιουσιακή διάθεση να τελεί σε άμεση αιτιώδη συνάφεια με την παραπλάνηση ενός φυσικού προσώπου. Αυτό σημαίνει πως η βλάβη θα πρέπει να είναι *άμεσο και αποκλειστικό αποτέλεσμα της παράστασης, απόκρυψης ή παρασιώπησης και όχι τυχαίο επακόλουθο των ψευδών παραστάσεων ή να οφείλεται σε άλλα περιστατικά* (Μαργαρίτης Μ.)

<u>Αντικειμενική υπόσταση του εγκλήματος</u>

Η απάτη μέσω υπολογιστή μπορεί να λάβει χώρα με τρεις (3) τρόπους:

1. **<u>Εν γνώσει παράσταση ψευδών γεγονότων ως αληθινών</u>**

Ως παράσταση ψευδών γεγονότων ως αληθινών, μπορεί να νοηθεί οποιαδήποτε ανακοίνωση, δήλωση ή διαβεβαίωση του δράστη, που περιλαμβάνει ανακριβή απεικόνιση της πραγματικότητας και έχει ως απώτερο σκοπό την απόκτηση από τον ίδιο ή από άλλον παράνομου περιουσιακού οφέλους. Η παράσταση μπορεί να είναι ρητή ή μπορεί να συναχθεί σιωπηρά υπό προϋποθέσεις. Ως γεγονότα μπορούν να χαρακτηριστούν *καταστάσεις ή συμβάντα του εξωτερικού κόσμου, που αναφέρονται στο παρελθόν ή στο παρόν, γίνονται αντιληπτά με τις αισθήσεις και μπορούν να αποτελέσουν αντικείμενο απόδειξης. Υπό αυτήν την έννοια, δεν μπορούν να υπαχθούν στην έννοια του γεγονότος οι καταστάσεις που αναφέρονται στο μέλλον και οι υποσχέσεις μελλοντικών δεσμεύσεων, καθώς και οι καταστάσεις του εσωτερικού κόσμου (όπως προθέσεις, αισθήματα ή κίνητρα), οι απλές αξιολογικές κρίσεις, εκτιμήσεις και γνώμες*(Παπαδαμάκης).[12] Σε κάθε περίπτωση η παράνομη απόκτηση περιουσιακού οφέλους θα πρέπει να βρίσκεται σε άμεση αιτιώδη συνάφεια με τις παραπλανητικές ενέργειες ή παραλείψεις του δράστη. [13]

2. **<u>Αθέμιτη απόκρυψη αληθινών γεγονότων</u>**

Η αθέμιτη απόκρυψη αληθινών γεγονότων συνιστά θετική συμπεριφορά με την οποία η πραγματική κατάσταση και ο παραπλανώμενος εμποδίζεται να πληροφορηθεί την αλήθεια. Η "απόκρυψη" διαφέρει από την "παρασιώπηση", καθώς η απόκρυψη προϋποθέτει και άλλη μία θετική ενέργεια, η οποία είναι συγκαλυπτική της αλήθειας. Η εν λόγω απόκρυψη χαρακτηρίζεται αθέμιτη όταν ο δράστης δεν διαθέτει νόμιμο δικαίωμα για να την πράξει. Κατ' αυτόν τον τρόπο, ο πλανώμενος θεωρεί πως έχει σχηματίσει πλήρη συνείδηση της πραγματικότητας, ωστόσο λόγω της απόκρυψης γεγονότων αγνοεί ουσιώδεις πληροφορίες, οι οποίες θα συνέβαλαν καθοριστικά στη διαμόρφωση της αντίληψής του για την πραγματικότητα. [14]

3. **<u>Παρασιώπηση των αληθινών γεγονότων</u>**

[12]Α. Παπαδαμάκη, Τα περιουσιακά εγκλήματα, 2000, εκδ. Α.Ν. Σάκκουλα, σελ. 92-93.
[13] Μιχαήλ Μαργαρίτης, ΠοινικόςΚώδικας, ερμηνεία-εφαρμογή 2η έκδοση, ΣΑΚΚΟΥΛΑΣ Π.Ν.,2009, σελ. 1151
[14] Μιχαήλ Μαργαρίτης, Ποινικός Κώδικας, ερμηνεία-εφαρμογή 2η έκδοση, ΣΑΚΚΟΥΛΑΣ Π.Ν.,2009, σελ.1152

Ο εν λόγω τρόπος τέλεσης της απάτης συντελείται απλά με την παράλειψη ανακοίνωσης αληθινών γεγονότων, για την οποία ο δράστης δεν διέθετε σχετικό εκ του νόμου δικαίωμα. Σε αντίθεση με την αθέμιτη απόκρυψη, σε αυτή την περίπτωση ,δεν απαιτείται κάποια άλλη ενέργεια εκ μέρους του δράστη προκειμένου να ενισχυθεί η συγκάλυψη της αλήθειας. [15]

Υποκειμενική υπόσταση του εγκλήματος

Το έγκλημα της απάτης μέσω υπολογιστή απαιτεί δόλο του δράστη για να τελεστεί. Απάτη από αμέλεια δεν τυποποιείται ούτε μπορεί να νοηθεί. Πιο συγκεκριμένα, για να στοιχειοθετηθεί το έγκλημα της απάτης θα πρέπει να αποδεικνύεται τόσο ο δόλος του δράστη ως προς τη γνώση της ψευδούς παράστασης γεγονότων ως αληθινών ή της αθέμιτης απόκρυψης ή παρασιώπησης αληθινών γεγονότων όσο και ο δόλος του ως προς τον προσπορισμό παράνομου περιουσιακού οφέλους.[16] Το είδος του δόλου όμως που απαιτείται προς όλα τα στοιχεία της αντικειμενικής υπόστασης δεν είναι το ίδιο. Ως προς την παράσταση ψευδών γεγονότων σαν αληθινών ή την απόκρυψη ή παρασιώπηση γεγονότων απαιτείται τουλάχιστον άμεσος δόλος β' βαθμού (« εν γνώσει») και δεν αρκεί ο ενδεχόμενος δόλος. Ως προς τα υπόλοιπα στοιχεία της αντικειμενικής υπόστασης αρκεί ο ενδεχόμενος δόλος. Στην υποκειμενική υπόσταση αυτού του εγκλήματος υπάρχει κι ένα πρόσθετο στοιχείο, αυτό της προσπόρισης στο δράστη ή άλλον παράνομου περιουσιακού οφέλους. Για το στοιχείο αυτό απαιτείται άμεσος δόλος α' βαθμού. Επομένως, είναι σαφές ότι η απάτη μέσω υπολογιστή κατατάσσεται στα εγκλήματα της «υπερχειλούς υποκειμενικής υπόστασης».

Απόπειρα

'Όπως και στο έγκλημα της απάτης με υπολογιστή 386^{A} ΠΚ, έτσι και στο έγκλημα της απάτης μέσω υπολογιστή 386 ΠΚ, για να θεωρηθεί το έγκλημα τετελεσμένο, θα πρέπει ο δράστης να έχει αποκομίσει το περιουσιακό όφελος στο οποίο αποσκοπούσε με την πράξη του. Έτσι, θεωρείται ότι υπάρχει απόπειρα και όχι τετελεσμένο έγκλημα, όταν έχει γίνει τουλάχιστον αρχή εκτέλεσης του αδικήματος, δηλαδή πραγμάτωση μέρους της αντικειμενικής του υπόστασης χωρίς ωστόσο ο δράστης να έχει αποκομίσει το

[15] Μιχαήλ Μαργαρίτης, Ποινικός Κώδικας, ερμηνεία-εφαρμογή 2η έκδοση, ΣΑΚΚΟΥΛΑΣ Π.Ν.,2009, σελ.1154
[16] ΑΠ.88/2019, ΤΝΠ ΝΟΜΟΣ

επιδιωκόμενο περιουσιακό όφελος. Πιο συγκεκριμένα, στο αδίκημα αυτό υπάρχει απόπειρα όταν έχει ξεκινήσει η εξαπάτηση με την εν γνώσει παράσταση ψευδών γεγονότων ως αληθινών ή αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων , η οποία έχει σκοπό παράνομης απόκτησης περιουσιακής ωφέλειας για το δράστη ή τρίτον μέσω της βλάβης ξένης περιουσίας. Αν δεν συντρέχουν τα παραπάνω γεγονότα, τότε δεν υπάρχει καν απόπειρα.

2.3 Εμβάθυνση των αδικημάτων με παραδείγματα

2.3.1 Το φαινόμενο της χωρίς δικαίωμα χρήσης μαγνητικής κάρτας αυτόματης συναλλαγής σε ΑΤΜ για ανάληψη χρημάτων

Η χωρίς δικαίωμα χρήση μαγνητικής κάρτας αυτόματης συναλλαγής σε ΑΤΜ για ανάληψη χρημάτων έχει δημιουργήσει διχογνωμία στην ελληνική θεωρία και νομολογία σχετικά με τη νομική της φύση. Έχουν υποστηριχθεί οι απόψεις, πως συνιστά το έγκλημα της κλοπής ή της υπεξαίρεσης, οι οποίες ωστόσο δεν επικράτησαν. Το Ναυτοδικείο Πειραιά με την υπ'αριθμ. 418/1996 απόφασή του έκρινε τη χωρίς δικαίωμα χρήση μαγνητικής κάρτας αυτόματης συναλλαγής σε ΑΤΜ ως απάτη με υπολογιστή.[17] Την άποψη αυτή υιοθέτησε εν συνεχεία και η νομολογία. Καθοριστικό ρόλο, όμως, για το νομικό χαρακτηρισμό αυτής της πράξης διαδραμάτισαν οι Οδηγίες 2000/46/ΕΚ και 2009/110/ΕΚ , με τις οποίες αποσαφηνίστηκε η έννοια του "ηλεκτρονικού χρήματος". Ως "ηλεκτρονικό χρήμα, νοείται οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό απόθεμα νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για το σκοπό της πραγματοποίησης πράξεων πληρωμών και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη.

Σύμφωνα με τα παραπάνω, η πράξη αυτή χαρακτηρίζεται ως απάτη με υπολογιστή 386Α ΠΚ., τελούμενη κατά τον δεύτερο περιγραφόμενο τρόπο στην 1η παράγραφο της διάταξης, ήτοι τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή. Τίθεται αυστηρή προϋπόθεση πως η μαγνητική κάρτα συναλλαγών είναι γνήσια. Κατ' αυτόν τον τρόπο, ο δράστης, ο οποίος δεν είναι ο νόμιμος κάτοχος της κάρτας, ούτε έχει νόμιμο δικαίωμα ή εξουσιοδότηση για τη χρήση της, επηρεάζει τα

[17] Γ. Νούσκαλης, Ποιν. Δικαιοσύνη, 2/2003 (Έτος 6ο), σελ.182

στοιχεία του υπολογιστή με τέτοιο τρόπο ώστε το αποτέλεσμα που προκύπτει από την επεξεργασία των δεδομένων είναι διαφορετικό από αυτό θα προέκυπτε αν η χρήση της κάρτας γινόταν από το νόμιμο κάτοχο.

2.3.2 Το φαινόμενο "phishing"

Το φαινόμενο "phishing", γνωστό και ως ηλεκτρονικό ψάρεμα, αποτελεί μια μορφή κυβερνοεπίθεσης, ευρέως διαδεδομένης, η οποία λαμβάνει χώρα συχνά μέσω email, μέσων κοινωνικής δικτύωσης αλλά και τηλεφώνου. Σε αυτήν ο δράστης προσποιείται κάποιο αξιόπιστο πρόσωπο, φορέα ή υπάλληλο (λ.χ. κάποιο χρηματοπιστωτικό ίδρυμα ή επιχείρηση κοινής ωφέλειας) και ζητά από το θύμα να του αποκαλύψει ευαίσθητες πληροφορίες όπως τον κωδικό πρόσβασης της υπηρεσίας e-banking που διαθέτει για να προβεί σε κάποια ενέργεια όπως την κατάθεση χρηματικού ποσού σε έναν τραπεζικό λογαριασμό για την εξόφληση κάποιας υποτιθέμενης οφειλής. Αυτό έχει ως αποτέλεσμα την εξαπάτηση του θύματος και κατά συνέπεια την περιουσιακή βλάβη του ιδίου ή και τρίτου.

Ο συνηθέστερος τρόπος εξαπάτησης των θυμάτων συνίσταται στη μαζική αποστολή "spam " μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) από τους δράστες, οι οποίοι εμφανίζονται ως χρηματοπιστωτικά ιδρύματα στα οποία τα θύματα διατηρούν τραπεζικό λογαριασμό. [18]Με την πρόφαση της αναβάθμισης της ασφάλειας του ιστοτόπου του e-banking της τράπεζας και με τη χρήση πανομοιότυπου περιβάλλοντος στο e-mail με αυτό που αποστέλλεται από τα χρηματοπιστωτικά ιδρύματα στους πελάτες, οι δράστες παραθέτουν έναν υπερσύνδεσμο στον οποίο παρακινούν τα θύματα να συνδεθούν με το όνομα χρήστη και τον κωδικό πρόσβασης που χρησιμοποιούν για την υπηρεσία e-banking.Με αυτό τον τρόπο, οι επιτήδειοι δράστες αποκτούν ευαίσθητα προσωπικά στοιχεία των θυμάτων, τα οποία εν συνεχεία αξιοποιούν για να αποκομίσουν περιουσιακό όφελος σε βάρος της περιουσίας των τελευταίων ή τρίτων.

Η πρακτική αυτή αποτελεί την πλέον διαδεδομένη μορφή εξαπάτησης των πολιτών και είναι εξαιρετικά επιτυχής, ιδίως σε άτομα μεγαλύτερης ηλικίας , τα οποία δεν είναι τόσο εξοικειωμένα στη χρήση ηλεκτρονικών υπολογιστών ή στην αναγνώριση μεταξύ γνησίων

[18] Ιστότοπος https://cyberalert.gr/phising/

emails από χρηματοπιστωτικά ιδρύματα και άλλους φορείς ή emails από κακόβουλους χρήστες.

2.3.3. Το φαινόμενο "pharming".

Το φαινόμενο "pharming" αποτελεί μία σύνθετη έννοια η οποία δομείται από την έννοια "phishing" και την έννοια " DNS poisoning". Πιο συγκεκριμένα, οι δράστες αρχικά εξαπατούν τα θύματα πείθοντάς τους όπως αναφέρθηκε παραπάνω να τους αποκαλύψουν προσωπικά στοιχεία, όπως τους κωδικούς πρόσβασης στο ebanking κάποιου τραπεζικού λογαριασμού. Έπειτα, αφού αποκτήσουν πρόσβαση σε αυτούς, ωθούν τα θύματα να συνδεθούν σε κάποιον ιστότοπο, ο οποίος είναι αυθεντικός κι εν συνεχεία αφού «μολύνουν» το DNS server ή τον ηλεκτρονικό υπολογιστή με κάποιο κακόβουλο λογισμικό, αναδρομολογούν το θύμα χωρίς τη συγκατάθεσή του σε κάποιον άλλον ιστότοπο τον οποίο διαχειρίζονται πλήρως οι δράστες.[19]Κατ' αυτόν τον τρόπο αποκτούν πρόσβαση στον τραπεζικό τους λογαριασμό και προβαίνουν σε παράνομες περιουσιακές μεταφορές σε βάρος των θυμάτων.

