

Ελληνικό Ανοικτό Πανεπιστήμιο

ΠΜΣ Τραπεζική & Χρηματοοικονομική Τεχνολογία (Fintech)

Διπλωματική Εργασία

«Απάτες και Κίνδυνοι στις Τραπεζικές Συναλλαγές: Η
περίπτωση χρηματοπιστωτικού ιδρύματος και η εξέλιξη των
φαινομένων από την περίοδο της πανδημίας COVID-19 έως
σήμερα»

«Κωνσταντίνος Σμπυράκος»

Επιβλέπων καθηγητής:

«ΜΠΑΛΙΟΣ ΔΗΜΗΤΡΙΟΣ»

Πάτρα, «Ιούνιος» «2026»

© Ελληνικό Ανοικτό Πανεπιστήμιο, 2025-26

Η παρούσα Εργασία καθώς και τα αποτελέσματα αυτής, αποτελούν συνιδιοκτησία του ΕΑΠ και του φοιτητή, ο καθένας από τους οποίους έχει το δικαίωμα ανεξάρτητης χρήσης, αναπαραγωγής και αναδιανομής τους (στο σύνολο ή τμηματικά) για διδακτικούς και ερευνητικούς σκοπούς, σε κάθε περίπτωση αναφέροντας τον τίτλο και το συγγραφέα της Εργασίας καθώς και το όνομα του ΕΑΠ όπου εκπονήθηκε.

«Απάτες και Κίνδυνοι στις Τραπεζικές Συναλλαγές: Η περίπτωση χρηματοπιστωτικού ιδρύματος και η εξέλιξη των φαινομένων από την περίοδο της πανδημίας COVID-19 έως σήμερα»

«Κωνσταντίνος Σμπυράκος»

Επιτροπή Επίβλεψης Διπλωματικής
Εργασίας

Α΄ Επιβλέπων Καθηγητής:
«ΜΠΑΛΙΟΣ ΔΗΜΗΤΡΙΟΣ»
«Ελληνικό Ανοικτό Πανεπιστήμιο»

Β΄ Επιβλέπων Καθηγητής:
«ΜΑΝΔΗΛΑΣ ΑΘΑΝΑΣΙΟΣ»
«Ελληνικό Ανοικτό Πανεπιστήμιο»

Πάτρα, «Ιούνιος» «2026»

Ευχαριστίες.

Με το παρόν θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου κ. Δημήτριο Μπάλιο για την επιστημονική καθοδήγηση και ενθάρρυνσή του, κατά τη διάρκεια εκπόνησης της παρούσας διπλωματικής μεταπτυχιακής εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τη Διευθύντρια μου και τον Αντιπρόεδρο της NBGPAY (Εθνικής Τράπεζας της Ελλάδος-Global Payments) κ. Δεδε Ναταλία & κ. Παπαδόπουλο Αντίγονο που με χαρά συναίνεσαν στη διεξαγωγή της έρευνας και στη βοήθεια συλλογής αρκετών τραπεζικών δεδομένων, παρόλο των αυστηρών δικλίδων ασφάλειας.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και την Σοφία που στάθηκαν δίπλα μου και ήταν αρωγοί σε αυτή την σημαντική προσπάθεια.

ΠΕΡΙΛΗΨΗ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η παρούσα διπλωματική εργασία εξετάζει το φαινόμενο του χρηματοοικονομικού ρίσκου και των περιστατικών απάτης που εμφανίζονται στις τραπεζικές συναλλαγές, με έμφαση στις ψηφιακές πληρωμές και στα σύγχρονα ηλεκτρονικά συστήματα διαχείρισής τους. Αρχικά, παρουσιάζεται το θεωρητικό υπόβαθρο που αφορά τους τρόπους με τους οποίους μπορεί να προκύψει ρίσκο ή να εκδηλωθεί μια μορφή απάτης σε συναλλαγές μεγάλου οικονομικού ύψους, καθώς και οι γενικότερες κατηγορίες απατών που συναντώνται στον τραπεζικό τομέα. Στο πλαίσιο αυτό αναλύονται οι κίνδυνοι που αντιμετωπίζουν οι κάτοχοι καρτών, οι επιχειρήσεις και οι χρήστες της διαδικτυακής τραπεζικής, τα είδη των απατών που καταγράφονται συχνότερα, καθώς και βασικοί μηχανισμοί πρόληψης και αντιμετώπισής τους.

Σε πρακτικό επίπεδο, η εργασία εστιάζει σε ένα συγκεκριμένο χρηματοπιστωτικό ίδρυμα, το σύστημα ψηφιακών πληρωμών **NBG Pay της Εθνικής Τράπεζας της Ελλάδος**, καθώς και σε ορισμένες από τις συνεργαζόμενες επιχειρήσεις του. Εξετάζεται ο τρόπος με τον οποίο οι επιχειρήσεις αυτές μπορεί να αποτελέσουν στόχο ηλεκτρονικής απάτης, με συνέπεια οικονομικές απώλειες τόσο για τις ίδιες όσο και για την τράπεζα. Παρουσιάζονται επίσης οι διαδικασίες ελέγχου που εφαρμόζονται για την ανίχνευση και αποτροπή ύποπτων συναλλαγών, καθώς και τα συστήματα που ενεργοποιούνται μετά την εμφάνιση περιστατικών απάτης, με στόχο την αποφυγή ή τη μείωση της ζημίας.

Τέλος, πραγματοποιείται ανάλυση της επίδρασης που είχε η περίοδος της πανδημίας **COVID-19** στην εξέλιξη των ηλεκτρονικών πληρωμών διεθνώς, μέσα από τη μελέτη δεδομένων από περίπου 15 ευρωπαϊκές χώρες. Εξετάζεται η αύξηση του όγκου των ψηφιακών συναλλαγών, η μεταβολή του σχετικού ρίσκου και η συχνότητα εμφάνισης απατών κατά την περίοδο αυτή και στα επόμενα χρόνια. Τα ευρήματα της έρευνας

συμβάλλουν στην κατανόηση των σύγχρονων προκλήσεων στον τομέα των ηλεκτρονικών πληρωμών και στη διαμόρφωση προτάσεων για πιο αποτελεσματικούς μηχανισμούς πρόληψης και διαχείρισης κινδύνου.

ABSTRACT

This dissertation examines the phenomenon of financial risk and fraud in banking transactions, with a particular emphasis on digital payments and the modern electronic systems that support them. Initially, the study presents the theoretical framework concerning the ways in which risk or fraudulent activity may arise in high-value transactions, along with the general categories of fraud encountered within the banking sector. In this context, the analysis covers the risks faced by cardholders, businesses, and online banking users, the most common types of fraud, and the principal mechanisms used for prevention and detection.

At a practical level, the research focuses on a specific financial institution, the **NBG Pay digital payment system of the National Bank of Greece**, as well as selected partner businesses. The study investigates how these enterprises may become targets of electronic fraud, resulting in financial losses either for the businesses themselves or for the bank. Moreover, the procedures implemented for monitoring, identifying, and preventing suspicious transactions are presented, together with the systems activated after a fraud incident to mitigate or avoid financial damage.

Finally, the dissertation analyzes the impact of the **COVID-19** period on the development of digital payments across approximately 15 European countries. The research examines the increase in transaction volumes, the changes in associated risk levels, and the frequency of fraud incidents during and after the pandemic. The findings contribute to a deeper understanding of the contemporary challenges in electronic payments and support the formulation of proposals for more effective risk-management and fraud - prevention mechanisms.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες.....	4
ΠΕΡΙΛΗΨΗ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ.....	5
ABSTRACT.....	7
ΠΡΟΛΟΓΟΣ	11
ΚΕΦΑΛΑΙΟ 1 – ΕΙΣΑΓΩΓΗ.....	13
1.1 Σκοπός της Έρευνας	14
1.2 Ερευνητικά Ερωτήματα.....	15
1.3 Σημαντικότητα της Μελέτης	16
1.4 Μεθοδολογία της Έρευνας.....	16
1.5 Δομή της Διπλωματικής Εργασίας	17
ΚΕΦΑΛΑΙΟ 2 – ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ	18
2.1 Ψηφιακές Πληρωμές στα Χρηματοπιστωτικά Ιδρύματα	19
2.1.1 Έννοια και Εξέλιξη των Ψηφιακών Πληρωμών	19
2.1.2 Είδη Ψηφιακών Πληρωμών	20
2.1.3 Ρόλος των Τραπεζών στο Σύστημα Ηλεκτρονικών Συναλλαγών	21
2.1.4 Ρυθμιστικό Πλαίσιο	24
2.2 Ψηφιακές Πληρωμές στην Ευρώπη	26
2.2.1 Επίπεδο Ψηφιοποίησης.....	26
2.2.2 Στατιστικά Χρήσης.....	28
2.2.3 Κίνδυνοι και Προκλήσεις.....	30
2.2.4 Συγκριτική Ανάλυση Επιπέδων Απάτης	31
ΚΕΦΑΛΑΙΟ 3 – ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΑΠΑΤΩΝ.....	35
3.1 Απάτες Issuing (Κάρτες Πληρωμών).....	35
3.1.1 Card Theft (Κλοπή Κάρτας)	36
3.1.2 Card-Not-Present (CNP) Fraud	36
3.1.3 Skimming	37
3.1.4 BIN Attacks / FraudMIDs	38
3.1.5 SIM Swap	39
3.1.6 Compromised Cards – Data Breaches	40
3.1.7 Friendly Fraud / Chargeback Abuse.....	40
3.2 Απάτες Web & Mobile Banking – Αναλυτική Ανάλυση	42
3.2.1 Περιστατικοαπατης με Phishing.....	42
3.2.2 Smishing	44
3.2.3 Vishing	45
3.2.4 Investment Fraud	46

3.2.5 Microsoft / Tech Support Scam	48
3.2.6 Account Takeover (ATO).....	49
3.2.7 Social Engineering Attacks	50
3.2.8 Money Mules και Νομιμοποίηση Εσόδων	51
3.2.9 Συνδυασμένες Επιθέσεις (Hybrid Fraud)	53
3.3 Παράγοντες που Ενισχύουν την Ηλεκτρονική Απάτη	54
3.4 Επιπτώσεις της Ηλεκτρονικής Απάτης	55
3.5 Μηχανισμοί Πρόληψης	56
3.6 Προκλήσεις στην Αντιμετώπιση	57
3.7 Συστημική Προσέγγιση	57
ΚΕΦΑΛΑΙΟ 4 - ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΑΠΑΤΩΝ.....	58
4.1 Επιπτώσεις στους πελάτες	58
4.2 Επιπτώσεις στις επιχειρήσεις	60
4.3 Οικονομικό κόστος για τα χρηματοπιστωτικά ιδρύματα.....	61
4.4 Επιπτώσεις στη φήμη των τραπεζών	62
4.5 Ρυθμιστικές κυρώσεις & νομικοί κίνδυνοι.....	62
ΚΕΦΑΛΑΙΟ 5 – ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΟΥ ΙΔΡΥΜΑΤΟΣ (NBG Pay)	63
5.1 Παρουσίαση του οργανισμού NBG Pay	63
5.2 Ρόλος στις ψηφιακές πληρωμές.....	64
5.3 Υποδομές POS, e-commerce και APIs	67
5.4 Ανάλυση κινδύνων και ευπαθειών	68
5.5 Παραδείγματα περιστατικών απάτης από εταιρείες-πελάτες	68
5.6 Οικονομικές και λειτουργικές επιπτώσεις.....	69
Κεφάλαιο 6 – Μηχανισμοί Ανίχνευσης και Πρόληψης Απάτης.....	70
6.1 Ανίχνευση Απάτης (Fraud Detection).....	71
6.1.1 Risk Scoring Models	75
6.1.2 Machine Learning & AI Fraud Engines.....	79
6.1.3 Behavioral Analytics	80
6.1.4 Transaction Monitoring	80
6.1.5 Device Fingerprinting & Geolocation	83
6.2 Πρόληψη Απάτης (Fraud Prevention), ως πρωτογενής μηχανισμός διαχείρισης κινδύνου	84
6.2.1 Strong Customer Authentication (SCA)	87
6.2.2 Tokenization & Encryption.....	88
6.2.3 Limits, Velocity Checks & Rule Engines.....	88
6.2.5 Governance & Internal Controls	89

Κεφάλαιο 7 – Ανάλυση Εκτενούς Δείγματος 15 Ευρωπαϊκών Χωρών	89
7.1 Δεδομένα Χρήσης Ψηφιακών Πληρωμών.....	90
7.2 Συχνότητα και Ένταση Περιστατικών Απάτης	91
7.3 Συσχέτιση Ψηφιακής Ωριμότητας και Κινδύνου Απάτης	92
7.5 Συγκριτική Αξιολόγηση και Ευρήματα.....	93
Κεφάλαιο 8 – Ξεπλύμα Χρήματος και Μηχανισμοί Καταπολέμησης (AML) – Αναλυτικά.....	97
8.1 Εισαγωγή	97
8.2 Έννοια και Ορισμός της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες (AML)	98
8.3 Στάδια του Ξεπλύματος Χρήματος.....	99
8.3.1 Placement – Εισαγωγή κεφαλαίων στο χρηματοπιστωτικό σύστημα	99
8.3.2 Layering – Διαστρωμάτωση κεφαλαίων.....	100
8.3.3 Integration – Επανένταξη στην οικονομία.....	100
8.4 Κανάλια Ξεπλύματος Χρήματος στις Ψηφιακές Πληρωμές.....	101
8.5 Μορφές Ξεπλύματος Χρήματος στο Ηλεκτρονικό Περιβάλλον	101
8.6 Red Flags και Δείκτες Υποπτων Συναλλαγών.....	102
8.7 Θεσμικό Πλαίσιο και Κανονιστική Συμμόρφωση	102
8.8 Μηχανισμοί Καταπολέμησης της Νομιμοποίησης Εσόδων	103
8.9 Σύγχρονες Προκλήσεις για Χρηματοπιστωτικά Ιδρύματα.....	104
ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΕΦΑΛΑΙΩΝ.....	104
ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ	105

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο ολοκλήρωσης των σπουδών μου και έχει ως αντικείμενο τη μελέτη του ρίσκου και των μορφών απάτης που παρουσιάζονται στις τραπεζικές συναλλαγές επιχειρήσεων, με έμφαση στις συναλλαγές που πραγματοποιούνται μέσω των συστημάτων πληρωμών της Εθνικής Τράπεζας της Ελλάδος (NBG Pay) και των γενικών τραπεζικών συστημάτων ασφάλειας των Ελληνικών συστημικών τραπεζών

Η επιλογή του συγκεκριμένου θέματος προέκυψε από το έντονο ενδιαφέρον μου για τον τραπεζικό και χρηματοπιστωτικό τομέα, καθώς και για τις σύγχρονες προκλήσεις που αντιμετωπίζει ο κλάδος των ηλεκτρονικών πληρωμών. Στη σημερινή εποχή, όπου η τεχνολογία εξελίσσεται ραγδαία και οι ηλεκτρονικές συναλλαγές αποτελούν αναπόσπαστο κομμάτι της επιχειρηματικής δραστηριότητας, η κατανόηση των κινδύνων που τις συνοδεύουν είναι απαραίτητη τόσο για τις ίδιες τις επιχειρήσεις όσο και για τα χρηματοπιστωτικά ιδρύματα.

Μέσα από τη συγγραφή της εργασίας επιδιώκεται να παρουσιαστεί ένα ολοκληρωμένο θεωρητικό και πρακτικό πλαίσιο αναφορικά με το πώς προκύπτουν οι απάτες στις ηλεκτρονικές συναλλαγές, ποιοι παράγοντες τις εντείνουν, αλλά και ποια μέτρα μπορούν να εφαρμοστούν για την πρόληψη και διαχείρισή τους. Παράλληλα, η εργασία στοχεύει να αναδείξει τον ρόλο της NBG Pay στη διαχείριση του ρίσκου των συναλλαγών, καθώς και τις προκλήσεις που αντιμετωπίζει στο σημερινό περιβάλλον των ηλεκτρονικών πληρωμών.

Ιδιαίτερη έμφαση δίνεται, επίσης, στη μεταβολή των τάσεων στις ηλεκτρονικές πληρωμές κατά την περίοδο της πανδημίας COVID-19 και μετά, τόσο στην Ελλάδα όσο και διεθνώς, καθώς και στις νέες μορφές κινδύνου που προέκυψαν από τη ραγδαία αύξηση της χρήσης ψηφιακών μέσων συναλλαγής.

ΚΕΦΑΛΑΙΟ 1 – ΕΙΣΑΓΩΓΗ

Η παγκόσμια οικονομική δραστηριότητα βρίσκεται σε φάση βαθιάς ψηφιακής μετάβασης, κατά την οποία οι χρηματοοικονομικές συναλλαγές μετατοπίζονται από το φυσικό περιβάλλον στο ψηφιακό οικοσύστημα. Η χρήση μετρητών μειώνεται σταθερά, ενώ οι ηλεκτρονικές και άυλες μορφές πληρωμής αναδεικνύονται σε κυρίαρχο μέσο ανταλλαγής αξίας. Η εξέλιξη αυτή δεν αποτελεί απλώς τεχνολογική καινοτομία, αλλά δομικό μετασχηματισμό του χρηματοπιστωτικού συστήματος.

Οι ψηφιακές πληρωμές στηρίζονται σε δίκτυα πληροφορικής, συστήματα εκκαθάρισης, κρυπτογραφικές μεθόδους και διασυνδεδεμένες τραπεζικές υποδομές. Μέσω αυτών, η οικονομική αξία μεταφέρεται με τη μορφή δεδομένων, γεγονός που μετατρέπει τη χρηματοοικονομική συναλλαγή σε διαδικασία διαχείρισης πληροφοριών. Η μετάβαση αυτή δημιουργεί ένα περιβάλλον αυξημένης ταχύτητας, ευκολίας και αποδοτικότητας, αλλά ταυτόχρονα μεταφέρει τον κίνδυνο από τον φυσικό χώρο στον ψηφιακό.

Στο νέο αυτό περιβάλλον, η έννοια της εμπιστοσύνης αποκτά τεχνολογική διάσταση. Οι συναλλασσόμενοι δεν βασίζονται πλέον στη φυσική παρουσία, αλλά σε μηχανισμούς ταυτοποίησης, πρωτόκολλα ασφαλείας και συστήματα επαλήθευσης. Η ψηφιοποίηση συνεπώς αναδιαμορφώνει το πλαίσιο διαχείρισης κινδύνων. Ο λειτουργικός κίνδυνος, ο τεχνολογικός κίνδυνος και ο κίνδυνος απάτης αποκτούν κεντρική θέση στη στρατηγική των χρηματοπιστωτικών ιδρυμάτων.

Η ηλεκτρονική απάτη αναδύεται ως συστημική απειλή, διότι εκμεταλλεύεται τόσο τεχνικές αδυναμίες όσο και ανθρώπινες ευπάθειες. Σε αντίθεση με τις παραδοσιακές

μορφές οικονομικού εγκλήματος, η ψηφιακή απάτη χαρακτηρίζεται από διασυννοριακότητα, ανωνυμία, ταχύτητα εκτέλεσης και δυνατότητα μαζικής κλιμάκωσης. Το γεγονός ότι η απάτη εξελίσσεται παράλληλα με την τεχνολογία καθιστά αναγκαία τη συνεχή επιστημονική μελέτη του φαινομένου.

Η παρούσα διπλωματική εργασία εξετάζει το οικοσύστημα των ψηφιακών πληρωμών υπό το πρίσμα του κινδύνου ηλεκτρονικής απάτης, αναλύοντας τις μορφές της, τις επιπτώσεις της και τους μηχανισμούς αντιμετώπισής της.

European Central Bank (ECB). (2023). Payment cards fraud statistics.)

1.1 Σκοπός της Έρευνας

Ο βασικός σκοπός της παρούσας έρευνας είναι η εις βάθος κατανόηση της σχέσης μεταξύ της ανάπτυξης των ψηφιακών πληρωμών και της εξέλιξης της ηλεκτρονικής απάτης στο σύγχρονο χρηματοπιστωτικό περιβάλλον. Η εργασία δεν περιορίζεται στην απλή περιγραφή φαινομένων, αλλά επιδιώκει τη συστηματική ανάλυση των μηχανισμών που συνδέουν την τεχνολογική πρόοδο με τη μεταβολή της φύσης του κινδύνου.

Ειδικότερα, η μελέτη στοχεύει:

- Στην εννοιολογική αποτύπωση του οικοσυστήματος των ψηφιακών πληρωμών
- Στην κατανόηση του τρόπου λειτουργίας των βασικών τεχνολογιών πληρωμών
- Στην κατηγοριοποίηση των μορφών ηλεκτρονικής απάτης και των μεθόδων δράσης
- Στην ανάλυση των επιπτώσεων της απάτης σε πελάτες, επιχειρήσεις και τράπεζες

- Στην παρουσίαση των σύγχρονων μηχανισμών ανίχνευσης και πρόληψης

Ο σκοπός της έρευνας είναι επομένως διττός: αφενός η θεωρητική θεμελίωση του φαινομένου, αφετέρου η πρακτική κατανόηση των προκλήσεων που αντιμετωπίζουν τα χρηματοπιστωτικά ιδρύματα.

1.2 Ερευνητικά Ερωτήματα

Η διαμόρφωση ερευνητικών ερωτημάτων αποτελεί βασικό στοιχείο της επιστημονικής διαδικασίας, καθώς κατευθύνει τη δομή της ανάλυσης. Στην παρούσα εργασία τα ερωτήματα προκύπτουν από την ανάγκη κατανόησης ενός δυναμικού και μεταβαλλόμενου περιβάλλοντος.

Τα κύρια ερευνητικά ερωτήματα είναι:

- Πώς μετασχηματίζει η ψηφιοποίηση των πληρωμών το προφίλ κινδύνου του χρηματοπιστωτικού συστήματος;
- Ποιες μορφές ηλεκτρονικής απάτης αναπτύσσονται εντονότερα στο σύγχρονο περιβάλλον;
- Ποιος είναι ο ρόλος της ανθρώπινης συμπεριφοράς στην επιτυχία των επιθέσεων κοινωνικής μηχανικής;
- Πώς επηρεάζονται οι οικονομικές και λειτουργικές δομές των τραπεζών από την αύξηση της απάτης;
- Ποιοι μηχανισμοί άμυνας είναι αποτελεσματικοί και γιατί;

Τα ερωτήματα αυτά δεν έχουν μόνο περιγραφικό χαρακτήρα, αλλά διερευνούν αιτιακές σχέσεις και δομικές αλληλεπιδράσεις.

1.3 Σημαντικότητα της Μελέτης

Η σημασία της μελέτης είναι πολυεπίπεδη.

