ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΤΙΚΩΝ, ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
«ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ – ΔΗΜΟΣΙΟ MANAGEMENT»

Μεταπτυχιακή Διπλωματική Εργασία

Τίτλος εργασίας

Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο Δημόσιο Τομέα της Ελλάδας σε θέματα ασφάλειας Πληροφοριακών Συστημάτων

Συγγραφέας
ΑΝΑΤΟΛΙΤΗΣ ΘΕΟΔΩΡΟΣ
ΑΜ: 2259

Επιβλέπουσα:
Δρ ΓΚΙΚΑ ΕΛΕΝΗ

ΑΘΗΝΑ
ΙΟΥΝΙΟΣ 2024

UNIVERSITY OF WEST ATTICA
SCHOOL OF ADMINISTRATIVE, ECONOMICS AND SOCIAL SCIENCES
DEPARTMENT OF BUSINESS ADMINISTRATION
«MSc IN PUBLIC ADMINISTRATION – PUBLIC MANAGEMENT»

Diploma Thesis

TITLE

Measuring the level of Information Security Awareness among employees in the Greek Public Sector

Student
ANATOLITIS THEODOROS
Registration number: 2259

Supervisor
GKIKA ELENH

ATHENS
JUNE 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΤΙΚΩΝ, ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

«ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ – ΔΗΜΟΣΙΟ MANAGEMENT»

Τίτλος: «Μέτρηση του βαθμού ευαισθητοποίησης των εργαζομένων στο Δημόσιο Τομέα της Ελλάδας σε θέματα ασφάλειας Πληροφοριακών Συστημάτων»

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	Ελένη Γκίκα	Μέλος του Εργαστηριακού και Διδακτικού προσωπικού του τμήματος Διοίκησης Επιχειρήσεων στο Πανεπιστήμιο Δυτικής Αττικής.	ΕΛΕΝΗ ΓΚΙΚΑ Digitally signed by ΕΛΕΝΗ ΓΚΙΚΑ Date: 2024.06.10 22:25:12 +03'00'
2	Σταμάτης Ντάνος	Μέλος του Εργαστηριακού και Διδακτικού προσωπικού του τμήματος Διοίκησης Επιχειρήσεων στο Πανεπιστήμιο Δυτικής Αττικής.	Stamatios Ntanos Digitally signed by Stamatios Ntanos Date: 2024.06.11 21:34:48 +03'00'
3	Σάββας Μακρίδης	Μέλος Συμβουλευτικού Επιστημονικού Προσωπικού Σ.Ε.Π.	SAVVAS MAKRIDIS Digitally signed by SAVVAS MAKRIDIS Date: 2024.06.11 11:39:21 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ανατολίτης Θεόδωρος του Χρήστου με αριθμό μητρώου 2259 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών Δημόσια Διοίκηση - Δημόσιο Management του Τμήματος Διοίκησης Επιχειρήσεων της Σχολής Διοικητικών Οικονομικών και Κοινωνικών Επιστημών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι: «Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

**Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι 31/12/2024 και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.*

*** Ονοματεπώνυμο /Ιδιότητα** Ο Δηλών

Ψηφιακή Υπογραφή Επιβλέποντα

(Υπογραφή)

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των απαιτήσεων του Μεταπτυχιακού Προγράμματος Δημόσια Διοίκηση – Δημόσιο Management του Τμήματος Διοίκησης Επιχειρήσεων του Πανεπιστημίου Δυτικής Αττικής. Η έγκρισή της δεν υποδηλώνει απαραιτήτως και την αποδοχή των απόψεων του συγγραφέα εκ μέρους του τμήματος.

Βεβαιώνω ότι η παρούσα μεταπτυχιακή εργασία είναι αποτέλεσμα δικής μου δουλειάς και δεν αποτελεί προϊόν αντιγραφής. Στις δημοσιευμένες ή μη δημοσιευμένες πηγές που αναφέρω έχω χρησιμοποιήσει εισαγωγικά, όπου απαιτείται και έχω παραθέσει τις πηγές τους στο τμήμα της βιβλιογραφίας

ΑΝΑΤΟΛΙΤΗΣ ΘΕΟΔΩΡΟΣ

Ευχαριστίες

Στο σημείο αυτό, αισθάνομαι την ανάγκη να ευχαριστήσω την επιβλέπουσα καθηγήτρια της διπλωματικής μου εργασίας, την κα. Γκίκα Έλενα, διότι χωρίς την υποστήριξη και τις πολύτιμες συμβουλές της, η ολοκλήρωση αυτής της εργασίας θα ήταν αδύνατη.

Επίσης, οφείλω ένα μεγάλο ευχαριστώ στη σύζυγό μου Έλενα, που με στηρίζει ώστε να συνεχίζω να αγωνίζομαι και να προσπαθώ να πετύχω τους στόχους μου, ακόμη και στις πιο δύσκολες στιγμές. Της αφιερώνω αυτή την εργασία με όλη μου την αγάπη και ευγνωμοσύνη.

Πίνακας περιεχομένων

Πίνακας γραφημάτων

Περίληψη

Ο ανθρώπινος παράγοντας στην ασφάλεια πληροφοριακών συστημάτων είναι ζωτικής σημασίας, καθώς οι άνθρωποι συχνά αποτελούν τον πιο αδύναμο κρίκο σε ένα σύστημα ασφάλειας. Οι εργαζόμενοι μπορούν ακούσια να εκθέσουν τα συστήματα σε κινδύνους μέσω πράξεων όπως η χρήση αδύναμων κωδικών πρόσβασης, η μη τήρηση των πρωτοκόλλων ασφαλείας, ή η απερισκεψία στην ανταλλαγή ευαίσθητων πληροφοριών. Σκοπός της παρούσας εργασίας είναι η αξιολόγηση του επιπέδου γνώσεων και αντιλήψεων των υπαλλήλων του δημόσιου τομέα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων καθώς και τομείς όπως η κουλτούρα του οργανισμού και η υιοθέτηση πολιτικών με κατεύθυνση την ασφάλεια των πληροφορίων. Επιπρόσθετα τέθηκαν οκτώ (8) ερευνητικές υποθέσεις με σκοπό τη διερεύνηση του βαθμού επιρροής ορισμένων δημογραφικών χαρακτηριστικών όπως το επίπεδο σπουδών, η ηλικία και το φύλο στο επίπεδο δημιουργίας ευαισθητοποίησης. Για την αξιολόγηση του επιπέδου ευαισθητοποίησης διεξήχθη ποσοτική έρευνα με δείγμα 172 υπαλλήλους του δημοσίου τομέα της Ελλάδας και χρησιμοποιήθηκε ένα ερωτηματολόγιο πενήντα έξι (56) συνολικά ερωτήσεων ως εργαλείο μέτρησης του βαθμού ευαισθητοποίησης σε θέματα ασφάλειας των πληροφοριών. Το είδος της δειγματοληψίας που εφαρμόστηκε είναι η δειγματοληψία μη πιθανότητας με δείγμα ευκολίας (conveniencesampling) και η ανάλυση των δεδομένων έγινε με τη χρήση του στατιστικού πακέτου SPSS. Η πλειοψηφία των συμμετεχόντων ανήκει στην ηλικιακή μάδα 50-59 ετών με ποσοστό 43,6% και ακολουθεί η ηλικιακή ομάδα 40-49 ετών με ποσοστό 35,5%. Το 55,2% είναι απόφοιτοι μεταπτυχιακού προγράμματος σπουδών και η πλειοψηφία των συμμετεχόντων εργάζονται στο Δημόσιο Τομέα από 15 έως 25 χρόνια ενώ το μεγαλύτερο ποσοστό του δείγματος (34,9%) είναι εργαζόμενοι στη τοπική αυτοδιοίκηση. Σύμφωνα με τα αποτελέσματα εντοπίστηκαν ορισμένες συνήθειες των εργαζομένων που θα μπορούσαν να υπονομεύσουν την ασφάλεια. Επίσης, η πολιτική των οργανισμών σε ορισμένες περιπτώσεις δεν είναι πολύ αυστηρή και οι εκπαιδεύσεις δεν καλύπτουν πάντα τις ανάγκες των εργαζομένων ωστόσο φαίνεται να πραγματοποιούνται αξιόλογα βήματα προς τη σωστή κατεύθυνση. Η έρευνα έδειξε επίσης ότι χαρακτηριστικά όπως το φύλο, η ηλικία και τα έτη υπηρεσίας μπορούν να επηρεάσουν το βαθμό ευαισθητοποίησης. Συνεπώς, η εκπαίδευση και η ευαισθητοποίηση των χρηστών, η ανάπτυξη μιας κουλτούρας ασφάλειας, και η συνεχής αναβάθμιση των γνώσεων τους σχετικά με τις νέες απειλές και τις βέλτιστες πρακτικές, είναι απαραίτητα στοιχεία για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων.