ΚΕΦΑΛΑΙΟ Γ'

3)ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ- ΑΝΤΙΜΕΤΩΠΙΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1) Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Σύμβαση της Βουδαπέστης 23/11/2001)

Η πρώτη προσπάθεια για τη νομοθετική προστασία από το ηλεκτρονικό έγκλημα συντελέστηκε από το Συμβούλιο της Ευρώπης. Η Σύμβαση για το έγκλημα στον Κυβερνοχώρο, που έλαβε χώρα στη Βουδαπέστη στις 23/11/2001, υπεγράφη αμέσως από την πλειοψηφία των Κρατών-μελών του Συμβουλίου της Ευρώπης, αλλά και από άλλα τρίτα κράτη μη μέλη , όπως οι ΗΠΑ και η Αυστραλία. Η Σύμβαση τέθηκε σε ισχύ την 1/7/2004. Αντίθετα, η Ελλάδα δεν ανταποκρίθηκε άμεσα στη Σύμβαση αυτή και προέβη στην υπογραφή και κύρωσή της 15 χρόνια μετά, ήτοι το 2016 με τη θέσπιση του

[19] Ιστότοπος https://www.techtarget.com/searchsecurity/definition/pharming

ν.4411/2016 και τη μεταφορά της οδηγίας 2013/40/ΕΕ σχετικά με τις επιθέσεις σε συστήματα πληροφοριών.

Η Σύμβαση αυτή περιλαμβάνει διατάξεις τόσο ουσιαστικού όσο και δικονομικού δικαίου, οι οποίες αποσκοπούν στη θέσπιση κρατικών δικονομικών κανόνων σχετικά με την έρευνα και τη δίωξη κυβερνοεγκλημάτων αλλά και την εκδίκασή τους, στην εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των συμβαλλόμενων μερών, ώστε να υπάρχει ενιαίο νομοθετικό πλαίσιο ανάμεσα στα συμβαλλόμενα κράτη και τέλος στην πρόβλεψη διεθνούς συνεργασίας στον τομέα αυτό.20

Όπως αναφέρθηκε παραπάνω, η Σύμβαση περιλαμβάνει διατάξεις τόσο ουσιαστικού όσο και δικονομικού ποινικού χαρακτήρα, οι οποίες διαρθρώνονται σε 4 κεφάλαια. Πιο συγκεκριμένα, το 1ο κεφάλαιο, το οποίο αποτελείται από ένα άρθρο περιλαμβάνει ορισμούς όρων της σύμβασης. Στο 2ο κεφάλαιο (α. 2-22) γίνεται αναφορά σε διατάξεις ποινικού ουσιαστικού δικαίου, που ποινικοποιούν ορισμένες συμπεριφορές στο Διαδίκτυο, καθώς και σε διατάξεις ποινικού δικονομικού δικαίου, οι οποίες καλύπτουν μια πληθώρα κυβερνοεγκλημάτων. Στο 3ο κεφάλαιο (α.23-35) προβλέπονται διατάξεις σχετικές με την έρευνα, τη διεθνή αντιμετώπιση και συνεργασία των κρατών, καθώς και τις διαδικασίες που ακολουθούνται σε περίπτωση απουσίας εφαρμοστέων διεθνών συμβάσεων. Τέλος , το 4ο κεφάλαιο της Σύμβασης περιλαμβάνει τις τελικές διατάξεις.

3.1.1) Άρθρο 8 Σύμβασης Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα

Ρηξικέλευθη πρόβλεψη στη Σύμβαση αποτέλεσε το άρθρο 8 για την απάτη σχετική με τους υπολογιστές.

Άρθρο 8 - Απάτη σχετική με υπολογιστές

Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της

α. εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή,

β. παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο.

[20]Αγγελή Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο», ΠοινΔικ 12/2001, σελ. 1218-1220

Σκοπός της ανωτέρω ρύθμισης ήταν να ποινικοποιηθεί οποιαδήποτε χωρίς δικαίωμα παρέμβαση σε σύστημα Η/Υ, η οποία έχει ως σκοπό την απόκτηση παράνομου περιουσιακού οφέλους από το δράστη. Η αιτιολογική έκθεση της εν λόγω Σύμβασης ήταν ιδιαίτερα λεπτομερής ως προς την ερμηνεία του εδαφίου β' του άρθρου 8. Πιο συγκεκριμένα, με τον όρο «επέμβαση» στη λειτουργία υπολογιστή ή συστήματος υπολογιστή περιλαμβάνεται οποιαδήποτε παρέμβαση στα μέρη του ηλεκτρονικού υπολογιστή, καθώς και οποιαδήποτε ενέργεια μπορεί να επηρεάσει την αποθήκευση, επεξεργασία και ροή δεδομένων.

Όπως γίνεται αντιληπτό, πρόκειται για μια διάταξη «ομπρέλα» , διότι συμπεριλαμβάνει ένα ευρύ φάσμα ηλεκτρονικών εγκλημάτων. Σκοπός αυτής της διάταξης ήταν να ποινικοποιηθύν ενέργειες όπως η απάτη με πιστωτική και χρεωστική κάρτα αλλά και αδικήματα με «ηλεκτρονικό χρήμα».21 Παράλληλα, με αυτό το σκεπτικό και λόγω του διασυνοριακού χαρακτήρα που μπορεί να λάβει το ηλεκτρονικό έγκλημα, με τη διάταξη αυτή έγινε προσπάθεια να τεθεί ένα ευρέως αποδεκτό στα συμβαλλόμενα μέρη νομοθετικό πλαίσιο, ιδίως για κράτη μέρη της Σύμβασης που δεν διέθεταν αντίστοιχες διατάξεις στο εσωτερικό ποινικό τους δίκαιο.

3.2) Ν.4411/2016

Με το Ν.4411/2016 κυρώθηκε η Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο κι ενσωματώθηκε με αυτό τον τρόπο στην ελληνική έννομη τάξη. Με το νόμο αυτό επήλθε και η τροποποίηση του άρθρου 386^{α} ΠΚ σχετικά με την απάτη με υπολογιστή. Πιο συγκεκριμένα, με το νέο Ποινικό Κώδικα του Ν.4619/2019, συμπεριλήφθηκε στο αδίκημα της απάτης με υπολογιστή και η χρήση μη ορθών δεδομένων χωρίς δικαίωμα. Βασικός στόχος της εν λόγω τροποποίησης ήταν να εκσυγχρονιστεί η άποψη των πολιτών σχετικά με την έννοια του χρήματος. Τα χρήματα δεν είναι σήμερα κατά κύριο λόγο κέρματα και τραπεζογραμμάτια στοιβαγμένα σε ένα θησαυροφυλάκιο, αλλά δεδομένα αποθηκευμένα σε ηλεκτρονικά συστήματα.[22] Για το λόγο αυτό με το Ν.4411/2016 αφαιρέθηκε από το άρθρο 386^{Α} ΠΚ η γενική ρήτρα «με οποιονδήποτε άλλο τρόπο» και η παλιά υπαλλαγή της «επέμβασης κατά την εφαρμογή προγράμματος»,

[21] Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2019, σελ.14
[22] Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2019, σελ.168

διευρύνθηκε και υποκαταστάθηκε από τη «χωρίς δικαίωμα χρήση δεδομένων» και τη «χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα». Ωστόσο, τι νοείται ως χρήση δεδομένων «χωρίς δικαίωμα»; Για τη δημιουργία ενός περιεχομένου που να ανταποκρίνεται στο σκοπό της Σύμβασης της Βουδαπέστης για το Κυβερνοέγκλημα εκφράστηκαν ποικίλες απόψεις από διεθνείς αλλά και εγχώριους νομικούς. Ως επικρατέστερη κρίθηκε η άποψη πως «χωρίς δικαίωμα» χρήση δεδομένων είναι η χρήση που γίνεται χωρίς τη συναίνεση του δικαιούχου ή χωρίς την ύπαρξη άλλου νόμιμου δικαιολογητικού λόγου.[23]Πιο συγκεκριμένα είναι η εισαγωγή ορθών δεδομένων αλλά αντίθετα με το νόμο, τη σύμβαση ή τη βούληση του δικαιούχου.

3.3) Ευρωπαϊκές Οδηγίες

3.3.1. Οδηγία 2013/40/ΕΕ

Βασικός στόχος της εν λόγω Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, η οποία υπεγράφη στις 12 Αυγούστου 2013, ήταν να ενταχθούν στο ποινικό δίκαιο των συμβαλλομένων κρατών-μελών στον τομέα της κυβερνοασφάλειας οι ελάχιστοι κανόνες σχετικά με την ποινικοποίηση ορισμένων συμπεριφορών καθώς και οι σχετικές κυρώσεις. Μεταξύ άλλων, προβλέφθηκε με την παρούσα Οδηγία και η βελτίωση της συνεργασίας ανάμεσα στα αρμόδια όργανα των συμβαλλομένων κρατών-μελών, με το σκεπτικό πως το κυβερνοέγκλημα αποτελεί έγκλημα με έντονο διασυνοριακό χαρακτήρα. Ενσωματώθηκε στην ελληνική έννομη τάξη με το ν.4411/2016 κι επέφερε σημαντικές τροποποιήσεις στο άρθρο 386^{A} του νέου Ποινικού Κώδικα.

3.3.2. Οδηγία 2019/713/ΕΕ

Η παρούσα Οδηγία της 17^{ης} Απριλίου 2019 αφορούσε στην πάταξη της απάτης και της πλαστογραφίας των μέσων πληρωμής. Στην Οδηγία, ωστόσο, δεν υπήρξε πρόβλεψη για την απάτη και πλαστογραφία των μετρητών. Με αυτήν αντικαταστάθηκε η απόφαση-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου. Για την ενσωμάτωσή της στην ελληνική έννομη τάξη, τέθηκε σε δημόσια διαβούλευση η νομοθετική πρωτοβουλία του Υπουργείου Δικαιοσύνης στις 20/05/2022 κι εν τέλει ενσωματώθηκε με το Ν.4947/2022.

[23] Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2019, σελ.174

ΚΕΦΑΛΑΙΟ Δ'

4.1) Ποινική δίωξη και κυρώσεις του εγκλήματος της απάτης μέσω υπολογιστή 386 ΠΚ

Η απάτη μέσω υπολογιστή, στη βασική της μορφή, συνιστά πλημμέλημα και τιμωρείται με φυλάκιση από 5 μέρες μέχρι 5 χρόνια και χρηματική ποινή σωρευτικά μέχρι 360 ημερήσιες μονάδες. Το ύψος κάθε ημερήσιας μονάδας μπορεί να ανέρχεται από 1€ μέχρι 100€. Για την ποινική δίωξη του εγκλήματος απαιτείται πλέον έγκληση, σύμφωνα με το α.405 του νΠΚ, ενώ όταν η απάτη στρέφεται κατά των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης ή συνδέεται με την προσβολή των συμφερόντων αυτών, η ποινική δίωξη ασκείται αυτεπαγγέλτως (α.25 και 26 Ν.4689/2020). Το ίδιο υφίσταται και για την απάτη που στρέφεται κατά του Ελληνικού Δημοσίου η οποία εξακολουθεί να διώκεται αυτεπαγγέλτως.

Η πρώτη διακεκριμένη μορφή της κοινής απάτης μέσω υπολογιστή υφίσταται, όταν το ποσό της περιουσιακής διάθεσης ξεπερνά τις 120.000€. Σύμφωνα με το τελευταίο εδάφιο της πρώτης παραγράφου του άρθρου 386 ΠΚ, η προβλεπόμενη ποινή είναι κάθειρξη μέχρι 5 έτη (πλαίσιο ποινής 5-10 έτη) και χρηματική ποινή, όπως αυτή περιεγράφηκε παραπάνω.

Η δεύτερη και τελευταία διακεκριμένη μορφή του εγκλήματος αφορά στην απάτη κατά του Δημοσίου όπου το ποσό της περιουσιακής διάθεσης ξεπερνά τις 120.000€.Αναγράφεται ρητά στη δεύτερη παράγραφο του α.386 νΠΚ και η απειλούμενη ποινή ορίζεται σε κάθειρξη τουλάχιστον 10 ετών (πλαίσιο ποινής 10- 20 έτη) και χρηματική ποινή μέχρι χίλιες ημερήσιες μονάδες.

4.2) Ποινική δίωξη και κυρώσεις της απάτης με υπολογιστή 386^{Α} ΠΚ.

Η απάτη με υπολογιστή, όπως έχει προαναφερθεί, αποτελεί ιδιώνυμο έγκλημα κι ως εκ τούτου εμφανίζει αρκετά κοινά σημεία με το έγκλημα της κοινής απάτης. Μεταξύ αυτών των κοινών σημείων βρίσκεται και ο χαρακτηρισμός ορισμένων συμπεριφορών του εγκλήματος αυτού σε πλημμελήματα και κακουργήματα.

Πιο συγκεκριμένα, η απάτη με υπολογιστή στη βασική της μορφή συνιστά πλημμέλημα και τιμωρείται με φυλάκιση (πλαίσιο ποινής 5 μέρες έως 5 έτη), ενώ αν η ζημία που προκλήθηκε είναι ιδιαίτερα μεγάλη, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών (πλαίσιο ποινής 3 μήνες έως 5 έτη) και χρηματική ποινή σωρευτικά.

Η πρώτη διακεκριμένη μορφή αφορά σε προκληθείσα ζημία όπου το ποσό της ξεπερνά τις 120.000€ και η απειλούμενη ποινή αποτελεί κάθειρξη έως 10 έτη (πλαίσιο ποινής 5 έως 10 έτη) και χρηματική ποινή σωρευτικά.

Η δεύτερη και τελευταία διακεκριμένη μορφή υφίσταται όταν η απάτη με υπολογιστή στρέφεται κατά του Ελληνικού Δημοσίου , των ΝΠΔΔ ή των ΟΤΑ και η προκληθείσα ζημία ξεπερνά το ποσό των 120.000€. Προβλέπεται ποινή κάθειρξης τουλάχιστον 10 ετών (πλαίσιο ποινής 10 έως 20 έτη) και χρηματική ποινή έως 1000 ημερήσιες μονάδες, όπως αναφέρεται ρητά στην 3η παράγραφο του άρθρου αυτού.

Τέλος, σύμφωνα με τη δεύτερη παράγραφο του άρθρου 386Α ΠΚ, η κατασκευή, διάθεση ή κατοχή προγράμματος ή πληροφοριακού συστήματος που προορίζεται για την διάπραξη του εγκλήματος της 1ης παραγράφου του άρθρου αυτού, τιμωρείται με φυλάκιση έως 2 έτη(πλαίσιο ποινής 5 μέρες έως 2 έτη) και χρηματική ποινή σωρευτικά.

ΚΕΦΑΛΑΙΟ Ε’

5) ΤΑ ΟΙΚΟΝΟΜΙΚΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

5.1) Το κοινωνικό κόστος του εγκλήματος

Σύμφωνα με την προσέγγιση του οικονομολόγου Paul Ehrlich υποστηρίζεται πως στην εγκληματικότητα υπάρχει ένα μοντέλο προσφοράς και ζήτησης. Στις αντίστοιχες θέσεις βρίσκονται καταναλωτές μη νόμιμων προϊόντων και υπηρεσιών και από την άλλη εν δυνάμει θύματα. Από αυτά καθορίζεται η ζήτηση για ορισμένες παράνομες δραστηριότητες. Ισορροπία επέρχεται όταν τίθεται από το Κράτος ένα πρόστιμο , το ύψος του οποίου είναι τέτοιο ώστε να μειώνει τις απολαβές από την παραβατική συμπεριφορά.

Πιο συγκεκριμένα, το ύψος του προστίμου για να είναι αποτελεσματικό, θα πρέπει να πλησιάζει τις οριακές τιμές του κέρδους που θα προέκυπτε από τη διάπραξη του εγκλήματος.

Σε αυτό το σημείο είναι κρίσιμο να αναφερθεί και ο ευρύτερος αντίκτυπος που έχει η εγκληματικότητα στην κοινωνία και δη στην οικονομία. Το έγκλημα, είτε τελείται εκούσια είτε ακούσια, δεν βλάπτει μόνο το θύμα ή τρίτους που μπορεί να εμπλέκονται εμμέσως, αλλά έχει επιπτώσεις και στην οικονομία της χώρας. Αυτό συμβαίνει διότι η τελευταία καλείται να το αντιμετωπίσει με άμεσο ή έμμεσο τρόπο. Τα οικονομικά κυρίως εγκλήματα είναι αυτά που προκαλούν μια απορρύθμιση στην εθνική οικονομία. Η ανισορροπία αυτή οδηγεί σε χρηματοοικονομικές κρίσεις με αποτέλεσμα την αδυναμία στην ορθή κατανομή των πόρων. Κατά συνέπεια, γεννάται αβεβαιότητα στην κοινωνία με αποτέλεσμα να οδηγείται σε νέα φαινόμενα εγκληματικότητας και να δημιουργείται έτσι ένας ατέρμονος κύκλος.

