2026-02

þÿ Î Â ± ½ Ä ¹ » ® È µ ¹ Â Ç Á · Ã Ä Î ½ Ã Ç µ

þÿ Ä ¿ º Å ² µ Á ½ ¿ - ³ º » · ¼ ± ,

þÿ º Å ² µ Á ½ ¿ ± Ã Æ ¬ » µ ¹ ± º ± ¹ Ä µ Ç ½ · Ä

þÿ ½ ¿ · ¼ ¿ Ã Í ½ · µ À · Á µ ¬ ¶ ¿ Å ½ Ä ·

þÿ Ã Å ¼ À µ Á ¹ Æ ¿ Á ¬ º ± ¹ À Á Ì ¸ µ Ã · Ç

þÿ B a s e d e - c o m m e r c e Ã Å Ã Ä · ¼ ¬

Papoute, Anna-Klio

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± ¨ · Æ ¹ ± º Ì œ ¬ Á º µ Ä ¹ ½ ³ º , £ Ç ¿ » ® Ÿ ¹ º ¿ ½ ¿ ¼ ¹ º Î ½ • À ¹ Ã
þÿ ” ¹ ¿ ¯ º · Ã · Â , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â ¬ Æ ¿ Å

Πανεπιστήμιο Νεάπολις Πάφος

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΔΙΟΙΚΗΣΗΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ

MSc DIGITAL MARKETING

"Πώς αντιλήψεις χρηστών σχετικά με το κυβερνοέγκλημα, κυβερνοασφάλεια και τεχνητή νοημοσύνη επηρεάζουν τη συμπεριφορά και πρόθεση χρήσης AI – Based e-commerce συστημάτων;"

Papoute Anna-Klio

Επιβλέπων: Dr. Spiliotopoulos Dimitrios

Φεβρουάριος 2026

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΔΙΟΙΚΗΣΗΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ

MSc DIGITAL MARKETING

"Πώς αντιλήψεις χρηστών σχετικά με το κυβερνοέγκλημα, κυβερνοασφάλεια και τεχνητή νοημοσύνη επηρεάζουν τη συμπεριφορά και πρόθεση χρήσης AI – Based e-commerce συστημάτων;"

Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση μεταπτυχιακού τίτλου σπουδών στο Digital Marketing στο Πανεπιστήμιο Νεάπολις Πάφος

Papoute Anna-Klio

Φεβρουάριος 2026

Ονοματεπώνυμο Φοιτητή: Papoute Anna-Klio

Τίτλος Διπλωματικής Εργασίας: "Πώς οι αντιλήψεις των χρηστών σχετικά με το κυβερνοέγκλημα και η εμπιστοσύνη στις μεθόδους κυβερνοασφάλειας και τεχνητής νοημοσύνης επηρεάζουν την πρόθεση χρήσης AI-e-commerce διαδικτυακών συστημάτων εμπορίου;"

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις (ημερομηνία έγκρισης)…….…… από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)

Ονοματεπώνυμο: Dr. Spiliotopoulos Dimitrios **Βαθμίδα:** **Υπογραφή:**
Μέλος Εξεταστικής Επιτροπής:

Ονοματεπώνυμο Dr. Anastasiou Athanasios **Βαθμίδα:** **Υπογραφή:**
Μέλος Εξεταστικής Επιτροπής:

Ονοματεπώνυμο Dr. Dermatis Zacharias **Βαθμίδα:** **Υπογραφή:**

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Η **Papoute Anna-klio**., γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «**Πώς οι αντιλήψεις των χρηστών σχετικά με το κυβερνοέγκλημα και η εμπιστοσύνη στις μεθόδους κυβερνοασφάλειας και τεχνητής νοημοσύνης επηρεάζουν την πρόθεση χρήσης AI-e-commerce διαδικτυακών συστημάτων εμπορίου;***»,* αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Ο/Η Δηλών /σα