Abstract

The human factor in information systems security is of vital importance, as people often constitute the weakest link in a security system. Employees can inadvertently expose systems to risks through actions such as using weak passwords, failing to follow security protocols, or being careless in sharing sensitive information. The purpose of this study is to assess the level of knowledge and perceptions of public sector employees regarding information systems security, as well as areas such as organizational culture and the adoption of policies aimed at information security. Additionally, eight (8) research hypotheses were proposed to investigate the degree of influence of certain demographic characteristics such as education level, age and gender on the level of awareness. To assess the level of awareness, a quantitative survey was conducted with a sample of 172 public sector employees in Greece, using a questionnaire with a total of fifty-six (56) questions as a tool to measure the degree of awareness on information security issues. The type of sampling applied was non-probability convenience sampling and data analysis was conducted using the statistical package SPSS (26). The majority of participants belong to the age group of 50-59 years old (43.6%) followed by the age group 40-49 years old (35.5%). 55.2% of the participants are graduates of a postgraduate program and the majority of participants have been working in the public sector for 15 to 25 years, while the largest percentage of the sample (34.9%) are employees in local government.

According to the results, certain employee habits that could undermine security were identified. Furthermore, in some cases, organizations policies are not very strict and the training programs fail to meet the needs of employees, although significant steps appear to be taken in the right direction. The research also showed that characteristics such as gender, age and years of employment can affect the degree of employee awareness. Therefore, user training and awareness, by continuous updating of their knowledge regarding new threats and the development of a security culture, are among the best practices which are essentials for enhancing the security of information systems.

Keywords: Information security awareness, public sector, measuring the level of Information security awareness, malware, phishing, social engineering

Εισαγωγή

Το διαδίκτυο πλέον έχει καταστεί αναπόσπαστο κομμάτι της καθημερινότητας εκατομμυρίων ανθρώπων σε παγκόσμιο επίπεδο. Οι τεχνολογίες πληροφόρησης και επικοινωνίας (ICT) και οι σύγχρονες τεχνολογικές εφαρμογές χρησιμοποιούνται καθημερινά από ανθρώπους κάθε ηλικίας, εξυπηρετώντας ένα ευρύ φάσμα αναγκών και απλουστεύοντας ταυτόχρονα τις διαδικασίες. Στην Ευρώπη το έτος 2022 το 89,2% του πληθυσμού χρησιμοποιεί το διαδίκτυο, ποσοστό ραγδαία αυξανόμενο. Ειδικότερα, στην Ελλάδα οι χρήστες του διαδικτύου αποτελούν το 78,5% του πληθυσμού (https://www.internetworldstats.com/stats.html). Μια από τις τεχνολογίες με ραγδαία ανάπτυξη είναι η τεχνολογία Internet of Things (IoT), η οποία θα επιφέρει δραστικές αλλαγές προσθέτοντας μια νέα διάσταση στην επικοινωνία και αλληλεπίδραση των έξυπνων συσκευών (Atzori L. et al., 2010) Ωστόσο, η ανάπτυξη του διαδικτύου επισύρει νέες προκλήσεις και απειλές κατά της φυσικής και ηλεκτρονικής ασφάλειας. Πλέον, όλες οι κρίσιμες πληροφορίες αλλά και οι σημαντικές εργασίες εκτελούνται και διακινούνται στο διαδίκτυο μέσω έξυπνων συσκευών.

Τα tablets και smartphones αποτελούν έξυπνες συσκευές που χρησιμοποιούνται ευρέως τη τελευταία δεκαετία. Τα smartphones, ειδικότερα, έχουν αναδειχτεί σε προσωπικοί βοηθοί, που προσφέρουν πολυδιάστατες δυνατότητες και είναι εύκολα στη χρήση. Υφίσταται ωστόσο, μεγάλη ανησυχία για την πιθανότητα παραβίασης της ασφάλειας και του απορρήτου εξαιτίας κακόβουλου λογισμικού ή αν η συσκευή χαθεί ή κλαπεί (Alzubaidi A., Kalita J., 2016).

Δεδομένου ότι το Διαδίκτυο αναπτύσσεται ραγδαία, οι εγκληματίες άρχισαν να διαπράττουν εγκλήματα στο διαδίκτυο συχνότερα από ότι στον πραγματικό κόσμο. Οι δράστες προσαρμόζουν συνεχώς τη δράση τους στο περιβάλλον ακολουθώντας τις κοινωνικές και οικονομικές αλλαγές και εκμεταλλεύονται θέματα της επικαιρότητας.

Κάθε λογισμικό που εκτελεί σκόπιμα κακόβουλη δραστηριότητα στοχεύοντας σε πληροφοριακά συστήματα (υπολογιστές, έξυπνα τηλέφωνα, δίκτυα υπολογιστών κ.λπ.) θεωρείται κακόβουλο λογισμικό. Οι εγκληματίες χρησιμοποιούν κακόβουλο λογισμικό για να εξαπολύσουν επιθέσεις στον κυβερνοχώρου Υπάρχουν διάφοροι τύποι κακόβουλου λογισμικού, συμπεριλαμβανομένων ιών, τύπου σκουλήκια (worm) δούρειου ίππου, rootkit και ransomware. Κάθε τύπος και οικογένεια κακόβουλου λογισμικού έχει σχεδιαστεί για να επηρεάζει το στόχο με διαφορετικούς τρόπους, όπως καταστροφή του συστήματος, απομακρυσμένη εκτέλεση κώδικα, κλοπή εμπιστευτικών δεδομένων κ.λπ. (Aslan and Samet, 2020)

Το 2022 το 71% των επιχειρήσεων παγκοσμίως έχει επηρεαστεί από επιθέσεις κακόβουλου λογισμικού της οικογένειας ransomware, η οποία παραμένει η πιο σημαντική απειλή για τη διαδικτυακή ασφάλεια (State of Malware 2023, https://go.malwarebytes.com). Σύμφωνα με την

ετήσια έκθεση της IBM, το μέσο κόστος παραβίασης δεδομένων αυξήθηκε στο υψηλότερο επίπεδο όλων των εποχών των 4.35 εκατομμυρίων δολαρίων το 2022, αύξηση 2,6% από 4,24 εκατομμύρια δολάρια το 2021 (https://www.ibm.com/reports/data-breach). Οι τομείς των χρηματοπιστωτικών υπηρεσιών, της βιομηχανίας, των μεταφορών και της υγειονομικής περίθαλψης ήταν μεταξύ των τομέων που επηρεάστηκαν περισσότερο από τις κυβερνοεπιθέσεις που οδήγησαν σε παραβίαση δεδομένων. Αξίζει επίσης να αναφερθεί ότι το 74% των περιστατικών παράνομης πρόσβασης οφείλεται στο ανθρώπινο στοιχείο και ειδικότερα σε επιθέσεις κοινωνικής μηχανικής, λάθη ή κακή χρήση λογαριασμών και διαπιστευτηρίων (2023 Data Breach Investigations Report | Verizon.) Μία άλλη έρευνα υπογραμμίζει τη προσαρμοστικότητα των εγκληματιών στον κυβερνοχώρο και την αδιάκοπη αναζήτηση νέων οδών για την επίτευξη των στόχων τους, μέσω της εκμετάλλευσης τρωτών σημείων, της απόκτησης μη εξουσιοδοτημένης πρόσβασης, της παραβίασης ευαίσθητων πληροφοριών ή της εξαπάτησης ατόμων (https://www.eset.com). Οι εγκληματίες πλέον δε χρειάζεται να έχουν εξειδικευμένες τεχνικές γνώσεις και δεξιότητες καθώς μπορούν εύκολα να αποκτήσουν εργαλεία και έτοιμες εξατομικευμένες λύσεις στο σκοτεινό διαδίκτυο (Darkweb) (Chebac A., 2023) Το «έγκλημα στον κυβερνοχώρο ως υπηρεσία» (Cybercrime-as-a-service) είναι ένα ταχέως αναπτυσσόμενο παράνομο επιχειρηματικό μοντέλο στο οποίο οι δράστες νοικιάζουν ή πωλούν κακόβουλο λογισμικό σε άλλες εγκληματικές ομάδες για να ξεκινήσουν επιθέσεις και να κρυπτογραφήσουν υπολογιστές (https://www.eurojust.europa.eu/)

Τα τελευταία χρόνια έχει παρατηρηθεί ότι το έγκλημα στο κυβερνοχώρο έχει αλλάξει τόσο σε τεχνικό επίπεδο όσο και σε επίπεδο τελικού στόχου. Οι σημερινοί δράστες είναι συχνά μέλη εγκληματικών οργανώσεων ενώ τέτοιες ενέργειες είναι συχνά υποκινούμενες και έχουν κίνητρα πολιτικά, κοινωνικά ή αποσκοπούν σε χρηματικά κέρδη (https://www.cybercc.gr/el/). Σύμφωνα με τον ENISA, οι στόχοι που στοχοποιήθηκαν περισσότερο από πλήθος κυβερνο-επιθέσεων το πρώτο εξάμηνο του 2022 είναι οι δημόσιοι οργανισμοί και εταιρείες-πάροχοι υπηρεσιών διαδικτύου. Ο υψηλός αριθμός επιθέσεων κατά των δημόσιων οργανισμών πιθανότατα επηρεάστηκε από την εισβολή στην Ουκρανία, η οποία έχει προκαλέσει ένα κύμα επιθέσεων, κυρίως επιθέσεων D.D.o.S. εναντίον χωρών της ΕΕ που καταδικάζουν τις ενέργειες της Ρωσίας (www.enisa.europa.eu).