Σε **οικονομικό επίπεδο**, η απάτη επηρεάζει τη σταθερότητα των χρηματοπιστωτικών ιδρυμάτων και αυξάνει το λειτουργικό κόστος. Οι απώλειες δεν περιορίζονται σε άμεσες χρηματικές ζημιές, αλλά περιλαμβάνουν δαπάνες συμμόρφωσης, επενδύσεις σε συστήματα ασφαλείας και κόστος διαχείρισης περιστατικών.

Σε **κοινωνικό επίπεδο**, η ηλεκτρονική απάτη διαβρώνει την εμπιστοσύνη των πολιτών προς τις ψηφιακές συναλλαγές. Η εμπιστοσύνη αποτελεί θεμέλιο της οικονομικής λειτουργίας και η απώλειά της μπορεί να επιβραδύνει την υιοθέτηση καινοτομιών.

Σε **ρυθμιστικό επίπεδο**, οι αρχές καλούνται να ισορροπήσουν μεταξύ καινοτομίας και προστασίας. Η κατανόηση του φαινομένου συμβάλλει στη διαμόρφωση αποτελεσματικών πολιτικών.

Σε **επιστημονικό επίπεδο**, η μελέτη γεφυρώνει πεδία όπως η τραπεζική διοίκηση, η κυβερνοασφάλεια, η συμπεριφορική οικονομική και η διαχείριση κινδύνων.

[PwC – Global Economic CrimeSurvey](#)

1.4 Μεθοδολογία της Έρευνας

Η έρευνα βασίζεται σε θεωρητική και αναλυτική προσέγγιση. Αξιοποιείται εκτενής βιβλιογραφία από:

- επιστημονικά άρθρα
- εκθέσεις διεθνών οργανισμών
- κανονιστικά κείμενα
- τραπεζικές πρακτικές

Η μεθοδολογία περιλαμβάνει:

1. **Θεωρητική ανάλυση εννοιών** (ψηφιακές πληρωμές, απάτη, κίνδυνος)
2. **Συστηματική κατηγοριοποίηση μορφών απάτης**
3. **Λειτουργική ανάλυση μηχανισμών άμυνας**
4. **Μελέτη περίπτωσης χρηματοπιστωτικού οργανισμού**

Η προσέγγιση είναι ερμηνευτική και στοχεύει στην κατανόηση των μηχανισμών, όχι μόνο στην καταγραφή φαινομένων.

1.5 Δομή της Διπλωματικής Εργασίας

Η εργασία οργανώνεται σε διαδοχικά κεφάλαια που ακολουθούν λογική εξέλιξη:

- Το Κεφάλαιο 2 παρουσιάζει το θεωρητικό πλαίσιο των ψηφιακών πληρωμών
- Το Κεφάλαιο 3 αναλύει τις μορφές ηλεκτρονικής απάτης
- Το Κεφάλαιο 4 εξετάζει τις επιπτώσεις
- Το Κεφάλαιο 5 περιλαμβάνει μελέτη περίπτωσης
- Το Κεφάλαιο 6 παρουσιάζει μηχανισμούς ανίχνευσης και πρόληψης
- Το Κεφάλαιο 7 περιλαμβάνει συγκριτική ανάλυση
- Το Κεφάλαιο 8 συνοψίζει τα συμπεράσματα

Η δομή αυτή επιτρέπει σταδιακή εμβάθυνση από το γενικό στο ειδικό.

ΚΕΦΑΛΑΙΟ 2 – ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

Το οικοσύστημα των ψηφιακών πληρωμών αποτελεί ένα σύνθετο δίκτυο τεχνολογικών, τραπεζικών και ρυθμιστικών δομών, μέσω των οποίων η οικονομική αξία μεταφέρεται σε ηλεκτρονική μορφή. Δεν πρόκειται για ένα απλό τεχνολογικό εργαλείο, αλλά για ένα πολυεπίπεδο σύστημα που βασίζεται στην εμπιστοσύνη, την ασφάλεια, τη διαλειτουργικότητά και τη νομική αναγνώριση.

Οι ψηφιακές πληρωμές αποτελούν βασικό πυλώνα της σύγχρονης οικονομικής δραστηριότητας, καθώς διευκολύνουν το εμπόριο, επιταχύνουν τη ροή κεφαλαίων και ενισχύουν τη διαφάνεια. Ωστόσο, η λειτουργία τους στηρίζεται σε υποδομές που εκτείνονται πέρα από τα όρια μιας μεμονωμένης τράπεζας, δημιουργώντας ένα διασυνδεδεμένο περιβάλλον όπου ο κίνδυνος διαχέεται.

Ουσιαστικά διενεργούνται συναλλαγές σε μεγάλο εύρος και αυτές πραγματοποιούνται σε καθημερινή βάση, με οποιοδήποτε τρόπο και τραπεζικό μέσο. Φυσικά παράλληλα με τις συναλλαγές προκύπτουν και οι απάτες με βασικούς υπαίτιους τους επιτήδειους, όπου πλέον με την αρωγή και του AI(Artificial Intelligence) technology, έχουν αυξηθεί σε μεγάλο βαθμό και στοχεύουν κυρίως σε ευπαθείς ηλικιακές ομάδες που δεν είναι τόσο εξοικειωμένοι με τα σύγχρονα τραπεζικά προϊόντα.

2.1 Ψηφιακές Πληρωμές στα Χρηματοπιστωτικά Ιδρύματα

Οι ψηφιακές πληρωμές αποτελούν τη βασική λειτουργική δραστηριότητα των σύγχρονων τραπεζών. Η μετάβαση από τα φυσικά μέσα πληρωμής (μετρητά, επιταγές) στα ηλεκτρονικά συστήματα σηματοδοτεί την αλλαγή του ρόλου των τραπεζών από απλούς διαχειριστές ρευστότητας σε παρόχους τεχνολογικών χρηματοοικονομικών υπηρεσιών.

Η τράπεζα πλέον λειτουργεί ως:

- φορέας ταυτοποίησης
- διαχειριστής κινδύνου
- διαμεσολαβητής εμπιστοσύνης
- πάροχος ψηφιακών υποδομών

Η ψηφιακή πληρωμή είναι ουσιαστικά μια αλληλουχία μηνυμάτων μεταξύ συστημάτων, μέσω των οποίων επιβεβαιώνεται η ταυτότητα του πληρωτή, η διαθεσιμότητα κεφαλαίων και η νομιμότητα της συναλλαγής.

[\(European Central Bank \(ECB\). \(2023\). Payment cards fraud statistics.\)](#)

2.1.1 Έννοια και Εξέλιξη των Ψηφιακών Πληρωμών

Ψηφιακή πληρωμή είναι η μεταφορά χρηματικής αξίας με ηλεκτρονικά μέσα, όπου η συναλλαγή καταγράφεται, επεξεργάζεται και εκκαθαρίζεται μέσω πληροφοριακών συστημάτων. Η αξία δεν μετακινείται φυσικά, αλλά αντιπροσωπεύεται από λογιστικές εγγραφές.

Η εξέλιξη των ψηφιακών πληρωμών συνδέεται με τρεις βασικούς άξονες:

1.Τεχνολογική πρόοδος

Από τις μαγνητικές κάρτες στις κάρτες με μικροτσίπ, στις ανέπαφες πληρωμές και στα ψηφιακά πορτοφόλια. Κάθε τεχνολογική φάση ενσωματώνει νέα επίπεδα κρυπτογράφησης και ασφάλειας.

2.Αλλαγή καταναλωτικής συμπεριφοράς

Η ανάγκη για ταχύτητα και ευκολία οδήγησε σε μαζική υιοθέτηση ηλεκτρονικών καναλιών.

3.Ρυθμιστική ενοποίηση

Η Ευρωπαϊκή Ένωση προώθησε ενιαία αγορά πληρωμών, διευκολύνοντας διασυνοριακές συναλλαγές.

Η εξέλιξη αυτή χαρακτηρίζεται από έναν συνεχή κύκλο: κάθε νέα τεχνολογία μειώνει συγκεκριμένους κινδύνους, αλλά ταυτόχρονα δημιουργεί νέες ευπάθειες.

[Bank for International Settlements \(BIS\). \(2022\). Digital payments and financial stability.](#)

[World Bank \(2021\). Digital Financial Services.](#)

2.1.2 Είδη Ψηφιακών Πληρωμών

POS (CardPresent)

Η πληρωμή πραγματοποιείται με φυσική παρουσία κάρτας. Η ασφάλεια βασίζεται στο μικροτσίπ, το PIN και την κρυπτογράφηση. Θεωρείται πιο ασφαλής μορφή, αλλά δεν εξαλείφει τον κίνδυνο κλοπής ή αντιγραφής.

E-commerce (Card Not Present)

Η συναλλαγή γίνεται εξ αποστάσεως. Η απουσία φυσικής επαλήθευσης καθιστά τη συναλλαγή ευάλωτη σε κλοπή στοιχείων και κατάχρηση.

Ψηφιακά Πορτοφόλια (Wallets)

Οι κάρτες αντικαθίστανται από ψηφιακά tokens. Η τεχνολογία αυτή μειώνει τη διαρροή πραγματικών στοιχείων, αλλά η ασφάλεια εξαρτάται από τη συσκευή και τον χρήστη.

Άμεσες Πληρωμές (Instant Payments)

Η μεταφορά χρημάτων γίνεται σε πραγματικό χρόνο. Η ταχύτητα μειώνει τη δυνατότητα παρέμβασης σε περίπτωση απάτης.

[European Central Bank – Payment methods report](#)

[Bank of Greece – Payment Systems Report](#)

2.1.3 Ρόλος των Τραπεζών στο Σύστημα Ηλεκτρονικών Συναλλαγών

Στο οικοσύστημα των ψηφιακών πληρωμών οι τράπεζες δεν λειτουργούν απλώς ως οικονομικοί διαμεσολαβητές, αλλά ως θεσμικοί φορείς εμπιστοσύνης και ως τεχνολογικές πλατφόρμες διαχείρισης ρίσκου. Η λειτουργία τους ενσωματώνει οικονομικές, τεχνολογικές και κανονιστικές διαστάσεις, οι οποίες διαμορφώνουν τη σταθερότητα του συστήματος.

Υποδομές Λογαριασμών

Οι τραπεζικοί λογαριασμοί αποτελούν τη βασική λογιστική μονάδα αποθήκευσης αξίας στο σύγχρονο χρηματοπιστωτικό σύστημα. Σε ένα ψηφιακό περιβάλλον, ο λογαριασμός δεν είναι απλώς μια καταγραφή χρημάτων, αλλά μια **ψηφιακή ταυτότητα οικονομικής δραστηριότητας**.

Η τράπεζα:

- καταγράφει δικαιώματα και υποχρεώσεις

- διασφαλίζει τη νομική αναγνώριση των συναλλαγών
- εγγυάται τη διαθεσιμότητα κεφαλαίων
- παρέχει πρόσβαση σε δίκτυα πληρωμών

Οι λογαριασμοί αποτελούν σημείο σύγκλισης νομικής ευθύνης, τεχνολογικής ασφάλειας και εποπτικής συμμόρφωσης.

Μηχανισμοί Ταυτοποίησης

Η ταυτοποίηση είναι η διαδικασία με την οποία επαληθεύεται ότι ένα πρόσωπο είναι πράγματι αυτό που ισχυρίζεται. Στο ψηφιακό περιβάλλον, η φυσική παρουσία αντικαθίσταται από:

- κωδικούς πρόσβασης
- βιομετρικά δεδομένα
- συσκευές
- δυναμικούς κωδικούς

Οι τράπεζες διαχειρίζονται την ψηφιακή ταυτότητα του πελάτη, η οποία αποτελεί κρίσιμο στοιχείο ασφάλειας. Η αποτυχία ταυτοποίησης οδηγεί σε απάτη, ενώ η υπερβολική αυστηρότητα μειώνει τη χρηστικότητα. Συνεπώς, η ταυτοποίηση αποτελεί ισορροπία μεταξύ ασφάλειας και εμπειρίας χρήστη.

Συστήματα Παρακολούθησης Συναλλαγών

Οι τράπεζες διαθέτουν μηχανισμούς που αναλύουν σε πραγματικό χρόνο τη συμπεριφορά συναλλαγών. Τα συστήματα αυτά:

- εντοπίζουν ασυνήθιστα πρότυπα
- συγκρίνουν με ιστορική συμπεριφορά
- ενεργοποιούν ελέγχους

Η παρακολούθηση συναλλαγών συνδέεται τόσο με την πρόληψη απάτης όσο και με την καταπολέμηση ξεπλύματος χρήματος. Αποτελεί συνεχή διαδικασία επιτήρησης που μετατρέπει τις τράπεζες σε φορείς εποπτικής λειτουργίας.

Διαχείριση Κινδύνου

Οι ψηφιακές πληρωμές δημιουργούν:

- λειτουργικό κίνδυνο
- τεχνολογικό κίνδυνο
- κίνδυνο απάτης
- κανονιστικό κίνδυνο

Οι τράπεζες αναπτύσσουν πολιτικές, ελέγχους και διαδικασίες για τον εντοπισμό, την αξιολόγηση και τον περιορισμό των κινδύνων αυτών. Η διαχείριση κινδύνου δεν είναι απλώς τεχνική λειτουργία αλλά στρατηγική προτεραιότητα.

Ο Διττός Ρόλος των Τραπεζών

Οι τράπεζες καλούνται να ισορροπήσουν μεταξύ:

1. Διευκόλυνσης συναλλαγών (ταχύτητα, απλότητα)
2. Πρόληψης παράνομων δραστηριοτήτων (έλεγχοι, περιορισμοί)

Αυτή η αντίφαση αποτελεί βασικό χαρακτηριστικό της σύγχρονης τραπεζικής λειτουργίας.

[Bank for International Settlements \(BIS\). \(2022\). Digital payments and financial stability.](#)

[ECB – Retail Payments Strategy](#)

2.1.4 Ρυθμιστικό Πλαίσιο

Το ρυθμιστικό πλαίσιο δεν είναι εξωτερικός περιορισμός, αλλά παράγοντας που καθορίζει τη δομή των ψηφιακών πληρωμών.

PSD2 (Payment Services Directive 2)

Η PSD2 εισήγαγε την έννοια της ανοιχτής τραπεζικής, επιτρέποντας σε τρίτους παρόχους να αποκτούν πρόσβαση σε τραπεζικά δεδομένα μέσω APIs. Στόχος είναι:

- ενίσχυση ανταγωνισμού
- καινοτομία
- διαφάνεια

Ωστόσο, η διασύνδεση πολλών φορέων αυξάνει την επιφάνεια κινδύνου, καθιστώντας την ασφάλεια πολυδιάστατο ζήτημα.

[European Commission. \(2018\). PSD2 Directive on Payment Services.](#)

SCA (Strong Customer Authentication)

Η SCA απαιτεί τουλάχιστον δύο στοιχεία ταυτοποίησης από διαφορετικές κατηγορίες:

- γνώση
- κατοχή
- βιομετρία

Στόχος είναι η μείωση της μη εξουσιοδοτημένης πρόσβασης. Παρότι ενισχύει την ασφάλεια, μεταβάλλει και τη συμπεριφορά απάτης, καθώς οι εγκληματίες στρέφονται σε κοινωνική μηχανική.

[European Commission. \(2018\). PSD2 Directive on Payment Services.](#)

AMLD (Anti-Money Laundering Directive)

Η AMLD εστιάζει στην πρόληψη νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Υποχρεώνει τις τράπεζες να:

- γνωρίζουν τον πελάτη τους (KYC)
- παρακολουθούν συναλλαγές
- αναφέρουν ύποπτες δραστηριότητες

Έτσι, οι τράπεζες λειτουργούν ως μηχανισμός ελέγχου του χρηματοπιστωτικού συστήματος.

[European Commission AML Directive](#)

GDPR (General Data Protection Regulation)

Ο GDPR ρυθμίζει τη συλλογή, αποθήκευση και επεξεργασία προσωπικών δεδομένων.

Οι τράπεζες καλούνται να εξισορροπήσουν:

- ανάγκη ανάλυσης δεδομένων για ασφάλεια
- προστασία ιδιωτικότητας

Η διαχείριση δεδομένων γίνεται πλέον στρατηγικός και νομικός παράγοντας.

Συνολική Επίδραση Ρυθμιστικού Πλαισίου

Οι κανονισμοί:

- καθορίζουν τεχνολογικές προδιαγραφές
- διαμορφώνουν διαδικασίες
- επηρεάζουν την εμπειρία χρήστη
- μεταβάλλουν τη φύση του κινδύνου

Το ρυθμιστικό πλαίσιο επομένως αποτελεί ενεργό παράγοντα διαμόρφωσης του οικοσυστήματος ψηφιακών πληρωμών.

[European Parliament GDPR Regulation](#)

2.2 Ψηφιακές Πληρωμές στην Ευρώπη

Η Ευρώπη παρουσιάζει ανομοιογένεια ως προς το επίπεδο ψηφιοποίησης. Ο βορράς εμφανίζει σχεδόν πλήρη υποκατάσταση μετρητών, ενώ ο νότος και η ανατολική Ευρώπη διατηρούν ισχυρή χρήση φυσικού χρήματος.

2.2.1 Επίπεδο Ψηφιοποίησης

Η έννοια της ψηφιακής ωριμότητας μιας χώρας στο πεδίο των πληρωμών αναφέρεται στο βαθμό στον οποίο οι ηλεκτρονικές συναλλαγές έχουν ενσωματωθεί στην καθημερινή οικονομική δραστηριότητα. Δεν πρόκειται μόνο για τεχνολογικό ζήτημα, αλλά για σύνθετο αποτέλεσμα υποδομών, οικονομικών συνθηκών, κοινωνικής συμπεριφοράς και θεσμικών παρεμβάσεων.

Τεχνολογικές Υποδομές

Οι τεχνολογικές υποδομές αποτελούν τη βάση της ψηφιακής οικονομίας.

Περιλαμβάνουν:

- δίκτυα τηλεπικοινωνιών υψηλής ταχύτητας
- ευρεία πρόσβαση στο διαδίκτυο
- διάδοση «έξυπνων» συσκευών

- ψηφιακές πλατφόρμες τραπεζικών υπηρεσιών

Χωρίς αξιόπιστη τεχνολογική υποδομή, η υιοθέτηση ψηφιακών πληρωμών περιορίζεται. Η τεχνολογία καθορίζει τη διαθεσιμότητα υπηρεσιών, την ταχύτητα συναλλαγών και την εμπειρία χρήστη. Παράλληλα, η ποιότητα των υποδομών επηρεάζει και την ασφάλεια, καθώς αδύναμα δίκτυα αυξάνουν την ευπάθεια σε επιθέσεις.

Οικονομική Ανάπτυξη

Η οικονομική ανάπτυξη συνδέεται άμεσα με την ψηφιοποίηση. Χώρες με υψηλότερο εισόδημα εμφανίζουν:

- μεγαλύτερη πρόσβαση σε τραπεζικές υπηρεσίες
- υψηλότερη κατανάλωση τεχνολογίας
- μεγαλύτερη συμμετοχή στο ηλεκτρονικό εμπόριο

Η οικονομική ευρωστία επιτρέπει επενδύσεις σε τεχνολογία και εκπαίδευση, ενισχύοντας την υιοθέτηση ψηφιακών μέσων πληρωμής. Αντίθετα, σε οικονομίες με χαμηλότερο επίπεδο ανάπτυξης, τα μετρητά παραμένουν κυρίαρχα λόγω κόστους, έλλειψης εμπιστοσύνης ή περιορισμένης πρόσβασης σε τραπεζικές δομές.

Κουλτούρα Πληρωμών

Η κουλτούρα πληρωμών αφορά τις κοινωνικές στάσεις απέναντι στη χρήση χρήματος. Σε ορισμένες χώρες, τα μετρητά συνδέονται με αίσθηση ελέγχου και ιδιωτικότητας, ενώ σε άλλες οι ψηφιακές συναλλαγές θεωρούνται φυσική εξέλιξη.

Η κουλτούρα επηρεάζεται από:

- ιστορικές εμπειρίες οικονομικής αστάθειας

- επίπεδο εμπιστοσύνης στους θεσμούς
- εξοικείωση με τεχνολογία

Η συμπεριφορά των καταναλωτών μπορεί να επιταχύνει ή να επιβραδύνει την τεχνολογική υιοθέτηση ανεξάρτητα από την υποδομή.

Κρατικές Πολιτικές

Οι κυβερνητικές πολιτικές διαμορφώνουν το περιβάλλον πληρωμών μέσω:

- φορολογικών κινήτρων για ηλεκτρονικές συναλλαγές
- περιορισμών στη χρήση μετρητών
- επενδύσεων σε ψηφιακές δημόσιες υπηρεσίες
- ρυθμιστικών πλαισίων

Το κράτος λειτουργεί ως επιταχυντής ή επιβραδυντής της ψηφιοποίησης.

[Eurostat – Digital Economy Statistics](#)

[OECD – Digital Payments](#)

2.2.2 Στατιστικά Χρήσης

Η χρήση ψηφιακών πληρωμών διαφέρει σημαντικά μεταξύ χωρών, αντανακλώντας το επίπεδο ψηφιακής ωριμότητας.

Χρήση Καρτών

Οι κάρτες αποτελούν το πρώτο βήμα μετάβασης από τα μετρητά. Η συχνότητα χρήσης καρτών δείχνει:

- βαθμό τραπεζικής ένταξης
- εξοικείωση με ηλεκτρονικές συναλλαγές
- υποδομές αποδοχής από εμπόρους

Η αυξημένη χρήση καρτών μειώνει τη φυσική διαχείριση μετρητών αλλά μεταφέρει τον κίνδυνο στον ψηφιακό χώρο.

Διείσδυση E-commerce

Το ηλεκτρονικό εμπόριο αποτελεί ένδειξη ψηφιακής οικονομικής δραστηριότητας.

Υψηλή διείσδυση e-commerce συνεπάγεται:

- αυξημένες απομακρυσμένες συναλλαγές
- εξάρτηση από διαδικτυακές πλατφόρμες
- μεγαλύτερη έκθεση σε απάτες χωρίς φυσική παρουσία

Το e-commerce λειτουργεί ως καταλύτης για την εξέλιξη των πληρωμών αλλά και για τη μετατόπιση των κινδύνων.

Χρήση Mobile Wallets

Τα ψηφιακά πορτοφόλια ενσωματώνουν πληρωμές σε οικοσυστήματα κινητών συσκευών. Η χρήση τους δείχνει:

- υψηλό επίπεδο τεχνολογικής εξοικείωσης
- μετάβαση σε ανέπαφες και άυλες μορφές πληρωμής
- ενοποίηση χρηματοοικονομικών και τεχνολογικών υπηρεσιών

Αν και προσφέρουν αυξημένη ασφάλεια μέσω tokenization, εξαρτώνται από την ασφάλεια της συσκευής και του χρήστη.