Papoute Anna-Klio

ΠΕΡΙΛΗΨΗ

Η ταχεία επέκταση ηλεκτρονικού εμπορίου και αυξανόμενη ενσωμάτωση τεχνητής νοημοσύνης σε ψηφιακά επιχειρηματικά περιβάλλοντα έχουν μετασχηματίσει τις αλληλεπιδράσεις καταναλωτών-εταιρειών, ενώ παράλληλα εντείνει την έκθεση σε κίνδυνους κυβερνοεγκλήματος. Καθώς διαδικτυακές συναλλαγές εξελίσσονται μακροπρόθεσμα, αντιλήψεις σχετικά με το κυβερνοέγκλημα, εμπιστοσύνη στους μηχανισμούς κυβερνοασφάλειας και αποδοχή συστημάτων που βασίζονται στην τεχνητή νοημοσύνη αναδεικνύονται κρίσιμοι καθοριστικοί παράγοντες συμπεριφοράς και πραγματικής πρόθεσης χρήσης πλατφορμών ηλεκτρονικού εμπορίου που στηρίζονται στην AI. Η μελέτη αυτή διερευνά την εξέταση αντίκτυπου στοχεύοντας πώς συνδυαστικά αντιλήψεις ψηφιακών χρηστών για το κυβερνοέγκλημα βάσει των ψυχολογικών, συναισθηματικών αντιδράσεων και επιπτώσεων από κυβερνοαπειλές και πεποιθήσεων για κυβερνοεγκληματίες, εμπιστοσύνη στις εφαρμοσμένες μεθόδους κυβερνοασφάλειας και δυνατότητες τεχνητής νοημοσύνης επηρεάζουν τη στάση και πρόθεση χρήσης συστημάτων ηλεκτρονικού εμπορίου με AI. Για την επίτευξη στόχου, η έρευνα ενσωματώνει το Μοντέλο Αποδοχής Τεχνολογίας (TAM) και Θεωρία Σχεδιασμένης Συμπεριφοράς (TPB) σε ένα νέο εννοιολογικό πλαίσιο, επεκτείνοντας τα υπάρχοντα μοντέλα ενσωματώνοντας την εμπειρία κυβερνοεγκλήματος, αντιλήψεις για κυβερνοεγκληματίες, παράγοντα κυβερνοψυχολογικής διαταραχής χρηστών και αντιληπτή εμπιστοσύνη ως βασικές δομές.

Υιοθετήθηκε μικτή μεθοδολογική προσέγγιση. Το ποιοτικό σκέλος συστάθηκε μέσω εκτενούς ανασκόπησης σύγχρονης ακαδημαϊκής βιβλιογραφίας από διάφορους επιστημονικούς τομείς σχετικά με κυβερνοέγκλημα, κυβερνοασφάλεια και τεχνητή νοημοσύνη στο ηλεκτρονικό εμπόριο, ενώ ποσοτικό σκέλος περιλάμβανε ένα δομημένο διαδικτυακό ερωτηματολόγιο που διανεμήθηκε σε ενεργούς ψηφιακούς καταναλωτές με εμπειρία στις διαδικτυακές συναλλαγές και κύριο στοιχείο την πιθανή έκθεση στο κυβερνοέγκλημα. Τα δεδομένα αναλύθηκαν χρησιμοποιώντας το στατιστικό πακέτο λογισμικού Jamovi. Διεξήχθησαν περιγραφικές στατιστικές δοκιμές αξιοπιστίας, εγκυρότητας, αναλύσεις συσχέτισης, ανεξάρτητα t-tests δειγμάτων και απλές-πολλαπλές αναλύσεις παλινδρομήσεων για να δοκιμαστούν ερευνητικές υποθέσεις και αξιολογηθούν δομικές σχέσεις μεταξύ κατασκευών του νέου εννοιολογικού μοντέλου.