Οι κακόβουλοι χρήστες εφευρίσκουν συνεχώς νέους τρόπους για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα με κυριότερο σκοπό το παράνομο οικονομικό κέρδος και ο Δημόσιος τομέας είναι ο πιο ευάλωτος. Ο λόγος είναι ότι οι οργανισμοί αυτοί κατέχουν εξαιρετικά μεγάλες ποσότητες ευαίσθητων δεδομένων. Επιπλέον, ο Δημόσιος τομέας χρηματοδοτείται κατά κύριο λόγο από τα χρήματα των φορολογουμένων με αποτέλεσμα οι οργανισμοί του Δημοσίου να λειτουργούν με περιορισμένο προϋπολογισμό. Αυτό σημαίνει ότι αυτοί οι οργανισμοί λειτουργούν με ξεπερασμένη

τεχνολογία παλαιού τύπου, γεγονός που τον καθιστά πιο ευάλωτο σε παραβιάσεις ασφάλειας (https://www.idb.org/top-5-cyberthreats-facing-the-public-sector/).

Η τεχνολογία αλλάζει ταχύτατα με την πάροδο του χρόνου και οι απειλές για την ασφάλεια ακολουθούν αυτές τις αλλαγές (Valentine A., 2006). Αν και η τεχνολογία θα αναπτύσσεται πάντα ώστε να καλύπτει τα πιθανά κενά ασφαλείας των συστημάτων, πάντα θα υπάρχουν διαφορετικοί τρόποι για τους εγκληματίες να δράσουν. Στην εξίσωση της ασφάλειας, ένας παράγοντας, ο άνθρωπος παράγοντας, εξακολουθεί να υπάρχει και προκαλεί μεγάλη ανησυχία σε θέματα ασφάλειας. Οι χρήστες πρέπει να γνωρίζουν τις τακτικές και τις διαδικασίες ασφαλείας και πρέπει να γνωρίζουν πώς να χρησιμοποιούν τη τεχνολογία με ασφαλή τρόπο. Με άλλα λόγια, ακόμη και ένα σύγχρονο και ιδιαίτερα ανεπτυγμένο σύστημα, δέχεται σοβαρές απειλές λόγω της εξάρτησής του από τους χρήστες του.

Κεφάλαιο 1^0 – Θεωρητικό Μέρος

1.1 Βιβλιογραφική ανασκόπηση

Το έγκλημα στον κυβερνοχώρο έχει κερδίσει την προσοχή τελευταία, ειδικά στις ανεπτυγμένες χώρες, λόγω της αύξησης των επιθέσεων και του κόστους που επιφέρει. Αυτή η ενότητα παρουσιάζει τις πρόσφατες προσεγγίσεις για την αξιολόγηση των γνώσεων των χρηστών σχετικά με τα εγκλήματα στον κυβερνοχώρο σε όλο τον κόσμο, καθώς και μελέτες επικεντρωμένες στην Ελλάδα.

Μία έρευνα που διεξήχθη το 2011 (Papagiannakis K., 2011) σχετικά με το επίπεδο ευαισθητοποίησης των εργαζομένων σε θέματα ασφάλειας στον ελληνικό ιδιωτικό τομέα, αναφέρει ότι μόνο το 34% των συμμετεχόντων έχει συμμετάσχει σε πρόγραμμα ευαισθητοποίησης (ISA – Information Security Awareness program) σχετικά με την κυβερνοασφάλεια που οργανώθηκε από την εταιρεία που εργάζονται. Επιπρόσθετα, το 38% των συμμετεχόντων που δε συμμετείχαν σε πρόγραμμα ανέφερε ως αιτία την απροθυμία της ανώτατης διοίκησης, καθώς δε το θεωρούσε σημαντικό για την ασφάλεια των συστημάτων της.

Σε άλλη μελέτη (Filippidis et al., 2018), μεταξύ φοιτητών τριτοβάθμιας εκπαίδευσης στην Ελλάδα, προέκυψε ότι οι μισοί φοιτητές χρησιμοποιούν τον ίδιο κωδικό πρόσβασης σε διαφορετικούς ιστοτόπους. Σχεδόν ένας στους πέντε δεν προσπαθεί να επαληθεύσει τη ταυτότητα ενός ατόμου πριν δώσει πληροφορίες, ενώ φαίνεται πως το επίπεδο σπουδών επηρεάζει τη συμπεριφορά των ατόμων στο διαδίκτυο.

Πιο συγκεκριμένα, , η έρευνα των Evans, M. et al. (2019) στο Δημόσιο τομέα έχει καταδείξει ότι το 92.5% των περιστατικών ασφαλείας που αναφέρθηκαν σχετίζονται με ανθρώπινο λάθος, ενώ παράλληλα υποστηρίζει ότι δεν δίδεται η δέουσα προσοχή στον ανθρώπινο παράγοντα σε αντίθεση με άλλους παράγοντες που επηρεάζουν την ασφάλεια των πληροφοριών. Ωστόσο, σε έρευνα ανάμεσα σε ελληνικούς οργανισμούς του Δημοσίου τομέα (Drivas, G. et al., 2020), μόλις το 25% των συμμετεχόντων πιστεύει ότι η πιο σημαντική απειλή για την ασφάλεια των συστημάτων τους αποτελεί το ανθρώπινο λάθος.

Έρευνες στο Δημόσιο τομέα έχουν αναδείξει την ανάγκη για βελτίωση του επιπέδου ευαισθητοποίησης των εργαζομένων αλλά και των πρακτικών για την διασφάλιση της ασφάλειας των πληροφοριών. Οι Loukis and Spinellis, D. (2001) διαπίστωσε ότι οι οργανισμοί του ελληνικού Δημοσίου τομέα έχουν μόνο ένα βασικό επίπεδο ευαισθητοποίησης για την ασφάλεια των πληροφοριακών συστημάτων, δίνοντας ιδιαίτερη έμφαση στην εμπιστευτικότητα των δεδομένων. Σε μία άλλη μελέτη (Van Veenstra and Ramilli, 2011) διαπιστώθηκε ότι ο έλεγχος του βαθμού πρόσβασης των υπαλλήλων στα δεδομένα του οργανισμού είναι πολύ σημαντική διαδικασία για τη διασφάλιση

των πληροφοριών, σε συνδυασμό με τεχνικές λύσεις, όπως πρόσθετα οργανωτικά μέτρα, παροχή εκπαίδευσης, εφαρμογή κοινών κανόνων και πολιτικών και η τιμωρία για μη εξουσιοδοτημένες ενέργειες που επηρεάζουν την ασφάλεια των πληροφορικών συστημάτων.

Δυστυχώς, και σε νεότερες έρευνες (Al-Shanfari, I. et al., 2022) διαπιστώνεται το χάσμα μεταξύ της τεχνολογικής ανάπτυξης και του βαθμού ευαισθητοποίησης των εργαζομένων σε θέματα ασφαλείας παραμένει, γεγονός που καθιστά δύσκολο για τους δημόσιους φορείς να προστατεύσουν τα περιουσιακά τους στοιχεία. παράλληλα επισημαίνεται ο παράγοντας της ψυχολογίας των εργαζομένων για την ανάπτυξη αποτελεσματικών στρατηγικών που θα βελτιώσουν την ανθρώπινη συμπεριφορά. Η έρευνα για την ευαισθητοποίηση σχετικά με την ασφάλεια των πληροφοριών στον δημόσιο τομέα έχει απασχολήσει ερευνητές σε όλες τις ηπείρους. Δυο ακόμα σύγχρονες έρευνες (Masilela and and Nel, 2021) (Szczepaniuk, et al., 2020) υπογραμμίζουν την έλλειψη επαρκών μέτρων ασφάλειας δεδομένων και πληροφοριών στον δημόσιο τομέα της Νότιας Αφρικής και της Ευρώπης, αντίστοιχα, γεγονός που είναι ιδιαίτερα ανησυχητικό δεδομένης της προόδου της ηλεκτρονικής διακυβέρνησης τα τελευταία χρόνια, λόγω και τον περιορισμών του COVID-19.