[\(European Central Bank \(ECB\). \(2023\). Payment cards fraud statistics.\)](#)

[Eurostat – E-commerce statistics](#)

2.2.3 Κίνδυνοι και Προκλήσεις

Η ψηφιοποίηση δημιουργεί ένα περιβάλλον όπου οι συναλλαγές είναι γρήγορες, αλλά και ευάλωτες σε νέες μορφές απειλών.

Κυβερνο-επιθέσεις

Οι ψηφιακές πληρωμές βασίζονται σε πληροφοριακά συστήματα. Αυτό τις καθιστά στόχο επιθέσεων όπως:

- παραβιάσεις δεδομένων
- κακόβουλο λογισμικό
- επιθέσεις σε δίκτυα

Οι κυβερνο-επιθέσεις δεν στοχεύουν μόνο μεμονωμένους χρήστες αλλά και κεντρικές υποδομές, με πιθανές συστημικές επιπτώσεις.

Κοινωνική Μηχανική

Οι επιθέσεις κοινωνικής μηχανικής εκμεταλλεύονται την ανθρώπινη συμπεριφορά. Οι δράστες δεν παραβιάζουν συστήματα, αλλά πείθουν τα θύματα να αποκαλύψουν στοιχεία ή να εκτελέσουν συναλλαγές.

Η αυξημένη πολυπλοκότητα των συστημάτων καθιστά τους χρήστες ευάλωτους, καθώς η κατανόηση των διαδικασιών ασφαλείας δεν είναι πάντα επαρκής.

Διασυνοριακή Απάτη

Η ψηφιακή οικονομία δεν περιορίζεται από σύνορα. Οι εγκληματικές ομάδες μπορούν να δραστηριοποιούνται σε διαφορετικές χώρες, εκμεταλλευόμενες:

- νομικές διαφοροποιήσεις

- χρονικές ζώνες
- τεχνολογική ανωνυμία

Η διασυνοριακή φύση της απάτης δυσκολεύει την ανάχνευση και τη δίωξη.

[Europol – Internet Organised Crime Report](#)

[Interpol – Financial Cybercrime Report](#)

2.2.4 Συγκριτική Ανάλυση Επιπέδων Απάτης

Η απάτη στις ψηφιακές πληρωμές δεν εμφανίζεται ομοιόμορφα σε όλες τις χώρες. Οι διαφοροποιήσεις αφορούν όχι μόνο την ένταση των περιστατικών αλλά κυρίως τη μορφή που λαμβάνουν. Το επίπεδο ψηφιακής ωριμότητας ενός οικονομικού συστήματος επηρεάζει το «οικοσύστημα κινδύνου», διαμορφώνοντας διαφορετικά πρότυπα εγκληματικής δραστηριότητας.

Οι εγκληματίες προσαρμόζουν τις τεχνικές τους στις τεχνολογικές και κοινωνικές συνθήκες, γεγονός που καθιστά την απάτη ένα δυναμικό και εξελισσόμενο φαινόμενο.

Απάτη σε Χώρες Υψηλής Ψηφιοποίησης

Σε οικονομίες όπου οι ψηφιακές πληρωμές είναι κυρίαρχες και οι υποδομές προηγμένες, τα παραδοσιακά φυσικά εγκλήματα μειώνονται, αλλά αναδύονται σύνθετες μορφές απάτης που βασίζονται στην εκμετάλλευση της ανθρώπινης συμπεριφοράς και της ψηφιακής διασύνδεσης.

Χαρακτηριστικά περιβάλλοντος

- ευρεία χρήση e-banking και mobile banking
- υψηλή διείσδυση καρτών και wallets

- άμεσες πληρωμές και αυτοματοποιημένες διαδικασίες
- μεγάλη εμπιστοσύνη στις ψηφιακές υπηρεσίες

Σε αυτό το πλαίσιο, οι δράστες στοχεύουν το «ασθενέστερο σημείο», δηλαδή τον χρήστη.

Κυρίαρχες μορφές απάτης

Social engineering

Οι επιθέσεις στηρίζονται στην εξαπάτηση μέσω επικοινωνίας (email, SMS, τηλεφωνικές κλήσεις). Οι χρήστες πείθονται να παραχωρήσουν διαπιστευτήρια ή να εγκρίνουν συναλλαγές.

Account Takeover (ATO)

Η πρόσβαση σε λογαριασμούς επιτυγχάνεται μέσω κλεμμένων στοιχείων, malware ή phishing.

Authorized Push Payment Fraud

Το θύμα εκτελεί το ίδιο τη μεταφορά, πιστεύοντας ότι πρόκειται για νόμιμη εντολή.

Investment & impersonation scams

Εκμεταλλεύονται την ψηφιακή παρουσία και τη δυσκολία επαλήθευσης ταυτότητας στο διαδίκτυο.

Θεωρητική ερμηνεία

Σε περιβάλλον υψηλής ασφάλειας υποδομών, οι τεχνικές επιθέσεις στα συστήματα γίνονται δυσκολότερες. Οι εγκληματίες στρέφονται σε **ψυχολογική χειραγώγηση**, όπου η τεχνολογία λειτουργεί ως μέσο και όχι ως στόχος. Το ρίσκο μετατοπίζεται από την υποδομή στον άνθρωπο.

Απάτη σε Χώρες Χαμηλότερης Ψηφιοποίησης

Σε οικονομίες όπου τα μετρητά και οι φυσικές συναλλαγές παραμένουν σημαντικές, οι μορφές απάτης είναι πιο παραδοσιακές και σχετίζονται με φυσικά μέσα πληρωμής.

Χαρακτηριστικά περιβάλλοντος

- περιορισμένη χρήση e-commerce
- χαμηλή διείσδυση mobile wallets
- λιγότερο ανεπτυγμένες τραπεζικές εφαρμογές
- αυξημένη χρήση ATM και φυσικών καρτών

Κυρίαρχες μορφές απάτης

Skimming

Υποκλοπή δεδομένων κάρτας μέσω συσκευών σε ATM ή POS.

Card-present fraud

Χρήση κλεμμένων ή χαμένων καρτών σε φυσικά καταστήματα.

Counterfeit cards

Δημιουργία πλαστών καρτών με αντιγραφή στοιχείων.

Φυσική υποκλοπή στοιχείων

Κλοπή εγγράφων ή παρακολούθηση PIN.

Θεωρητική ερμηνεία

Όταν οι ψηφιακές υποδομές είναι λιγότερο εκτεταμένες, οι εγκληματίες αξιοποιούν φυσικά σημεία επαφής. Ο κίνδυνος συνδέεται με την υλική παρουσία του μέσου πληρωμής και όχι με την ψηφιακή ταυτότητα.

Μεταβατικές Οικονομίες

Σε χώρες που βρίσκονται σε φάση μετάβασης, εμφανίζεται συνδυασμός και των δύο κατηγοριών. Οι εγκληματίες εκμεταλλεύονται:

- τεχνολογικά κενά
- χαμηλή εκπαίδευση χρηστών
- μη ώριμες διαδικασίες ασφάλειας

Αυτό δημιουργεί **υβριδικά μοντέλα απάτης**, όπου ψηφιακές και φυσικές τεχνικές συνδυάζονται.

Δομική Σχέση Ψηφιοποίησης – Απάτης

Η σύγκριση δείχνει ότι η ψηφιοποίηση δεν αυξάνει απλώς την απάτη· **μεταβάλλει τη φύση της**.

Επίπεδο ψηφιοποίησης	Κυρίαρχος κίνδυνος
Χαμηλό	Φυσική απάτη καρτών
Μεσαίο	Μικτό μοντέλο
Υψηλό	Social engineering & ATO

Η απάτη λειτουργεί ως «προσαρμοστικό φαινόμενο». Όσο εξελίσσονται τα συστήματα ασφαλείας, τόσο οι επιθέσεις μετακινούνται προς λιγότερο προστατευμένα σημεία του οικοσυστήματος.

Συμπέρασμα Ενότητας

Η συγκριτική ανάλυση αποδεικνύει ότι το επίπεδο απάτης δεν μπορεί να αξιολογηθεί αποκομμένα από το επίπεδο ψηφιακής ανάπτυξης. Η τεχνολογική πρόοδος μειώνει

ορισμένους κινδύνους αλλά δημιουργεί νέους, περισσότερο άυλους και ψυχολογικά βασισμένους. Επομένως, η στρατηγική αντιμετώπισης της απάτης πρέπει να προσαρμόζεται στο στάδιο ψηφιακής ωριμότητας κάθε χώρας.

[\(European Central Bank \(ECB\). \(2023\). Payment cards fraud statistics.\)](#)

[Europol – Cybercrime Report](#)

ΚΕΦΑΛΑΙΟ 3 – ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΠΑΤΗΣ

Η ανάπτυξη ψηφιακών συναλλαγών και υπηρεσιών mobile/online banking έχει δημιουργήσει νέες ευκαιρίες για ηλεκτρονική απάτη. Παράλληλα, οι φυσικές επιθέσεις σε ΑΤΜ, όπως skimming, παραμένουν ενεργές.

Οι μορφές ηλεκτρονικής απάτης διακρίνονται σε δύο βασικές κατηγορίες:

1. Απάτες που αφορούν issuing (κάρτες πληρωμών)
2. Απάτες Web & Mobile Banking

3.1 Απάτες Issuing (Κάρτες Πληρωμών)

Οι απάτες issuing αφορούν περιπτώσεις όπου το μέσο πληρωμής (η κάρτα) ή τα στοιχεία της χρησιμοποιούνται χωρίς τη συγκατάθεση του νόμιμου κατόχου. Το issuing ίδρυμα (η τράπεζα που εκδίδει την κάρτα) φέρει την κύρια ευθύνη για την ανίχνευση, πρόληψη και απορρόφηση των ζημιών.

Η φύση αυτών των απατών συνδέεται με την έννοια της ταυτοποίησης του κατόχου και της αυθεντικότητας του μέσου πληρωμής.

3.1.1 Card Theft (Κλοπή Κάρτας)

Η κλοπή κάρτας αποτελεί την πιο παραδοσιακή μορφή απάτης καρτών και σχετίζεται με τη φυσική απώλεια του μέσου πληρωμής.

Θεωρητική φύση της απάτης

Σε αυτή την περίπτωση, ο δράστης αποκτά **φυσικό έλεγχο** της κάρτας. Η κάρτα λειτουργεί ως φορέας πληρωμής που, εάν δεν απαιτείται επιπλέον ισχυρή ταυτοποίηση, μπορεί να χρησιμοποιηθεί από τρίτο πρόσωπο.

Η απάτη βασίζεται στην υπόθεση ότι η κατοχή της κάρτας ισοδυναμεί με εξουσιοδότηση — υπόθεση που δεν ισχύει, αλλά σε πρακτικό επίπεδο δημιουργεί κενό ασφαλείας.

Τρόποι εκδήλωσης

- κλοπή πορτοφολιού ή τσάντας
- αφαίρεση κάρτας σε ΑΤΜ ή κατάστημα
- χρήση για ανέπαφες ή μικρές συναλλαγές χωρίς PIN

Θεωρητική πρόκληση

Η δυσκολία έγκειται στη διάκριση μεταξύ νόμιμης και παράνομης χρήσης πριν την αναφορά της κλοπής.

Πρόληψη (θεωρητική προσέγγιση)

Η πρόληψη βασίζεται στη μείωση του χρόνου μεταξύ απώλειας και απενεργοποίησης, καθώς και σε μηχανισμούς συμπεριφορικής ανάλυσης που ανιχνεύουν αποκλίσεις.

[\(European Central Bank \(ECB\). \(2023\). Payment cards fraud statistics.\)](#)

3.1.2 Card-Not-Present (CNP) Fraud

Αφορά συναλλαγές όπου η κάρτα δεν βρίσκεται φυσικά παρούσα.

Θεωρητική βάση

Η CNP απάτη εκμεταλλεύεται τη **μετατροπή της κάρτας από φυσικό αντικείμενο σε σύνολο ψηφιακών δεδομένων**. Η επαλήθευση δεν γίνεται μέσω φυσικής παρουσίας αλλά μέσω στοιχείων (αριθμός, ημερομηνία λήξης, CVV).

Χαρακτηριστικά

- απουσία φυσικής ταυτοποίησης
- αυξημένη εξάρτηση από πληροφοριακά δεδομένα
- διεθνής διάσταση

Θεωρητικό πρόβλημα

Η απόδειξη ταυτότητας βασίζεται στη γνώση και όχι στην κατοχή, κάτι που αυξάνει την επιφάνεια επίθεσης.

[European Central Bank – FraudReport](#)

3.1.3 Skimming

Το skimming συνδέεται με την υποκλοπή στοιχείων από φυσικά τερματικά.

Θεωρητική διάσταση

Αποτελεί «τεχνολογική επέκταση» της φυσικής απάτης. Ο δράστης δεν κλέβει την κάρτα αλλά αντιγράφει την ταυτότητά της.

Μηχανισμός

Η πληροφορία της μαγνητικής ταινίας αναπαράγεται, επιτρέποντας τη δημιουργία αντιγράφου.

Κρίσιμο σημείο

Η ύπαρξη παλαιών τεχνολογιών (μαγνητική ταινία) δημιουργεί δομική ευπάθεια.

3.1.4 BIN Attacks / Fraud MIDs

Οι επιθέσεις τύπου BIN είναι καθαρά ψηφιακές και συνήθως στοχεύουν σε συγκεκριμένες ομάδες καρτών, με βάση τα **BIN (Bank Identification Numbers)** τους. Σε ορισμένες περιπτώσεις, παρατηρούνται διαρροές στοιχείων καρτών, οι οποίες στη συνέχεια χρησιμοποιούνται για μαζικές, παράνομες συναλλαγές. Τέτοιες επιθέσεις συνήθως πραγματοποιούνται μέσω **mail order** ή **e-commerce** συναλλαγών, όπου η εισαγωγή των στοιχείων γίνεται χειροκίνητα, γεγονός που τις καθιστά δύσκολες στον εντοπισμό.

Η επίδραση αυτών των επιθέσεων στις επιχειρήσεις μπορεί να είναι σημαντική, καθώς εκτός από τη ζημιά στη φήμη, μπορεί να προκληθεί και **ουσιαστική οικονομική απώλεια**, λόγω ακυρωμένων συναλλαγών, επιστροφών χρημάτων και πιθανών προστίμων από χρηματοπιστωτικά ιδρύματα. Συνεπώς, η πρόληψη και η προστασία από τέτοιου είδους επιθέσεις είναι κρίσιμη για την ασφάλεια των ψηφιακών συναλλαγών και τη διατήρηση της εμπιστοσύνης των πελατών.

Θεωρητική φύση

Η κάρτα αντιμετωπίζεται ως αριθμητικό πρότυπο. Οι εγκληματίες χρησιμοποιούν αλγοριθμική λογική για παραγωγή έγκυρων συνδυασμών.

Ιδιαιτερότητα

Δεν απαιτείται φυσική ή προηγούμενη κλοπή στοιχείων — πρόκειται για στατιστική εκμετάλλευση της δομής αρίθμησης.

[Visa Fraud Prevention Guide](#)

[Mastercard Fraud Manual](#)

3.1.5 SIM Swap

Θεωρητική διάσταση

Η απάτη αυτού του τύπου δεν στοχεύει απευθείας την κάρτα, αλλά τον **δεύτερο παράγοντα ταυτοποίησης** του χρήστη. Για παράδειγμα, ο έλεγχος του **τηλεφωνικού αριθμού** ισοδυναμεί ουσιαστικά με έλεγχο του μηχανισμού ασφαλείας, καθώς επιτρέπει στον επιτήδριο πρόσβαση σε όλα τα στοιχεία του θύματος, από οικονομικά δεδομένα έως προσωπικές πληροφορίες.

Σε αυτήν την περίπτωση, ακόμη και η αλλαγή της **SIM (κάρτας τηλεφωνικού παρόχου)** δεν είναι αρκετή για να σταματήσει την απάτη. Το συγκεκριμένο είδος επίθεσης μπορεί να αντιμετωπιστεί μόνο μέσω **αλλαγής της συσκευής ή ολοκληρωτικού καθαρισμού από εξειδικευμένο τεχνικό**, ώστε να αφαιρεθεί τυχόν κακόβουλο λογισμικό ή ιός.

Λόγω του υψηλού κινδύνου, τα **τμήματα ασφαλείας των τραπεζών** προβαίνουν άμεσα σε μέτρα όπως:

- **Κλείδωμα των κωδικών ηλεκτρονικής τραπεζικής**
- **Ακύρωση φυσικών ή εικονικών καρτών**

Τα παραπάνω γίνονται για να προστατευτούν οι πελάτες από οικονομικές απώλειες και για να περιοριστεί οποιαδήποτε περαιτέρω κακόβουλη πρόσβαση στα δεδομένα τους.

Σημασία

Αποδεικνύει ότι η ασφάλεια πληρωμών εξαρτάται από εξωτερικά συστήματα (τηλεπικοινωνίες).

[Europol – CybercrimeReport](#)

3.1.6 Compromised Cards – Data Breaches

Θεωρητική βάση

Η κάρτα ως δεδομένο αποθηκεύεται σε πολλαπλά συστήματα. Κάθε σημείο αποθήκευσης αποτελεί πιθανό σημείο διαρροής.

Διάσταση

Η απάτη εδώ δεν είναι μεμονωμένο γεγονός αλλά αποτέλεσμα συστημικής παραβίασης.

[IBM Security – Cost of Data Breach Report](#)

3.1.7 Friendly Fraud / Chargeback Abuse

Θεωρητική φύση

Πρόκειται για **καταχρηστική εκμετάλλευση των μηχανισμών προστασίας καταναλωτή**. Σε αυτήν την περίπτωση, η απάτη δεν στηρίζεται σε τεχνολογική παραβίαση, αλλά στην **νομική και διαδικαστική εκμετάλλευση των κανόνων**.

Συνήθως, η επιχείρηση πραγματοποιεί **πακέτα ηλεκτρονικών συναλλαγών** και φυσικών συναλλαγών μέσω POS. Ωστόσο, όταν πραγματοποιηθεί η πληρωμή για αυτά τα πακέτα, την επόμενη ημέρα μπορεί κάποιοι πελάτες να **μην αναγνωρίζουν τις**

συναλλαγές ή να μην είναι ικανοποιημένοι με τις παρεχόμενες υπηρεσίες της επιχείρησης.

Ως αποτέλεσμα, οι πελάτες προχωρούν σε **αμφισβήτηση των συναλλαγών (chargeback)**. Για να προστατευθεί η επιχείρηση από οικονομική ζημία, ζητάει πίσω τα χρήματα από τον εκάστοτε πάροχο υπηρεσιών ή τράπεζα, με στόχο να περιοριστούν οι απώλειες και να διατηρηθεί η οικονομική σταθερότητα της επιχείρησης.

Ιδιαιτερότητα

Ο δράστης είναι ο ίδιος ο πελάτης. Θολώνει τα όρια μεταξύ απάτης και διαφωνίας συναλλαγής.

Συμπέρασμα Ενότητας 3.1

Οι απάτες issuing δείχνουν ότι η κάρτα μπορεί να παραβιαστεί:

- ως φυσικό αντικείμενο
- ως σύνολο δεδομένων
- ως αριθμητικό πρότυπο
- μέσω τρίτων συστημάτων
- μέσω νομικών διαδικασιών

Αυτό αποδεικνύει ότι η ασφάλεια καρτών είναι **πολυεπίπεδο ζήτημα** που συνδυάζει τεχνολογία, ανθρώπινη συμπεριφορά και θεσμικό πλαίσιο.

[Mastercard Chargeback Guide](#)

[Visa Chargeback Management](#)

3.2 Απάτες Web & Mobile Banking – Αναλυτική Ανάλυση

Οι απάτες που αφορούν Web και Mobile Banking εκμεταλλεύονται τόσο τεχνικές αδυναμίες των συστημάτων όσο και ανθρώπινα λάθη ή ψυχολογικές αδυναμίες των χρηστών.

Οι απάτες που αφορούν **Web και Mobile Banking** εκμεταλλεύονται τόσο **τεχνικές αδυναμίες των συστημάτων** όσο και **ανθρώπινα λάθη ή ψυχολογικές αδυναμίες των χρηστών**. Αυτές οι ηλεκτρονικές απάτες χαρακτηρίζονται από **δυναμική εξέλιξη και πολυεπίπεδη φύση**, γεγονός που απαιτεί την εφαρμογή **συνδυαστικών μέτρων πρόληψης**: τεχνολογικά, οργανωτικά και εκπαιδευτικά.

Σε αυτόν τον τύπο απάτης, το **τραπεζικό σύστημα** **ανίχνευσης και αποτροπής** είναι ιδιαίτερα σύνθετο, καθώς η αποτελεσματικότητα εξαρτάται από:

- Τι **στοιχεία** έχει παραχωρήσει ο χρήστης στον επιτήδαιο
- Σε ποιες **συσκευές** έχει γίνει πρόσβαση
- Τι **ενέργειες** πραγματοποιεί στη συνέχεια ο επιτήδειος

Παράλληλα, κρίσιμο ρόλο παίζει η **άμεση και σωστά συντονισμένη αντίδραση** του εκάστοτε τραπεζικού ιδρύματος, προκειμένου να περιοριστεί η απώλεια και να προστατευτούν τα δεδομένα και τα οικονομικά του πελάτη.

Παρακάτω παρουσιάζονται οι κύριες μορφές, με πλήρη ανάλυση.

3.2.1 Περιστατικό απάτης με Phishing

Ορισμός:

Το Phishing είναι η προσπάθεια υποκλοπής διαπιστευτηρίων, προσωπικών ή

χρηματοοικονομικών στοιχείων μέσω αποστολής πλαστών email ή ιστοσελίδων που μιμούνται νόμιμους οργανισμούς.

Μηχανισμός:

- Ο χρήστης λαμβάνει email που φαίνεται ότι προέρχεται από τράπεζα ή άλλο επίσημο φορέα.
- Περιλαμβάνει link σε ψεύτικη ιστοσελίδα, όπου ζητούνται login credentials ή OTP.
- Ο χρήστης εισάγει τα στοιχεία του, τα οποία καταγράφονται από τον επιτήδαιο.