Πιο συγκεκριμένα, το κόστος των ηλεκτρονικών οικονομικών εγκλημάτων δεν είναι μονοδιάστατο. Εκτός από το άμεσο χρηματικό κόστος που προκαλείται στο θύμα ή σε τρίτον από την απώλεια της περιουσίας του, υφίσταται και ένα έμμεσο, αφανές κόστος το οποίο βαρύνει τόσο τον παθόντα όσο και την κοινωνία. Η έμμεση αυτή ζημία που προκαλείται περιλαμβάνει τόσο το κόστος για την αποκατάσταση της ηθικής βλάβης του παθόντα από την απώλεια της περιουσίας του όσο και το κοινωνικό κόστος για τη λήψη μέτρων πρόληψης και αντιμετώπισης των ηλεκτρονικών οικονομικών εγκλημάτων. Στα μέτρα αυτά συγκαταλέγεται η αγορά και χρήση ειδικών λογισμικών για την ανίχνευση και αντιμετώπιση ύποπτων και επικίνδυνων διαδικτυακών ενεργειών σε όποιο στάδιο της κυβερνοεπίθεσης κι αν βρίσκονται, καθώς και η αναβάθμιση των πληροφοριακών συστημάτων και ηλεκτρονικών υπολογιστών ώστε να συμβαδίζουν με την εξέλιξη της τεχνολογίας των κυβερνοεπιθέσεων.

Σύμφωνα με έρευνα του Κέντρου Στρατηγικών και Διεθνών Ερευνών (Center of Strategic and International Studies- CSIS)[24] σε συνεργασία με την εταιρία κατασκευής λογισμικών κυβερνοασφάλειας McAfee, το άμεσο κόστος του ηλεκτρονικού οικονομικού εγκλήματος

[24]Report: The Hidden Costs of Cybercrime, by Zhanna Malekos Smith and Eugenia Lostri, James A. Lewis, Project Director, December 2020)

παγκοσμίως για το έτος 2019 ανερχόταν στα 945 δισεκατομμύρια δολάρια, περίπου 600 δις.$ παραπάνω από το 2018. Σήμερα, το ηλεκτρονικό οικονομικό έγκλημα επιβαρύνει την παγκόσμια οικονομία με 1 τρισεκατομμύριο δολάρια. Εξαιτίας της αλματώδους αύξησης στη χρήση του Διαδικτύου και των ηλεκτρονικών υπολογιστών και κατά συνέπεια και των κυβερνοεπιθέσεων, η αξία των παγκόσμιων δαπανών για κυβερνοασφάλεια ανήλθε το 2020 στα 145 δις. $, το 2022 στα 179 δις $, ενώ αναμένεται μέχρι το 2027 να ξεπεράσει τα 225 δις $.

Παράλληλα, τα ηλεκτρονικά οικονομικά εγκλήματα επιφέρουν και κόστος ευκαιρίας. Το κόστος ευκαιρίας αποτελεί το εισόδημα ή την παραγωγή που χάνεται ή μια υπηρεσία που δεν παρέχεται εξαιτίας κάποιου συμβάντος, στην προκειμένη περίπτωση διαδικτυακού. Για το λόγο αυτό και για να είναι πιο ολοκληρωμένος και ακριβής ο υπολογισμός του κόστους των ηλεκτρονικών οικονομικών εγκλημάτων, θα πρέπει να συμπεριληφθεί σε αυτό και το κόστος ευκαιρίας, όπως οι χαμένες ευκαιρίες και τα οφέλη που θα μπορούσαν να αποκτηθούν από άλλες δραστηριότητες στο Διαδίκτυο.

Ένα από τα πιο χαρακτηριστικά παραδείγματα κόστους ευκαιρίας που εμφανίζεται στα ηλεκτρονικά οικονομικά εγκλήματα είναι η δαπάνη μεγαλύτερου χρηματικού ποσού για την κυβερνοασφάλεια απ’ ότι θα απαιτούνταν σε ένα πιο ασφαλές περιβάλλον. Έτσι τα επιπλέον χρήματα που αναγκάζεται να δαπανήσει ο χρήστης του Διαδικτύου προκειμένου να προστατευτεί από τις αυξανόμενες και πιο επικίνδυνες κυβερνοεπιθέσεις, δεν μπορεί να τα αξιοποιήσει για άλλες δραστηριότητές του που πιθανότατα επιθυμούσε. Πέρα απ’ το ατομικό επίπεδο κυβερνοασφάλειας και ο ίδιος ο κρατικός μηχανισμός αναγκάζεται να δαπανήσει επιπλέον κονδύλια προκειμένου να ανταπεξέλθει στις αυξανόμενες και πιο απαιτητικές προκλήσεις του Διαδικτύου. Κατ’ αυτόν τον τρόπο,αποστερεί τα συγκεκριμένα κονδύλια από άλλους τομείς κοινής ωφέλειας στους οποίους θα μπορούσε να τα δαπανήσει.

ΚΕΦΑΛΑΙΟ ΣΤ'

6)Η ΕΞΕΛΙΞΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ-ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΑΝΑ ΤΟΝ ΚΟΣΜΟ

6.1) Η εμφάνιση των ηλεκτρονικών –οικονομικών εγκλημάτων στις ΗΠΑ

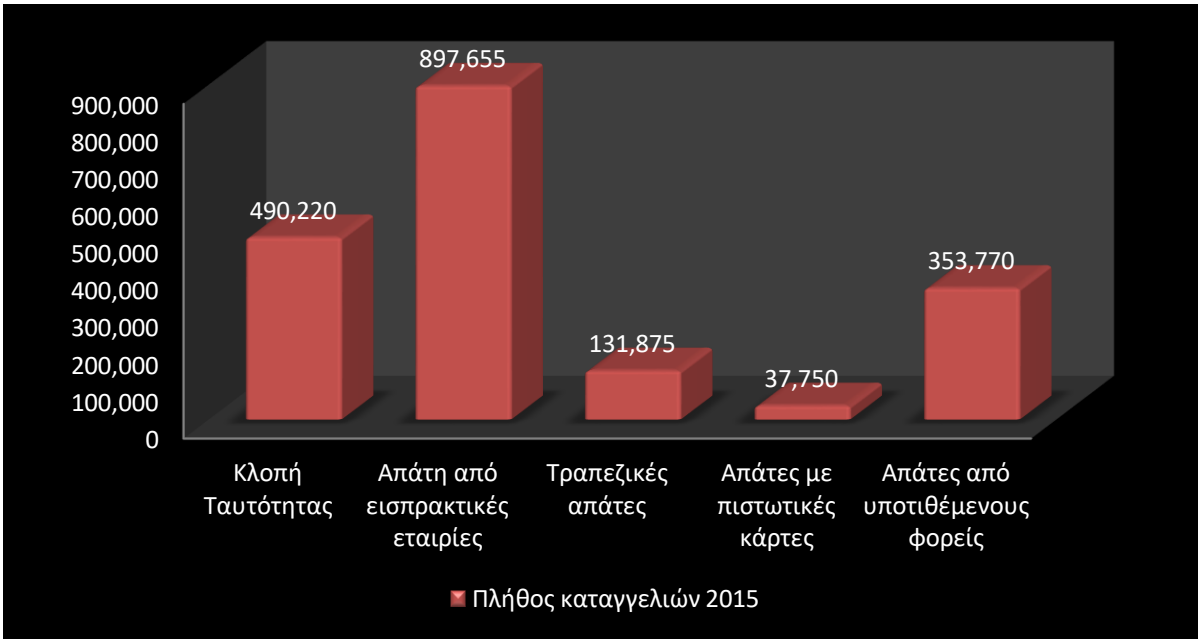
Τα ηλεκτρονικά οικονομικά εγκλήματα αποτελούν ένα παγκόσμιο φαινόμενο, το οποίο δεν είναι πρωτόγνωρο. Δεδομένου ότι εμφανίζεται με ποικίλες μορφές, συνοδεύει την ιστορία του Διαδικτύου ήδη από τις απαρχές του. Όσο εξελίσσεται η τεχνολογία και το Διαδίκτυο, τόσο αυξάνεται και λαμβάνει νέες μορφές το ηλεκτρονικό έγκλημα. Οι συνθήκες και οι ανάγκες κάθε εποχής αποτελούν ένα σημαντικό παράγοντα που πρέπει να ληφθεί υπόψιν όταν αξιολογείται η εξέλιξη της ηλεκτρονικής οικονομικής εγκληματικότητας διαχρονικά.

Στην παρούσα εργασία θα αξιολογηθούν στατιστικά δεδομένα σχετικά με το πλήθος και το είδος ηλεκτρονικών οικονομικών εγκλημάτων που έχουν λάβει χώρα στις ΗΠΑ, την Ευρώπη και την Ελλάδα στο διάστημα της πενταετίας 2015-2019, τον τρόπο με τον οποίο οι δράστες προτιμούν να προσεγγίζουν τα θύματα αλλά και την επίπτωση της συνθήκης που επικράτησε λόγω του Covid-19 το έτος 2020 στην εξέλιξη του φαινομένου.

Σύμφωνα με τα στατιστικά στοιχεία που αντλούμε από την Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (Federal Trade Commission) κατά το έτος 2015 καταγράφηκαν 3.083.379 καταγγελίες πολιτών ότι έπεσαν θύματα κάποιας μορφής ηλεκτρονικού οικονομικού εγκλήματος. Πιο συγκεκριμένα όπως εμφανίζεται και στο παρακάτω διάγραμμα 490.220 πολίτες έπεσαν θύματα κλοπής ταυτότητας, 897.655 υπέστησαν απάτη από εισπρακτικές εταιρίες, 131.875 ήταν θύματα τραπεζικής απάτης, 37.750 απάτης με πιστωτικές κάρτες, ενώ 353.770 άτομα έπεσαν θύματα υποτιθέμενων φορέων ,πχ. έλαβαν emails δήθεν από φορείς της κυβέρνησης όπου τους ζητούσαν κάποια μεταφορά χρημάτων για πληρωμή υποτιθέμενου φόρου.

Είναι φανερό πως οι δράστες επέλεξαν να χρησιμοποιήσουν μια μορφή απάτης στην οποία υποδύονται διαπιστευμένους φορείς της κυβέρνησης ή εισπρακτικές εταιρίες ώστε οι απαιτήσεις τους να είναι αληθοφανείς στα θύματα και να μην υποψιάζονται ότι πρόκειται

για απάτη. Άλλωστε, στις ΗΠΑ, δεδομένου ότι η πλειοψηφία των πολιτών λαμβάνει δάνεια προκειμένου να αποπληρώσει τα πανεπιστημιακά δίδακτρα ή να προβεί στην αγορά κάποιου ακινήτου, είναι εύλογο να γίνεται και στην πραγματικότητα επικοινωνία με εισπρακτικές εταιρίες για τακτοποίηση των οφειλών τους. Επομένως, οι δράστες προσαρμοζόμενοι στις συνθήκες της κοινωνίας προτιμούν τις προαναφερθείσες μορφές απάτης έναντι άλλων.

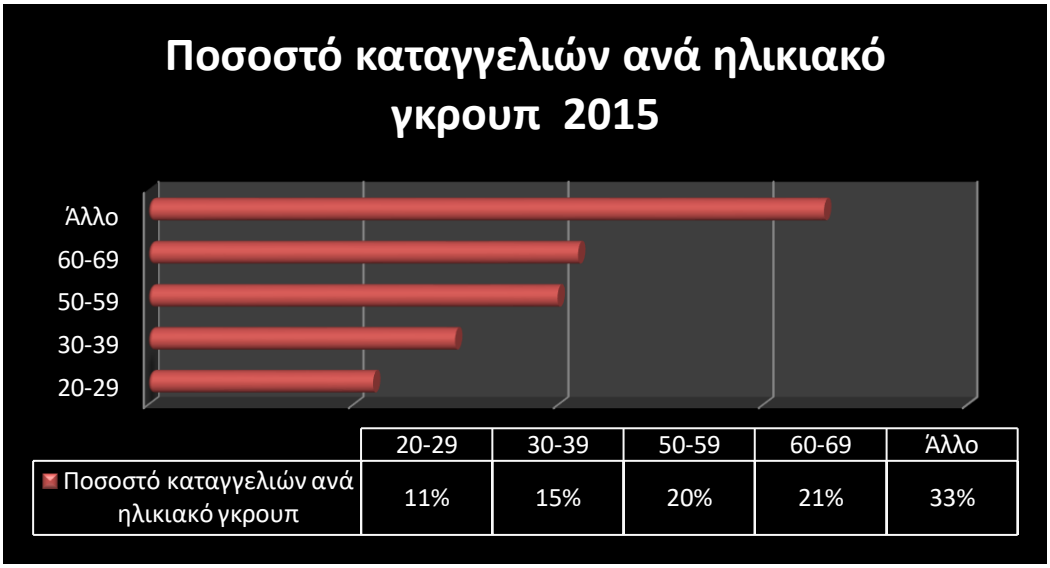


1

Όσον αφορά τον τρόπο προσέγγισης των θυμάτων, σύμφωνα με τα στοιχεία της Ομοσπονδιακής Επιτροπής Εμπορίου, το 75% των δραστών επέλεξε τηλεφωνική επικοινωνία, το 8% ηλεκτρονική αλληλογραφία (e-mail), το 6% το Διαδίκτυο ενώ το υπόλοιπο 11% επέλεξε άλλους τρόπους προσέλκυσης των θυμάτων.

2

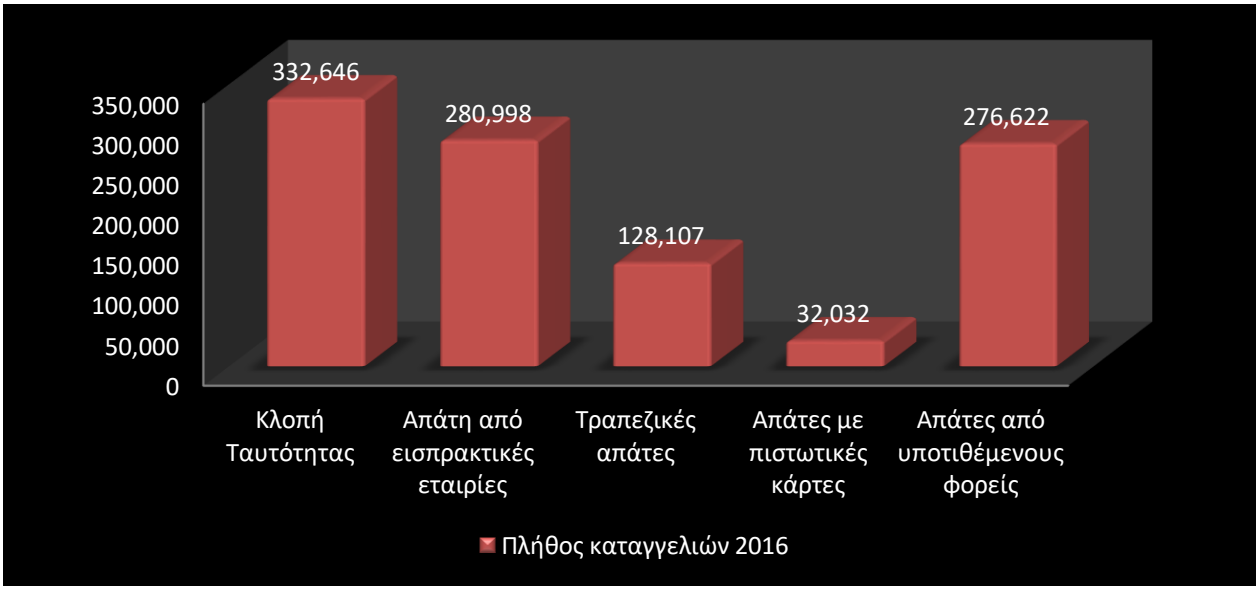
Τέλος, όσον αφορά το ηλικιακό γκρουπ των θυμάτων φαίνεται πως η πλειοψηφία τους ανήκει στη μέση ηλικία ήτοι στο ηλικιακό γκρουπ των 60-69 ετών, γεγονός που δικαιολογείται από την ελάχιστη ή και μηδαμινή εξοικείωση ή ακόμα και επαφή ατόμων αυτής της ηλικίας με τις νέες τεχνολογίες και το Διαδίκτυο. Ακολουθεί το ηλικιακό γκρουπ 50-59 έτη με ποσοστό 20%, για το οποίο ισχύουν αντιστοίχως τα προλεγόμενα, το γκρουπ 30-39 έτη με ποσοστό 15% και τέλος το νεότερο ηλικιακό γκρουπ 20-29 έτη αποτελεί τα λιγότερο δελεαστικά θύματα εξαιτίας της εξοικείωσης που διαθέτουν με τις νέες τεχνολογίες άρα και της γνώσης των κινδύνων που υπάρχουν.