Το πρόβλημα επιδεινώνεται περαιτέρω από την παρουσία και άλλων προβληματικών παραγόντων, όπως η ελλιπής ή ξεπερασμένη εφαρμογή ISMS (Information Security Management System) και η περιορισμένη χρήση μέτρων προστασίας (Al-Izki and Weir, 2016). Στο Ομάν, οι στάσεις της διοίκησης απέναντι στην ασφάλεια των πληροφοριών διαπιστώθηκε ότι επηρεάζουν σημαντικά τη συμμόρφωση των χρηστών με τις διαδικασίες τήρησης κανόνων ασφαλείας. Τέλος, σε έρευνα που διενεργήθηκε σε υπηρεσίες της τοπικής αυτοδιοίκησης της Ολλανδίας (Homburg and and Kokje, 2020), οι ερευνητές υπογραμμίζουν τη σημασία της επίγνωσης των κινδύνων από τους υπαλλήλους στον επίδραση της συμμόρφωσης τους με τις πολιτικές ασφαλείας.

Αυτές οι μελέτες υποδεικνύουν συλλογικά την ανάγκη για μια συνολική προσέγγιση για την ασφάλεια των πληροφοριών στο δημόσιο τομέα, η οποία θα περιλαμβάνει τόσο τεχνικούς όσο και ανθρώπινους παράγοντες.

1.2 Βασικές απειλές κυβερνοασφάλειας

1.2.1 Κακόβουλο λογισμικό (malware)

«Με τον όρο malware (malicious and software) αναφερόμαστε στο λογισμικό που έχει σχεδιαστεί για να χρησιμοποιηθεί κακόβουλα (κακόβουλο λογισμικό)» (Γέρμανος και Γεωργίου , 2021). Σύμφωνα με τους συγγραφείς υπάρχουν πέντε βασικοί τρόποι με τους οποίους μπορεί να μολυνθεί ένα πληροφοριακό σύστημα.

Τρόποι-πηγές μόλυνσης από κακόβουλο λογισμικό

1. **Ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam)**
   Οι δράστες εμπεριέχουν κακόβουλα συνημμένα αρχεία μέσα σε ένα μήνυμα το οποίο προτρέπει το παραλήπτη να ανοίξει. Ο αποστολέας μπορεί να προσποιείται μία γνωστή εταιρεία και να ενημερώνει το παραλήπτη για κάποια προσφορά που βρίσκεται στο συνημμένο αρχείο. Σε περίπτωση που ο παραλήπτης ανοίξει το συνημμένο αρχείο θα εγκαταστήσει παράλληλα και το κακόβουλο λογισμικό, χωρίς να το γνωρίζει. Συνήθως οι επιθέσεις αυτές δεν είναι στοχευμένες και τα μηνύματα αποστέλλονται μαζικά.
2. **Μολυσμένες φορητές μονάδες δίσκου**
   Πολλοί ιοί τύπου worm εξαπλώνονται μολύνοντας φορητές μονάδες δίσκου, όπως μονάδες flash USB ή εξωτερικούς σκληρούς δίσκους. Το λογισμικό κακόβουλης λειτουργίας μπορεί να εγκατασταθεί αυτόματα όταν συνδέεται μια μολυσμένη μονάδα δίσκου στον υπολογιστή. Μερικές φορές οι εισβολείς θα αφήσουν σκόπιμα μολυσμένες συσκευές USB σε δημοφιλείς τοποθεσίες με την ελπίδα ότι κάποιος θα τις βρει και θα τις συνδέσει στον υπολογιστή του. Επίσης, συχνά σε δημόσιες υπηρεσίες εργαζόμενοι παραλαμβάνουν φορητά μέσα αποθήκευσης όπως USB stick προκειμένου να εξυπηρετήσουν πολίτες και να παραλάβουν ή να εκτυπώσουν κάποιο έγγραφο.
3. **Εγκατάσταση μαζί με άλλο λογισμικό**
   Ορισμένα προγράμματα λογισμικού κακόβουλης λειτουργίας μπορούν να εγκατασταθούν ταυτόχρονα με άλλα προγράμματα. Αυτό περιλαμβάνει λογισμικό από τοποθεσίες web τρίτων ή αρχεία που κοινοποιούνται μέσω ομότιμων δικτύων. Επιπρόσθετα, ιστότοποι οι οποίοι προσφέρουν παράνομες υπηρεσίες όπως συνδρομητικά κανάλια, ταινίες ή και βιβλία μπορεί να κρύβουν το κίνδυνο εγκατάστασης κακόβουλου λογισμικού, κατεβάζοντας ένα αρχείο ή κάνοντας «κλικ» σε μια περιοχή της σελίδας με κρυμμένες λειτουργίες (πλήκτρο “play”).

4. **Ιστοσελίδες που έχουν δεχτεί επίθεση ή έχουν παραβιαστεί**

   Το λογισμικό κακόβουλης λειτουργίας μπορεί να χρησιμοποιήσει γνωστές ευπάθειες λογισμικού για να μολύνει έναν υπολογιστή. Η τοποθεσία web μπορεί να είναι κακόβουλη ή μπορεί να είναι μια γνήσια τοποθεσία web που έχει παραβιαστεί ή έχει δεχτεί επίθεση, θέτοντας έτσι σε κίνδυνο τον επισκέπτη.

5. **Άλλο λογισμικό κακόβουλης λειτουργίας.**

   Ορισμένοι τύποι λογισμικού κακόβουλης λειτουργίας μπορούν να κατεβάσουν άλλες απειλές στον υπολογιστή σας. Όταν αυτές οι απειλές εγκατασταθούν στον υπολογιστή, θα συνεχίσουν να κατεβάζουν περισσότερες απειλές.

Είδη κακόβουλου λογισμικού

Σύμφωνα με τη Europol και τον ENISA (European Union Agency for Cybersecurity) υπάρχουν τα εξής δέκα πιο βασικά είδη κακόβουλου λογισμικού:

1. **Virus**

   Ο ιός είναι ένας τύπος κακόβουλου λογισμικού που συνδέεται με ένα πρόγραμμα, αρχείο ή έγγραφο που του επιτρέπει να εξαπλωθεί από τον έναν υπολογιστή στον άλλο. Αυτοί οι ιοί μπορούν να μεταδοθούν με πολλούς διαφορετικούς τρόπους. Είναι σημαντικό να σημειωθεί ότι ένας ιός απαιτεί ανθρώπινη δράση (όπως η εκτέλεση ενός μολυσμένου προγράμματος) για να διαδοθεί.

2. **Worm**

   Ένα σκουλήκι είναι παρόμοιο με έναν ιό και μερικές φορές θεωρείται υποκατηγορία ενός ιού. Ακριβώς όπως ένας ιός, ένα σκουλήκι εξαπλώνεται από υπολογιστή σε υπολογιστή. Ωστόσο, αυτό που διακρίνει κυρίως ένα σκουλήκι από έναν ιό είναι ότι ένα σκουλήκι έχει την ικανότητα να εξαπλώνεται χωρίς ανθρώπινη δράση. Ένα worm συνήθως εκμεταλλεύεται αδυναμίες, όπως ευπάθειες του λειτουργικού συστήματος ή αδύναμους κωδικούς πρόσβασης, προκειμένου να εξαπλωθεί σε δίκτυα υπολογιστών.

3. **Spyware**

   Το Spyware είναι ένα είδος κακόβουλου λογισμικού που κατασκοπεύει τις δραστηριότητες ενός χρήστη χωρίς τη γνώση ή τη συγκατάθεσή του. Αυτές οι κατασκοπευτικές δραστηριότητες μπορεί να περιλαμβάνουν την καταγραφή πληκτρολογιου, παρακολούθηση δραστηριότητας και συλλογή δεδομένων, καθώς και άλλες μορφές κλοπής δεδομένων. Το λογισμικό υποκλοπής spyware διαδίδεται συνήθως ως Trojan ή με την εκμετάλλευση ευπαθειών του λογισμικού.

4. **Trojan**

   Ο Δούρειος Ίππος (Trojan Horse) είναι ένας τύπος κακόβουλου λογισμικού που μεταμφιέζεται ως νόμιμο λογισμικό προκειμένου να πείσει ένα θύμα να το εγκαταστήσει. Μόλις εγκατασταθεί, το κακόβουλο λογισμικό μπορεί να εκτελέσει την κακόβουλη δραστηριότητά του στο παρασκήνιο.