Επιπτώσεις:

- Άμεση πρόσβαση σε λογαριασμούς πελατών
- Αποκάλυψη ευαίσθητων προσωπικών δεδομένων
- Οικονομικές απώλειες

Πρόληψη:

- Εκπαίδευση χρηστών για αναγνώριση ύποπτων email
- Φίλτρα spam και anti-phishing
- Υποχρεωτική χρήση 2FA (Two-Factor Authentication)

Παράδειγμα:

Το 2020, λόγω της πανδημίας **COVID-19**, παρατηρήθηκε σημαντική αύξηση των **phishing e-mails**, τα οποία εμφανίζονταν ως ειδοποιήσεις τραπεζών για υποτιθέμενες αλλαγές στα όρια ανέπαφων πληρωμών, ως πληρωμές προς τον ΕΟΠΠΥ για ιατρικές υπηρεσίες, αλλά και ως επικοινωνίες από υποτιθέμενους λογιστές ή τεχνικούς της ΔΕΔΔΗΕ.

Γενικά, όπως φαίνεται και στους πίνακες που ακολουθούν, κατά το διάστημα 2020-2021 οι ηλεκτρονικές απάτες παρουσίασαν σημαντική αύξηση, με ποικίλους τρόπους και μεθόδους εκτέλεσης.

[Europol – CybercrimeReport](#)

3.2.2 Smishing

Ορισμός:

Smishing είναι το μήνυμα που στέλνουν οι επιτήδαιοι σε κινητές συσκευές μέσω SMS.

Μηχανισμός:

- Ο χρήστης λαμβάνει SMS με link σε πλαστή ιστοσελίδα.
- Συνήθως ζητείται η εισαγωγή διαπιστευτηρίων ή OTP (One Time Password).

Επιπτώσεις:

- Υποκλοπή credentials (Κωδικών πρόσβασης ηλεκτρονικής τραπεζικής ή κωδικούς καρτών)
- Άμεση παραβίαση λογαριασμών
- Δυνατότητα πολλαπλών επιθέσεων μέσω κινητού

Πρόληψη:

- Μην ανοίγετε ύποπτους συνδέσμους
- Έλεγχος αποστολέα και επαλήθευση τους
- Σε περίπτωση που συμβεί ένα τέτοιο περιστατικό άμεση επικοινωνία με τους εκπροσώπους των εκάστοτε τραπεζικών ιδρυμάτων

- Αποφυγή εγκατάστασης εφαρμογών εκτός επίσημων καταστημάτων (PlayStore/AppStore)

Παράδειγμα:

Επιτήδριοι στέλνουν SMS που υποδύονται την τράπεζα και ζητούν “επικαιροποίηση στοιχείων”, με στόχο την υποκλοπή OTP, υποτιθέμενη επιστροφή φόρου, οφειλές λογαριασμών στην ΔΕΗ ή σε κάποιον άλλο πάροχο.

[Europol – CybercrimeReport](#)

3.2.3 Vishing

Ορισμός:

Vishing ουσιαστικά είναι η επικοινωνία μέσω τηλεφώνου του επιτήδειου στο θύμα. Ο δράστης προσποιείται υπάλληλο τράπεζας ή δημόσιας αρχής ή κάποιου άλλου επίσημου φορέα.

Μηχανισμός:

- Κλήση στον πελάτη
- Αίτηση για διαπιστευτήρια ή OTP
- Στόχος η παραβίαση λογαριασμού

Επιπτώσεις:

- Άμεση πρόσβαση σε τραπεζικό λογαριασμό
- Δυνατότητα συνδυασμού με άλλες τεχνικές (π.χ. SIM swap/ Smishing)

Πρόληψη:

- Επιβεβαίωση καλούντων μέσω επίσημων καναλιών και επαλήθευση αυτών.

- Εκπαίδευση για αναγνώριση fraud κλήσεων
- Μη παροχή προσωπικών στοιχείων τηλεφωνικά

Παράδειγμα:

Οι τράπεζες αναφέρουν **αύξηση κλήσεων** όπου ο αριθμός εμφανίζεται με **Caller ID τράπεζας**, με στόχο τη **λήψη του OTP** από τον πελάτη. Συχνά πρόκειται για περιστατικά όπου οι επιτήδριοι προσποιούνται **υποτιθέμενους λογιστές**, ενημερώνοντας τους πελάτες ότι έχουν **επιστροφή φόρου** ή ότι πρέπει να **καταβάλουν κάποιο επιπλέον ποσό** σε πάροχο ηλεκτρικής ενέργειας.

Τέτοιες πρακτικές βασίζονται στην **ψυχολογική πίεση και στην εκμετάλλευση της εμπιστοσύνης** του χρήστη, καθιστώντας απαραίτητη την **ενημέρωση και ευαισθητοποίηση των πελατών** για την προστασία των προσωπικών και οικονομικών τους δεδομένων.

[Europol – Cyber crime Report](#)

3.2.4 Investment Fraud

Ορισμός:

Αυτό το είδος απάτης έχει πλέον καταστεί **ένα από τα μεγαλύτερα και πιο διαδεδομένα προβλήματα** σχεδόν σε όλες τις τράπεζες. Στην περίπτωση αυτή, **υποτιθέμενες επενδυτικές εταιρείες** προσεγγίζουν πιθανούς επενδυτές, υποσχόμενες **υψηλές αποδόσεις σε κρυπτονομίσματα**.

Η συνήθης τακτική των επιτηδίων είναι να πείσουν το θύμα να παρέχει **απομακρυσμένη πρόσβαση** στον ηλεκτρονικό του υπολογιστή ή τη συσκευή του.

Με αυτόν τον τρόπο, ο επιτήδειος αποκτά **πλήρη πρόσβαση στα τραπεζικά και προσωπικά δεδομένα** του θύματος.

Στη συνέχεια, η επίθεση ολοκληρώνεται με την αποστολή **συνδέσμου (link)**, ο οποίος, αν ανοιχθεί, εγκαθιστά **κακόβουλο λογισμικό** στη συσκευή του θύματος, είτε πρόκειται για κινητό τηλέφωνο είτε για ηλεκτρονικό υπολογιστή, επιτρέποντας στον επιτήδειο να εκμεταλλευτεί πλήρως την πρόσβαση.

Μηχανισμός:

- Διαφήμιση ψεύτικων πλατφορμών ή apps
- Υποκλοπή χρημάτων κατά την κατάθεση
- Συχνά εκμετάλλευση COVID-19 ή οικονομικής αβεβαιότητας

Επιπτώσεις:

- Οικονομικές απώλειες
- Απώλεια εμπιστοσύνης σε ηλεκτρονικές επενδύσεις

Πρόληψη:

- Έλεγχος αδειών επενδυτικών πλατφορμών
- Ενημέρωση χρηστών για ύποπτες επενδύσεις

Παράδειγμα:

Η **Ευρωπαϊκή Αρχή** έχει αναφέρει πλατφόρμες που εμφανίζονται ως **“crypto trading apps”** και απορροφούν κεφάλαια μέσω **phishing επιθέσεων**. Συχνά, οι επιτήδειοι προσπαθούν να **διαφημίσουν και επίσημα site**, τα οποία υποτίθεται ότι ανήκουν σε επενδυτικές τράπεζες, ενώ στην πραγματικότητα τα θύματα λειτουργούν για **ιδιωτικό όφελος των επιτηδείων**.

Για να ενισχύσουν την αξιοπιστία τους, χρησιμοποιούν **γνωστά ονόματα τραπεζών ή πλατφορμών** όπως η **Binance, Moonpay** κ.ά., εξαπατώντας έτσι τους χρήστες και καθιστώντας δύσκολη την αναγνώριση της απάτης.

[European Securities and Markets Authority \(ESMA\)](#)

3.2.5 Microsoft / Tech Support Scam

Ορισμός:

Σε αυτήν την περίπτωση, οι επιτήδριοι καλούν από **άγνωστα νούμερα**, κυρίως σε **κινητές συσκευές** ανυποψίαστων πολιτών, προσποιούμενοι **υποτιθέμενους τεχνικούς της Microsoft**. Το συγκεκριμένο είδος απάτης είναι από τα **πιο επικίνδυνα**, καθώς μπορεί να λάβει **μεγάλες διαστάσεις**.

Μέσω αυτής της απάτης, ο επιτήδειος μπορεί να αποκτήσει:

- **Απομακρυσμένη πρόσβαση** στη συσκευή του θύματος
- Πρόσβαση σε **τραπεζικούς κωδικούς** και **άλλα προσωπικά στοιχεία**
- Να εγκαταστήσει **κακόβουλο λογισμικό (malware / Trojan)** μέσω προγραμμάτων που το θύμα θα κατεβάσει

Στην περίπτωση που η συσκευή έχει μολυνθεί, η **επίλυση του προβλήματος απαιτεί εκκαθάριση ολόκληρου του υπολογιστή από εξειδικευμένο τεχνικό**, για να αφαιρεθεί πλήρως το κακόβουλο λογισμικό και να αποκατασταθεί η ασφάλεια των δεδομένων.

Μηχανισμός:

- Κλήση ή email

- Πειθώ για εγκατάσταση remote access software
- Αποκτούν έλεγχο συστήματος ή ζητούν πληρωμή

Επιπτώσεις:

- Κατάληψη συσκευής
- Υποκλοπή προσωπικών/τραπεζικών δεδομένων
- Πιθανή εγκατάσταση malware

Πρόληψη:

- Αποφυγή παροχής πρόσβασης
- Επιβεβαίωση από επίσημη υποστήριξη
- Εκπαίδευση χρηστών

[Microsoft Cybersecurity Report](#)

3.2.6 Account Takeover (ATO)

Ορισμός:

Παραβίαση λογαριασμού πελάτη μέσω compromised credentials ή phishing.

Μηχανισμός:

- Αποκτούν login + password ή OTP
- Εκτελούν μη εξουσιοδοτημένες συναλλαγές

Επιπτώσεις:

- Άμεσες οικονομικές απώλειες
- Αλλοίωση ιστορικού συναλλαγών

Πρόληψη:

- 2FA
- Real-time alerts σε ασυνήθιστες κινήσεις
- Παρακολούθηση suspicious login patterns

[Accenture – Fraud Detection in Banking](#)

3.2.7 Social Engineering Attacks

Ορισμός:

Χειραγώγηση ανθρώπων για να παραδώσουν ευαίσθητες πληροφορίες (password, PIN).

Μηχανισμός:

- Αλληλεπιδράσεις που δημιουργούν εμπιστοσύνη ή φόβο
- Εκμετάλλευση ανθρώπινων αντιδράσεων

Επιπτώσεις:

- Παραβίαση λογαριασμών
- Συνδυασμένες επιθέσεις με phishing ή CNP fraud

Πρόληψη:

- Εκπαίδευση χρηστών
- Awareness campaigns
- Διαδικασίες ασφαλείας

[Europol – CybercrimeReport](#)

3.2.8 Money Mules και Νομιμοποίηση Εσόδων

Ορισμός:

Ο όρος **Money Mule** αναφέρεται σε άτομα που χρησιμοποιούνται από εγκληματικές οργανώσεις για τη μεταφορά ή την απόκρυψη **παράνομων χρημάτων**, συχνά με σκοπό τη **νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες (money laundering)**. Συχνά, οι moneymules δεν γνωρίζουν πλήρως ότι συμμετέχουν σε παράνομη δραστηριότητα, γεγονός που τους καθιστά **ανυποψίαστους συνεργούς**.

Τρόποι λειτουργίας:

- Οι εγκληματίες προσεγγίζουν τα θύματα μέσω **διαδικτύου**, email, social media ή αγγελιών εργασίας.
- Το άτομο καλείται να **λάβει και να μεταφέρει χρήματα** σε λογαριασμούς τρίτων, είτε ηλεκτρονικά είτε μέσω τραπεζικών καταθέσεων.
- Σε άλλες περιπτώσεις, ζητείται από το θύμα να ανοίξει **λογαριασμό ή ηλεκτρονικό πορτοφόλι** για λογαριασμό τρίτου, χωρίς να γνωρίζει την παράνομη προέλευση των χρημάτων.

Σκοπός των εγκληματιών:

- Απόκρυψη της πηγής των χρημάτων (π.χ., απάτες, phishing, cybercrime)
- Μεταφορά χρημάτων σε διαφορετικές χώρες, καθιστώντας δύσκολη την ανάχνευση από τις αρχές
- Διευκόλυνση της **νομιμοποίησης εσόδων από παράνομες δραστηριότητες** μέσω δικτύων money mules

Κίνδυνοι για τα θύματα:

- **Ποινικές ευθύνες:** Ακόμη και αν το άτομο είναι ανυποψίαστο, η νομοθεσία σε πολλές χώρες προβλέπει ποινικές κυρώσεις για συμμετοχή σε παράνομες οικονομικές δραστηριότητες.
- **Οικονομικές απώλειες:** Αν τα χρήματα κατασχεθούν από τις αρχές, το θύμα μπορεί να χάσει οποιοδήποτε ποσό έχει μεταφέρει.
- **Απώλεια προσωπικών δεδομένων:** Οι εγκληματίες συχνά συλλέγουν προσωπικά στοιχεία κατά τη διαδικασία, τα οποία μπορούν να χρησιμοποιηθούν για περαιτέρω απάτες ή κλοπή ταυτότητας.

Παραδείγματα:

- Οι τράπεζες αναφέρουν συχνά περιπτώσεις όπου χρήστες προσεγγίζονται με πρόσχημα ευκαιρίες εργασίας από το σπίτι ή επενδύσεις υψηλής απόδοσης, και εν συνεχεία καλούνται να «μεταφέρουν» τα χρήματα για λογαριασμό της εταιρείας.
- Σε διαδικτυακές απάτες τύπου phishing ή romance scams, τα θύματα συχνά χρησιμοποιούνται ως money-mules χωρίς να αντιλαμβάνονται ότι εξυπηρετούν εγκληματικά δίκτυα.

Μέτρα πρόληψης:

- Εκπαίδευση του κοινού σχετικά με τις απάτες και τα προειδοποιητικά σημάδια
- Έλεγχος προσφορών εργασίας ή επενδύσεων που ζητούν πρόσβαση σε λογαριασμούς τρίτων
- Άμεση αναφορά ύποπτων συναλλαγών στις τράπεζες ή στις αρμόδιες αρχές

Μηχανισμός:

- Εγκληματίες χρησιμοποιούν λογαριασμούς τρίτων για μεταφορά κεφαλαίων
- Συνδυάζεται συχνά με phishing ή ΑΤΟ

Επιπτώσεις:

- Νομικές ευθύνες για ανυποψίαστους πολίτες
- Επιπλέον οικονομική απώλεια για τράπεζες

Πρόληψη:

- KYC διαδικασίες
- Παρακολούθηση συναλλαγών
- Εκπαίδευση χρηστών

Europol – Money Mule Campaign Report

3.2.9 Συνδυασμένες Επιθέσεις (Hybrid Fraud)

Ορισμός:

Συνδυασμός πολλαπλών τεχνικών για μεγαλύτερη αποτελεσματικότητα (π.χ., phishing + card fraud + SIM swap).

Μηχανισμός:

- Εκμετάλλευση τεχνικών κενών και ανθρώπινων αδυναμιών
- Πολυεπίπεδη επίθεση που συχνά παρακάμπτει κανόνες fraud detection

Επιπτώσεις:

- Πολυδιάστατες οικονομικές απώλειες
- Δυσκολία ανίχνευσης

Πρόληψη:

- Ολοκληρωμένα συστήματα ανίχνευσης fraud
- Εκπαίδευση προσωπικού και πελατών
- Συνδυαστική ανάλυση κινδύνων

3.3 Παράγοντες που Ενισχύουν την Ηλεκτρονική Απάτη

Η αύξηση της ηλεκτρονικής απάτης δεν αποτελεί τυχαίο φαινόμενο, αλλά αποτέλεσμα της σύγκλισης τεχνολογικών, κοινωνικών και οικονομικών παραμέτρων. Οι παράγοντες αυτοί δημιουργούν ένα περιβάλλον αυξημένης τρωτότητας, όπου η ταχύτητα της ψηφιοποίησης υπερβαίνει συχνά την ωριμότητα των μηχανισμών ασφάλειας.

• Ψηφιακός μετασχηματισμός των πληρωμών

Η ραγδαία μετάβαση σε ψηφιακές πλατφόρμες πληρωμών αύξησε δραματικά την επιφάνεια επίθεσης (attack surface). Κάθε νέα εφαρμογή mobile banking, API open banking, e-wallet ή online merchant portal αποτελεί δυνητικό σημείο εισόδου κακόβουλων δραστηριοτήτων.

Ο ψηφιακός μετασχηματισμός χαρακτηρίζεται από:

- αυξημένη διασυνδεσιμότητα συστημάτων
- cloud υποδομές
- απομακρυσμένη πρόσβαση χρηστών

Αυτά τα στοιχεία, ενώ ενισχύουν την αποδοτικότητα, δημιουργούν περιβάλλοντα όπου η παραβίαση ενός συστήματος μπορεί να επιφέρει αλυσιδωτές συνέπειες.

• Ανθρώπινος παράγοντας

Η πλειονότητα των επιθέσεων εκμεταλλεύεται γνωστικές αδυναμίες και όχι τεχνικά κενά. Φαινόμενα όπως:

- υπερβολική εμπιστοσύνη σε φαινομενικά επίσημες επικοινωνίες
- έλλειψη ψηφιακού αλφαριθμητισμού
- βιασύνη σε διαδικασίες πληρωμών

οδηγούν σε επιτυχία phishing, vishing και social engineering. Ο ανθρώπινος παράγοντας μετατρέπεται έτσι σε κρίσιμο σημείο τρωτότητας του οικοσυστήματος πληρωμών.

• Οικονομικές πιέσεις και κοινωνικές συνθήκες

Περίοδοι οικονομικής αβεβαιότητας, όπως μετά την πανδημία, συνδέονται με αύξηση επενδυτικών απατών και απάτης μέσω ψευδών ευκαιριών εργασίας. Οι πολίτες γίνονται πιο ευάλωτοι σε υποσχέσεις γρήγορου κέρδους ή οικονομικής ανακούφισης.

• Τεχνολογική πρόοδος των δραστών

Οι εγκληματικές ομάδες χρησιμοποιούν:

- αυτοματοποιημένα bot-nets
- AI για δημιουργία πειστικών phishing emails
- darkweb αγορές δεδομένων

Η επαγγελματικοποίηση της απάτης μετατρέπει τις επιθέσεις σε βιομηχανική δραστηριότητα.

3.4 Επιπτώσεις της Ηλεκτρονικής Απάτης

Η απάτη δεν επηρεάζει μόνο μεμονωμένους χρήστες αλλά ολόκληρο το χρηματοπιστωτικό σύστημα.

- **Οικονομικές επιπτώσεις**

Περιλαμβάνουν άμεσες ζημίες από μη εξουσιοδοτημένες συναλλαγές και έμμεσες απώλειες από:

- αποζημιώσεις
- νομικά έξοδα
- επενδύσεις σε συστήματα ασφάλειας

- **Επιπτώσεις στη φήμη**

Η εμπιστοσύνη αποτελεί θεμέλιο των ψηφιακών πληρωμών. Συνεχόμενα περιστατικά απάτης μειώνουν την προθυμία χρήσης ηλεκτρονικών καναλιών.

- **Ψυχολογικές επιπτώσεις στους χρήστες**

Θύματα απάτης συχνά εμφανίζουν άγχος, απώλεια εμπιστοσύνης στην τεχνολογία και αποφυγή ψηφιακών συναλλαγών.

- **Συστημικός κίνδυνος**

Μαζικές επιθέσεις μπορούν να διαταράξουν τη σταθερότητα του συστήματος πληρωμών, ιδίως όταν συνδυάζονται με κυβερνοεπιθέσεις.

3.5 Μηχανισμοί Πρόληψης

- **Τεχνολογικοί μηχανισμοί**

Περιλαμβάνουν κρυπτογράφηση, tokenization, biometric authentication, behaviour analytics. Η πρόληψη μετατοπίζεται από στατικές άμυνες σε δυναμικά συστήματα ανίχνευσης ανωμαλιών.

- **Κανονιστικά μέτρα**

Η εφαρμογή SCA, PSD2 και reporting υποχρεώσεων δημιουργεί δομικά εμπόδια στην απάτη, αλλά απαιτεί συνεχή προσαρμογή.

- **Εκπαίδευση χρηστών**

Η ενίσχυση της ψηφιακής παιδείας μειώνει την αποτελεσματικότητα social engineering.

3.6 Προκλήσεις στην Αντιμετώπιση

- **Εξισορρόπηση ασφάλειας – εμπειρίας χρήστη**

Η αυστηρή ασφάλεια μπορεί να οδηγήσει σε εγκατάλειψη συναλλαγών.

- **Προσαρμοστικότητα των δραστών**

Κάθε νέο μέτρο οδηγεί σε εξέλιξη των τεχνικών απάτης.

- **Διασυνοριακή φύση**

Οι επιθέσεις ξεπερνούν εθνικές δικαιοδοσίες, δυσχεραίνοντας τη δίωξη.

3.7 Συστημική Προσέγγιση

Η απάτη πρέπει να αντιμετωπίζεται ως **οικοσύστημα κινδύνου**. Απαιτείται:

- συνεργασία τραπεζών
- ανταλλαγή πληροφοριών

- ενοποιημένη εποπτεία
- τεχνολογική και ανθρώπινη θωράκιση

Η ολιστική προσέγγιση συνδυάζει τεχνολογία, ρύθμιση και συμπεριφορική ανάλυση.

ΚΕΦΑΛΑΙΟ 4 - ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΑΠΑΤΩΝ

Οι ηλεκτρονικές απάτες αποτελούν έναν από τους σημαντικότερους και ταχύτερα εξελισσόμενους κινδύνους στο σύγχρονο χρηματοπιστωτικό περιβάλλον. Οι επιπτώσεις τους είναι πολυεπίπεδες και επηρεάζουν άμεσα όχι μόνο τους τελικούς χρήστες των υπηρεσιών (καταναλωτές), αλλά και τις επιχειρήσεις που δέχονται πληρωμές, καθώς και τα ίδια τα χρηματοπιστωτικά ιδρύματα που λειτουργούν ως πάροχοι υπηρεσιών πληρωμών. Το σύνολο αυτών των επιπτώσεων δημιουργεί ένα πλέγμα οικονομικών, λειτουργικών, νομικών και θεσμικών συνεπειών, οι οποίες καθιστούν επιτακτική την ανάπτυξη ολοκληρωμένων στρατηγικών αντιμετώπισης του φαινομένου.