Τα στατιστικά αποτελέσματα αποκάλυψαν ότι εμπιστοσύνη σε AI, στάση, υποκείμενες νόρμες και αντιληπτός έλεγχος συμπεριφοράς επηρεάζουν άμεσα και στατιστικά σημαντικά την πρόθεση αγοράς, αναδεικνύοντας τα καθοριστικούς δείκτες υιοθέτησης πλατφορμών ηλεκτρονικού εμπορίου με τεχνητή νοημοσύνη. Αντίθετα, εμπιστοσύνη σε μεθόδους κυβερνοασφάλειας και αρνητική αντίληψη χρηστών για κυβερνοέγκλημα δεν είχαν άμεση επίδραση στην πρόθεση. Παράλληλα, διαπιστώθηκε, τόσο

εμπιστοσύνη στους μηχανισμούς κυβερνοπροστασίας, όσο και AI, καθώς και αρνητική αντίληψη για κυβερνοεγκληματικά προφίλ ασκούν σημαντική επιρροή στη στάση, επιβεβαιώνοντας τον έμμεσο ρόλο τους στη διαμόρφωση πρόθεσης. Παρότι το κυβερνοέγκλημα συνολικά παρουσίασε στατιστικά σημαντική επίδραση στην πρόθεση, ο διαμεσολαβητικός του ρόλος αποδείχτηκε περιορισμένος, καθώς δεν ασκεί ουσιώδη αρνητική επίδραση μέσω της εμπιστοσύνης στις μεθόδους κυβερνοασφάλειας. Καθοριστικός μόνο, υπήρξε ο ρόλος εμπιστοσύνης σε AI στην ενίσχυση πρόθεσης μέσω της αντιλαμβανόμενης επίπτωσης κυβερνοεγκλήματος στους χρήστες, ενώ υπόλοιπες διαμεσολαβητικές σχέσεις κρίθηκαν μη στατιστικά σημαντικές. Τα μέσα επίπεδα εμπιστοσύνης χρηστών για χρήση AI-Based E-commerce συστημάτων με προηγούμενη κυβερνοεγκληματική εμπειρία σε σύγκριση με εκείνους χωρίς αντίστοιχη, δεν υπέδειξαν σημαντική στατιστική απόκλιση υπογραμμίζοντας τον μετριαστικό ρόλο της προσωπικής έκθεσης σε κυβερνοαπειλές, ενώ δεν υπήρξε αξιοσημείωτη ουσιώδη συσχέτιση μεταξύ κυβερνοεγκληματικής εμπειρίας και πρόθεσης χρήσης τέτοιων συστημάτων παρά την αρνητική κατεύθυνση σχέσης. Περιεκτικά, τα ευρήματα υπογραμμίζουν τον κεντρικό ρόλο εμπιστοσύνης στην τεχνητή νοημοσύνη και ψυχοκοινωνικών παραγόντων στη λήψη αποφάσεων των ψηφιακών χρηστών, υποδεικνύοντας ότι η υιοθέτηση AI στο ηλεκτρονικό εμπόριο εξαρτάται περισσότερο από αντιλήψεις εμπιστοσύνης και ελέγχου παρά το φόβο κυβερνοεγκλήματος.

Η παρούσα μελέτη συμβάλλει θεωρητικά και πρακτικά επεκτείνοντας τα καθιερωμένα μοντέλα αποδοχής μέσω ενσωμάτωσης των κυβερνοψυχολογικών διαστάσεων και κυβερνοασφάλειας με την υποστήριξη τεχνητής νοημοσύνης. Τα ευρήματα παρέχουν εφαρμόσιμες γνώσεις για εταιρείες ηλεκτρονικού εμπορίου, υπεύθυνους χάραξης πολιτικής και επαγγελματίες κυβερνοασφάλειας με στόχο την ενίσχυση εμπιστοσύνης χρηστών και βιωσιμότητα πλατφορμών. Ενθαρρύνεται μελλοντική έρευνα σχετικά με τις διαχρονικές επιπτώσεις, διαπολιτισμικές διαφορές και προηγμένους μηχανισμούς διακυβέρνησης της τεχνητής νοημοσύνης για περαιτέρω ενίσχυση ασφαλών και αξιόπιστων οικοσυστημάτων ψηφιακού εμπορίου.