5. **Ransomware**

   Το Ransomware εμποδίζει τους χρήστες να έχουν πρόσβαση στις συσκευές τους και τους απαιτεί να πληρώσουν λύτρα μέσω ορισμένων τρόπων ηλεκτρονικής πληρωμής για να ανακτήσουν την πρόσβαση

6. **Rootkits**

   Το rootkit είναι ένα σύνολο κακόβουλων εφαρμογών που επιτρέπουν πρόσβαση σε επίπεδο διαχειριστή σε έναν υπολογιστή ή ένα δίκτυο υπολογιστών, επιτρέποντας έτσι στον εισβολέα να αποκτήσει πρόσβαση σε κρίσιμες λειτουργίες του συστήματος ή και σε άλλα μηχανήματα στο ίδιο δίκτυο. Τα Rootkits μπορούν να μολύνουν έναν υπολογιστή και να τον κάνουν μέρος ενός botnet.

7. **Adware**

   Το Adware εμφανίζει διαφημιστικά banner ή αναδυόμενα παράθυρα που περιλαμβάνουν κώδικα για την παρακολούθηση της συμπεριφοράς του χρήστη στο διαδίκτυο.

8. **Botnet**

   Ένα botnet (συντομογραφία ro**bot net**work) αποτελείται από υπολογιστές που επικοινωνούν μεταξύ τους μέσω του Διαδικτύου. Ένα κέντρο εντολών και ελέγχου τα χρησιμοποιεί για την αποστολή ανεπιθύμητων μηνυμάτων, την προσάρτηση κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) και τη διάπραξη άλλων εγκλημάτων.

9. **Backdoor/remote-access trojan (RAT)**

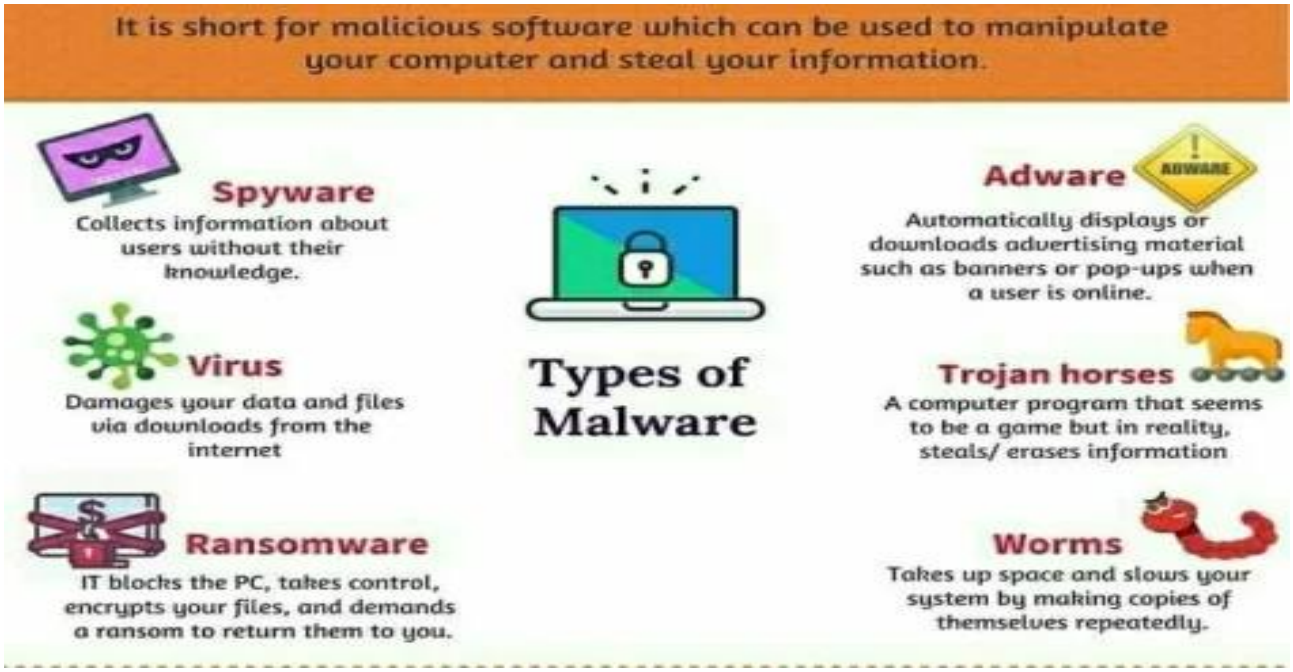
   Remote access trojans (δούρειοι ίπποι απομακρυσμένης πρόσβασης - RATs), είναι κακόβουλα λογισμικά Trojan που δίνουν στον εισβολέα απομακρυσμένο έλεγχο στον μολυσμένο υπολογιστή. Μόλις εγκατασταθεί το RAT στον υπολογιστή μπορεί να ελέγξει τη συσκευή του θύματος από απόσταση, αφού του επιτρέπει να εγκαταστήσει keyloggers, να ενεργοποιήσει την κάμερα και το μικρόφωνο να ενεργοποιήσει ένα botnet και πολλά άλλα.

10. **Mobile Malware**

    Κακόβουλο λογισμικό που στοχεύει κινητές συσκευές.

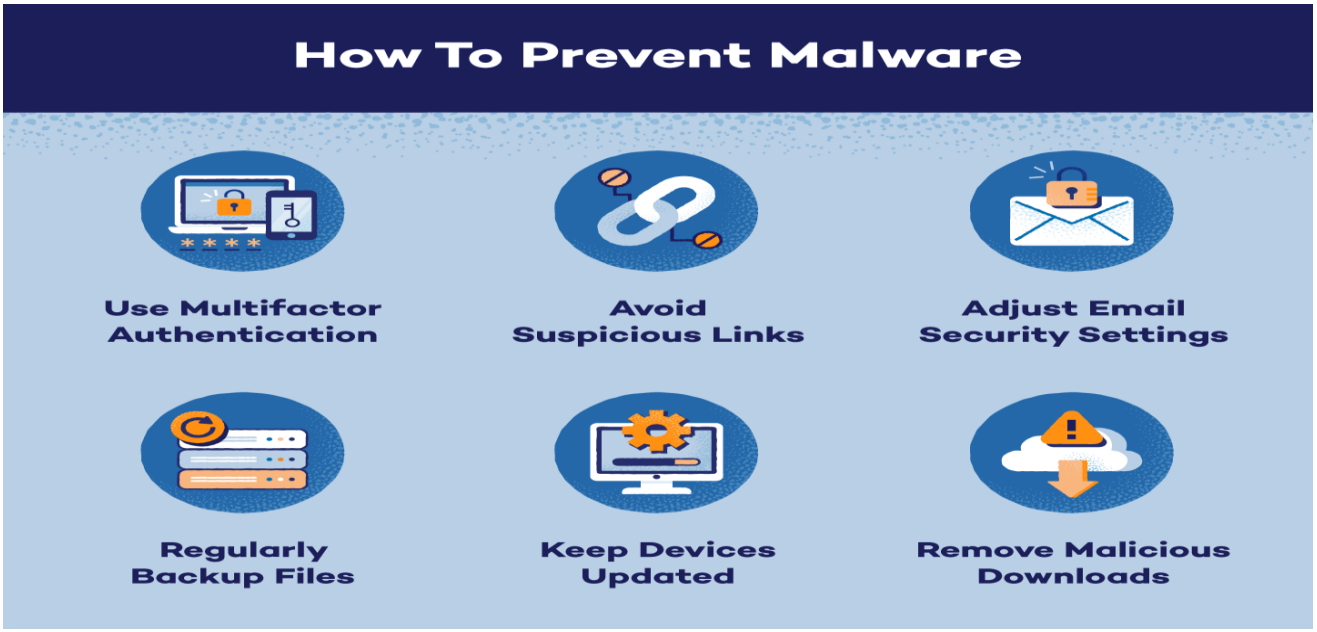
(https://www.europol.europa.eu/crime-areas/cybercrime/high-tech-crime)

(https://www.enisa.europa.eu/topics/incident-response/glossary/malware)



Εικόνα 1 types of malware

(Πηγή εικόνας 1: https://sameer9247.wordpress.com/2017/12/28/types-of-malware/)



Εικόνα 2 How to prevent malware

(Πηγή εικόνας 2: https://www.pandasecurity.com/en/mediacenter/types-of-malware/)

1.2.2 Ransomware

Καθώς το κακόβουλου λογισμικό της οικογενείας ¨Ransomware¨ θεωρείται εξέχουσα απειλή για την ασφάλεια των πληροφοριακών συστημάτων (Alenezi M., et al 2020) δημοσίων οργανισμών και επιχειρήσεων και επειδή οι επιπτώσεις του είναι μέχρι σήμερα δύσκολα αναστρέψιμες, με ανυπολόγιστες συνέπειες, θεωρείται σκόπιμη η αναφορά σε αυτό με περισσότερη λεπτομέρεια σε ξεχωριστή ενότητα.