4.1 Επιπτώσεις στους πελάτες

Οι πελάτες –είτε πρόκειται για ιδιώτες είτε για μικρές επιχειρήσεις– αποτελούν συχνά τον πιο ευάλωτο κρίκο στην αλυσίδα των ψηφιακών συναλλαγών. Οι βασικές επιπτώσεις της ηλεκτρονικής απάτης στους χρήστες περιλαμβάνουν:

1. Οικονομική ζημία

- Απώλεια χρημάτων μέσω μη εξουσιοδοτημένων συναλλαγών.
- Καθυστέρηση στην επιστροφή ποσών, ακόμα και όταν η τράπεζα αναγνωρίζει την απάτη.
- Κίνδυνος μη αποζημίωσης όταν αποδειχθεί αμέλεια εκ μέρους του πελάτη (π.χ. αποκάλυψη PIN ή κωδικών).

2. Ψυχολογική επιβάρυνση

- Αίσθηση ανασφάλειας κατά τη χρήση ηλεκτρονικών υπηρεσιών.
- Απώλεια εμπιστοσύνης στην τεχνολογία και στις τράπεζες.
- Άγχος και φόβος επανάληψης του περιστατικού.

3. Λειτουργική ταλαιπωρία

- Απενεργοποίηση καρτών, επανέκδοση νέων μέσων πληρωμών, αλλαγή κωδικών.
- Ενδεχόμενοι προσωρινοί περιορισμοί στους λογαριασμούς κατά τη διάρκεια της έρευνας.
- Χρονοβόρες διαδικασίες υποβολής καταγγελιών και δικαιολογητικών.

4. Παραβίαση προσωπικών δεδομένων

- Διαρροή ευαίσθητων δεδομένων (credentials, ΑΦΜ, τηλέφωνο, στοιχεία identity).
- Μακροχρόνιος κίνδυνος περαιτέρω εκμετάλλευσης σε νέες μορφές απάτης (π.χ. social engineering).

4.2 Επιπτώσεις στις επιχειρήσεις

Οι επιχειρήσεις επηρεάζονται άμεσα από τις ηλεκτρονικές απάτες, ειδικά όταν λειτουργούν με υψηλούς όγκους ηλεκτρονικών πληρωμών μέσω POS, e-commerce ή τιμολογήσεων.

1. Οικονομική ζημία

- Χρεώσεις chargebacks όταν η συναλλαγή αμφισβητηθεί από τον πελάτη.
- Απώλεια εσόδων σε περιπτώσεις disputed fraud ή card-not-present fraud.
- Πιθανή κάλυψη του ποσού απάτης όταν η επιχείρηση δεν τήρησε τα security protocols.

2. Λειτουργικό κόστος

- Διακοπή συναλλαγών λόγω ελέγχου ασφαλείας.
- Κίνδυνος αποκλεισμού ή περιορισμού από παρόχους πληρωμών σε υποθέσεις υψηλού ρίσκου.
- Ανάγκη επενδύσεων σε συστήματα ασφαλείας, monitoring, training προσωπικού.

3. Επιπτώσεις στη φήμη της επιχείρησης

- Μείωση εμπιστοσύνης των πελατών που ενδεχομένως θεωρούν την επιχείρηση «μη ασφαλή».
- Απώλεια πελατείας, ιδιαίτερα στο ηλεκτρονικό εμπόριο.
- Αρνητική προβολή στα μέσα κοινωνικής δικτύωσης σε περίπτωση μεγάλης παραβίασης.

4. Νομικοί και συμβατικοί κίνδυνοι

- Ποινές από παρόχους πληρωμών (π.χ. Visa/Mastercard monitoring programs).
- Ευθύνη σε περιπτώσεις παραβίασης οδηγιών PCI-DSS ή GDPR.
- Δικαστικές διεκδικήσεις από πελάτες.

4.3 Οικονομικό κόστος για τα χρηματοπιστωτικά ιδρύματα

Τα χρηματοπιστωτικά ιδρύματα φέρουν ένα σημαντικό μέρος του συνολικού κόστους της απάτης, τόσο άμεσα όσο και έμμεσα.

1. Άμεσο οικονομικό κόστος

- Κάλυψη μη εξουσιοδοτημένων συναλλαγών όταν ο πελάτης δεν ευθύνεται.
- Αποζημιώσεις προς επιχειρήσεις ή τρίτους.
- Κόστη επιστροφών (refunds), chargebacks και dispute management.

2. Κόστος λειτουργίας συστημάτων ασφαλείας

- Συνεχής αναβάθμιση συστημάτων fraud detection & fraud prevention.
- Επενδύσεις σε τεχνολογίες AI/ML για real-time transaction monitoring.
- Εξειδικευμένο προσωπικό σε τμήματα security, anti-fraud, compliance και risk management.

3. Έμμεσες χρηματοοικονομικές επιπτώσεις

- Αύξηση λειτουργικής πολυπλοκότητας λόγω νέων κανονιστικών απαιτήσεων.
- Πιθανή μείωση εσόδων σε περίπτωση περιορισμού ύποπτων συναλλαγών.
- Κόστος αντιμετώπισης περιστατικών σε επίπεδο crisis management.

4.4 Επιπτώσεις στη φήμη των τραπεζών

Η φήμη αποτελεί στρατηγικό πόρο για κάθε χρηματοπιστωτικό ίδρυμα. Η εμφάνιση περιστατικών απάτης επηρεάζει την αξιοπιστία της τράπεζας με διάφορους τρόπους:

1. Μείωση εμπιστοσύνης των πελατών

- Αμφισβήτηση της ικανότητας της τράπεζας να προστατεύει τα χρήματα και τα δεδομένα τους.
- Μετακίνηση πελατών σε άλλους παρόχους με perceived καλύτερη ασφάλεια.

2. Αρνητική δημοσιότητα

- Παρουσίαση περιστατικών σε MME, ειδησεογραφικά portals, social media.
- Δημιουργία αρνητικής εικόνας για την τεχνολογική επάρκεια της τράπεζας.

3. Επιπτώσεις στη σχέση με επιχειρηματικούς συνεργάτες

- Αμφισβήτηση της αξιοπιστίας σε εξωτερικούς παρόχους, fintechs, επιχειρήσεις.
- Απροθυμία συνεργασιών σε περιβάλλον αυξημένου ρίσκου.

[Accenture Banking Fraud Study](#)

4.5 Ρυθμιστικές κυρώσεις & νομικοί κίνδυνοι

Οι τράπεζες και τα ιδρύματα πληρωμών υπόκεινται σε αυστηρό κανονιστικό πλαίσιο (PSD2, AML, GDPR, οδηγίες EKT και ΤτΕ). Παραβάσεις οδηγούν σε σημαντικούς κινδύνους:

1. Ρυθμιστικές κυρώσεις

- Πρόστιμα από εθνικές εποπτικές αρχές (Τράπεζα της Ελλάδος, EKT).
- Κυρώσεις από ευρωπαϊκούς οργανισμούς σε περίπτωση μη συμμόρφωσης.
- Ένταξη σε monitoring programs από διεθνή card schemes.

2. Νομικές διεκδικήσεις

- Αγωγές από θύματα απάτης που ζητούν αποζημίωση.
- Ευθύνη της τράπεζας σε περιστατικά διαρροής δεδομένων (GDPR fines).
- Ποινικές ευθύνες σε περιπτώσεις συστημικών αδυναμιών ή ελλιπούς ελέγχου.

3. Αυξημένες υποχρεώσεις συμμόρφωσης

- Ενίσχυση διαδικασιών KYC, AML & transaction monitoring.
- Αυξημένος διοικητικός φόρτος για reporting περιστατικών απάτης.
- Επικαιροποίηση πολιτικών ασφάλειας και auditing.

ΚΕΦΑΛΑΙΟ 5 – ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΟΥ ΙΔΡΥΜΑΤΟΣ (NBG Pay)

Η μελέτη περίπτωσης της NBG Pay στοχεύει στην παρουσίαση της λειτουργίας ενός σύγχρονου χρηματοπιστωτικού οργανισμού ψηφιακών πληρωμών, στην ανάλυση των κινδύνων απάτης που αντιμετωπίζει, καθώς και στη διερεύνηση των επιπτώσεων τόσο για τις επιχειρήσεις–πελάτες όσο και για την ίδια την τράπεζα.

5.1 Παρουσίαση του οργανισμού NBG Pay

Η επιλογή της NBG Pay ως μελέτης περίπτωσης βασίστηκε στον κομβικό ρόλο της στην ελληνική αγορά ψηφιακών πληρωμών, στη συνεργασία της με μεγάλο αριθμό επιχειρήσεων και στη δυνατότητα πρόσβασης σε πρακτικά δεδομένα και διαδικασίες διαχείρισης κινδύνου. Επιπλέον, η NBG Pay αποτελεί χαρακτηριστικό παράδειγμα

σύγχρονου παρόχου υπηρεσιών πληρωμών που συνδυάζει τραπεζικές και τεχνολογικές υποδομές.

Το NBG Pay αποτελεί τον άμεσο συνεργάτη της Εθνικής Τράπεζας της Ελλάδος και το μεγαλύτερο ποσοστό της ανήκει στην μεγάλη πολυεθνική πάροχο πληρωμών την Global Payments. Κυρίως, εξειδικεύεται στις ηλεκτρονικές πληρωμές και η λειτουργία του οργανισμού περιλαμβάνει τα εξής κάτωθι:

- **Στρατηγικός ρόλος:** Ενίσχυση της ψηφιακής παρουσίας του Ομίλου της Εθνικής Τράπεζας και παροχή ολοκληρωμένων λύσεων ηλεκτρονικών πληρωμών όσον αφορά στις επιχειρήσεις και άλλους κλάδους
- **Ρυθμιστικό πλαίσιο:** Συμμόρφωση με τις ευρωπαϊκές οδηγίες PSD2, AML, και τις απαιτήσεις της Τράπεζας της Ελλάδος.
- **Πελατολόγιο:** Μικρές και μεσαίες επιχειρήσεις, μεγάλες εταιρείες και τελικοί χρήστες που χρησιμοποιούν mobile payments, POS και e-commerce πλατφόρμες.
- **Κύριες υπηρεσίες:** Διαχείριση πληρωμών μέσω POS και e-commerce, ασφαλής επεξεργασία συναλλαγών, παροχή APIs για ενοποίηση με ERP και CRM συστήματα επιχειρήσεων.

5.2 Ρόλος στις ψηφιακές πληρωμές

Η NBG Pay λειτουργεί ως ενδιάμεσος φορέας παροχής υπηρεσιών πληρωμών, διαδραματίζοντας καθοριστικό ρόλο στη διασφάλιση της ομαλής εκτέλεσης των χρηματοοικονομικών συναλλαγών και της προστασίας του ψηφιακού οικοσυστήματος πληρωμών. Η λειτουργία της συμβάλλει στη διατήρηση της αξιοπιστίας των ηλεκτρονικών συναλλαγών, μέσω μηχανισμών ελέγχου, διαχείρισης κινδύνου και

συμμόρφωσης με το κανονιστικό πλαίσιο. Ειδικότερα, οι βασικές λειτουργίες της περιλαμβάνουν τα ακόλουθα:

Εκκαθάριση και μεταφορά κεφαλαίων

Η NBG Pay είναι υπεύθυνη για τη διαχείριση της εκκαθάρισης και μεταφοράς κεφαλαίων μεταξύ καταναλωτών και επιχειρήσεων, διασφαλίζοντας την ταχεία και ασφαλή ολοκλήρωση των συναλλαγών, συχνά σε πραγματικό χρόνο. Η διαδικασία αυτή μειώνει λειτουργικούς κινδύνους, περιορίζει καθυστερήσεις και διασφαλίζει την ακεραιότητα των χρηματοοικονομικών ροών, ενισχύοντας την εμπιστοσύνη των χρηστών στο σύστημα ηλεκτρονικών πληρωμών.

Παρακολούθηση συναλλαγών και πρόληψη απάτης (Fraud Detection and Prevention)

Κεντρικό στοιχείο της λειτουργίας της αποτελεί η συνεχής παρακολούθηση των συναλλαγών μέσω προηγμένων αυτοματοποιημένων συστημάτων ανάλυσης δεδομένων και συμπεριφορικών προτύπων. Συγκεκριμένα, εφαρμόζεται εξειδικευμένο εργαλείο ανίχνευσης απάτης, στο οποίο έχουν ενσωματωθεί συγκεκριμένοι κανόνες αξιολόγησης κινδύνου και μηχανισμοί φιλτραρίσματος συναλλαγών.

Οι μηχανισμοί αυτοί επιτρέπουν τον εντοπισμό ασυνήθιστων ή ύποπτων συναλλακτικών προτύπων και ενεργοποιούν διαδικασίες περαιτέρω ελέγχου, όπως πρόσθετη επιβεβαίωση συναλλαγής ή προσωρινή αναστολή εκτέλεσης. Η εφαρμογή τέτοιων συστημάτων συμβάλλει ουσιαστικά στη μείωση των περιστατικών οικονομικής απάτης, στην προστασία των χρηστών και στη διατήρηση της σταθερότητας του συστήματος πληρωμών.

Υποστήριξη και εκπαίδευση πελατών και επιχειρήσεων

Η εταιρεία παρέχει συνεχή υποστήριξη και ενημέρωση προς επιχειρήσεις και χρήστες σχετικά με την ασφαλή χρήση των υπηρεσιών πληρωμών και την αναγνώριση πιθανών απειλών. Η διάσταση αυτή είναι ιδιαίτερα σημαντική για οργανισμούς παροχής υπηρεσιών πληρωμών και τραπεζικούς οργανισμούς, καθώς το περιβάλλον των ψηφιακών συναλλαγών χαρακτηρίζεται από διαρκώς εξελισσόμενες μορφές απάτης.

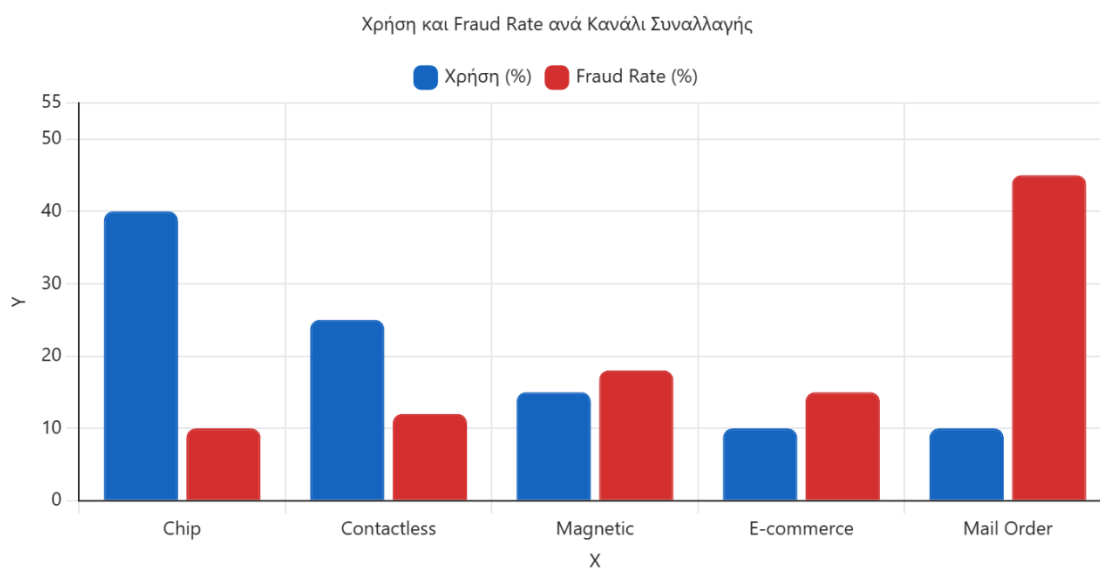
Η συστηματική εκπαίδευση των χρηστών συμβάλλει:

- στην ενίσχυση της πρόληψης περιστατικών απάτης,
- στη μείωση πιθανών οικονομικών απωλειών,
- στην ενίσχυση της εμπιστοσύνης προς τα ψηφιακά μέσα πληρωμών,
- στην προσαρμογή των χρηστών στις νέες τεχνολογικές και επιχειρησιακές προκλήσεις.

Συμμόρφωση με κανονιστικά και εποπτικά πλαίσια

Η λειτουργία της NBG Pay βασίζεται στην αυστηρή εφαρμογή εθνικών και διεθνών κανονιστικών απαιτήσεων που διέπουν τις υπηρεσίες πληρωμών και τη χρηματοοικονομική ασφάλεια. Οι διαδικασίες συμμόρφωσης περιλαμβάνουν την εφαρμογή κανόνων ασφάλειας συναλλαγών, την προστασία προσωπικών δεδομένων, καθώς και την πρόληψη οικονομικού εγκλήματος και απάτης.

Η συμμόρφωση με το κανονιστικό πλαίσιο ενισχύει τη διαφάνεια των συναλλαγών, διασφαλίζει τη νομιμότητα των χρηματοοικονομικών διαδικασιών και συμβάλλει στη βιωσιμότητα και αξιοπιστία του συστήματος ηλεκτρονικών πληρωμών.



5.3 Υποδομές POS, e-commerce και APIs

Οι τεχνολογικές υποδομές του NBG Pay είναι κρίσιμες για τη διασφάλιση ασφαλών ψηφιακών πληρωμών:

- **POS terminals:** Τερματικά ασφαλείας με ενσωματωμένη κρυπτογράφηση και δυνατότητες απομακρυσμένης παρακολούθησης.
- **E-commerce gateways:** Συστήματα επεξεργασίας online πληρωμών με δυνατότητα real-time authorization και anti-fraud checks.
- **APIs και διασυνδέσεις:** Διασύνδεση με ERP και CRM συστήματα, αυτοματοποίηση συναλλαγών και δημιουργία dashboards παρακολούθησης κινδύνων.
- **Συστήματα monitoring:** Ανάλυση δεδομένων συναλλαγών σε πραγματικό χρόνο για τον εντοπισμό ασυνήθιστων patterns (behavioral analytics).

Η τεχνολογική υποδομή υποστηρίζει την ασφαλή και αποτελεσματική λειτουργία του οργανισμού, μειώνοντας σημαντικά τους κινδύνους ηλεκτρονικής απάτης.

5.4 Ανάλυση κινδύνων και ευπαθειών

Η διαχείριση κινδύνου αποτελεί κεντρικό στοιχείο της στρατηγικής του NBG Pay. Οι κύριες κατηγορίες κινδύνου περιλαμβάνουν:

1. Τεχνολογικοί κίνδυνοι:

- Κακόβουλο λογισμικό (malware) και ransomware.
- Υποκλοπή credentials μέσω phishing, smishing ή vishing.
- SIM swap attacks για υποκλοπή OTP.

2. Διαδικαστικοί κίνδυνοι:

- Λάθη στην επεξεργασία συναλλαγών ή στην ενημέρωση πελατών.
- Ανεπαρκής έλεγχος των επιχειρηματικών πελατών για συμμόρφωση με AML και PSD2.

3. Ανθρώπινοι παράγοντες:

- Αμέλεια ή έλλειψη εκπαίδευσης των χρηστών και προσωπικού.
- Insider threats και social engineering attacks.

Η ανάλυση πραγματοποιείται μέσω **risk assessment matrices**, μοντέλων **fraud scoring** και συστημάτων προσομοίωσης, προκειμένου να εντοπιστούν ευάλωτα σημεία και να εφαρμοστούν προληπτικά μέτρα.

5.5 Παραδείγματα περιστατικών απάτης από εταιρείες–πελάτες

Μερικά χαρακτηριστικά περιστατικά που έχουν αναφερθεί περιλαμβάνουν:

1. Phishing σε εργαζόμενους επιχειρήσεων:

- Αποστολή ψευδών emails ή μηνυμάτων που οδηγούν στην αποκάλυψη διαπιστευτηρίων.

2. **Card-not-present fraud:**

- Χρήση κλεμμένων στοιχείων καρτών για online αγορές χωρίς φυσική παρουσία της κάρτας.

3. **Disputing fraud (αμφισβήτηση συναλλαγών):**

- Πελάτες επιχειρήσεων ζητούν chargeback, δημιουργώντας οικονομική ζημία στην επιχείρηση.

4. **SIM swap attacks:**

- Ανταλλαγή SIM τηλεφώνου για την υποκλοπή OTP και την πρόσβαση σε τραπεζικούς λογαριασμούς.

5. **Compromised credentials:**

- Χρήση προηγούμενων παραβιάσεων για μη εξουσιοδοτημένες συναλλαγές.

Αυτά τα περιστατικά αναλύονται ώστε να καταδειχθεί ο τρόπος λειτουργίας των επιτιθέμενων και οι τρόποι πρόληψης από το NBG Pay.

5.6 Οικονομικές και λειτουργικές επιπτώσεις

Οι επιπτώσεις των περιστατικών απάτης περιλαμβάνουν:

- **Για τις επιχειρήσεις–πελάτες:**
 - Απώλεια εσόδων λόγω chargebacks και επιστροφών.
 - Κόστος ενίσχυσης συστημάτων ασφαλείας.
 - Μείωση εμπιστοσύνης πελατών και αρνητικό αντίκτυπο στη φήμη.
- **Για την NBG Pay:**
 - Κάλυψη οικονομικών ζημιών όπου προβλέπεται.

- ο Κόστος διαχείρισης περιστατικών απάτης και επενδύσεις σε fraud detection systems.
- ο Επιπτώσεις στη φήμη και πιθανές ρυθμιστικές κυρώσεις.

Η ανάλυση περιστατικών βοηθά στην **εξαγωγή στρατηγικών πρόληψης**, την εκπαίδευση των επιχειρήσεων και την ενίσχυση των μηχανισμών ασφάλειας του οργανισμού.

Κεφάλαιο 6 – Μηχανισμοί Ανίχνευσης και Πρόληψης Απάτης

Η ραγδαία εξάπλωση των ψηφιακών πληρωμών έχει αυξήσει σημαντικά την επιφάνεια επίθεσης για τους κυβερνο εγκληματίες. Οι σύγχρονες μορφές απάτης είναι δυναμικές, πολύ επίπεδες και συχνά συνδυάζουν τεχνικές παραβίασης συστημάτων με κοινωνική μηχανική. Για τον λόγο αυτό, τα χρηματοπιστωτικά ιδρύματα εφαρμόζουν **ολιστικά πλαίσια διαχείρισης απάτης**, τα οποία βασίζονται σε δύο άξονες:

- **Ανίχνευση (Detection)** ύποπτων ενεργειών σε πραγματικό χρόνο
- **Πρόληψη (Prevention)** ώστε να μειωθεί η πιθανότητα επιτυχούς επίθεσης

Οι δύο αυτοί άξονες λειτουργούν συμπληρωματικά και εντάσσονται σε ευρύτερες πολιτικές διακυβέρνησης κινδύνου.