	20-29	30-39	50-59	60-69	Άλλο
Ποσοστό καταγγελιών ανά ηλικιακό γκρουπ	11%	15%	20%	21%	33%

3

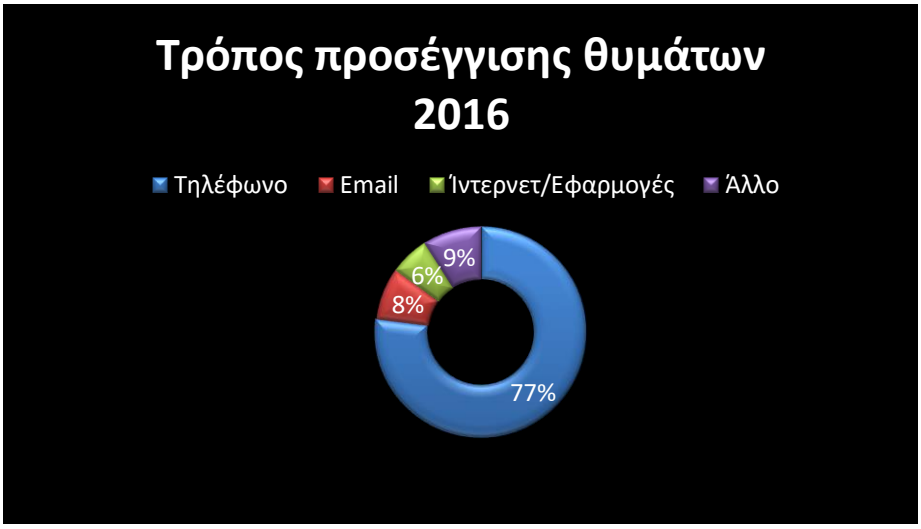
Το 2016 σημειώθηκαν από την Ομοσπονδιακή Επιτροπή Εμπορίου 3.050.374 καταγγελίες, 33.050 λιγότερες απ' ότι το 2015.



4

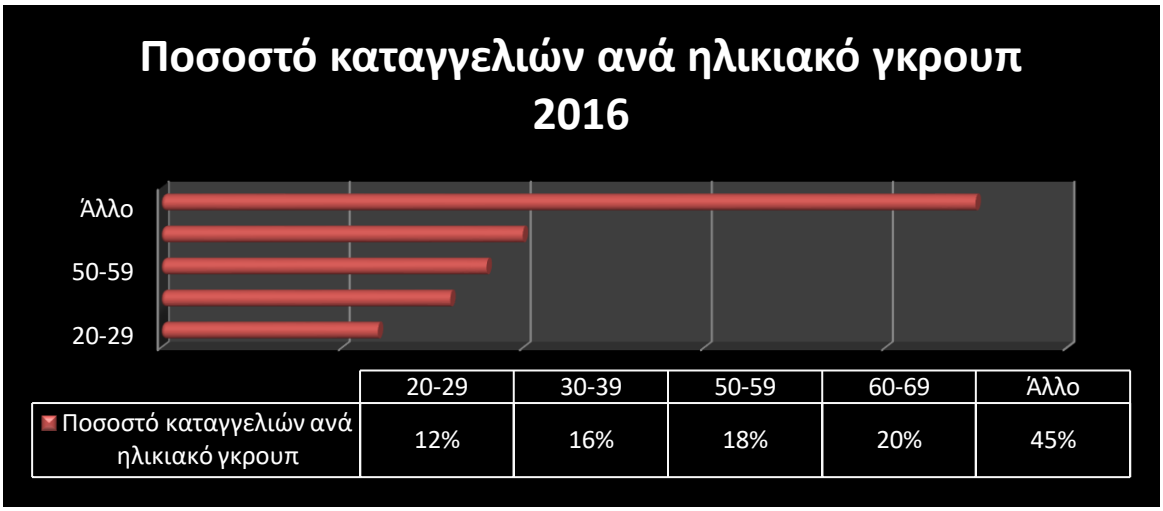
Όπως παρατηρείται στο παραπάνω ραβδόγραμμα, 332.646 άτομα έπεσαν θύματα κλοπής ταυτότητας, 280.998 θύματα απάτης από εισπρακτικές εταιρίες, 128.107 από τραπεζικές απάτες, 32.032 από απάτες με πιστωτικές κάρτες και τέλος 276.622 έπεσαν θύματα υποτιθέμενων φορέων. Παρατηρείται πως συγκριτικά με το 2015 προτιμάται η κλοπή ταυτότητας ως μέθοδος απάτης, σε σχέση με την απάτη από εισπρακτικές εταιρίες.

Όσον αφορά τον τρόπο προσέγγισης των θυμάτων επικρατέστερος εξακολουθεί να ητηλεφωνική επικοινωνία σε ποσοστό 77%, ακολουθεί το email σε ποσοστό 8%, το Διαδίκτυο σε ποσοστό 6%, ενώ το 9% αφορά άλλους τρόπους προσέγγισης όπως απεικονίζεται στο παρακάτω διάγραμμα.



5

Τέλος, όσον αφορά το ηλικιακό γκρουπ των θυμάτων παρατηρείται όπως και το 2015 μια προτίμηση σε άτομα μέσης ηλικίας δηλαδή στα ηλικιακά γκρουπ 50-59 και 60-69 έτη σε ποσοστό 18% και 20% αντίστοιχα για τους λόγους που αναφέρθηκαν προηγουμένως. Ακολουθούν με μικρότερη απήχηση τα ηλικιακά γκρουπ 20-29 και 30-39 με ποσοστά 12% και 16% αντιστοίχως.

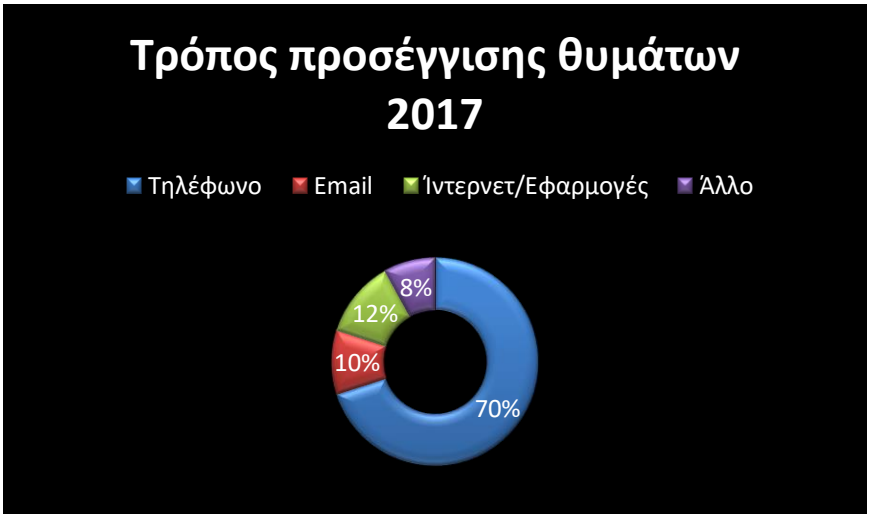


6

Το έτος 2017 σημειώθηκαν 2.904.329 καταγγελίες, 146.045 λιγότερες από το προηγούμενο έτος.

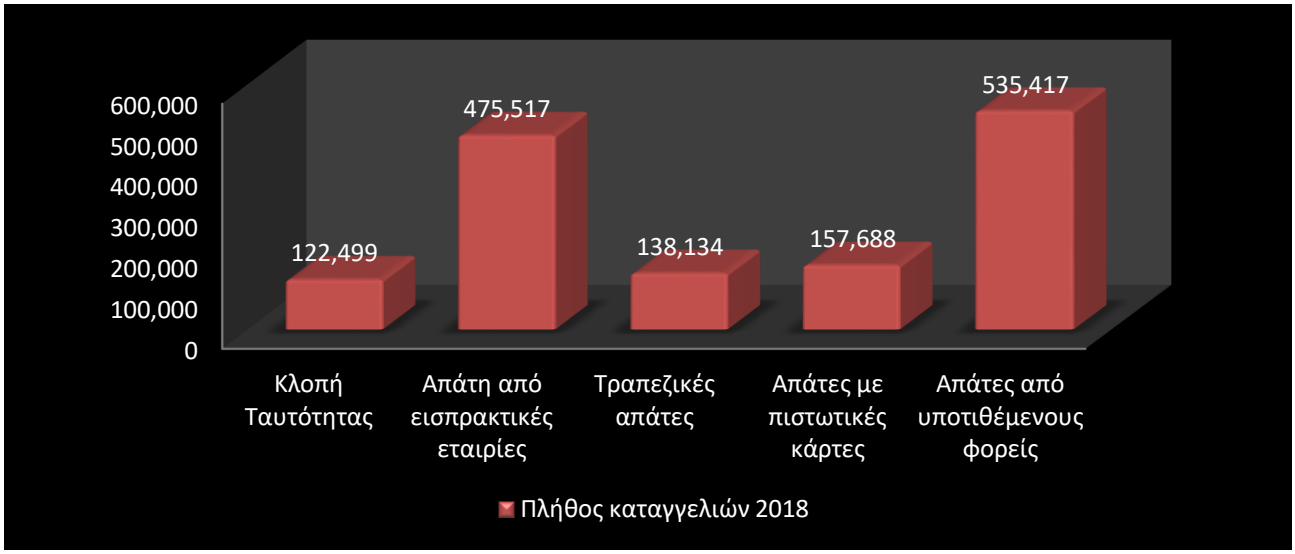
Οι 371.061 καταγγελίες αφορούσαν κλοπή ταυτότητας, 608.535 απάτη από εισπρακτικές εταιρίες που υποδηλώνει αύξηση του φαινομένου συγκριτικά με το προηγούμενο έτος, 149.316 τραπεζικές απάτες, 45.428 απάτες με πιστωτικές κάρτες και τέλος 347.829 απάτες από υποτιθέμενους φορείς.

Όσον αφορά τον τρόπο προσέγγισης των θυμάτων δεν παρουσιάζεται κάποια σημαντική αλλαγή συγκριτικά με τα προηγούμενα έτη καθώς κυρίαρχος τρόπο προσέγγισης παραμένει το τηλέφωνο με ποσοστό 70%, ακολουθεί το Διαδίκτυο με ποσοστό 12% ενώ ουραγός είναι το email με ποσοστό 10%.



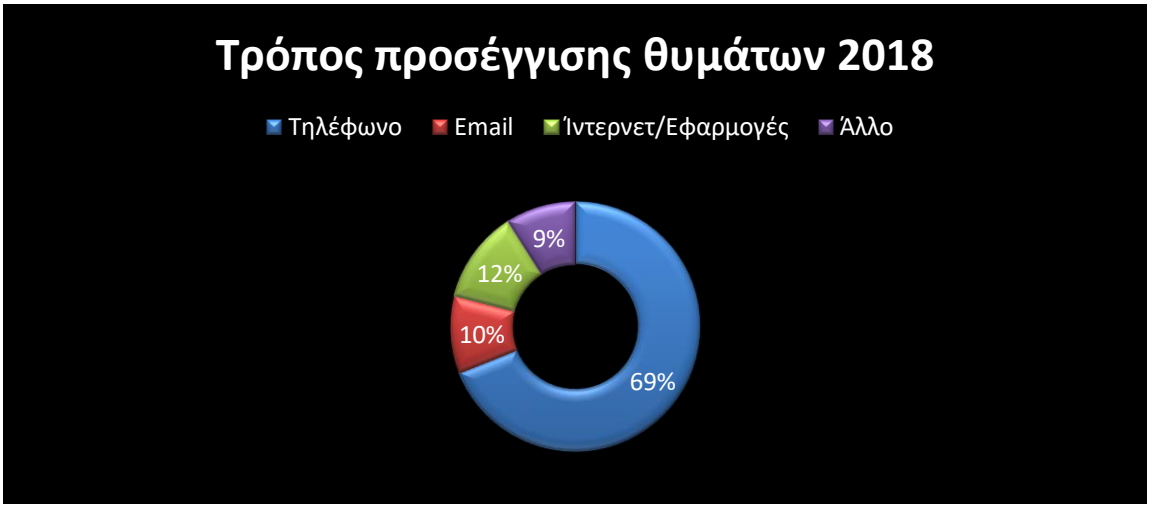
7

Το 2018 παρατηρήθηκαν 3.104.375 περιστατικά, 200.046 περισσότερα από την προηγούμενη χρονιά. Εντοπίζουμε μια σημαντική μείωση της απάτης με κλοπή ταυτότητας καθώς σημειώθηκαν μόνο 122.499 περιπτώσεις, ενώ στον αντίποδα παρατηρούμε μια εκτόξευση των περιπτώσεων απάτης από εισπρακτικές εταιρίες και απάτης από υποτιθέμενους φορείς, καθώς καταγγέλθηκαν 475.517 και 535.417 περιστατικά αντιστοίχως. Τέλος, εντοπίστηκαν 138.134 περιπτώσεις τραπεζικής απάτης και 157.688 απάτης με πιστωτική κάρτα.



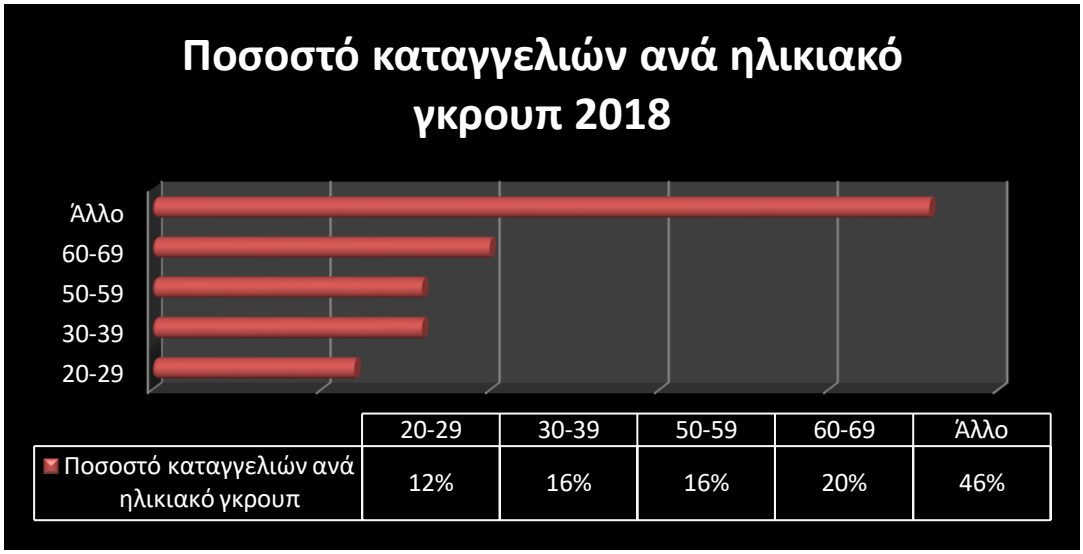
8

Ο τρόπος προσέγγισης των θυμάτων δεν παρουσιάζει αξιόλογη μεταβολή καθώς το 69% αφορά στο τηλέφωνο, το 12% στο Ίντερνετ, το 10% στο email ενώ το 9% σε άλλο τρόπο.