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού (όπως Ιοί, Trojans, κ.λπ.) που μολύνει τα συστήματα υπολογιστών των χρηστών και χειρίζεται το μολυσμένο σύστημα με τρόπο που το θύμα δεν μπορεί (εν μέρει ή πλήρως) να χρησιμοποιήσει τα δεδομένα που είναι αποθηκευμένα σε αυτό (www.enisa.europa.eu). Έπειτα, ο μολυσμένος υπολογιστής λαμβάνει ένα εκβιαστικό μήνυμα κειμένου σε αναδυόμενο παράθυρο, πιέζοντας το θύμα να πληρώσει λύτρα (ransom - εξ ου και το όνομα) για να αποκτήσει ξανά πλήρη πρόσβαση στο σύστημα και τα αρχεία του. Το ransomware φθάνει σε υπολογιστές και συσκευές με διάφορους τρόπους, συμπεριλαμβανομένων ανεπιθύμητων μηνυμάτων (με κακόβουλα συνημμένα αρχεία ή ενσωματωμένους συνδέσμους), παραβιασμένους ή ειδικά κατασκευασμένους κακόβουλους ιστότοπους ή ιστοσελίδες και κιτ εκμετάλλευσης. Υπάρχουν δύο κύριες κατηγορίες σύγχρονων ransomware: lockers και crypto-ransomware (Yilmaz, Y., et al, 2021).

Η συμπεριφορά του ransomware έχει αλλάξει δραματικά τα τελευταία χρόνια. (Teichmann, F., et al 2023). Το 2015, παρατηρήθηκε μια αλλαγή όσο αφορά τους στόχους επιλογής – πλέον στοχοποιούνται επιχειρήσεις και οργανισμοί αντί για άτομα. Αυτό έγινε εμφανές έπειτα από πολλές αναφορές μεγάλων εταιρειών που υπέκυψαν στην απειλή (https://documents.trendmicro.com). Επίσης, εκτός από το μολύνει υπολογιστές και κινητές συσκευές, το ransomware μολύνει επίσης κοινόχρηστες και αφαιρούμενες μονάδες δίσκου και διακομιστές. Ορισμένα λογισμικά της οικογενείας ransomware, έχουν επίσης αναλάβει την κρυπτογράφηση επιλεγμένων τύπων αρχείων, όπως αρχεία που σχετίζονται με τη φορολογία και αρχεία βάσεων δεδομένων, εξασφαλίζοντας μεγαλύτερα κέρδη για τους χειριστές του κακόβουλου λογισμικού (Razaulla, S. et al., 2023).

Μερικοί από τους πιο συνηθισμένους τρόπους με τους οποίους είναι δυνατή η μόλυνση από ransomware είναι οι εξής (UpGuard, Kely C, 2023):

- Μηνύματα ηλεκτρονικού ψαρέματος (phishing).
- Επίσκεψη επισφαλών ισοτόπων (drive-by downloading)

• Λήψη μολυσμένων επεκτάσεων αρχείων ή κακόβουλων συνημμένων
• Ευπάθειες συστήματος και δικτύου
• Απομακρυσμένη πρόσβαση (Remote desktop protocol (RDP) attacks)

Η λειτουργία επιχειρήσεων και οργανισμών πλέον εξαρτάται απόλυτα από την εύρυθμη λειτουργία των πληροφοριακών συστημάτων τους, μέσω των οποίων επιτελείται το σύνολο των λειτουργιών, κατά συνέπεια οι συνέπειες από μία πιθανή μόλυνση μπορούν μόνο να επιγραμματικά να αναφερθούν, καθώς η ζημία μπορεί να είναι καταστροφική (Lang et al., 2023), (Mohanty, et al., 2023)

- Προσωρινή ή μόνιμη απώλεια ευαίσθητων πληροφοριών
- Διακοπή της επιχειρησιακής λειτουργίας του οργανισμού
- Οικονομικές ζημίες που προκλήθηκαν για την αποκατάσταση συστημάτων και αρχείων
- Βλάβη στη φήμη ενός οργανισμού.
- Επιπτώσεις στην υγεία του πληθυσμού από κυβερνοεπιθέσεις που στοχεύουν νοσοκομεία και μονάδες υγείας και αποκαλούνται «threat-to-life crimes» (Van Boven, et al., 2023)

Σύμφωνα με μια μελέτη (Van Boven et al., 2023) για τις επιπτώσεις του ransomware στα νοσοκομεία, διαπιστώθηκε η ανάγκη να αναπτυχθούν τρία βασικά σημεία πρόληψης (α) βελτίωση της επικοινωνίας (cyber-event planning and emergency management planning), (β) βελτίωση της ασφάλειας των πληροφοριακών συστημάτων (ρύθμιση πιο ασφαλών διαδικασιών σύνδεσης, εφαρμογή εκτεταμένων περιορισμών στην απομακρυσμένη πρόσβαση στο σύστημα, κρυπτογράφηση διαβαθμισμένων πληροφορίων) και (γ) βελτίωση σχεδίων έκτακτης ανάγκης.

Μια πιθανή εξήγηση για το υψηλό ποσοστό θυματοποίησης ransomware μεταξύ των επιχειρηματιών είναι η έλλειψη δράσεων με σκοπό την προληπτική προστασία. Τα μέτρα ασφαλείας, όπως τείχη προστασίας, μπορούν να εφαρμοστούν για την αντιμετώπιση απειλών στον κυβερνοχώρο και μπορούν να εφαρμοστούν πρακτικές ασφαλείας, όπως ο εντοπισμός και η έγκαιρη προειδοποίηση για ύποπτη δραστηριότητα, η ελεγχόμενη πρόσβαση και η τήρηση αντίγραφων ασφαλείας (Bekkers, et al., 2023).

Ωστόσο, παρά το γεγονός ότι οι επιθέσεις ransomware αυξάνονται ραγδαία κατά επιχειρήσεων, μια έρευνα (Wilson et al., 2022) έδειξε ότι οι επιχειρηματίες γενικά δεν αντιλαμβάνονται το μέγεθος του κίνδυνου οι επιχειρήσεις τους να πέσουν θύματα επιθέσεων ransomware, επομένως χρειάζεται περισσότερη ενημέρωση σχετικά και ευαισθητοποίηση των εμπλεκομένων μερών.

Υπάρχουν μέτρα πρόληψης και προστασίας ώστε να αποφευχθεί η μόλυνση από ransomware. Παράλληλα, δεδομένου του δυναμικού και συνεχώς εξελισσόμενου τεχνολογικού περιβάλλοντος, είναι σημαντικό οι υπεύθυνοι ασφαλείας να είναι σε εγρήγορση και να τηρούνται σε όλο τον οργανισμό θεμελιώδεις διαδικασίες ασφάλειας στον κυβερνοχώρο για να διασφαλιστεί σε μεγάλο ποσοστό η ομαλή λειτουργία. Ωστόσο, κάθε οργανισμός θα πρέπει να προσαρμόσει τη στρατηγική ασφαλείας του στις δικές του ανάγκες και να υιοθετήσει μέτρα που ταιριάζουν στις απαιτήσεις του. Θα πρέπει επίσης να τονιστεί ότι καθώς το περιβάλλον στο κυβερνοχώρο είναι εξαιρετικά ασταθές, κάθε διαδικασία αξιολογείται συστηματικά και τροποποιείται ανάλογα.

Για το λόγο αυτό αναφέρονται ορισμένες γενικές αρχές οι οποίες θα προσαρμοστούν αναλόγως για την αποτελεσματικότερη και αποδοτικότερη λειτουργία των επιμέρους μέτρων ασφαλείας. (Erward K, 2023), (www.europol.europa.eu), (support.microsoft.com), (www.kaspersky.com)

- Συστηματική δημιουργία αντιγράφων ασφαλείας (Backup Data)
- Εγκατάσταση λογισμικού και τειχών προστασίας (Antivirus Software and Firewalls)
- Συνεχής Ενημέρωση και Διατήρηση ενημερωμένων όλων των συστημάτων και των λογισμικών (Systems And Software Updated)
- Τμηματοποίηση δικτύου (Network Segmentation - Επειδή το ransomware εξαπλώνεται γρήγορα σε ένα δίκτυο, σε περίπτωση επίθεσης, είναι σημαντικό να ελαχιστοποιηθεί η εξάπλωσή του)
- Ασφαλής διαχείριση email (οι επιθέσεις ηλεκτρονικού ψαρέματος είναι η κύρια αιτία μολύνσεων από κακόβουλο λογισμικό)
- Αυστηρός καθορισμός των εφαρμογών που μπορούν να εγκατασταθούν και να εκτελεστούν καθώς και των ιστοτόπων που μπορούν να λειτουργήσουν σε ένα δίκτυο.
- Περιορισμός των δικαιωμάτων πρόσβασης χρηστών (Limit User Access Privileges – και περιορισμός της πρόσβασης και των αδειών ενός χρήστη μόνο στα δεδομένα που χρειάζεται για να λειτουργήσει)
- Εκτέλεση δοκιμών ασφαλείας
- Εκπαίδευση και ευαισθητοποίηση όλων των εργαζομένων.