Λέξεις-Κλειδιά: Τεχνητή Νοημοσύνη, Ηλεκτρονικό Εμπόριο, Συμπεριφορά Καταναλωτών, Κυβερνοέγκλημα, Κυβερνοασφάλεια, Θεωρία Σχεδιασμένης Συμπεριφοράς, Εμπιστοσύνη, Πρόθεση Αγοράς.

ABSTRACT

The rapid expansion of e-commerce and the increasing integration of artificial intelligence into digital business environments have transformed consumer-business interactions, while also intensifying exposure to cybercrime risks. As online transactions evolve over time, perceptions of cybercrime, trust in cybersecurity mechanisms, and acceptance of AI-based systems are emerging as critical determinants of behavior and actual intention to use AI-enabled e-commerce platforms. This study explores the impact examination by aiming to examine how digital users' perceptions of cybercrime based on psychological, emotional reactions and impacts of cyberthreats and beliefs about cybercriminals, trust in applied cybersecurity methods, and AI capabilities collectively influence attitudes and intention to use AI-enabled e-commerce systems. To achieve this goal, research integrates the Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB) into a new conceptual framework, extending existing models by incorporating cybercrime experience, perceptions of cybercriminals, user cyberpsychological distress factor and perceived trust as key constructs.

A mixed methodological approach was adopted. The qualitative part was established through an extensive review of contemporary academic literature from various scientific fields related to cybercrime, cybersecurity and artificial intelligence in e-commerce, while the quantitative part included a structured online questionnaire distributed to active digital consumers with experience at online transactions and main element their potential exposure to cybercrime. The data were analyzed using the statistical software package Jamovi. Descriptive statistical tests of reliability, validity, correlation analyses, independent sample t-tests and simple-multiple regression analyses were conducted to test research hypotheses and assess structural relationships between constructs of the new conceptual model.

The statistical results revealed that trust in AI, attitude, subjective norms and perceived behavioral control directly and statistically significantly affect purchase intention, highlighting them as decisive indicators of adoption of e-commerce platforms with artificial intelligence. In contrast, trust in cybersecurity methods and negative user perception of cybercrime had no direct effect on intention. At the same time, it was found that both trust in cyberprotection mechanisms and AI, as well as negative perception of cybercrime profiles exert a significant influence on attitude, confirming their indirect role in the formation of intention. Although cybercrime overall had a statistically significant effect on intention, its mediating role proved to be limited, as it does not exert a significant negative effect through trust in cybersecurity methods. Only the role of trust in AI was decisive in enhancing intention through the perceived impact of cybercrime on users, while other mediating relationships were deemed not statistically significant. The average levels of trust of users for using AI-Based E-commerce systems with previous cybercrime

experience compared to those without, did not indicate a significant statistical difference, highlighting the moderating role of personal exposure to cyberthreats, while there was no significant correlation between cybercrime experience and intention to use such systems despite the negative direction of the relationship. Overall, the findings highlighted the central role of trust in AI and psychosocial factors in digital users' decision-making, suggesting that AI adoption in e-commerce depends more on perceptions of trust and control than fear of cybercrime.

This study contributes theoretically and practically by extending established acceptance models by incorporating cyberpsychological and cybersecurity dimensions with AI support. The findings provide actionable insights for e-commerce companies, policymakers, and cybersecurity practitioners to enhance users trust and platforms sustainability. Future research on the temporal implications, cross-cultural differences, and advanced governance mechanisms of AI is encouraged to further enhance safe and trustworthy digital commerce ecosystems.

Keywords: Artificial Intelligence, E-commerce, Customer Behavior, Cybercrime, Cybersecurity, Theory of Planned Behavior, Trust, Purchase Intention.