9

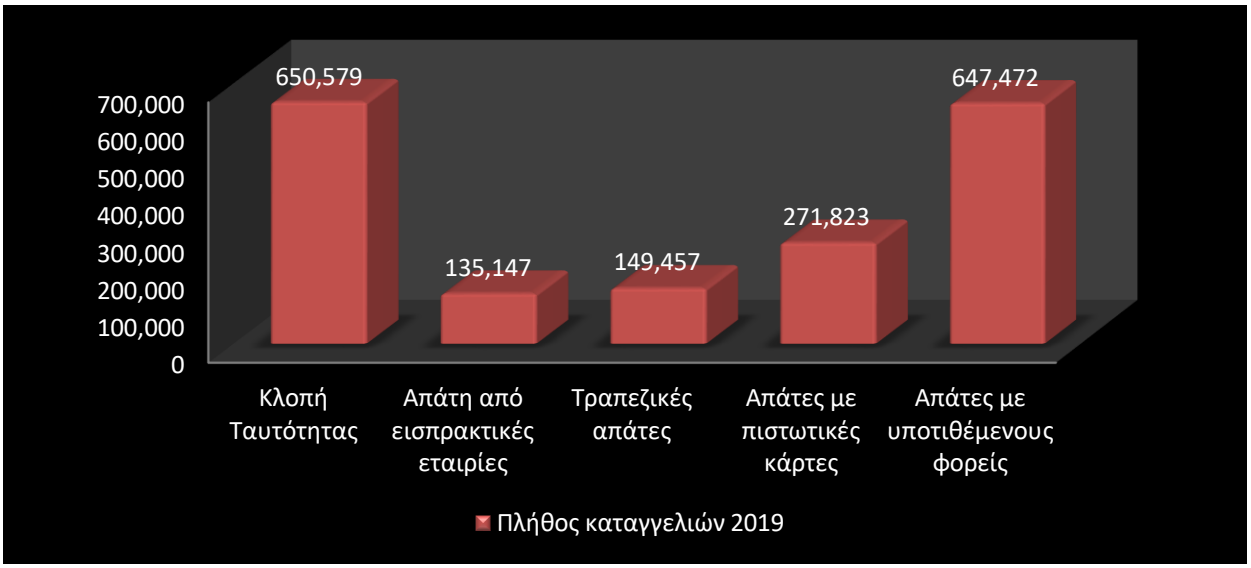
Σχετικά με τα ηλικιακά γκρουπ που έπεσαν θύματα απάτης εξακολουθεί η πλειοψηφία να είναι άτομα μέσης ηλικίας του ηλικιακού γκρουπ 60-69 έτη σε ποσοστό 20%, ακολουθούν τα ηλικιακά γκρουπ 30-39 και 50-59 σε ποσοστό 16% έκαστο, και τελευταίο βρίσκεται, όπως και κάθε έτος, το ηλικιακό γκρουπ 20-29 με ποσοστό 12%.



10

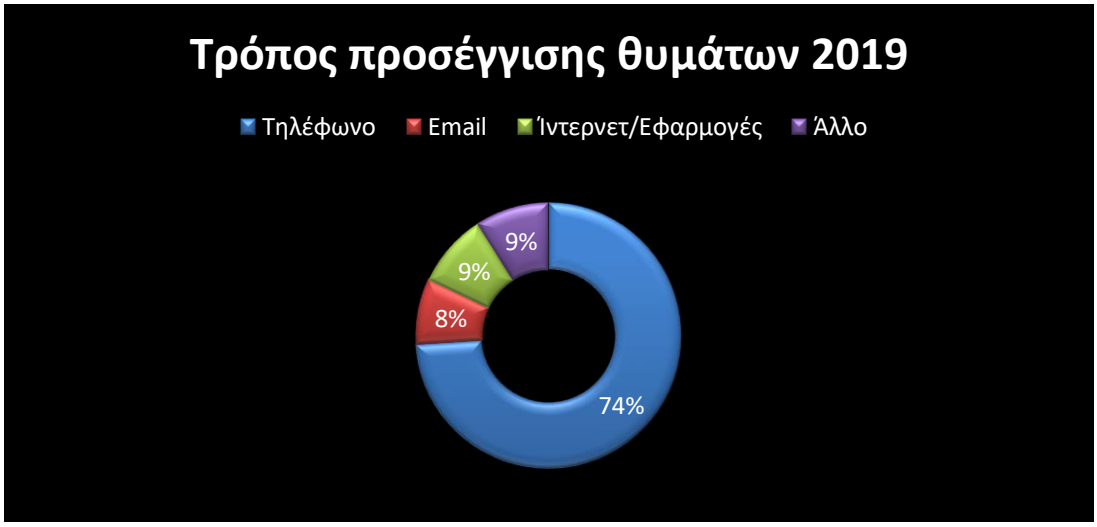
Τέλος, το έτος 2019 σημειώνεται μια ανιούσα πορεία των καταγγελιών καθώς καταγράφηκαν 3.200.329 καταγγελίες, 95.954 περισσότερες από το 2018.

Παρατηρήθηκε εκτόξευση των καταγγελιών για κλοπή ταυτότητας και απάτης από υποτιθέμενους φορείς καθώς καταγράφηκαν 650.579 και 647.472 περιστατικά αντίστοιχα. Παράλληλα, καταγγέλθηκαν 135.147 απάτες με εισπρακτικές εταιρίες, 149.457 τραπεζικές απάτες και 271.823 απάτες με πιστωτικές κάρτες.



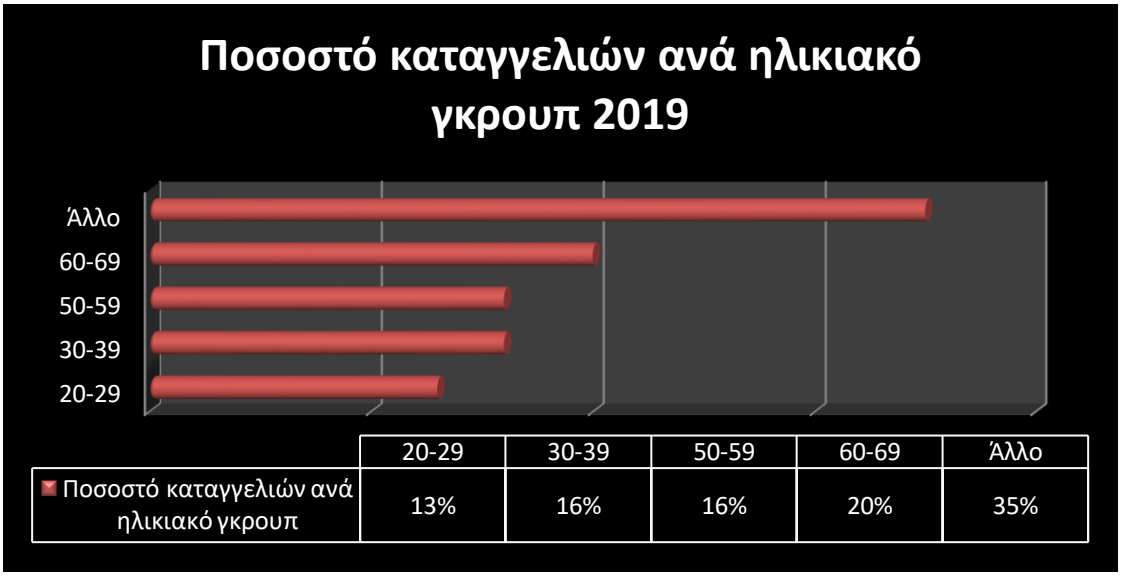
11

Ο τρόπος προσέγγισης των θυμάτων παραμένει ως έχει, με το τηλέφωνο να αποτελεί το 74%, το Διαδίκτυο το 9% και το email το 8%.



12

Τέλος, όσον αφορά τα ηλικιακά γκρουπ των θυμάτων, το γκρουπ 60-69 έτη εξακολουθεί να κατέχει την πρωτιά στις προτιμήσεις των δραστών με ποσοστό 20%, ακολουθούν τα ηλικιακά γκρουπ 30-39 και 50-59 με ποσοστό 16% το καθένα και τελευταίο βρίσκεται το ηλικιακό γκρουπ 20-29 που λόγω της μεγάλης εξοικείωσής του με την τεχνολογία και τους κινδύνους που ενέχει δεν αποτελεί συχνό θύμα απάτης, κατέχοντας έτσι ποσοστό 13%.

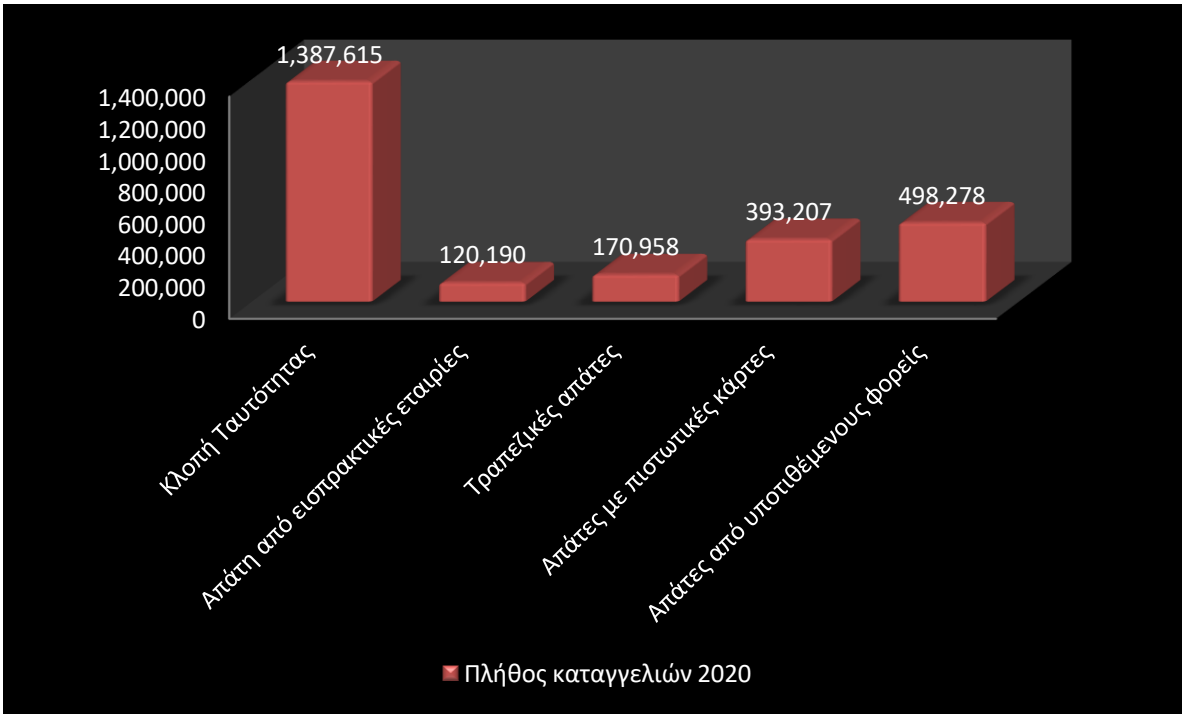


13

Στις αρχές του 2020 ολόκληρη η υφήλιος συγκλονίστηκε από την πανδημία που προκάλεσε η νόσος Covid 19. Η αυξημένη μολυσματικότητα του ιού και η επιτακτική ανάγκη για απομόνωση των κατοίκων προκειμένου να ανακοπεί η εξάπλωσή του έθεσαν σε παύση όλες τις δια ζώσεις συναναστροφές και συναλλαγές των ανθρώπων. Ως μοναδικός τρόπος επίτευξης ορισμένων δραστηριοτήτων, συναλλαγών ακόμα και επαγγελματικών δραστηριοτήτων κατέστη το Διαδίκτυο. Η χρήση του αυξήθηκε ραγδαία από άτομα όλων των ηλικιών και επεκτάθηκε σε τομείς που μέχρι πρότινος δεν υπήρχαν. Οι χρηματικές συναλλαγές και αγορές γίνονταν κατ' αποκλειστικότητα σχεδόν μέσω Διαδικτύου με τη χρήση χρεωστικών ή πιστωτικών καρτών, με τις εγγραφές των πολιτών σε υπηρεσίες e-banking να εκτοξεύονται. Η αύξηση στη χρήση του Διαδικτύου και στις ηλεκτρονικές-οικονομικές συναλλαγές ακολουθήθηκε και από αύξηση σε φαινόμενα απάτης και κλοπής ταυτότητας από επιτήδειους που εκμεταλλευόμενοι τις συνθήκες κατά την περίοδο της πανδημίας επεδίωξαν να πλουτίσουν αποκομίζοντας παράνομο περιουσιακό όφελος από την περιουσία των θυμάτων τους.

Σύμφωνα με την Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ το 2020 υπήρξε μια έκρηξη καταγγελιών οι οποίες έφτασαν τα 4.720.743. Πιο συγκεκριμένα υπήρξαν 1.387.615 καταγγελίες για κλοπή ταυτότητας, 120.190 για απάτες από εισπρακτικές εταιρίες, 170.958 για τραπεζικές απάτες, 393.207 για απάτες με πιστωτικές κάρτες και τέλος 498.278 για απάτες από υποτιθέμενους φορείς. Παρατηρούμε, λοιπόν, πως η απάτη με κλοπή ταυτότητας αποτελεί κατ' αυτή την περίοδο τον δημοφιλέστερο τρόπο εξαπάτησης των πολιτών. Αυτό δικαιολογείται από το γεγονός πως οι πολίτες κατά την περίοδο της πανδημίας χρησιμοποιούσαν αποκλειστικά για τις συναλλαγές τους ηλεκτρονικό χρήμα ή τις υπηρεσίες ebanking, με αποτέλεσμα τα στοιχεία της χρεωστικής τους κάρτας ή οι κωδικοί πρόσβασης της υπηρεσίας ebanking να μπορούν εύκολα να υποκλαπούν και να χρησιμοποιηθούν χωρίς άδεια του νόμιμου κατόχου. Δεύτερη δημοφιλέστερη μορφή απάτης είναι η απάτη από υποτιθέμενους φορείς όπως άτομα που προσποιούνται το Κράτος και αποστέλλουν ψεύτικα emails για ηλεκτρονική πληρωμή φόρων ή παρόχους τηλεπικοινωνιών, ρεύματος και άλλων υπηρεσιών (για ηλεκτρονική πληρωμή των λογαριασμών). Τα emails που αποστέλλουν οι δράστες μοιάζουν πανομοιότυπα με αυτά που αποστέλλουν οι πραγματικοί φορείς, με αποτέλεσμα το χρηματικό ποσό που

κατατίθεται στον κωδικό πληρωμής να καταλήγει σε τραπεζικό λογαριασμό των δραστών και να μην αντιστοιχεί σε πληρωμή λογαριασμού.



14

Όσον αφορά τα ηλικιακά γκρουπ των θυμάτων, παρατηρούμε πως και το 2020 οι δράστες στοχεύουν περισσότερο σε άτομα μέσης ηλικίας 60-69 καθώς αντιστοιχούν σε ποσοστό 18%. Ακολουθεί το ηλικιακό γκρουπ των 30-39 ετών σε ποσοστό 17%, το γκρουπ 50-59 έτη σε ποσοστό 16% και τελευταίο βρίσκεται για ευνόητους λόγους το νεότερο ηλικιακό γκρουπ 20-29 έτη σε ποσοστό 14%.