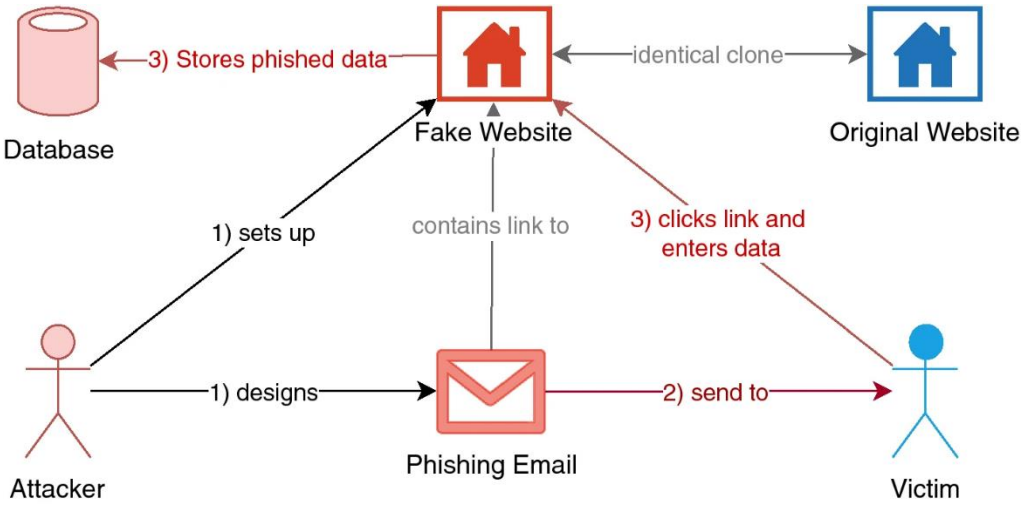
Αξίζει να αναφερθεί ότι μία από τις σοβαρότερες απειλές για την κυβερνοασφάλεια ενός οργανισμού αποτελεί το ανθρώπινο λάθος (Fusi et al., 2023). Πιστεύεται ότι το μεγαλύτερο ποσοστό των επιτυχημένων παραβιάσεων στον κυβερνοχώρο οφείλονται σε ανθρώπινο λάθος, υπογραμμίζοντας την ταχεία στροφή προς την εξ αποστάσεως εργασία τα τελευταία χρόνια ως έναν ιδιαίτερα σημαντικό παράγοντα. Για το λόγο αυτό, η εκπαίδευση του προσωπικού θα πρέπει να

αποτελεί αναπόσπαστο μέρος οποιασδήποτε πολιτικής ασφάλειας και θα πρέπει να δίνεται ιδιαίτερη σημασία και προσοχή στο παράγοντα αυτό.

1.2.3 Phishing

Ορισμός

Το Phishing, είναι ένας όρος που αναφέρεται στη κυβερνοεπίθεση κατά την οποία ο επιτιθέμενος υποδύεται μία αξιόπιστη οντότητα, με σκοπό την εξαπάτηση του θύματος και την αθέμιτη απόκτηση προσωπικών δεδομένων του, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί πρόσβασης (Bhuvana, A. Et al., 2021). Η ελληνική απόδοση του όρου είναι «Ηλεκτρονικό ψάρεμα». Η εικόνα (3) παρουσιάζει ένα παράδειγμα μιας επίθεσης ηλεκτρονικού ψαρέματος.



Εικόνα 3 Phishing email

(Πηγή Εικόνας 3: Jampen, D. et al., 2020). Don't click: towards an effective anti-phishing training.)

Ενώ το ηλεκτρονικό ψάρεμα μπορεί να εκδηλωθεί μέσω μηνυμάτων κειμένου, μέσων κοινωνικής δικτύωσης ή τηλεφωνικών κλήσεων, ο όρος «ψάρεμα» αναφέρεται κυρίως σε επιθέσεις μέσω email. Τα παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου έχουν την ικανότητα να προσεγγίζουν απευθείας εκατομμύρια χρήστες ταυτόχρονα και μπορούν εύκολα να συνδυαστούν με τον τεράστιο αριθμό νόμιμων email που λαμβάνουν συνεχώς οι χρήστες (www.ncsc.gov.uk.)

Τα μηνύματα ηλεκτρονικού ψαρέματος είναι το αρχικό βήμα επιθέσεων μεγάλης κλίμακας (π.χ. ransomware) και θα παραμείνουν μια σοβαρή απειλή που προσαρμόζεται συνεχώς (Bountakas and Xenakis, 2023) στις τρέχουσες ανάγκες (όπως με τον COVID-19, παροχή fuel pass κ.α.). Κατά συνέπεια, η συμπεριφορά των εργαζομένων στα μηνύματα ηλεκτρονικού ψαρέματος μπορεί να ενισχύσει ή να υπονομεύσει την ασφάλεια στον κυβερνοχώρο επιχειρήσεων και οργανισμών (Buckley et al., 2023).

Παρόλου που αρκετές τεχνικές, όπως και εργαλεία (e.g. anti-phishing algorithm) έχουν αποδειχθεί εξαιρετικά αποτελεσματικά στον εντοπισμό και πρόληψη επιθέσεων phishing (Sharma et

al., 2022), η πρόληψη του phishing στο χώρο εργασίας εξαρτάται σε μεγάλο βαθμό από τη συμπεριφορά των εργαζομένων, (Hillman et al., 2023). Ωστόσο, με βάση μία έρευνα (Tally et al., 2023) που διεξήχθη σε δύο πανεπιστήμια των ΗΠΑ, διαπιστώθηκε ότι λιγότερο από το 21% των συμμετεχόντων είχε επίσημη εκπαίδευση κατά του phishing. Πολλά από αυτά που γνωρίζουν οι συμμετέχοντες για το ηλεκτρονικό ψάρεμα προέρχονται από άτυπες πηγές που δίνουν έμφαση σε «συμβουλές» και «κόλπα», όπως σε συνομιλίες με φίλους, ειδήσεις, ενημερωτικά δελτία, μέσα κοινωνικής δικτύωσης και άλλα διαδικτυακά ανεπίσημα κανάλια.