6.1 Ανίχνευση Απάτης (Fraud Detection)

Η ανίχνευση και αποτροπή απάτης (fraud detection & prevention) αποτελεί κρίσιμο πυλώνα της σύγχρονης χρηματοοικονομικής τεχνολογίας, ιδιαίτερα σε οργανισμούς όπως η Visa, η Mastercard και η PayPal, οι οποίοι διαχειρίζονται δισεκατομμύρια συναλλαγές ημερησίως. Τα συστήματα αυτά βασίζονται σε εκτεταμένη ανάλυση δεδομένων, αλγοριθμικά μοντέλα πρόβλεψης και τεχνολογίες παρακολούθησης χρηστών και συσκευών, με σκοπό τον έγκαιρο εντοπισμό ύποπτων μοτίβων πριν αυτά οδηγήσουν σε οικονομική ζημία.

Στο παρόν κείμενο αναπτύσσεται το θεωρητικό και τεχνολογικό υπόβαθρο της ανίχνευσης απάτης, με ιδιαίτερη έμφαση στους περιορισμούς που προκύπτουν από τον μεγάλο όγκο δεδομένων (bigdata) και τη μοντελοποίηση βαθμολογίας κινδύνου (risk score modeling).

A. Θεωρητικό Πλαίσιο Ανίχνευσης Απάτης

Η ανίχνευση απάτης αφορά τον εντοπισμό ύποπτων συναλλαγών ή συμπεριφορών πριν αυτές εξελιχθούν σε επιβεβαιωμένη απάτη. Στην πράξη, τα συστήματα αυτά λειτουργούν ως ανασταλτικοί μηχανισμοί, αξιολογώντας σε πραγματικό χρόνο (real-time) τον κίνδυνο κάθε συναλλαγής.

Η λειτουργία τους βασίζεται σε τρεις βασικούς άξονες:

1. Συλλογή και ενοποίηση δεδομένων

- Δημογραφικά στοιχεία χρήστη
- Ιστορικό συναλλαγών
- Δεδομένα συσκευής (device finger-printing)
- Γεωγραφικά και χρονικά μοτίβα
- Συμπεριφορικά χαρακτηριστικά (behavioral biometrics)

2. Αλγοριθμική επεξεργασία

- ο Στατιστικά μοντέλα
- ο Μηχανική μάθηση (machine learning)
- ο Νευρωνικά δίκτυα (deep learning)
- ο Ανίχνευση ανωμαλιών (anomaly detection)

3. Απόδοση βαθμολογίας κινδύνου (Risk Scoring)

- ο Κάθε συναλλαγή λαμβάνει ένα riskscore.
- ο Αν η βαθμολογία υπερβεί συγκεκριμένο κατώφλι (threshold), η συναλλαγή μπλοκάρεται, ζητείται επιπλέον ταυτοποίηση ή απορρίπτεται.

B. Ο Ρόλος του Risk Score Modeling

Το risk score modeling αποτελεί τον πυρήνα των σύγχρονων συστημάτων αποτροπής απάτης. Πρόκειται για ένα μαθηματικό/στατιστικό μοντέλο που εκτιμά την πιθανότητα μια συναλλαγή να είναι δόλια.

Η γενική μορφή του μπορεί να περιγραφεί ως:

$$\text{Risk Score} = f(x_1, x_2, x_3, \dots, x_n)$$

όπου τα x_n είναι μεταβλητές όπως:

- Ποσό συναλλαγής
- Συχνότητα χρήσης κάρτας
- Αλλαγή τοποθεσίας
- Αλλαγή συσκευής
- Ιστορικό απορρίψεων

Τα μοντέλα αυτά εκπαιδεύονται σε ιστορικά δεδομένα (supervised learning). Ωστόσο, εδώ εντοπίζεται μία κρίσιμη πρόκληση: τα δεδομένα εκπαίδευσης αντικατοπτρίζουν

παλαιά μοτίβα απάτης. Οι απατεώνες όμως προσαρμόζονται διαρκώς, δημιουργώντας νέα μοτίβα που ενδέχεται να μην ανιχνεύονται επαρκώς.

Γ. Ο Μεγάλος Όγκος Δεδομένων ως Παράγοντας Αποτυχίας

Παρότι τα σύγχρονα συστήματα έχουν σχεδιαστεί για να διαχειρίζονται τεράστιους όγκους δεδομένων (big data architecture, real-time streaming, distributed systems), ο ίδιος ο όγκος μπορεί να αποτελέσει περιορισμό.

Γ.1 Το Πρόβλημα του “Signal-to-Noise Ratio”

Σε περιβάλλοντα με εκατομμύρια συναλλαγές ημερησίως, τα περιστατικά απάτης αποτελούν συνήθως μικρό ποσοστό (<1%). Αυτό δημιουργεί:

- **Classim balance problem**
- Υψηλό ποσοστό falsepositives
- Δυσκολία στον εντοπισμό σπάνιων αλλά κρίσιμων περιστατικών

Ένα πολύ σημαντικό περιστατικό μπορεί να “χαθεί” μέσα στον θόρυβο δεδομένων, εάν το riskscore του δεν ξεπεράσει το προκαθορισμένο κατώφλι.

Γ.2 Threshold Optimization και Επιχειρησιακός Κίνδυνος

Η επιλογή του ορίου (threshold) αποτελεί στρατηγική απόφαση risk management:

- Χαμηλό threshold → Πολλά false positives → Κακή εμπειρία πελάτη
- Υψηλό threshold → Λιγότερα false positives → Κίνδυνος μη εντοπισμού μεγάλης απάτης

Οι οργανισμοί συχνά ρυθμίζουν τα thresholds με βάση:

- Κόστος απάτης (fraudloss)
- Κόστος απόρριψης νόμιμης συναλλαγής
- Regulatory compliance

- Risk appetite του οργανισμού

Σε περιόδους υψηλού όγκου συναλλαγών (π.χ. Black Friday, festive seasons), τα thresholds ενδέχεται να τροποποιηθούν για να αποφευχθεί υπερφόρτωση των συστημάτων ή των fraud analysts, γεγονός που μπορεί να αυξήσει την πιθανότητα διαφυγής σοβαρών περιστατικών.

Δ. Risk Assessment και Ανάλυση Σεναρίων

Η συνολική αξιολόγηση κινδύνου (risk assessment) δεν βασίζεται μόνο σε στατικό μοντέλο. Περιλαμβάνει:

- Scenario-based rules
- Behavioral scoring
- Network analysis (συσχετισμοί μεταξύ χρηστών, IPs, συσκευών)
- Dynamic risk adaptation

Ωστόσο, όταν τα δεδομένα είναι υπερβολικά εκτεταμένα και ετερογενή:

- Η πολυπλοκότητα αυξάνεται εκθετικά
- Εμφανίζεται overfitting
- Μειώνεται η ερμηνευσιμότητα (model explainability)
- Δημιουργούνται “τυφλά σημεία” (blind spots)

Αυτά τα blind spots μπορεί να επιτρέψουν σε μεγάλης κλίμακας επιθέσεις (π.χ. coordinated fraud attacks) να περάσουν απαρατήρητες, ειδικά όταν μιμούνται φυσιολογική συμπεριφορά.

6.1.1 Risk Scoring Models

A. Εισαγωγή

Τα μοντέλα εκτίμησης κινδύνου αποτελούν τον θεμελιώδη μηχανισμό της αυτοματοποιημένης ανίχνευσης και αποτροπής απάτης στα σύγχρονα χρηματοπιστωτικά ιδρύματα. Στο πλαίσιο αυτό, κάθε συναλλαγή μετατρέπεται σε ένα ποσοτικοποιημένο επίπεδο κινδύνου μέσω στατιστικής επεξεργασίας και ανάλυσης δεδομένων. Η διαδικασία αυτή επιτρέπει την άμεση αξιολόγηση της πιθανότητας μια συναλλαγή να συνδέεται με δόλια δραστηριότητα ή άλλη μορφή παρατυπίας.

Η αποτελεσματικότητα των μοντέλων αυτών δεν εξαρτάται αποκλειστικά από τη μαθηματική τους ακρίβεια, αλλά από το ευρύτερο πλαίσιο αξιολόγησης κινδύνου (risk assessment) στο οποίο εντάσσονται. Το risk assessment συνιστά μια ολιστική διαδικασία αναγνώρισης, ανάλυσης και ιεράρχησης πιθανών μελλοντικών κινδύνων, καθώς και καθορισμού μέτρων πρόληψης και αποτροπής τους.

B. Η Έννοια του Risk Assessment σε Επιχειρησιακό Περιβάλλον

Για οποιαδήποτε εταιρεία ή πολυεθνικό οργανισμό, το risk assessment νοείται ως το σύνολο των διαδικασιών μέσω των οποίων εντοπίζονται πιθανοί κίνδυνοι, αξιολογείται η σοβαρότητά τους και καθορίζονται μηχανισμοί ελέγχου. Στόχος της διαδικασίας αυτής είναι η πρόληψη οικονομικής ζημίας, η διασφάλιση της επιχειρησιακής συνέχειας και η συμμόρφωση με το κανονιστικό πλαίσιο.

Η διαδικασία περιλαμβάνει συνήθως τα εξής στάδια:

1. Αναγνώριση κινδύνων (Risk Identification)

Καταγραφή πιθανών απειλών που μπορούν να επηρεάσουν τα πληροφοριακά συστήματα, τις συναλλαγές ή τη φήμη του οργανισμού.

2. Ανάλυση και εκτίμηση κινδύνου (Risk Analysis & Evaluation)

Εκτίμηση της πιθανότητας εμφάνισης κάθε κινδύνου και της δυνητικής του επίπτωσης.

3. Σχεδιασμός μέτρων αποτροπής (Risk Mitigation Planning)

Καθορισμός κανόνων, διαδικασιών και τεχνικών μηχανισμών για τη μείωση ή εξάλειψη του κινδύνου.

Στο πλαίσιο αυτό, τα μοντέλα εκτίμησης κινδύνου αποτελούν το τεχνολογικό εργαλείο εφαρμογής των συμπερασμάτων του risk assessment.

Γ. Risk Assessment σε Συστημική Τράπεζα ή Ίδρυμα Πληρωμών

Στην περίπτωση μιας συστημικής τράπεζας ή ενός τραπεζικού ιδρύματος πληρωμών, η διαδικασία αξιολόγησης κινδύνου αποκτά ιδιαίτερη βαρύτητα λόγω του μεγάλου όγκου και της πολυπλοκότητας των συναλλαγών.

Η αξιολόγηση κινδύνου αφορά:

- Τους κινδύνους που απορρέουν από τα συστήματα ασφαλείας.
- Τις ενδεχόμενες αδυναμίες των πληροφοριακών υποδομών.
- Τη χρήση ηλεκτρονικών καναλιών συναλλαγών.
- Την πιθανότητα εσωτερικής ή εξωτερικής απάτης.

Στο στάδιο αυτό παράγονται συγκεκριμένα σενάρια κινδύνου (risk scenarios). Τα σενάρια αυτά αποτελούν υποθετικές αλλά ρεαλιστικές περιγραφές περιστατικών, μέσω

των οποίων μπορεί να προκύψει απάτη ή άλλη παρατυπία. Η δημιουργία τους βασίζεται:

- Σε ιστορικά περιστατικά.
- Σε αναλύσεις προηγούμενων επιθέσεων.
- Σε κανονιστικές απαιτήσεις.
- Στην εμπειρία αναλυτών κινδύνου και στελεχών ασφαλείας.

Τα σενάρια αυτά αποτελούν τη βάση για την παραμετροποίηση του βασικού συστήματος ασφαλείας.

Δ. Εισαγωγή Κανόνων στο Σύστημα Ασφαλείας

Μετά την ανάπτυξη των σεναρίων κινδύνου, ακολουθεί η μετατροπή τους σε λειτουργικούς κανόνες (rules). Οι κανόνες αυτοί εισάγονται στο σύστημα ασφαλείας προκειμένου να:

- Συλλέγονται και να αξιολογούνται σωστά τα δεδομένα συναλλαγών.
- Παράγεται αξιόπιστη βαθμολογία κινδύνου.
- Λαμβάνονται ορθές αποφάσεις σχετικά με τον εντοπισμό και την αποτροπή περιστατικών.

Οι κανόνες λειτουργούν ως φίλτρα ή μηχανισμοί ενεργοποίησης (triggers). Για παράδειγμα, μπορεί να ενεργοποιούνται όταν:

- Το ποσό της συναλλαγής υπερβαίνει προκαθορισμένο όριο.
- Εντοπίζεται απόκλιση από τη συνήθη συμπεριφορά χρήστη.
- Παρατηρείται αλλαγή συσκευής ή γεωγραφικής τοποθεσίας.
- Υπάρχει υψηλή συχνότητα συναλλαγών σε σύντομο χρονικό διάστημα.

Η ποιότητα των κανόνων επηρεάζει άμεσα την αξιοπιστία του συστήματος. Ελλιπείς ή υπερβολικά γενικοί κανόνες μπορεί να οδηγήσουν είτε σε μη εντοπισμό σοβαρών περιστατικών είτε σε υπερβολικό αριθμό ψευδώς θετικών ενδείξεων.

E. Κατηγοριοποίηση Συναλλαγών (Short Category Classification)

Σημαντικό στοιχείο της διαδικασίας αποτελεί η κατηγοριοποίηση των συναλλαγών σε σύντομες κατηγορίες κινδύνου (short categories). Η κατηγοριοποίηση αυτή συμβάλλει:

- Στην καλύτερη οργάνωση και ιεράρχηση των περιστατικών.
- Στην αποτελεσματικότερη διαχείριση από τις ομάδες ανάλυσης.
- Στην προσαρμογή των ελέγχων ανάλογα με τη φύση της συναλλαγής.

Οι κατηγορίες μπορεί να βασίζονται:

- Στο ύψος του ποσού.
- Στο είδος της συναλλαγής (π.χ. διασυνοριακή, online, POS).
- Στο προφίλ του πελάτη.
- Στο ιστορικό συμπεριφοράς.

Η χρήση σύντομων κατηγοριών επιτρέπει τη γρήγορη διάκριση μεταξύ χαμηλού, μεσαίου και υψηλού κινδύνου συναλλαγών. Έτσι, καθίσταται σαφές ποιες περιπτώσεις απαιτούν άμεση παρέμβαση ή πρόσθετη διαδικασία ταυτοποίησης.

Βασικά χαρακτηριστικά τους:

- Κάθε συναλλαγή αξιολογείται με βάση:
 - το ποσό,
 - τη γεωγραφική τοποθεσία,
 - το ιστορικό του χρήστη,
 - τη συχνότητα συναλλαγών,

- τον τύπο εμπόρου ή υπηρεσίας.
- Το σύστημα αποδίδει **risk score** (βαθμολογία κινδύνου).
- Οι συναλλαγές με υψηλό σκορ:
 - μπλοκάρονται προσωρινά ή
 - προωθούνται για χειροκίνητο έλεγχο.

Έτσι επιτυγχάνεται:

- ιεράρχηση περιστατικών,
- βέλτιστη αξιοποίηση πόρων ελέγχου,
- μείωση λειτουργικού κόστους.

6.1.2 Machine Learning & AI Fraud Engines

Τα παραδοσιακά rule-based συστήματα δεν επαρκούν πλέον απέναντι σε εξελιγμένες επιθέσεις. Για τον λόγο αυτό χρησιμοποιούνται αλγόριθμοι μηχανικής μάθησης.

Οι δυνατότητές τους περιλαμβάνουν:

- Μάθηση από τεράστιους όγκους ιστορικών δεδομένων συναλλαγών.
- Αναγνώριση πολύπλοκων μοτίβων που δεν είναι εμφανή σε ανθρώπινους αναλυτές.
- Συνεχή προσαρμογή σε νέες τεχνικές απατεώνων.
- Μείωση:
 - **False positives** (νόμιμες συναλλαγές που θεωρούνται ύποπτες),
 - λειτουργικής επιβάρυνσης.

Ιδιαίτερα σημαντική είναι η ικανότητα πρόβλεψης επιθέσεων τύπου:

- velocity fraud (πολλές μικρές συναλλαγές σε μικρό χρόνο),

- card testing,
 - συνδυαστικές επιθέσεις με πολλαπλές μεταβλητές.
-

6.1.3 Behavioral Analytics

Η ανάλυση συμπεριφοράς μετατοπίζει το επίκεντρο από τη συναλλαγή στον ίδιο τον χρήστη.

Εξετάζονται:

- ώρες σύνδεσης,
- συχνότητα χρήσης,
- συνηθισμένα ποσά συναλλαγών,
- τύπος και σταθερότητα συσκευής.

Όταν εντοπίζεται απόκλιση από το «κανονικό» προφίλ:

- ενεργοποιούνται επιπλέον έλεγχοι,
- μπορεί να ζητηθεί επιπλέον ταυτοποίηση,
- αποτρέπεται πιθανό **Account Takeover (ATO)**.

Η προσέγγιση αυτή είναι κρίσιμη διότι πολλές επιθέσεις γίνονται με έγκυρα διαπιστευτήρια που έχουν υποκλαπεί.

6.1.4 Transaction Monitoring

Η παρακολούθηση συναλλαγών σε πραγματικό χρόνο αποτελεί βασικό επιχειρησιακό πυρήνα των σύγχρονων συστημάτων ανίχνευσης και διαχείρισης κινδύνου. Πρόκειται για μια κρίσιμη διαδικασία, η οποία στοχεύει στον άμεσο εντοπισμό ύποπτων ή μη

φυσιολογικών δραστηριοτήτων, συμβάλλοντας στην προστασία των πληροφοριακών συστημάτων και στη διασφάλιση της αξιοπιστίας των οικονομικών συναλλαγών.

Ειδικότερα, το σύστημα παρακολούθησης συναλλαγών λειτουργεί ως μηχανισμός αξιολόγησης κινδύνου, ο οποίος βασίζεται σε προκαθορισμένα κριτήρια και δείκτες ανάλυσης. Τα κριτήρια αυτά περιλαμβάνουν, μεταξύ άλλων, το ύψος της συναλλαγής, τη συχνότητα εκτέλεσης, τα χαρακτηριστικά συμπεριφοράς του χρήστη, καθώς και την απόκλιση από καθιερωμένα πρότυπα συναλλακτικής δραστηριότητας. Μέσω της συνεχούς ανάλυσης των δεδομένων, το σύστημα είναι σε θέση να εντοπίζει συναλλαγές που παρουσιάζουν αυξημένο επίπεδο κινδύνου ή ενδέχεται να σχετίζονται με δόλιες ενέργειες.

Όταν μια συναλλαγή χαρακτηριστεί ως υψηλού κινδύνου, ενεργοποιούνται διαδικασίες περαιτέρω διερεύνησης και ελέγχου, με στόχο την επιβεβαίωση της νομιμότητάς της και την αποτροπή πιθανών περιπτώσεων απάτης. Η διαδικασία αυτή συμβάλλει ουσιαστικά στη μείωση των οικονομικών απωλειών, στην ενίσχυση της ασφάλειας των πληροφοριακών υποδομών και στη συμμόρφωση των οργανισμών με κανονιστικές και νομοθετικές απαιτήσεις.

Συνολικά, η παρακολούθηση συναλλαγών σε πραγματικό χρόνο αποτελεί θεμελιώδες εργαλείο για την αποτελεσματική διαχείριση κινδύνου, την πρόληψη οικονομικών εγκλημάτων και τη διατήρηση της εμπιστοσύνης στο σύγχρονο ψηφιακό οικονομικό περιβάλλον.

Καλύπτει:

- εντοπισμό ασυνήθιστα υψηλών ποσών,
- πολλαπλές συναλλαγές προς τρίτους σε σύντομο χρόνο,

- γεωγραφικές ανωμαλίες,
- απότομες αλλαγές προτύπων κατανάλωσης.

Συχνά συνδυάζεται με:

- rule engines,
- αυτοματοποιημένες απορρίψεις συναλλαγών,
- ειδοποιήσεις σε κέντρα διαχείρισης απάτης.

Όσον αφορά την **NBG Pay**, σε σύγκριση με ένα κατεξοχήν τραπεζικό ίδρυμα, ο έλεγχος των συναλλαγών πραγματοποιείται βάσει διαφορετικών κριτηρίων και επιχειρησιακών προτεραιοτήτων. Ειδικότερα, στα παραδοσιακά τραπεζικά ιδρύματα ο έλεγχος συναλλαγών περιλαμβάνει το σύνολο των οικονομικών δραστηριοτήτων των πελατών, τόσο σε επίπεδο φυσικών προσώπων όσο και επιχειρήσεων, οι οποίοι διαθέτουν προσωπικούς ή εταιρικούς τραπεζικούς λογαριασμούς.

Στο πλαίσιο αυτό, εξετάζεται ένα ευρύ φάσμα συναλλαγών, το οποίο περιλαμβάνει τόσο ηλεκτρονικές όσο και μη ηλεκτρονικές συναλλαγές. Ειδικότερα, πραγματοποιείται διεξοδικός έλεγχος σε δραστηριότητες όπως αναλήψεις και μεταφορές μέσω ATM, συναλλαγές με χρήση τραπεζικών καρτών, πληρωμές σε επιχειρήσεις μέσω τερματικών POS, καθώς και ηλεκτρονικές μεταφορές κεφαλαίων μέσω τραπεζικών λογαριασμών (IBAN). Ο διεξοδικός αυτός έλεγχος αποσκοπεί στον εντοπισμό ύποπτων συναλλακτικών μοτίβων, στην αξιολόγηση του επιπέδου κινδύνου και στη διασφάλιση της νομιμότητας των οικονομικών δραστηριοτήτων.

Ωστόσο, η βασική διαφοροποίηση στην περίπτωση της NBG Pay έγκειται στο γεγονός ότι η διαδικασία παρακολούθησης συναλλαγών επικεντρώνεται κυρίως στον τομέα του acquiring. Συγκεκριμένα, η έμφαση δίνεται στις συναλλαγές που πραγματοποιούνται από επιχειρήσεις μέσω τερματικών POS και άλλων συστημάτων αποδοχής πληρωμών, και όχι στο σύνολο των τραπεζικών υπηρεσιών που παρέχονται στους πελάτες ενός παραδοσιακού τραπεζικού οργανισμού.

Πιο συγκεκριμένα, το acquiring αφορά τη διαχείριση και επεξεργασία συναλλαγών που πραγματοποιούνται με διάφορες μεθόδους πληρωμής, όπως συναλλαγές με χρήση κάρτας μέσω τεχνολογίας chip, ανέπαφες συναλλαγές (contactless), συναλλαγές εξ αποστάσεως (mailorder) και ηλεκτρονικές συναλλαγές στο πλαίσιο του ηλεκτρονικού εμπορίου (e-commerce). Η διαδικασία αυτή επικεντρώνεται κυρίως στην ασφάλεια των πληρωμών, στην πρόληψη περιστατικών απάτης και στη διασφάλιση της ορθής εκτέλεσης των συναλλαγών μεταξύ επιχειρήσεων και καταναλωτών.