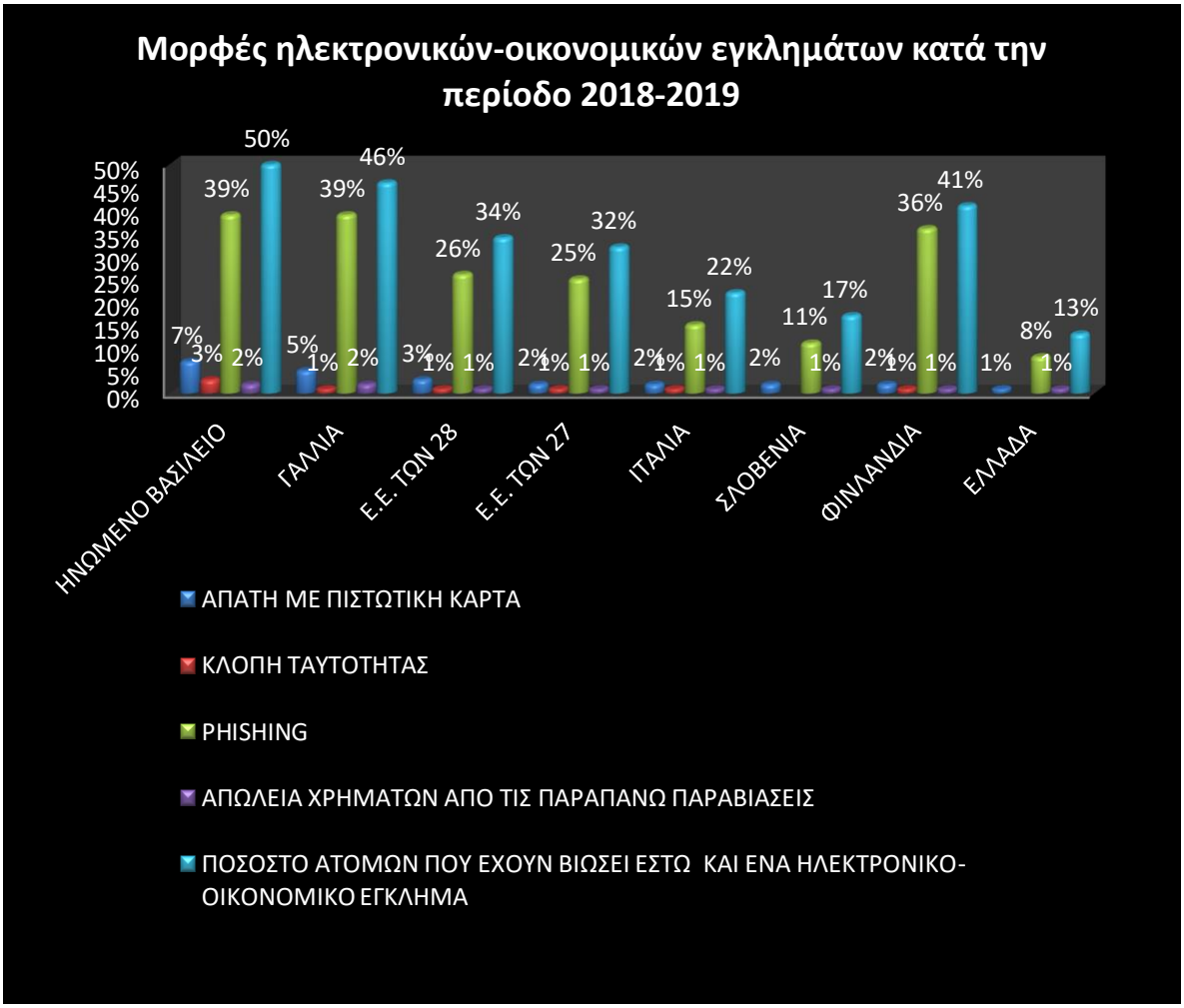
6.2)Η εμφάνιση των ηλεκτρονικών –οικονομικών εγκλημάτων στην Ευρώπη

Για την Ευρώπη, όπως και για τις ΗΠΑ, η απάτη μέσω Διαδικτύου δεν είναι ένα πρωτόγνωρο φαινόμενο. Η χρήση του Διαδικτύου είναι εξίσου διαδεδομένη και συχνή με αποτέλεσμα και οι κίνδυνοί του να είναι αυξημένοι.

Σύμφωνα με έρευνα της Κομισιόν για τις απάτες που έχουν βιώσει οι καταναλωτές το χρονικό διάστημα 2018-2019, στην οποία έλαβαν μέρος 171.000 πολίτες, το 56% των Ευρωπαίων βίωσε κατ' αυτό το χρονικό διάστημα κάποια μορφή απάτης. Το 39% των Ευρωπαίων έπεσε θύμα χρηματικής απάτης καθιστώντας την τη πιο συνήθη μορφή απάτης γι' αυτή τη διετία, ενώ δεύτερη έρχεται η απάτη με κλοπή ταυτότητας σε ποσοστό 33%.

ΠΗΓΗ: focusonbusiness.eu

Στο παρακάτω διάγραμμα παρατηρούμε τις διάφορες μορφές ηλεκτρονικών-οικονομικών εγκλημάτων που έχουν εντοπιστεί σε ορισμένες ευρωπαϊκές χώρες κατ' αυτή τη διετία και σε τι ποσοστό.



15

Παρατηρούμε πως η πιο συνηθισμένη μορφή απάτης είναι η απάτη με πιστωτική κάρτα. Το γεγονός αυτό δηλώνει, αφενός, πως υπάρχει μια προτίμηση των πολιτών στη χρήση ηλεκτρονικού χρήματος για τις συναλλαγές τους κι αφετέρου, ότι υπάρχει κάποιο κενό ασφαλείας κατά τη χρήση πιστωτικών καρτών, που να δικαιολογεί το ύψος των απατών που τελούνται. Έπεται το φαινόμενο phishing το οποίο στην πλειονότητά του τελείται μέσω email. Ένα από τα χαρακτηριστικότερα παραδείγματα phishing, που εμφανίστηκαν τα τελευταία έτη, είναι το παράδειγμα του πλούσιου Νιγηριανού πρίγκιπα ο οποίος μέσω email ζητούσε από τα υποψήφια θύματά του να του καταθέσουν ένα χρηματικό ποσό ώστε να αποπληρώσει τα διαδικαστικά για την αποδοχή κληρονομιάς του. Υποσχόταν ότι θα τους δώσει ως αντάλλαγμα ένα μεγάλο χρηματικό ποσό μόλις λάμβανε την κληρονομιά.

Φυσικά αυτό δεν συνέβη ποτέ, με αποτέλεσμα τα θύματα να χάνουν το χρηματικό ποσό που του είχαν καταθέσει.[25]

Το μέσο που χρησιμοποιήθηκε για την προσέγγιση των υποψηφίων θυμάτων ήταν το email στο ήμισυ σχεδόν των περιπτώσεων (49%), το τηλέφωνο σε ποσοστό 39%και οι υπόλοιπες μορφές επικοινωνίας σε ποσοστό 12%.

Σύμφωνα με την έρευνα το 25% των Ευρωπαίων που εκτέθηκαν σε κάποια μορφή απάτης έχουν υποστεί οικονομική βλάβη, η οποία ανέρχεται συνολικά στα 24 δις € γι' αυτή τη διετία .

Η περίοδος της πανδημίας λόγω του Covid 19 προκάλεσε σημαντική αλλαγή και εγκληματική καινοτομία στον τομέα του εγκλήματος στον Κυβερνοχώρο. Οι εγκληματίες επινόησαν νέες τεχνικές και προσάρμοσαν αντίστοιχα τη δράση τους και τις ομάδες θυμάτων τους εκμεταλλευόμενοι τη νέα κατάσταση. Σύμφωνα με την Έκθεση για Κλοπή Ταυτότητας το 2020, η κλοπή ταυτότητας αυξήθηκε κατά 41% τους τελευταίους 12 μήνες . Ο αντίστοιχος δείκτης έφτασε στο 5.8% συγκριτικά με το 4.1% του προηγούμενου έτους. Κατά τη Europol, η απάτη λόγω των συγκεκριμένων συνθηκών, έχει γίνει πλέον παράλληληπηγή εσόδων για τους δράστες.[26]

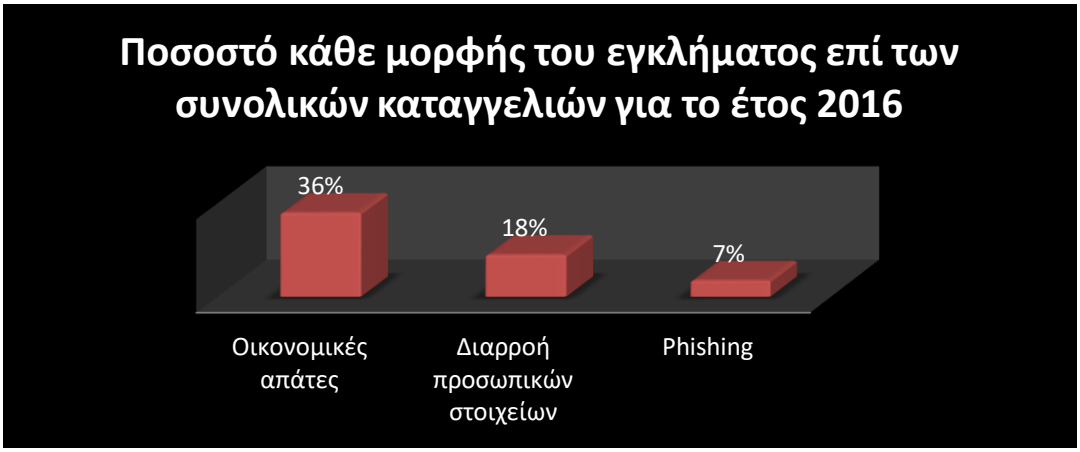
6.3)Η εμφάνιση των ηλεκτρονικών –οικονομικών εγκλημάτων στην Ελλάδα

Η χώρα μας δεν αποτελεί εξαίρεση στον κανόνα της εμφάνισης ηλεκτρονικών-οικονομικών εγκλημάτων. Αυτή, όπως οι ΗΠΑ και οι λοιπές χώρες της Ευρώπης, μετρά με τη σειρά της θύματα ηλεκτρονικών-οικονομικών επιθέσεων αλλά και απώλειες χρηματικών ποσών.

Σύμφωνα με τα ετήσια στατιστικά στοιχεία της SafeLine.gr, το 2016 έγιναν συνολικά 3.812 καταγγελίες για παραβιάσεις ασφαλείας στο Διαδίκτυο. Το 36% αυτών αφορούσε

[25] Ιστότοπος: https://www.phishing.org/phishing-examples
[26] Ιστότοπος: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

οικονομικές απάτες, το 18% διαρροή προσωπικών δεδομένων και το 7% φαινόμενα phishing.[27]



16

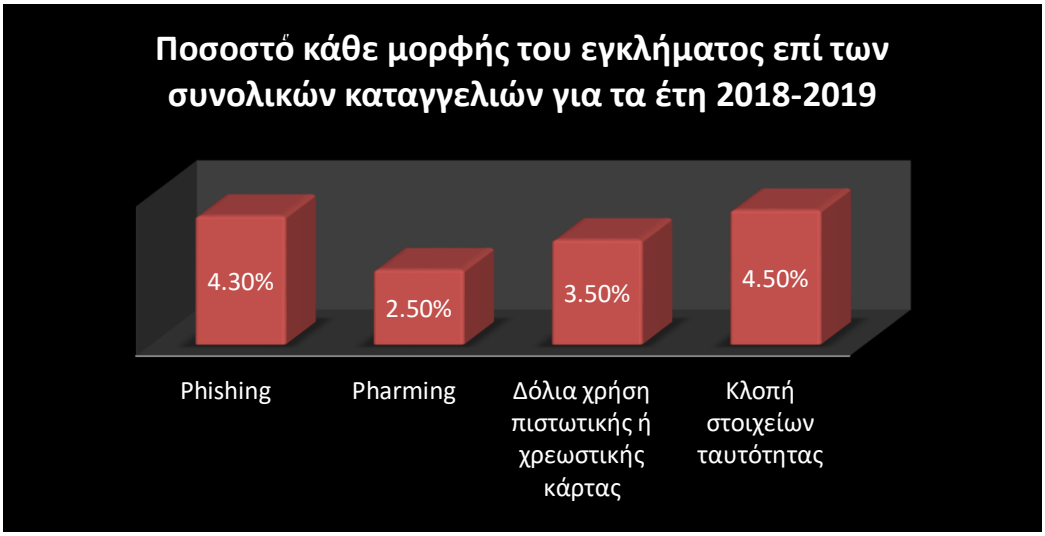
Το διάστημα 2018-2019, 2 στα 10 άτομα που χρησιμοποιούσαν το διαδίκτυο αντιμετώπισαν κάποιο πρόβλημα ασφαλείας.

Από αυτά το 4,3% έπεσε θύμα phishing, το 2,5% θύμα pharming, το 3,5% θύμα δόλιας χρήσης πιστωτικής ή χρεωστικής κάρτας και το 4,5% θύμα κλοπής στοιχείων ταυτότητας.

Σύμφωνα με στοιχεία της ΕΛΣΤΑΤ[28], 1 στα 100 άτομα που έπεσαν θύμα ενός από τα παραπάνω ηλεκτρονικά οικονομικά εγκλήματα υπέστη και οικονομική ζημία.

[27] Ιστότοπος: https://www.safeline.gr/2016/

[28] Ιστότοπος: https://www.statistics.gr/el/statistics/pop?p_p_id=com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3_mvcPath=%2Fview_content.jsp&_com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3_assetEntryId=16851454&_com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3_type=document



17

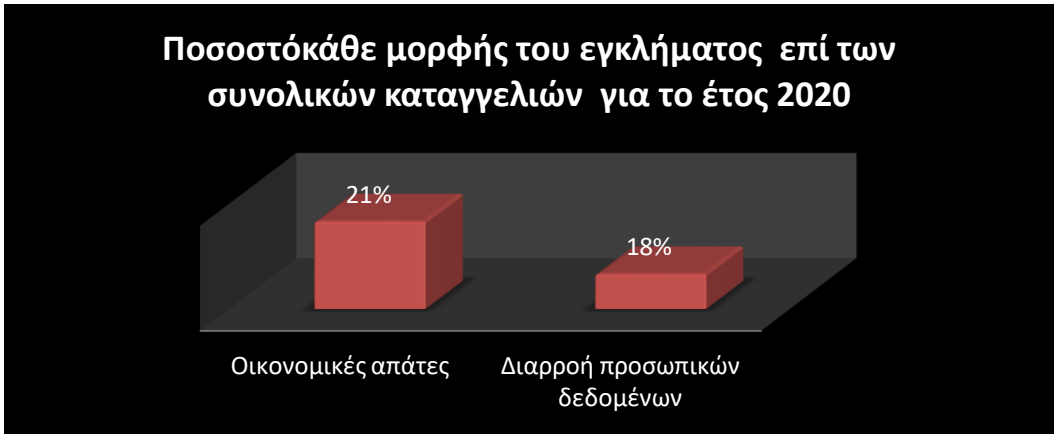
Κατά την έκθεση της safeline.gr[29], παρατηρείται από το 2011 μέχρι και το 2018, όσον αφορά τις ηλεκτρονικές οικονομικές απάτες, μια σταθερή αύξηση με 71 νέες καταγγελίες κατά μ.ό.. το χρόνο και μια γενικότερη αύξηση των καταγγελιών αυτού του φαινομένου κατά 6.3% το χρόνο κατά μέσο όρο.

Αντίστοιχα, για τη διαρροή προσωπικών στοιχείων, παρατηρείται μία μείωση των καταγγελιών από το 2011 μέχρι το 2018 κατά 3,7% κατά μ.ό, δηλαδή περίπου 56 καταγγελίες λιγότερες κατά μέσο όρο.

Το 2020, παρουσιάζεται μια έκρηξη στο ποσοστό καταγγελιών για οικονομικές απάτες ύψους 136%. Η γραμμή safeline[30] δέχτηκε 8.419 καταγγελίες, όπου το 21% αυτών αφορούσε σε οικονομικές απάτες και το 18% σε διαρροή προσωπικών δεδομένων. Η περίοδος αυτή αποτελεί την περίοδο του πρώτου lockdown εξαιτίας της πανδημίας του κορονοϊού, κατά την οποία η κοινωνική αποστασιοποίηση για την αποφυγή διασποράς του Covid -19 οδήγησε σε αύξηση της χρήσης του Διαδικτύου από άτομα όλων των ηλικιών. Σύμφωνα με στοιχεία της ΕΛΣΤΑΤ, το πρώτο τρίμηνο του 2020, χρησιμοποιούσαν σε καθημερινή βάση το Διαδίκτυο 5.246.022 άτομα ηλικίας 16-74 ετών, 730.291 παραπάνω απ' ότι το 2016 σύμφωνα με αντίστοιχη έρευνα. Έτσι, είναι λογικό να εκμεταλλευτούν αυτή την αυξημένη χρήση του Διαδικτύου ορισμένοι επιτήδειοι, προκειμένου να

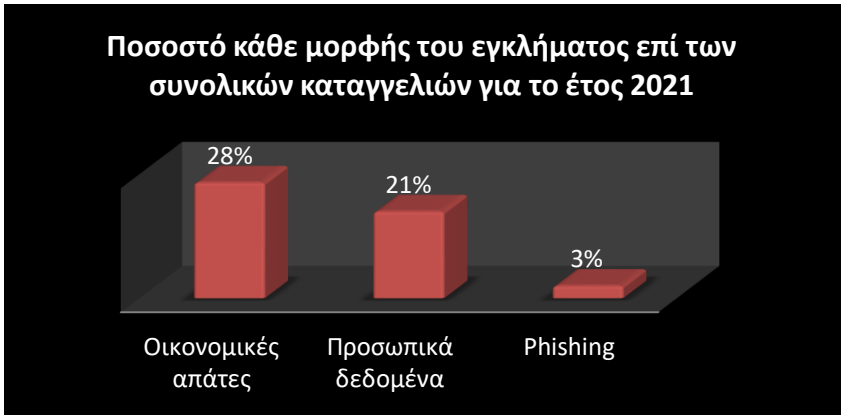
[29] Ιστότοπος: https://www.safeline.gr/2018/
[30] Ιστότοπος: https://www.safeline.gr/statistics2020/

αποκτήσουν παρανόμως περιουσιακό όφελος εξαπατώντας ανίδεους χρήστες του Διαδικτύου.



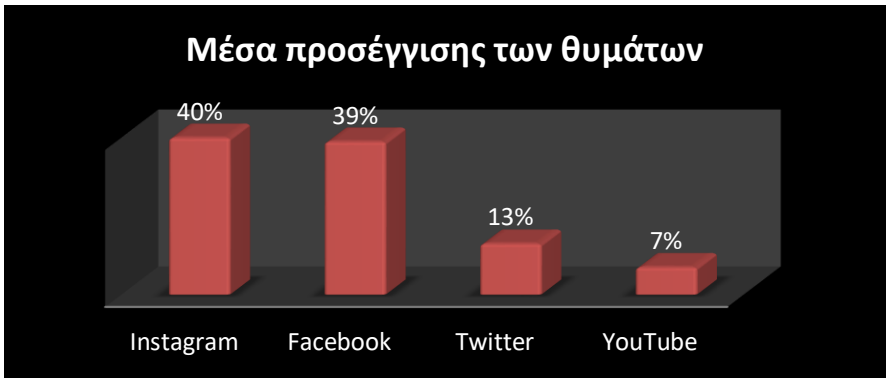
18

Τέλος, το 2021 καταγράφηκαν 8.571 νέες καταγγελίες στη γραμμή Safeline εκ των οποίων το 28% αφορούσε σε οικονομικές απάτες, το 21% σε διαρροή προσωπικών δεδομένων και το 3% σε φαινόμενα Phishing.



19

Η πλειοψηφία των περιστατικών έλαβε χώρα στα μέσα κοινωνικής δικτύωσης και πιο συγκεκριμένα το 40% στο Instagram, το 39% στο Facebook, το 13% στο Twitter και τέλος το 7% στο YouTube.[31]



20

7)ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

Τα ηλεκτρονικά οικονομικά εγκλήματα αποτελούν ένα σύγχρονο φαινόμενο που, όπως φαίνεται, πρόκειται να απασχολήσει σημαντικά την κοινωνία τα επόμενα χρόνια. Η αντιμετώπισή τους από νομικής άποψης δεν αποτελεί μία εύκολη διαδικασία. Πολλά από τα θύματα δεν καταγγέλλουν τα περιστατικά ή αν τα καταγγείλουν δεν υπάρχουν οι κατάλληλοι υπάλληλοι στους αρμόδιους φορείς ώστε να εξετάσουν και να φέρουν εις πέρας μια τέτοια καταγγελία. Συχνά δεν υπάρχουν και τα απαραίτητα αποδεικτικά στοιχεία, καθώς τα ψηφιακά ίχνη δεν επαρκούν για την εξιχνίαση του εγκλήματος. Επίσης, ακόμα κι αν εντοπιστούν τα ψηφιακά ίχνη του δράστη, πάλι είναι δυνατόν να υπάρξουν δυσκολίες στη δίωξη του εγκλήματος για θέματα που αφορούν στην ύπαρξη δόλου, στην έλλειψη μαρτύρων και άλλων ενοχοποιητικών στοιχείων. Όλα αυτά τα γεγονότα αποτελούν παράγοντα που δυσχεραίνει την αντιμετώπιση του φαινομένου.

[31] Ιστότοπος: https://www.safeline.gr/statistics-17-21/

Τόσο τα κράτη όσο και οι ίδιοι οι πολίτες δεν πρέπει να μένουν άπραγοι απέναντι στα ηλεκτρονικά οικονομικά εγκλήματα, ακόμα κι αν είναι δύσκολη η αντιμετώπισή τους. Σε προσωπικό επίπεδο, οι χρήστες του Διαδικτύου οφείλουν να είναι ιδιαίτερα προσεκτικοί κατά την περιήγησή τους σε αυτό και τη διενέργεια συναλλαγών. Πιο συγκεκριμένα, θα πρέπει να διατηρούν ενημερωμένα τα προγράμματα που έχουν εγκατεστημένα στις ηλεκτρονικές συσκευές τους, ιδίως τα προγράμματα περιήγησης στο Διαδίκτυο και τα προγράμματα προστασίας από ιούς και απειλές. Παράλληλα, είναι απαραίτητη η αλλαγή σε τακτά χρονικά διαστήματα των κωδικών πρόσβασης σε διάφορους λογαριασμούς και δη στους λογαριασμούς ebanking, ώστε να καθίσταται δυσχερέστερη η υποκλοπή τους. Μερικά από τα μέτρα που μπορούν να εφαρμόσουν οι χρήστες του Διαδικτύου και έχουν αποδειχθεί αποτελεσματικά είναι τα εξής:

1. Η συχνή δημιουργία αντιγράφων ασφαλείας των αρχείων τους, τόσο του Η/Υ όσο και του smartphone, ώστε σε περίπτωση υποκλοπής ή καταστροφής τους από ιούς να είναι πάντα διαθέσιμα στο χρήστη.
2. Η αποφυγή ανοίγματος μηνυμάτων ηλεκτρονικού ταχυδρομείου από άγνωστους ή ύποπτους αποστολείς και κυρίως υπερσυνδέσμων (links) που παραπέμπουν σε πληρωμές λογαριασμών ή μη έμπιστες ιστοσελίδες.
3. Η αποφυγή εισαγωγής κωδικών πρόσβασης εφαρμογών ebanking σε μη έμπιστες ιστοσελίδες, καθώς και η αποφυγή κοινοποίησης των στοιχείων της χρεωστικής/πιστωτικής κάρτας σε άγνωστους και μη έμπιστους φορείς/πρόσωπα.
4. Η χρήση επιπλέον σταδίων ασφαλείας κατά τη διενέργεια ηλεκτρονικών συναλλαγών με την ανέπαφη χρήση χρεωστικής/πιστωτικής κάρτας, όπως αποστολή μηνύματος για έγκριση της συναλλαγής από το χρήστη, ώστε να αποφευχθεί ο κίνδυνος μη εξουσιοδοτημένων συναλλαγών.

Αυτά αποτελούν μερικά μόνο από τα μέτρα πρόληψης που μπορούν να λάβουν οι χρήστες του Διαδικτύου, ώστε να προστατέψουν την περιουσία τους από τις δόλιες ενέργειες των κυβερνοεγκληματιών. Για την αντιμετώπιση του φαινομένου, όμως, δεν αρκεί μόνο η δράση σε ατομικό επίπεδο. Δεδομένου ότι τα ηλεκτρονικά οικονομικά εγκλήματα μπορεί να έχουν και διασυνοριακό χαρακτήρα, είναι απαραίτητη και η λήψη κατάλληλων μέτρων πρόληψης και αντιμετώπισης από τα ίδια τα κράτη.Η Ευρωπαϊκή Ένωση επέδειξε ιδιαίτερη ευαισθησία στο θέμα αυτό και έλαβε δράση. Με

την απόφαση 276/1999/ΕΚ του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου θεσμοθετήθηκε το κοινοτικό πρόγραμμα «SaferInternet», που αφορούσε στην προώθηση ενός ασφαλέστερου Διαδικτύου. Με το πρόγραμμα αυτό:

1. Δημιουργήθηκαν κατάλληλες δομές ώστε να λαμβάνουν καταγγελίες πολιτών σχετικά με ηλεκτρονικά εγκλήματα, πλαισιωμένες από το κατάλληλο προσωπικό που θα ήταν σε θέση να εξετάσει και να διεκπεραιώσει αυτές τις καταγγελίες.
2. Προωθήθηκαν καμπάνιες ενημέρωσης των πολιτών που αφορούσαν στους σύγχρονους κινδύνους που ενέχει η χρήση του Διαδικτύου με την αλματώδη αύξηση των χρηστών του. Ιδιαίτερα διενεργήθηκαν και εκπαιδευτικά προγράμματα ενημέρωσης γονέων και μαθητών για την ασφαλή περιήγηση των ανηλίκων σε αυτό.

Έπειτα, συνδυαστικά με το παραπάνω κοινοτικό πρόγραμμα, δημιουργήθηκε βάσει της Απόφασης 854/2005/ΕΚ ακόμα ένα κοινοτικό πρόγραμμα που επίσης είχε ως στόχο την προώθηση της πιο ασφαλούς χρήσης του Διαδικτύου. Σε αυτό προβλεπόταν η δημιουργία υποστηρικτικής γραμμής για καταγγελίες πολιτών σχετικά με κυβερνοεγκλήματα, οι οποίες εν συνεχεία θα αποστέλλονταν στους αρμόδιους φορείς για να τις διεκπεραιώσουν. Λόγω της αύξησης των παραβιάσεων ασφαλείας στις ηλεκτρονικές συναλλαγές, στις 14 Σεπτεμβρίου 2019 τέθηκε σε ισχύ ο Κανονισμός της Ευρωπαϊκής Ένωσης, με τον οποίο εξειδικεύτηκαν ορισμένες διατάξεις της Οδηγίας (ΕΕ) 2015/2366 «για τις υπηρεσίες πληρωμών» (PSD 2). Έτσι, με τον κανονισμό αυτό καθιερώθηκε, μεταξύ άλλων, η απαίτηση ισχυρής ταυτοποίησης των κατόχων των χρεωστικών/πιστωτικών καρτών κατά την ανέπαφη χρήση τους σε ηλεκτρονικές αγορές/συναλλαγές (e-commerce). Επομένως, για την αποφυγή δολίων συναλλαγών, απαιτείται πλέον και η έγκριση της συναλλαγής από τον κάτοχο της κάρτας κατά την αναδρομολόγησή του στο ασφαλές ηλεκτρονικό περιβάλλον πληρωμών του τραπεζικού ιδρύματος ή του εμπόρου. [32]

Εκτός από τις ευρωπαϊκές πρωτοβουλίες για την αντιμετώπιση του ζητήματος, έχουν ληφθεί και σε εθνικό επίπεδο δραστικά μέτρα για την αντιμετώπιση και πρόληψη των ηλεκτρονικών οικονομικών εγκλημάτων. Τα κράτη μεριμνούν για την αναβάθμιση του

[32] Ιστότοπος: https://www.hba.gr/Media/Details/397

ηλεκτρονικού εξοπλισμού τους με τα πιο σύγχρονα λογισμικά προστασίας από κακόβουλες επιθέσεις και αναγνώρισης απειλών και προωθούν καμπάνιες ενημέρωσης των πολιτών για τις απειλές αυτές και τον τρόπο αντιμετώπισής τους.

Καθοριστικό ρόλο στην ανωτέρω προσπάθεια διαδραματίζει η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας. Η ίδρυσή της προβλέφθηκε με το Π.Δ. 178/2014 και η αποστολή της περιλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Παράλληλα με την καταπολέμηση του ηλεκτρονικού εγκλήματος υλοποιεί και καινοτόμες δράσεις για την πρόληψη του φαινομένου, όπως ημερίδες ασφαλούς πλοήγησης στο Διαδίκτυο, τηλεδιασκέψεις, καθώς και ενημερωτικές επισκέψεις σε σχολεία για την πληροφόρηση γονέων και μαθητών σχετικά με τα ηλεκτρονικά οικονομικά εγκλήματα αλλά και τα κυβερνοεγκλήματα εν γένει.[33]

Χάρη στη δραστηριοποίηση των πολιτών αλλά και των αρμόδιων φορέων, τα εγκλήματα αυτά δεν μένουν ατιμώρητα. Το δεκάμηνο του 2022 καταγράφηκαν 4.005 καταγγελίες για τετελεσμένες απάτες του α. 386ΠΚ και 438 απόπειρες, από τις οποίες εξιχνιάστηκαν 1.476 υποθέσεις. Αντίστοιχα, καταγράφηκαν 4.912 καταγγελίες για τετελεσμένη απάτη με υπολογιστή $386^{α}$ ΠΚ και 384 απόπειρες, εκ των οποίων εξιχνιάστηκαν μόνο 755 υποθέσεις.[34] Η πρόοδος που συντελείται στην εξιχνίαση αυτών των εγκλημάτων είναι σημαντική, ωστόσο απαιτείται η λήψη δραστικότερων μέτρων ώστε να περιοριστούν αισθητά τα περιστατικά ηλεκτρονικών οικονομικών εγκλημάτων.

[33] Ιστότοπος: https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/

[34] Ιστότοπος: https://www.naftemporiki.gr/finance/economy/1414927/rekor-stis-ilektronikes-apates-efere-o-koronoios/

8) ΣΥΜΠΕΡΑΣΜΑΤΑ

Είναι εμφανές πως τα ηλεκτρονικά-οικονομικά εγκλήματα αποτελούν ένα καθημερινό πρόβλημα της σύγχρονης ζωής κι όχι απλά μια διάταξη νόμου τυπωμένη σε κάποιον ποινικό κώδικα. Όπως προκύπτει από τα στατιστικά στοιχεία που παρατέθηκαν παραπάνω, οι απάτες με και μέσω υπολογιστή δεν αποτελούν πρωτοεμφανιζόμενο φαινόμενο. Συνοδεύουν την εξέλιξη του Διαδικτύου και των πληροφοριακών συστημάτων και γίνονται τόσο πολύπλοκες όσο και αυτά. Ωστόσο, παράλληλα με αυτές, εξελίσσεται και αναβαθμίζεται και η ασφάλεια του Διαδικτύου. Καθώς οι ανάγκες και οι απειλές της εποχής αυξάνονται, όλο και περισσότερες προσωπικές πληροφορίες και στοιχεία χρηστών του Διαδικτύου χρήζουν προστασίας. Οι πολιτικές ασφαλείας των ηλεκτρονικών συστημάτων ανανεώνονται και εκσυγχρονίζονται συνεχώς τόσο σε τεχνικό όσο και σε νομοθετικό επίπεδο προκειμένου να πληρούν τις απαραίτητες προϋποθέσεις για την ασφάλεια των πολιτών κατά τη χρήση των ηλεκτρονικών υπολογιστών. Και πάλι όμως η ηλεκτρονική εγκληματικότητα τείνει να αυξάνεται και να παίρνει νέες μορφές, προσαρμοζόμενη στα δεδομένα της εκάστοτε εποχής. Η σύγχρονη εποχή χαρακτηρίζεται από τη χρήση πλαστικού χρήματος, ηλεκτρονικής τραπεζικής και αγορών μέσω διαδικτύου. Τους τομείς αυτούς στοχεύουν να βλάψουν και οι ηλεκτρονικοί εγκληματίες ώστε να αποκομίσουν εύκολα και γρήγορα προσωπικό οικονομικό όφελος. Τα στατιστικά στοιχεία που παρουσιάστηκαν εκτενώς παραπάνω, τόσο για τις ΗΠΑ, όσο και την Ευρώπη, αποδεικνύουν πως το φαινόμενο αυτό είναι διεθνές και παρουσιάζει έντονα διασυνοριακά στοιχεία εξαιτίας της παγκοσμιοποίησης των συναλλαγών.