Συνεπώς, ενώ τα παραδοσιακά τραπεζικά ιδρύματα εφαρμόζουν ολιστικό έλεγχο στο σύνολο των τραπεζικών δραστηριοτήτων των πελατών, η NBG Pay εστιάζει εξειδικευμένα στην παρακολούθηση και διαχείριση συναλλαγών αποδοχής πληρωμών, γεγονός που καθορίζει και τη διαφοροποίηση των κριτηρίων αξιολόγησης κινδύνου και των μηχανισμών ελέγχου.

6.1.5 Device Fingerprinting & Geolocation

Η τεχνολογία αυτή αναγνωρίζει τη «ψηφιακή ταυτότητα» της συσκευής.

Συλλέγονται στοιχεία όπως:

- λειτουργικό σύστημα,
- browser,
- IP διεύθυνση,
- μοτίβα χρήσης συσκευής.

Χρήση στην ανίχνευση:

- εντοπισμός ξαφνικής αλλαγής συσκευής,
- αναγνώριση ύποπτης γεωγραφικής μεταβολής,
- συσχέτιση με επιθέσεις phishing ή SIM swap.

6.2 Πρόληψη Απάτης (FraudPrevention), ως πρωτογενής μηχανισμός διαχείρισης κινδύνου

Η πρόληψη (prevention) συνιστά το πρώτο και πλέον κρίσιμο επίπεδο άμυνας σε ένα σύγχρονο σύστημα διαχείρισης κινδύνου. Σε αντίθεση με την ανίχνευση (detection), η οποία ενεργοποιείται όταν ένα περιστατικό βρίσκεται ήδη σε εξέλιξη ή έχει πραγματοποιηθεί, η πρόληψη εστιάζει στη μείωση της πιθανότητας επιτυχούς επίθεσης πριν απαιτηθεί οποιαδήποτε διορθωτική παρέμβαση.

Στο πλαίσιο χρηματοπιστωτικών οργανισμών, η πρόληψη δεν αφορά απλώς την τεχνολογική θωράκιση ενός συστήματος, αλλά έναν συνδυασμό στρατηγικών, πολιτικών, τεχνικών μηχανισμών και κανονιστικής συμμόρφωσης, που λειτουργούν αποτρεπτικά απέναντι σε δόλιες ενέργειες.

A. Εννοιολογική Διάκριση Πρόληψης και Ανίχνευσης

Η πρόληψη έχει προληπτικό και αποτρεπτικό χαρακτήρα, ενώ η ανίχνευση έχει αναγνωριστικό και κατασταλτικό χαρακτήρα. Συγκεκριμένα:

- **Πρόληψη:** Μειώνει την επιφάνεια επίθεσης (attack surface) και καθιστά δυσχερή την εκδήλωση απάτης.
- **Ανίχνευση:** Εντοπίζει ύποπτη δραστηριότητα όταν αυτή έχει ήδη ξεκινήσει.
- **Απόκριση (response):** Διαχειρίζεται το περιστατικό μετά τον εντοπισμό του.

Η αποτελεσματική στρατηγική ασφάλειας βασίζεται σε πολύ-επίπεδη προσέγγιση (defense in depth), όπου η πρόληψη αποτελεί το πρώτο φίλτρο προστασίας.

B. Μηχανισμοί Πρόληψης σε Τραπεζικά Συστήματα

Σε μια συστημική τράπεζα ή ίδρυμα πληρωμών, οι προληπτικοί μηχανισμοί ενσωματώνονται σε διάφορα επίπεδα της αρχιτεκτονικής ασφαλείας:

B.1 Ισχυρή Ταυτοποίηση Πελάτη (Strong Customer Authentication – SCA)

Η εφαρμογή πολύ-παραγοντικής αυθεντικοποίησης (MFA) μειώνει δραστικά την πιθανότητα μη εξουσιοδοτημένης πρόσβασης. Η χρήση:

- Κωδικών μιας χρήσης (OTP),
- Βιομετρικών δεδομένων,
- Συνδυασμού γνώσης, κατοχής και εγγενούς χαρακτηριστικού,

λειτουργεί ως προληπτικό εμπόδιο πριν καν επιχειρηθεί δόλια συναλλαγή.

B.2 Πολιτικές Πρόσβασης και Διαχείριση Δικαιωμάτων

Ο έλεγχος πρόσβασης (access control) περιορίζει τη δυνατότητα εκμετάλλευσης εσωτερικών συστημάτων. Η αρχή του “least privilege” διασφαλίζει ότι κάθε χρήστης ή υπάλληλος διαθέτει μόνο τα απολύτως απαραίτητα δικαιώματα.

Με τον τρόπο αυτό μειώνεται ο εσωτερικός λειτουργικός κίνδυνος (internal fraud-risk).

B.3 Προληπτική Κατηγοριοποίηση Πελατών και Συναλλαγών

Η κατηγοριοποίηση πελατών με βάση το προφίλ κινδύνου (risk-based segmentation) επιτρέπει διαφοροποιημένα επίπεδα ελέγχου. Για παράδειγμα:

- Πελάτες υψηλού κινδύνου υπόκεινται σε αυστηρότερη παρακολούθηση.
- Συναλλαγές υψηλής αξίας απαιτούν επιπλέον επαλήθευση.

Η κατηγοριοποίηση αυτή μειώνει την πιθανότητα επιτυχούς απάτης πριν ενεργοποιηθούν οι μηχανισμοί ανίχνευσης.

B.4 Όρια και Περιορισμοί Συναλλαγών

Η θέσπιση ημερήσιων ή ανά συναλλαγή ορίων (transaction limits) λειτουργεί αποτρεπτικά. Ακόμη και αν ένας επιτιθέμενος αποκτήσει πρόσβαση σε λογαριασμό, η δυνητική ζημία περιορίζεται σημαντικά.

B.5 Εκπαίδευση Χρηστών και Ενημέρωση

Η πρόληψη δεν είναι αποκλειστικά τεχνολογική διαδικασία. Η ενημέρωση των πελατών για πρακτικές phishing, social engineering και ασφαλή χρήση ψηφιακών καναλιών μειώνει την πιθανότητα επιτυχίας εξωτερικών επιθέσεων.

Ο ανθρώπινος παράγοντας αποτελεί συχνά τον πιο ευάλωτο κρίκο της αλυσίδας ασφάλειας.

Γ. Σχέση Πρόληψης και Risk Assessment

Η πρόληψη στηρίζεται άμεσα στα αποτελέσματα του risk assessment. Μέσω της ανάλυσης σεναρίων κινδύνου:

- Αναγνωρίζονται τα πιο πιθανά σημεία εκμετάλλευσης.
- Καθορίζονται προληπτικά μέτρα.
- Επαναξιολογούνται περιοδικά οι πολιτικές ασφαλείας.

Με άλλα λόγια, το risk assessment καθοδηγεί τη στρατηγική πρόληψης, ενώ η πρόληψη μειώνει το φορτίο που θα κληθούν να διαχειριστούν τα συστήματα αντίχρευσσης.

Δ. Στρατηγική Σημασία της Πρόληψης

Η έμφαση στην πρόληψη έχει σημαντικά πλεονεκτήματα:

1. Μειώνει τις οικονομικές απώλειες πριν αυτές προκύψουν.
2. Περιορίζει τον αριθμό ψευδώς θετικών συναγερμών.
3. Βελτιώνει την εμπειρία πελάτη, αποφεύγοντας άσκοπες παρεμβάσεις.
4. Ενισχύει τη φήμη και την αξιοπιστία του οργανισμού.

Σε περιβάλλοντα υψηλού όγκου συναλλαγών, η πρόληψη λειτουργεί ως μηχανισμός εξισορρόπησης μεταξύ ασφάλειας και λειτουργικής αποδοτικότητας.

6.2.1 Strong Customer Authentication (SCA)

Η πολυπαραγοντική ταυτοποίηση βασίζεται σε:

- γνώση (password/PIN),
- κατοχή (κινητό, token, OTP),
- εγγενές χαρακτηριστικό (βιομετρικά).

Αποτελέσματα:

- δυσκολία παράκαμψης ταυτότητας,
 - σημαντική μείωση accounttakeover,
 - ενίσχυση εμπιστοσύνης στις ψηφιακές πληρωμές.
-

6.2.2 Tokenization & Encryption

Οι τεχνικές αυτές προστατεύουν τα δεδομένα ακόμα και αν παραβιαστεί το σύστημα.

- **Tokenization:** αντικατάσταση πραγματικών στοιχείων κάρτας με tokens.
- **Encryption:** κρυπτογράφηση δεδομένων σε μεταφορά και αποθήκευση.

Συμβάλλουν σε:

- περιορισμό συνεπειών data breach,
 - προστασία προσωπικών και χρηματοοικονομικών δεδομένων.
-

6.2.3 Limits, Velocity Checks & Rule Engines

Μηχανισμοί περιορισμού κινδύνου μέσω ελέγχου συμπεριφοράς συναλλαγών:

- όρια ποσών ανά συναλλαγή ή ημέρα,
- περιορισμός αριθμού συναλλαγών σε μικρό διάστημα,
- αυτοματοποιημένοι κανόνες αποκλεισμού.

Ιδιαίτερα αποτελεσματικοί σε:

- micro-transaction fraud,
 - δοκιμές κλεμμένων καρτών.
-

6.2.4 Εκπαίδευση Χρηστών

Η ανθρώπινη παράμετρος αποτελεί τον πιο αδύναμο κρίκο. Η εκπαίδευση στοχεύει σε:

- αναγνώριση phishing και social engineering,
- σωστή χρήση 2FA,
- ασφαλή διαχείριση κωδικών.

Η ευαισθητοποίηση μειώνει δραστικά την επιτυχία επιθέσεων που βασίζονται στην εξαπάτηση.

6.2.5 Governance & Internal Controls

Η τεχνολογία δεν αρκεί χωρίς οργανωτικό πλαίσιο.

Περιλαμβάνει:

- πολιτικές διαχείρισης κινδύνου,
 - τακτικά audits,
 - σαφή κατανομή ευθυνών,
 - συμμόρφωση με κανονιστικά πλαίσια (π.χ. PSD2, GDPR).
-

Κεφάλαιο 7 – Ανάλυση Εκτενούς Δείγματος 15 Ευρωπαϊκών Χωρών

Η επιλογή δείγματος 15 ευρωπαϊκών χωρών πραγματοποιήθηκε με σκοπό τη δημιουργία ενός αντιπροσωπευτικού συνόλου διαφορετικών επιπέδων ψηφιακής ωριμότητας, οικονομικής ανάπτυξης και χρήσης ηλεκτρονικών πληρωμών. Το δείγμα περιλαμβάνει χώρες με υψηλή, μεσαία και χαμηλότερη διείσδυση ψηφιακών συναλλαγών, ώστε να καταστεί δυνατή η συγκριτική αξιολόγηση της σχέσης μεταξύ ψηφιοποίησης και ηλεκτρονικής απάτης. Η επιλογή περισσότερων χωρών θα δυσχέραινε τη συγκρισιμότητα των δεδομένων, ενώ μικρότερο δείγμα δεν θα παρείχε επαρκή γεωγραφική και οικονομική αντιπροσώπευση.

Τα βασικά ερευνητικά ερωτήματα του κεφαλαίου είναι τα εξής:

- Πώς επηρεάστηκε η χρήση ψηφιακών πληρωμών μετά την πανδημία COVID-19;
- Υπάρχει συσχέτιση μεταξύ ψηφιακής ωριμότητας και επιπέδου απάτης;
- Ποιες χώρες εμφάνισαν μεγαλύτερη αύξηση περιστατικών ηλεκτρονικής απάτης;
- Ποιοι παράγοντες επηρεάζουν τη διακύμανση του κινδύνου μεταξύ των χωρών;

Η μελέτη βασίστηκε σε δεδομένα διεθνών οργανισμών όπως η ECB, η Eurostat και η Europol, καθώς και σε συγκριτική ανάλυση δεικτών χρήσης ψηφιακών πληρωμών και περιστατικών απάτης.

Η ανάπτυξη των ψηφιακών πληρωμών σε διεθνές επίπεδο παρουσιάζει σημαντικές διαφοροποιήσεις μεταξύ χωρών. Η παρούσα ανάλυση βασίζεται σε δεδομένα από **15 ευρωπαϊκές χώρες**, εξετάζοντας τη χρήση ηλεκτρονικών πληρωμών, τη συχνότητα περιστατικών απάτης και τη συσχέτισή τους με επίπεδο ψηφιακής ωριμότητας και πολιτικές ασφαλείας.

7.1 Δεδομένα Χρήσης Ψηφιακών Πληρωμών

- Η συλλογή δεδομένων έγινε από **εθνικές κεντρικές τράπεζες, στατιστικές υπηρεσίες, οργανισμούς πληρωμών και διεθνείς εκθέσεις (ECB, EBA, World Payments Report).**
- Οι δείκτες που εξετάστηκαν περιλαμβάνουν:
 - Ποσοστό πληθυσμού που χρησιμοποιεί ψηφιακές πληρωμές (% χρήστες e-banking / mobile payments).
 - Ποσοστό συναλλαγών που πραγματοποιούνται μέσω καρτών vs μετρητών.
 - Μέσο ποσό ανά συναλλαγή σε ψηφιακά κανάλια.

- Επίπεδο υιοθέτησης νέων τεχνολογιών (contactless, mobile wallets, instant payments).

Ευρήματα:

- Χώρες όπως Σουηδία, Δανία και Ολλανδία εμφανίζουν υψηλή διείσδυση ψηφιακών πληρωμών (>80% του πληθυσμού).
- Νότιες και ανατολικές χώρες (Ελλάδα, Κύπρος, Ρουμανία) παρουσιάζουν χαμηλότερα ποσοστά χρήσης (<60%), αν και η τάση είναι αυξητική λόγω της πανδημίας COVID-19.
- Η χρήση mobile payments και contactless τεχνολογιών αυξάνεται με **γεωμετρική πρόοδο**, ιδιαίτερα στις χώρες με υψηλή ψηφιακή ωριμότητα.

[Eurostat](#)

[ECB payment statistics](#)

[OECD digital economy](#)

7.2 Συχνότητα και Ένταση Περιστατικών Απάτης

- Συλλέχθηκαν δεδομένα σχετικά με:
 - Τον αριθμό αναφερόμενων περιστατικών ηλεκτρονικής απάτης ανά χώρα.
 - Το ποσοστό απάτης ως προς το συνολικό όγκο συναλλαγών (fraud rate).
 - Την οικονομική ζημία που προκύπτει ανά περιστατικό.

Κύρια παρατήρηση:

- Υπάρχει **άμεση συσχέτιση** ανάμεσα στο επίπεδο χρήσης ψηφιακών πληρωμών και τον αριθμό περιστατικών απάτης.
- Χώρες με υψηλό επίπεδο ψηφιακών συναλλαγών παρουσιάζουν μεγαλύτερο απόλυτο αριθμό περιστατικών, αλλά **χαμηλότερο ποσοστό απάτης ανά συναλλαγή**, υποδεικνύοντας ανεπτυγμένα συστήματα πρόληψης και ανίχνευσης.

Παράδειγμα:

- Σουηδία: 0,02% fraud rate αλλά υψηλός απόλυτος αριθμός περιστατικών λόγω όγκου συναλλαγών.
- Ελλάδα: 0,08% fraud rate με χαμηλότερο συνολικό όγκο, υποδεικνύοντας ευάλωτες υποδομές και χαμηλότερη συμμόρφωση σε SCA.

7.3 Συσχέτιση Ψηφιακής Ωριμότητας και Κινδύνου Απάτης

- Η ψηφιακή ωριμότητα μετράται μέσω δεικτών όπως:
 - Χρήση ηλεκτρονικών πληρωμών ανά 100 κατοίκους.
 - Επίπεδο υιοθέτησης νέων τεχνολογιών (mobile wallets, instant payments, PSD2 compliance).
 - Ποιότητα και εφαρμογή κανονιστικών πλαισίων (AML, KYC).

Συσχέτιση:

- Υψηλή ψηφιακή ωριμότητα → χαμηλότερο fraudrate ανά συναλλαγή.
- Χαμηλή ψηφιακή ωριμότητα → αυξημένος κίνδυνος απάτης, κυρίως σε μορφές **phishing, SIM swap, account takeover**.

- Χώρες με ισχυρές ρυθμιστικές πολιτικές και επενδύσεις σε fraud detection παρουσιάζουν χαμηλότερο οικονομικό αντίκτυπο ανά περιστατικό.

7.4 Παράγοντες που Αυξάνουν / Μειώνουν τη Συχνότητα Απάτης

Παράγοντες που αυξάνουν:

1. Χαμηλή ενημέρωση και εκπαίδευση χρηστών.
2. Ανεπαρκής συμμόρφωση με κανονισμούς PSD2, AML, KYC.
3. Χαμηλή χρήση πολύ παραγοντικού ελέγχου ταυτότητας (SCA).
4. Περιορισμένες επενδύσεις σε fraud detection και monitoring.
5. Υψηλή χρήση καρτών σε e-commerce χωρίς προστασία tokenization.

Παράγοντες που μειώνουν:

1. Εκτεταμένη χρήση πολύ παραγοντικής ταυτοποίησης (SCA, biometric authentication).
2. Εφαρμογή advanced AI και machine learning συστημάτων fraud detection.
3. Εκπαίδευση χρηστών και προγράμματα awareness campaigns.
4. Συνεχής παρακολούθηση συναλλαγών (real-time monitoring).
5. Συνεργασία με διεθνείς οργανισμούς για sharing πληροφοριών σχετικά με fraud.

7.5 Συγκριτική Αξιολόγηση, ευρήματα και τρόπος υπολογισμού

Παράδειγμα

Fraud Transactions = €400.000 (ΕΛΛΑΔΑ)

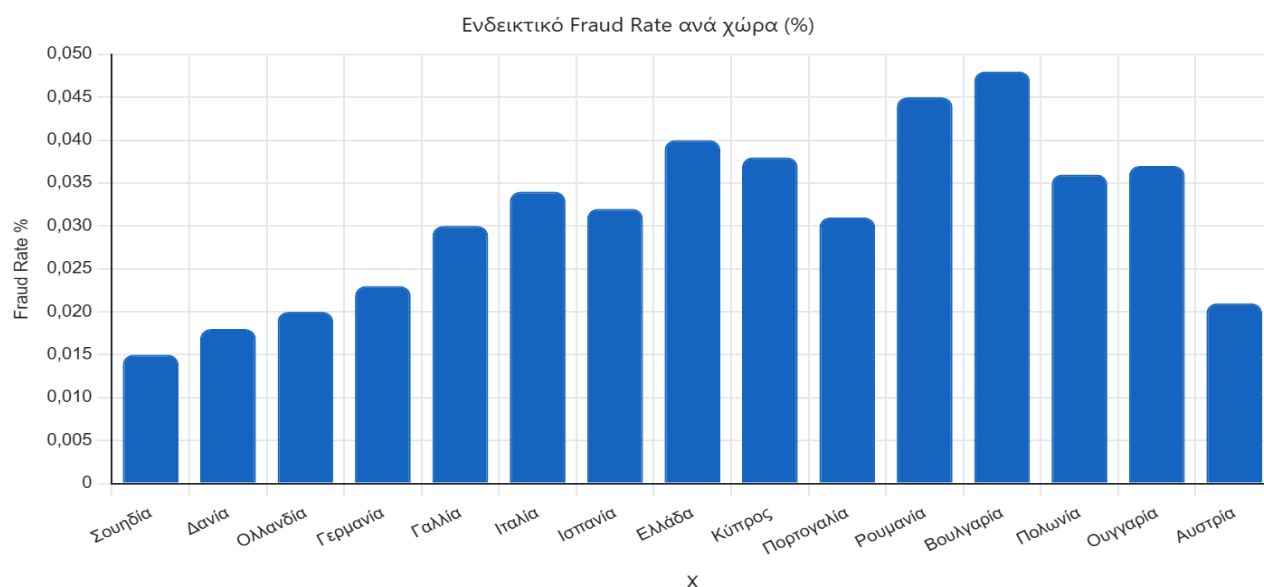
Total Transactions = €1.000.000.000

Fraud Rate = $400.000 / 1.000.000.000 \times 100 = 0,04\%$

Χώρα	Χρήση Ψηφιακών Πληρωμών	FraudRate (%)	Μέτρα Ασφαλείας	Σχόλια
Σουηδία	85%	0,02	Advanced AI, SCA, Tokenization	Υψηλή ωριμότητα, χαμηλός κίνδυνος ανά συναλλαγή
Δανία	82%	0,03	SCA, Real-time monitoring	Επενδύει συνεχώς σε τεχνολογία ανίχνευσης
Ολλανδία	80%	0,025	Tokenization, Behavioral analytics	Χαμηλό fraud rate με μεγάλο όγκο συναλλαγών
Γερμανία	70%	0,04	SCA, AI engines	Μέση ωριμότητα, περιορισμένα awareness campaigns
Γαλλία	68%	0,035	Fraud detection, limits & velocity checks	Υψηλή ευαισθητοποίηση χρηστών

Χώρα	Χρήση Ψηφιακών Πληρωμών	FraudRate (%)	Μέτρα Ασφαλείας	Σχόλια
Ιταλία	60%	0,034	Partial ruleengines	Μέτρια ωριμότητα, SCA, υψηλότερος κίνδυνος
Ισπανία	62%	0,032	Fraudengines, monitoring	Ενδιάμεση κατάσταση ψηφιακής ωριμότητας
Ελλάδα	55%	0,04	Basic manualmonitoring	SCA, Χαμηλή ωριμότητα, αυξημένος κίνδυνος
Κύπρος	50%	0,038	Limitedfrauddetection	Χαμηλή ψηφιακή ωριμότητα
Πορτογαλία	58%	0,031	SCA, AI engines	Μέση ωριμότητα, μειούμενος κίνδυνος
Ρουμανία	48%	0,045	Minimalprotection	Υψηλός κίνδυνος λόγω ανεπαρκών μέτρων
Βουλγαρία	45%	0,048	Manualcontrolonly	Χαμηλή ωριμότητα και προστασία
Πολωνία	53%	0,036	SCA, ruleengines	Μέτρια ωριμότητα, κίνδυνος μειώνεται με awareness

Χώρα	Χρήση Ψηφιακών Πληρωμών	FraudRate (%)	Μέτρα Ασφαλείας	Σχόλια
Ουγγαρία	52%	0,037	Partial monitoring	SCA, Παρόμοιο προφίλ με Πολωνία
Αυστρία	65%	0,021	Advanced tokenization	Σταθερή ψηφιακή AI, ωριμότητα, χαμηλός κίνδυνος



Κύρια Ευρήματα:

1. Η ψηφιακή ωριμότητα είναι **ο πιο καθοριστικός παράγοντας** για την ασφάλεια των πληρωμών.
2. Υψηλός όγκος συναλλαγών δεν σημαίνει απαραίτητα υψηλό ποσοστό fraud, εφόσον υπάρχει προηγμένη τεχνολογία ανίχνευσης και SCA.
3. Χώρες με χαμηλή επένδυση σε awareness και τεχνολογία εμφανίζουν υψηλότερα ποσοστά απάτης και μεγαλύτερο οικονομικό αντίκτυπο.