Η έρευνα των στατιστικών στοιχείων για τις μορφές εμφάνισης των ηλεκτρονικών-οικονομικών εγκλημάτων αλλά και των ποσοστών εμφάνισής τους διακρίθηκε χρονολογικά σε δύο μέρη, στην προ Covid-19 και στη Covid-19 περίοδο. Η κατάτμηση αυτή των χρονικών περιόδων βασίστηκε στο γεγονός, πως λόγω της κοινωνικής απομόνωσης και της απαγόρευσης κυκλοφορίας που εφαρμόστηκε ως καθολικό μέτρο για την αποφυγή διασποράς του κορονοϊού, το Διαδίκτυο αποτελούσε το μοναδικό τρόπο για να εκπληρώσουν τις υποχρεώσεις τους οι πολίτες. Καθημερινά, όλο και περισσότεροι άνθρωποι, όλων των ηλικιών, έρχονταν αναγκαστικά σε επαφή με το Διαδίκτυο για την εργασία τους, για το σχολείο, για την επικοινωνία, για τη διευθέτηση υποχρεώσεων.

Κάποια από αυτά τα άτομα, ιδίως τα άτομα μεγαλύτερης ηλικίας, δεν διέθεταν γνώσεις χρήσης ηλεκτρονικού υπολογιστή, ωστόσο οι νέες συνθήκες κατέστησαν αναγκαία την απόκτηση έστω των στοιχειωδών. Η χρήση του Διαδικτύου, λοιπόν, χωρίς τις απαραίτητες δεξιότητες, και επομένως χωρίς την αντίληψη των κινδύνων που ενέχει, οδήγησε στην εκμετάλλευση αυτής της κατάστασης από άτομα που επεδίωκαν να αποκομίσουν αναίμακτα και παράνομα οικονομικό όφελος σε βάρος άλλων.

Μέρα με τη μέρα, όλο και περισσότερα άτομα ηλικίας 49-69 ετών έπεφταν θύματα κάποιας μορφής διαδικτυακής απάτης, όπως phishing mails, αναδρομολόγηση σε ψευδείς ιστοσελίδεςαλλά και κλοπή στοιχείων ταυτότητας. Παρατηρήθηκε, πως η πλειοψηφία των χρηστών του Διαδικτύου στην Αμερική έπεσε θύμα κλοπής στοιχείων ταυτότητας και απάτης από υποτιθέμενους φορείς. Αντίστοιχα, στην Ευρώπη, η πλειοψηφία των χρηστών του Διαδικτύου σύμφωνα με τα στατιστικά στοιχεία έπεσε θύμα απάτης με πιστωτική κάρτα και Phishing. Τέλος, στην Ελλάδα, τη μεγαλύτερη απήχηση εμφανίζουν το φαινόμενο Phishing και η κλοπή στοιχείων ταυτότητας, όπως κωδικών πρόσβασης σε υπηρεσίες ebanking. Η εφευρετικότητα των δραστών σχετικά με τους τρόπους εξαπάτησης των χρηστών είναι απεριόριστη. Μέρα με τη μέρα, εμφανίζονται νέες τεχνικές εξαπάτησης των χρηστών, ιδίως με το περιεχόμενο των phishing emails ή την απάτη από υποτιθέμενους φορείς. Οι δράστες, περιορίζοντας τα λάθη και τις απροσεξίες τους, δημιουργούν με κάθε λεπτομέρεια ένα απόλυτα αληθοφανές περιβάλλον, με αποτέλεσμα το υποψήφιο θύμα να μην βρίσκεται σε θέση να διακρίνει το αναξιόπιστο του αποστολέα και το ψευδές του περιεχομένου. Έτσι, όλο και περισσότεροι χρήστες του Διαδικτύου μετατρέπονται σε θύματα τέτοιων μορφών εξαπάτησης, βιώνοντας παράλληλα και περιουσιακή ζημία.

Ακόμα και μετά την Covid-19 περίοδο, δηλαδή το χρονικό διάστημα μετά την άρση των πολύμηνων lockdowns, η χρήση του Διαδικτύου εξακολουθεί να είναι εκτεταμένη κι επεκτείνεται σε όλο και περισσότερους τομείς της καθημερινής ζωής. Το γεγονός αυτό συνεπάγεται και αύξηση των ηλεκτρονικών-οικονομικών εγκλημάτων που λαμβάνουν χώρα καθημερινά. Σύμφωνα με ρεπορτάζ της ιστοσελίδας ertnews.gr[35]και στοιχεία της ελληνικής αστυνομίας, τους τελευταίους οκτώ μήνες του 2022, έλαβαν χώρα 4.260 νέα

[35] Ιστότοπος: https://www.ertnews.gr/eidiseis/mono-sto-ertgr/ekrixi-stis-ilektronikes-apates-me-4-018-ypotheseis-to-2022-odigos-prostasias/

περιστατικά ηλεκτρονικής απάτης, ξεπερνώντας τα περιστατικά που είχαν καταγραφεί το 2021.

Είναι, λοιπόν, εμφανές πως ενώ εξελίσσεται και εμπλουτίζεται όλο και περισσότερο η ασφάλεια του Διαδικτύου με ειδικά λογισμικά και προγράμματα ανίχνευσης νέων απειλών, εντούτοις αυτό δεν αρκεί από μόνο του ώστε να περιοριστούν τα ηλεκτρονικά οικονομικά εγκλήματα. Η εφευρετικότητα των δραστών έχει φτάσει σε τέτοιο επίπεδο όπου η εκτεταμένη προσοχή και καχυποψία των χρηστών του Διαδικτύου είναι αναγκαία. Απαιτείται, λοιπόν, προσοχή όταν τους ζητείται η πληκτρολόγηση ή παροχή κωδικών πρόσβασης ebanking, στοιχείων χρεωστικής και πιστωτικής κάρτας, η είσοδος σε υπερσύνδεσμο όπου η μορφή του URL φαίνεται ύποπτη κτλ. Η κριτική σκέψη των χρηστών του Διαδικτύου αποτελεί καταλυτικής σημασίας εργαλείο για την καταπολέμηση του ηλεκτρονικού οικονομικού εγκλήματος.

Γι' αυτό το λόγο, είναι σημαντική η ενημέρωση για τους τρόπους εξαπάτησης που εμφανίζονται στο Διαδίκτυο και για τους τρόπους που θα μπορούν να ξεχωρίσουν πότε κάποια ενέργεια προέρχεται από πιστοποιημένο φορέα ή πρόσωπο. Η συχνή αλλαγή των κωδικών πρόσβασης τόσο του ebanking όσο και των πιστωτικών/χρεωστικών καρτών κρίνεται αναγκαία, ώστε να καθίσταται δυσχερής η υποκλοπή τους κατά τις ηλεκτρονικές συναλλαγές. Επίσης, οι χρήστες οφείλουν να ελέγχουν λεπτομερώς τα μηνύματα ηλεκτρονικού ταχυδρομείου όταν φαίνεται πως έχουν σταλεί από κάποιο χρηματοπιστωτικό ίδρυμα ή δημόσιο φορέα ή φαινομενικά υπαρκτό πρόσωπο και ζητείται η πληρωμή χρηματικού ποσού ή η είσοδος σε κάποιο link. Σε αυτή την περίπτωση, συνήθως, υπάρχουν τυπογραφικά ή συντακτικά λάθη τόσο στη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα όσο και στο σώμα του email, αποδεικνύοντας πως δεν έχει αποσταλεί από το φορέα που δηλώνει. Τέλος, η άμεση ενημέρωση της αρμόδιας αρχής καταπολέμησης ηλεκτρονικού εγκλήματος αποτελεί απαραίτητη προϋπόθεση ώστε να ξεκινήσει η διαδικασία εντοπισμού και σύλληψης των δραστών, εφόσον κάποιος χρήστης έχει πέσει θύμα ηλεκτρονικού οικονομικού εγκλήματος, ανεξάρτητα αν τελικά επήλθε ή όχι περιουσιακή ζημία από την απατηλή ενέργεια.

8)ΕΠΙΛΟΓΟΣ

Με την ανωτέρω ανάλυση δόθηκε μια ευρύτερη εικόνα των ηλεκτρονικών οικονομικών εγκλημάτων τόσο από τη σκοπιά της νομικής όσο και από τη σκοπιά της οικονομικής επιστήμης. Κατά τη νομική ανάλυση του φαινομένου δόθηκε ένας ευρέως αποδεκτά ορισμός για την έννοια των ηλεκτρονικών-οικονομικών εγκλημάτων αλλά και για το νομικό χαρακτηρισμό τους βάσει του εννόμου αγαθού που προσβάλλουν. Στη συνέχεια παρουσιάστηκαν συγκριτικά τα δύο βασικότερα διεθνή κείμενα που αφορούν στο ηλεκτρονικό έγκλημα, η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Σύμβαση της Βουδαπέστης) και οι Ευρωπαϊκές Οδηγίες 2013/40/ΕΕ και 2019/713/ΕΕ πάνω στις οποίες στηρίχθηκε η ελληνική νομοθεσία τόσο με το Ν.4411/2016 όσο και με το νέο Ποινικό Κώδικα Ν.4619/2019. Αναπτύχθηκαν σε βάθος τα αδικήματα της απάτης με υπολογιστή 386^{A} ΠΚ και της απάτης μέσω υπολογιστή 386ΠΚ καθώς και οι ποινές που αυτά επισύρουν. Περαιτέρω, δόθηκαν και αναλυτικά παραδείγματα απάτης με και μέσω υπολογιστή που λαμβάνουν χώρα καθημερινώς και προσβάλλουν το έννομο αγαθό της περιουσίας των θυμάτων και καθώς και η ποινική τους αντιμετώπιση ανάλογα με τη νομική τους φύση.

Όσον αφορά την οικονομική ανάλυση του φαινομένου, εκτέθηκαν το επιδιωκόμενο αποτέλεσμα, τα κίνητρα και το προφίλ των δραστών των ηλεκτρονικών-οικονομικών εγκλημάτων, με εξειδίκευση στις γενικότερες θεωρίες για τη συμπεριφορά και τα κίνητρα του εγκληματία. Παράλληλα, έγινε και μια συνοπτική αναφορά στο κοινωνικό κόστος του ηλεκτρονικού οικονομικού εγκλήματος. Τέλος, παρουσιάστηκαν εκτεταμένα στατιστικά στοιχεία για την εξέλιξη των ηλεκτρονικών εγκλημάτων στις ΗΠΑ, την Ευρώπη και την Ελλάδα κατά τις περιόδους πριν και κατά τη διάρκεια της πανδημίας του Covid-19 κι έγινε συγκριτική ανάλυση των ευρημάτων τόσο μεταξύ των εν λόγω κρατών όσο και μεταξύ των εν λόγω χρονικών περιόδων.

Παρά την ύπαρξη ισχυρών νομοθετικών διατάξεων, τόσο σε εθνικό όσο και διεθνές επίπεδο, το δραστικότερο μέτρο για την αντιμετώπιση του φαινομένου είναι η ενημέρωση και εκπαίδευση των χρηστών του Διαδικτύου για τον εντοπισμό πιθανών απειλών σαν αυτών που παρατέθηκαν παραπάνω, ενημέρωση για την ασφαλή χρήση του Διαδικτύου και των υπολογιστών αλλά και τις ασφαλείς συναλλαγές με χρεωστική/πιστωτική κάρτα και

ebanking. Η γνώση είναι δύναμη και αποτελεί το ισχυρότερο όπλο του ανθρώπου ενάντια στους κινδύνους και τις προκλήσεις της σύγχρονης τεχνολογικής εποχής του Διαδικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ-ΑΡΘΡΟΓΡΑΦΙΑ

- ***Αγγελή Ι.,*** *«Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο», ΠοινΔικ 12/2001*
- ***Αλεξιάδης Στέργιος****, Τα οικονομικά του εγκλήματος, Σάκκουλας, 2010*
- ***Λάζος Γρηγόρης*** *(2013)*
- ***Μαργαρίτης Μιχαήλ*** *, Ποινικός Κώδικας, ερμηνεία-εφαρμογή 2ηέκδοση,ΣΑΚΚΟΥΛΑΣ Π.Ν., 2009*
- ***Νούσκαλης Γ.,****Ποιν. Δικαιοσύνη, 2/2003 (Έτος 6ο)*
- ***Παπαδαμάκης Α.,*** *Τα περιουσιακά εγκλήματα, 2000, εκδ. Α.Ν. Σάκκουλα*
- ***Ρεπούσης Σπυρίδων****, Χρηματοοικονομική απάτη και διαφθορά, Σάκκουλας, 2010*
- ***Σπυρόπουλος Φ.,*** *Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking), Σάκκουλα Ε.Ε.,2016*
- ***Χαραλαμπάκης Α.,*** *Ποινικός Κώδικας, Ερμηνεία Κατ' άρθρο, Τόμος Δεύτερος, 2011*
- ***Χαραλαμπάκης Α****., Ποινικός Κώδικας, Ερμηνεία Κατ' άρθρο, Τόμος Δεύτερος, 2020*
- ***Δαλακούρας Θεοχάρης****, «Ηλεκτρονικό Έγκλημα», ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2019*

ΞΕΝΟΓΛΩΣΣΗ

- ***Anderson R****, Security Engineering: A guide to building dependable distributed systems, John Wiley & Son Inc.,New York.*
- ***Malekos Smith and Eugenia Lostri, James A. Lewis****, The Hidden Costs of Cybercrime, Zhanna, Project Director, December 2020)*

ΔΙΑΔΙΚΤΥΑΚΗ

- *https://cyberalert.gr/phising/*
- *https://www.techtarget.com/searchsecurity/definition/pharming*
- *https://www.ertnews.gr/eidiseis/mono-sto-ertgr/ekrixi-stis-ilektronikes-apates-me-4-018-ypotheseis-to-2022-odigos-prostasias/*
- *https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020*
- *https://www.phishing.org/phishing-examples*
- *https://www.safeline.gr/2016/*
- *https://www.safeline.gr/2018/*
- *https://www.safeline.gr/statistics-17-21/*
- *https://www.safeline.gr/statistics2020/*
- *https://www.statistics.gr/el/statistics/pop?p_p_id=com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3_mvcPath=%2Fview_content.jsp&_com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3_assetEntryId=16851454&_com_liferay_portal_search_web_portlet_SearchPortlet_INSTANCE_3_type=document*
- *https://www.hba.gr/Media/Details/397*
- *https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/*
- *https://www.naftemporiki.gr/finance/economy/1414927/rekor-stis-ilektronikes-apates-efere-o-koronoios/*

ΝΟΜΟΛΟΓΙΑ

- ***ΑΠ.1726/2019**, ΤΝΠ ΝΟΜΟΣ*
- ***ΑΠ.88/2019**, ΤΝΠ ΝΟΜΟΣ*