4. Η συγκριτική αξιολόγηση υπογραμμίζει την **ανάγκη για εκπαίδευση χρηστών και συμμόρφωση με διεθνείς κανονισμούς** σε όλες τις χώρες με μέτρια ή χαμηλή ψηφιακή ωριμότητα.

[Eurostat](#)

[ECB payment statistics](#)

[OECD digital economy](#)

Κεφάλαιο 8 – Ξέπλυμα Χρήματος και Μηχανισμοί Καταπολέμησης (AML) – Αναλυτικά

8.1 Εισαγωγή

1. Το ξέπλυμα χρήματος αποτελεί μία από τις πλέον σοβαρές μορφές οικονομικού εγκλήματος, καθώς υπονομεύει τη χρηματοπιστωτική σταθερότητα, μειώνει τη διαφάνεια των αγορών και ενέχει κίνδυνο φθοράς της εμπιστοσύνης προς τα τραπεζικά και ψηφιακά συστήματα πληρωμών. Η ψηφιοποίηση των πληρωμών, οι fintech εφαρμογές και τα instantpayments έχουν αυξήσει τα κανάλια μέσω των οποίων τα παράνομα κεφάλαια μπορούν να εισαχθούν στο οικονομικό σύστημα, καθιστώντας επιτακτική την ανάπτυξη προηγμένων μηχανισμών ανίχνευσης και πρόληψης.
2. Η κατανόηση των μεθόδων που χρησιμοποιούν εγκληματικές οργανώσεις για τη νομιμοποίηση εσόδων και η εφαρμογή συστημάτων παρακολούθησης και

πρόληψης είναι κρίσιμη για την προστασία των χρηματοπιστωτικών ιδρυμάτων και των πελατών τους. Η αποτελεσματική AML στρατηγική επιτρέπει την έγκαιρη αναγνώριση ύποπτων συναλλαγών και μειώνει τον κίνδυνο συστημικών και οικονομικών επιπτώσεων.

8.2 Έννοια και Ορισμός της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες (AML)

1. Η AML αναφέρεται στη διαδικασία μετατροπής κεφαλαίων που προέρχονται από εγκληματικές δραστηριότητες σε νόμιμα εμφανιζόμενα κεφάλαια. Οι παράνομες δραστηριότητες περιλαμβάνουν, μεταξύ άλλων:
 - απάτες,
 - διαφθορά,
 - παράνομη διακίνηση αγαθών ή ουσιών,
 - χρηματοδότηση τρομοκρατικών ομάδων,
 - φοροδιαφυγή και κυβερνοεγκλήματα.
2. Σύμφωνα με εκτιμήσεις διεθνών οργανισμών (FATF, OECD), το 2–5% του παγκόσμιου ΑΕΠ «ξεπλένεται» ετησίως, με αυξανόμενο μέρος των κεφαλαίων να διακινείται μέσω ψηφιακών συναλλαγών και ηλεκτρονικών πληρωμών.
3. Ο σκοπός της AML διαδικασίας περιλαμβάνει:
 - **Αναγνώριση ύποπτων συναλλαγών** ώστε να αποτρέπεται η εισροή παράνομων κεφαλαίων στο σύστημα.

- ο **Πρόληψη αξιοποίησης του τραπεζικού συστήματος** για εγκληματικές δραστηριότητες, προστατεύοντας την αξιοπιστία των τραπεζών και των fintech πλατφορμών.
 - ο **Διασφάλιση εμπιστοσύνης** μεταξύ χρηματοπιστωτικών φορέων και καταναλωτών, ενισχύοντας την ακεραιότητα των συναλλαγών.
-

8.3 Στάδια του Ξεπλύματος Χρήματος

8.3.1 Placement – Εισαγωγή κεφαλαίων στο χρηματοπιστωτικό σύστημα

1. Στο πρώτο στάδιο, τα παράνομα κεφάλαια εισάγονται με τρόπο που να μην προκαλέσουν υποψίες στις αρχές. Η στρατηγική αφορά **απόκρυψη της προέλευσης** των κεφαλαίων μέσω διασποράς σε μικρά ποσά ή μέσω τεχνητών συναλλαγών.
2. Συχνές μέθοδοι:
 - ο **Κατάθεση μικρών ποσών (smurfing)**: Η τμηματική κατάθεση κεφαλαίων σε πολλούς λογαριασμούς αποσκοπεί στη μη ενεργοποίηση ορίων αναφοράς των τραπεζών.
 - ο **Χρήση POS επιχειρήσεων βιτρίνας**: Δημιουργία ψευδούς τζίρου μέσω πληρωμών με κάρτες τρίτων.
 - ο **Αγορά προπληρωμένων καρτών και fintechwallets**: Εισαγωγή κεφαλαίων σε ηλεκτρονικά πορτοφόλια με ελάχιστο έλεγχο ταυτότητας.
 - ο **Εικονικές αγορές e-commerce**: Χρήση πλατφορμών για φαινομενική αγοραπωλησία προϊόντων που δεν υφίστανται, δίνοντας «νομιμότητα» στα κεφάλαια.

8.3.2 Layering – Διαστρωμάτωση κεφαλαίων

1. Στο στάδιο αυτό δημιουργείται ένα σύνθετο δίκτυο συναλλαγών που **αποκρύπτει την προέλευση των κεφαλαίων**, καθιστώντας δύσκολη την ανίχνευσή τους.
2. Τεχνικές:
 - Μεταφορές κεφαλαίων σε πολλούς λογαριασμούς εντός και εκτός χώρας.
 - Χρήση εικονικών τιμολογίων (invoicefraud) για τεχνητή μετακίνηση κεφαλαίων.
 - Αγοραπωλησία κρυπτονομισμάτων, όπου η αποκεντρωμένη φύση των συναλλαγών δυσχεραίνει την παρακολούθηση.
 - Αγορά αγαθών υψηλής αξίας (π.χ., τέχνη, πολυτελή αντικείμενα) και άμεση μεταπώληση για «ξέπλυμα» κεφαλαίων.

8.3.3 Integration – Επανένταξη στην οικονομία

1. Στο τελικό στάδιο, τα κεφάλαια επανεντάσσονται στο νόμιμο οικονομικό κύκλωμα.
2. Μέθοδοι:
 - Επενδύσεις σε επιχειρήσεις και start-ups για δημιουργία φαινομενικά νόμιμου εισοδήματος.
 - Αγορά ακινήτων, η οποία επιτρέπει τη μετατροπή μεγάλων κεφαλαίων σε νόμιμη ιδιοκτησία.
 - Εμπορικές δραστηριότητες και μεταβιβάσεις μέσω τραπεζικών συστημάτων που δίνουν οικονομικό «χαρτοφυλάκιο» στα κεφάλαια.

8.4 Κανάλια Ξεπλύματος Χρήματος στις Ψηφιακές Πληρωμές

1. **POS και e-commerce συστήματα:** Επιχειρήσεις βιτρίνες δημιουργούν τεχνητό τζίρο με συνεχή μικρά ποσά, χρήση καρτών τρίτων χωρών και επιστροφές σε «ελεγχόμενους» λογαριασμούς.
 2. **Web & Mobile Banking:** Ταχύτατες μεταφορές κεφαλαίων, muleaccounts και εικονικές πληρωμές διευκολύνουν την απόκρυψη κεφαλαίων χωρίς φυσική παρουσία.
 3. **Κρυπτονομίσματα και mixers:** Αποκεντρωμένα ανταλλακτήρια, privacycoins (Monero, Zcash) και mixers/tumblers καθιστούν την παρακολούθηση κεφαλαίων σχεδόν αδύνατη.
 4. **Digitalwallets και fintech συστήματα:** Η ευκολία ανοίγματος λογαριασμού και η χαμηλή εφαρμογή KYC αυξάνουν τον κίνδυνο placement και layering.
-

8.5 Μορφές Ξεπλύματος Χρήματος στο Ηλεκτρονικό Περιβάλλον

1. **Money Mules:** Άτομα που μεταφέρουν παράνομα κεφάλαια έναντι αμοιβής, συχνά στρατολογούμενα μέσω phishing, socialengineering ή αγγελιών «εύκολου κέρδους».
2. **Απάτες επενδύσεων & romancescams:** Χρήματα θυμάτων χρησιμοποιούνται για layering με συνεχείς μεταφορές σε πολλαπλούς λογαριασμούς, καθιστώντας δύσκολη την ιχνηλάτηση.

3. **Corporatelaundering:** Υπερτιμολογήσεις, εικονικά τιμολόγια, μεταφορά κεφαλαίων εντός πολυεθνικών σχημάτων και κινήσεις μέσω εταιρειών βιτρίνα αποτελούν κύρια εργαλεία απόκρυψης κεφαλαίων.
-

8.6 Red Flags και Δείκτες Ύποπτων Συναλλαγών

1. Συνεχείς μικρές καταθέσεις κάτω από το όριο αναφοράς.
 2. Συχνές διεθνείς μεταφορές χωρίς οικονομική αιτιολόγηση.
 3. Απότομη αύξηση δραστηριότητας αδρανών λογαριασμών.
 4. POS με δυσανάλογα υψηλό αριθμό συναλλαγών σε σχέση με την αγορά.
 5. Λογαριασμοί που χρησιμοποιούνται μόνο για εισροές και άμεσες εκροές κεφαλαίων.
 6. Συναλλαγές με χώρες υψηλού κινδύνου (σύμφωνα με FATF highrisklist).
-

8.7 Θεσμικό Πλαίσιο και Κανονιστική Συμμόρφωση

1. **Οδηγίες AML 4–6 της ΕΕ:** Ενισχυμένη δέουσα επιμέλεια (EDD), υποχρεωτικό KYC/KYB, αναφορές ύποπτης δραστηριότητας σε FIUs και αυστηρές κυρώσεις για μη συμμόρφωση.
2. **PSD2 και Strong Customer Authentication:** Πολυπαραγοντική ταυτοποίηση, έλεγχος συσκευής και ανάλυση συμπεριφοράς σε πραγματικό χρόνο για πρόληψη απάτης.

3. **FATF Recommendations:** Διεθνές πρότυπο AML πολιτικών με λίστες χωρών υψηλού κινδύνου, απαιτήσεις για AML συστήματα και αξιολόγηση συμμόρφωσης κρατών.
-

8.8 Μηχανισμοί Καταπολέμησης της Νομιμοποίησης Εσόδων

1. **KYC/KYB & UBO Verification:** Ταυτοποίηση πελατών και επιχειρήσεων, συλλογή οικονομικού προφίλ και συνεχής παρακολούθηση για διασφάλιση ότι ο πραγματικός δικαιούχος (UBO) είναι νόμιμος.
 2. **Συστήματα AML Transaction Monitoring:** Παρακολούθηση συναλλαγών σε πραγματικό χρόνο, εφαρμογή κανόνων και ταξινόμηση ύποπτης συμπεριφοράς.
 3. **Τεχνητή Νοημοσύνη και Μηχανική Μάθηση:** Προβλεπτικά μοντέλα κινδύνου, ανάλυση μοτίβων, μείωση falsepositives και προσαρμογή σε νέες μορφές εγκλήματος.
 4. **Screening Systems:** Έλεγχοι κυρώσεων (OFAC, UN, EU), έλεγχοι PEP & RCA, παρακολούθηση adversedia για έγκαιρη αναγνώριση κινδύνων.
 5. **Εσωτερικός Έλεγχος, Governance και Whistleblowing:** Πολιτικές αποτροπής εσωτερικής απάτης, διαφθοράς και σύγκρουσης συμφερόντων.
-

8.9 Σύγχρονες Προκλήσεις για Χρηματοπιστωτικά Ιδρύματα

1. Αύξηση διασυνοριακών ψηφιακών συναλλαγών που δυσκολεύουν την παρακολούθηση.
2. Δυσκολία ανίχνευσης κεφαλαίων σε κρυπτονομίσματα.
3. Fragmentation στο κανονιστικό πλαίσιο μεταξύ χωρών.
4. Νέες τεχνικές κυβερνοεγκλήματος που εξελίσσονται συνεχώς.
5. Ανάγκη συνεχούς αναβάθμισης συστημάτων AML για συμμόρφωση και πρόληψη.

ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΕΦΑΛΑΙΩΝ

Η ραγδαία ανάπτυξη των ψηφιακών πληρωμών έχει μετασχηματίσει ουσιαστικά το σύγχρονο χρηματοπιστωτικό σύστημα, ενισχύοντας την ταχύτητα, την αποδοτικότητα και την ευκολία των συναλλαγών. Ωστόσο, η μετάβαση αυτή συνοδεύεται από την ανάδυση νέων και πιο σύνθετων κινδύνων, με την ηλεκτρονική απάτη να αποτελεί μία από τις σημαντικότερες προκλήσεις.

Η ανάλυση ανέδειξε ότι η ηλεκτρονική απάτη εξελίσσεται δυναμικά, εκμεταλλευόμενη τόσο τεχνολογικές αδυναμίες όσο και ανθρώπινους παράγοντες, ενώ οι επιπτώσεις της εκτείνονται πέρα από τις άμεσες οικονομικές απώλειες, επηρεάζοντας τη λειτουργία των οργανισμών και την εμπιστοσύνη των χρηστών. Παράλληλα, η μελέτη περίπτωσης και η συγκριτική ανάλυση ευρωπαϊκών χωρών κατέδειξαν ότι το επίπεδο ψηφιακής ωριμότητας και η ένταση χρήσης των ηλεκτρονικών πληρωμών συνδέονται άμεσα με τη φύση και την έκταση των απειλών.

Επιπλέον, η προσαρμογή φαινομένων όπως το ξέπλυμα χρήματος στο ψηφιακό περιβάλλον ενισχύει περαιτέρω την πολυπλοκότητα του κινδύνου, καθιστώντας αναγκαία τη συνεχή εξέλιξη των μηχανισμών συμμόρφωσης. Σε αυτό το πλαίσιο, καθίσταται σαφές ότι η αποτελεσματική αντιμετώπιση των σύγχρονων απειλών δεν μπορεί να βασιστεί σε μεμονωμένες λύσεις, αλλά απαιτεί μια ολιστική προσέγγιση που συνδυάζει προηγμένες τεχνολογίες, ισχυρό κανονιστικό πλαίσιο και ενεργό συμμετοχή των χρηστών μέσω εκπαίδευσης και ευαισθητοποίησης.

Συνολικά, η διασφάλιση της εμπιστοσύνης και της σταθερότητας του χρηματοπιστωτικού συστήματος στην ψηφιακή εποχή εξαρτάται από την ικανότητα των οργανισμών να προσαρμόζονται συνεχώς, να καινοτομούν και να διαχειρίζονται αποτελεσματικά τους αναδυόμενους κινδύνους.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

[PwC – Global Economic Crime Survey](#)

[\(European Central Bank \(ECB\). \(2023\). Payment cards fraud statistics.\)](#)

[Bank for International Settlements \(BIS\). \(2022\). Digital payments and financial stability.](#)

[World Bank \(2021\). Digital Financial Services.](#)

[European Central Bank – Payment methods report](#)

[Bank of Greece – Payment Systems Report](#)

[Bank for International Settlements \(BIS\). \(2022\). Digital payments and financial stability.](#)

[ECB – Retail Payments Strategy](#)

[European Commission. \(2018\). PSD2 Directive on Payment Services.](#)

[European Commission AML Directive](#)

[European Parliament GDPR Regulation](#)

[Eurostat – Digital Economy Statistics](#)

[OECD – Digital Payments](#)

[National Bank of Greece Annual Report](#)

[NBG Pay Payment System](#)

[Accenture Banking Fraud Study](#)

[IBM AI Fraud Detection](#)

[Accenture AI in Banking](#)

[Eurostat](#)

[ECB payment statistics](#)

[OECD digital economy](#)

[Financial Action Task Force \(FATF\) – Anti-Money Laundering Guidelines](#)

[Basel Committee – AML compliance](#)

[European Banking Authority – AML guidelines](#)

[European Banking Authority](#)

[FATF Reports](#)

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1 – Εισαγωγή

- 1.1 Σκοπός της Έρευνας
 - 1.2 Ερευνητικά Ερωτήματα
 - 1.3 Σημαντικότητα της Μελέτης
 - 1.4 Μεθοδολογία της Έρευνας
 - 1.5 Δομή της Διπλωματικής Εργασίας
-

Κεφάλαιο 2 – Θεωρητικό Υπόβαθρο

2.1 Ψηφιακές Πληρωμές στα Χρηματοπιστωτικά Ιδρύματα

- 2.1.1 Έννοια και εξέλιξη των ψηφιακών πληρωμών
- 2.1.2 Είδη ψηφιακών πληρωμών (POS, e-commerce, wallets, instantpayments)
- 2.1.3 Ρόλος των τραπεζών στο σύστημα ηλεκτρονικών συναλλαγών
- 2.1.4 Ρυθμιστικό πλαίσιο (PSD2, SCA, AMLD, GDPR)

2.2 Ψηφιακές Πληρωμές στην Ευρώπη – Συγκριτικό Πλαίσιο 15 χωρών

- 2.2.1 Επίπεδο ψηφιοποίησης και διείσδυση ηλεκτρονικών πληρωμών
 - 2.2.2 Στατιστικά χρήσης ανά χώρα
 - 2.2.3 Κίνδυνοι και προκλήσεις στις ευρωπαϊκές ψηφιακές πληρωμές
 - 2.2.4 Συγκριτική ανάλυση επιπέδων απάτης
-

Κεφάλαιο 3 – Μορφές Ηλεκτρονικής Απάτης

3.1 Απάτες που αφορούν Issuing (Κάρτες Πληρωμών)

- 3.1.1 Card Theft (κλοπήκάρτας)
 - 3.1.2 Card Not Present Fraud
 - 3.1.3 Skimming
-

3.1.4 BIN Attacks

3.1.5 SIM Swap ως μέθοδος παράκαμψης SCA

3.1.6 Compromised Cards – Data Breaches

3.1.7 Friendly Fraud / Chargeback Abuse

3.2 Απάτες Web & Mobile Banking

3.2.1 Phishing

3.2.2 Smishing

3.2.3 Vishing

3.2.4 Investment Fraud

3.2.5 Microsoft / Tech Support Scam

3.2.6 Account Takeover (ATO)

3.2.7 Social Engineering Attacks

3.2.8 Money Mules και νομιμοποίηση εσόδων

3.2.9 Συνδυασμένες επιθέσεις (hybrid fraud)

Κεφάλαιο 4 – Επιπτώσεις των Ηλεκτρονικών Απατών

4.1 Επιπτώσεις στους πελάτες

4.2 Επιπτώσεις στις επιχειρήσεις

4.3 Οικονομικό κόστος για τα χρηματοπιστωτικά ιδρύματα

4.4 Επιπτώσεις στη φήμη των τραπεζών

4.5 Ρυθμιστικές κυρώσεις & νομικοί κίνδυνοι

Κεφάλαιο 5 – Μελέτη Περίπτωσης Χρηματοπιστωτικού

Ιδρύματος (NBG Pay)

- 5.1 Παρουσίαση του οργανισμού NBG Pay
 - 5.2 Ρόλος στις ψηφιακές πληρωμές
 - 5.3 Υποδομές POS, e-commerce και APIs
 - 5.4 Ανάλυση κινδύνων και ευπαθειών
 - 5.5 Παραδείγματα περιστατικών απάτης από εταιρείες–πελάτες
 - 5.6 Οικονομικές επιπτώσεις για τις επιχειρήσεις και την τράπεζα
-

Κεφάλαιο 6 – Μηχανισμοί Ανίχνευσης και Πρόληψης

Απάτης

6.1 Detection

- 6.1.1 Risk Scoring Models
- 6.1.2 Machine Learning & AI Fraud Engines
- 6.1.3 Behavioral Analytics
- 6.1.4 Transaction Monitoring
- 6.1.5 Device Fingerprinting & Geolocation

6.2 Prevention

- 6.2.1 Πολύ παραγοντικός έλεγχος ταυτότητας (SCA)
 - 6.2.2 Tokenization & Encryption
 - 6.2.3 Limits, velocity checks & rule engines
 - 6.2.4 Εκπαίδευση των χρηστών
 - 6.2.5 Governance & Internal Controls
-

Κεφάλαιο 7 – Ανάλυση Εκτενούς Δείγματος 15 Ευρωπαϊκών

Χωρών

- 7.1 Δεδομένα χρήσης ψηφιακών πληρωμών
 - 7.2 Συχνότητα και ένταση περιστατικών απάτης
 - 7.3 Συσχέτιση ψηφιακής ωριμότητας και κινδύνου απάτης
 - 7.4 Παράγοντες που αυξάνουν / μειώνουν τη συχνότητα απάτης
 - 7.5 Συγκριτική αξιολόγηση και ευρήματα
-

Κεφάλαιο 8 – Ξέπλυμα Χρήματος και Μηχανισμοί Καταπολέμησης (AML)

- 8.1 Εισαγωγή
- 8.2 Έννοια και Ορισμός της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες (AML)
- 8.3 Στάδια του Ξεπλύματος Χρήματος
- 8.4 Κανάλια Ξεπλύματος Χρήματος στις Ψηφιακές Πληρωμές
- 8.5 Μορφές Ξεπλύματος Χρήματος στο Ηλεκτρονικό Περιβάλλον
- 8.6 Red Flags και Δείκτες Ύποπτων Συναλλαγών
- 8.7 Θεσμικό Πλαίσιο και Κανονιστική Συμμόρφωση
- 8.8 Μηχανισμοί Καταπολέμησης της Νομιμοποίησης Εσόδων
- 8.9 Σύγχρονες Προκλήσεις για Χρηματοπιστωτικά Ιδρύματα

Σημείωση για Βιβλιογραφικές Αναφορές

Οι βιβλιογραφικές αναφορές της εργασίας θα πρέπει να ακολουθούν ενιαίο σύστημα παραπομπών Harvard Style. Ενδεικτική μορφή:

European Central Bank (2023) Payment Cards Fraud Statistics. Frankfurt: ECB.

Europol (2022) Internet Organised Crime Threat Assessment. The Hague: Europol.

World Bank (2021) Digital Financial Services. Washington DC: World Bank.