Εντοπισμός και προστασία

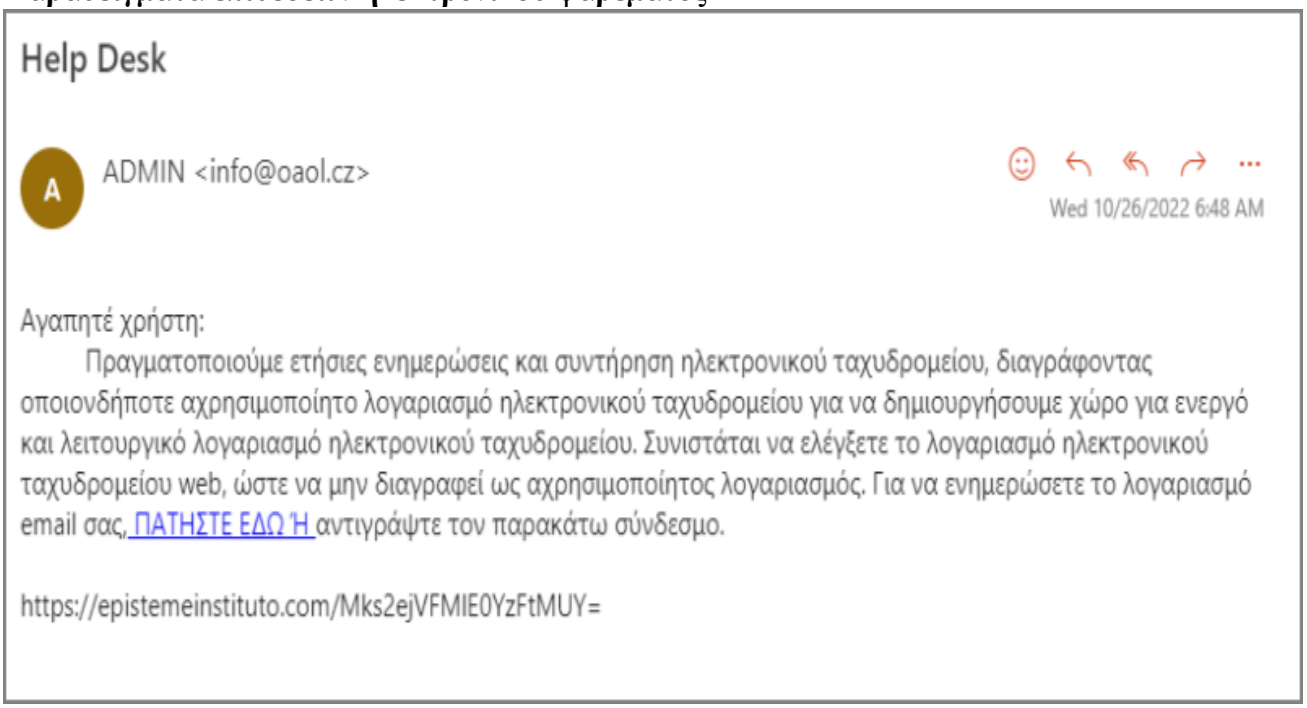
Υπάρχουν πολλά διαθέσιμα εργαλεία, τεχνικές και αλγόριθμοι εντοπισμού και αποκλεισμού επιθέσεων ηλεκτρονικού ψαρέματος, (Safi and Singh, 2023) αλλά δεν μπορούν να εντοπίσουν αποτελεσματικά νέες απάτες ηλεκτρονικού ψαρέματος (Salloum et al., 2021), όπως παρατηρούμε και στη καθημερινότητα, οι επιθέσεις είναι συνεχείς τόσο σε προσωπικούς όσο και σε επαγγελματικούς λογαριασμούς και οι μέθοδοι προσαρμόζονται ταχέως και εναλλάσσονται. Ωστόσο, οι επιθέσεις ηλεκτρονικού ψαρέματος δεν μπορούν να ελεγχθούν μόνο από τεχνικά μέσα και είναι επιτακτική ανάγκη τα προγράμματα κυβερνοασφάλειας να περιλαμβάνουν προγράμματα εκπαίδευσης και ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο για την επιτυχή καταπολέμηση των επιθέσεων (Back and Guerette, 2021; Naqvi et al., 2023).

Στη συνέχεια και κατόπιν επισκόπησης σχετικής βιβλιογραφίας, παρατίθενται ορισμένες συμβουλές με σκοπό τον εντοπισμό επιθέσεων ηλεκτρονικού ψαρέματος. (Tally et al., 2023; Young and Farshadkhah, 2023; Davidson, 2022; Carroll et al., 2022) (Microsoft: support.microsoft.com), (Υπουργείο Ψηφιακής Διακυβέρνησης, 2023: https://mindigital.gr)

- Πίεση χρόνου, μηνύματα που απαιτούν επείγουσα δράση. Τα μηνύματα ηλεκτρονικού ψαρέματος συνήθως απειλούν με συνέπειες ή την απώλεια μιας ευκαιρίας εάν δεν προβεί ο αποδέκτης σε άμεση ενέργεια. Αυτή η τακτική χρησιμοποιείται συχνά από τους εισβολείς για να αναγκάσουν τους παραλήπτες να απαντήσουν γρήγορα προτού έχουν την ευκαιρία να ελέγξουν το email για τυχόν σφάλματα ή ασυνέπειες.
- Μηνύματα κειμένου με γραμματικά και ορθογραφικά λάθη. Τα ορθογραφικά και γραμματικά λάθη στα μηνύματα ηλεκτρονικού ταχυδρομείου είναι ένας άλλος δείκτης των μηνυμάτων ηλεκτρονικού ψαρέματος. Επιχειρήσεις και οργανισμοί χρησιμοποιούν λογισμικό ορθογραφικού ελέγχου από προεπιλογή στα email που στέλνουν για να βεβαιωθούν ότι η γραμματική είναι σωστή.

- Email με έναν άγνωστο χαιρετισμό. Οι συνάδελφοι συνήθως ξεκινούν τα email τους με έναν άτυπο χαιρετισμό. Κάποιος θα πρέπει να είναι καχύποπτος με εκείνα που ξεκινούν με "Αγαπητέ" ή περιέχουν λέξεις που δεν χρησιμοποιούνται γενικά σε περιστασιακές συνομιλίες.
- Ασυμφωνία σε διευθύνσεις email, συνδέσμους και ονόματα τομέα. Μια άλλη μέθοδος αναγνώρισης του phishing είναι μέσω της αναζήτησης αποκλίσεων στα ονόματα τομέα, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου και τους συνδέσμους. Για παράδειγμα σύγκριση της διεύθυνση του αποστολέα με άλλα email που λάβατε από τον ίδιο.
- Ύποπτα Συνημμένα. Τα μηνύματα ηλεκτρονικού ταχυδρομείου με συνημμένα πρέπει πάντα να αντιμετωπίζονται με ύποπτο τρόπο – ειδικά εάν έχουν μια άγνωστη επέκταση ή κάποια συνήθως σχετίζεται με κακόβουλο λογισμικό (.zip, .exe, .scr, κ.λπ.), είναι μη αναμενόμενα ή δεν αναγνωρίζετε τον αποστολέα.
- Email που ζητούν διαπιστευτήρια σύνδεσης ή κρίσιμες πληροφορίες. Τα μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από έναν απροσδόκητο ή άγνωστο αποστολέα που ζητά διαπιστευτήρια σύνδεσης, πληροφορίες πληρωμής ή άλλα ευαίσθητα δεδομένα θα πρέπει πάντα να αντιμετωπίζονται ως ύποπτα. Είναι δυνατόν να δημιουργηθούν εικονικοί ιστότοποι σύνδεσης που μοιάζουν με το πραγματικό και να αποστέλλονται μηνύματα ηλεκτρονικού ταχυδρομείου με συνδέσμους που οδηγούν τους παραλήπτες στο ψεύτικο δικτυακό τόπο.
- Τα «πολύ καλά για να είναι αληθινά» μηνύματα ηλεκτρονικού ταχυδρομείου είναι αυτά που δίνουν κίνητρο στον παραλήπτη να κάνει κλικ σε έναν σύνδεσμο ή να ανοίξει ένα συνημμένο, υποστηρίζοντας ότι θα υπάρξει κάποια ανταμοιβή. Εάν ο αποστολέας του μηνύματος ηλεκτρονικού ταχυδρομείου δεν είναι γνωστός ή ο παραλήπτης δεν ξεκίνησε τη συνομιλία, το πιθανότερο είναι ότι πρόκειται για μήνυμα ηλεκτρονικού "ψαρέματος" (phishing).

Παραδείγματα επιθέσεων ηλεκτρονικού ψαρέματος


Help Desk

A ADMIN <info@oaol.cz>

Wed 10/26/2022 6:48 AM

Αγαπητέ χρήστη:

Πραγματοποιούμε ετήσιες ενημερώσεις και συντήρηση ηλεκτρονικού ταχυδρομείου, διαγράφοντας οποιονδήποτε αχρησιμοποίητο λογαριασμό ηλεκτρονικού ταχυδρομείου για να δημιουργήσουμε χώρο για ενεργό και λειτουργικό λογαριασμό ηλεκτρονικού ταχυδρομείου. Συνιστάται να ελέγξετε το λογαριασμό ηλεκτρονικού ταχυδρομείου web, ώστε να μην διαγραφεί ως αχρησιμοποίητος λογαριασμός. Για να ενημερώσετε το λογαριασμό email σας, ΠΑΤΗΣΤΕ ΕΔΩ Ή αντιγράψτε τον παρακάτω σύνδεσμο.

https://epistemeinstituto.com/Mks2ejVFMIE0YzFtMUY=

Εικόνα 4 Παράδειγμα επιθέσεων ηλεκτρονικού ψαρέματος 1

Πηγή Εικόνας 4: https://wiki.noc.uniwa.gr/doku.php?id=spamdetectionadvices)


Είστε κατάλληλοι για επιστ

ΑΑΔΕ
Ανεξάρτητη Αρχή Δημοσίων Εγκλημάτων

Η φορολογική σας δήλωση έχει υπολογιστεί από την Ελληνική Δ.Ο.Υ.

Είστε κατάλληλοι για επιστροφή φόρου 634,13 €.

Δυστυχώς, δεν μπορέσαμε να επαληθεύσουμε τον τρέχοντα αριθμό λογαριασμού σας όταν προσπαθήσαμε να μεταφέρουμε τα χρήματα στον λογαριασμό σας.

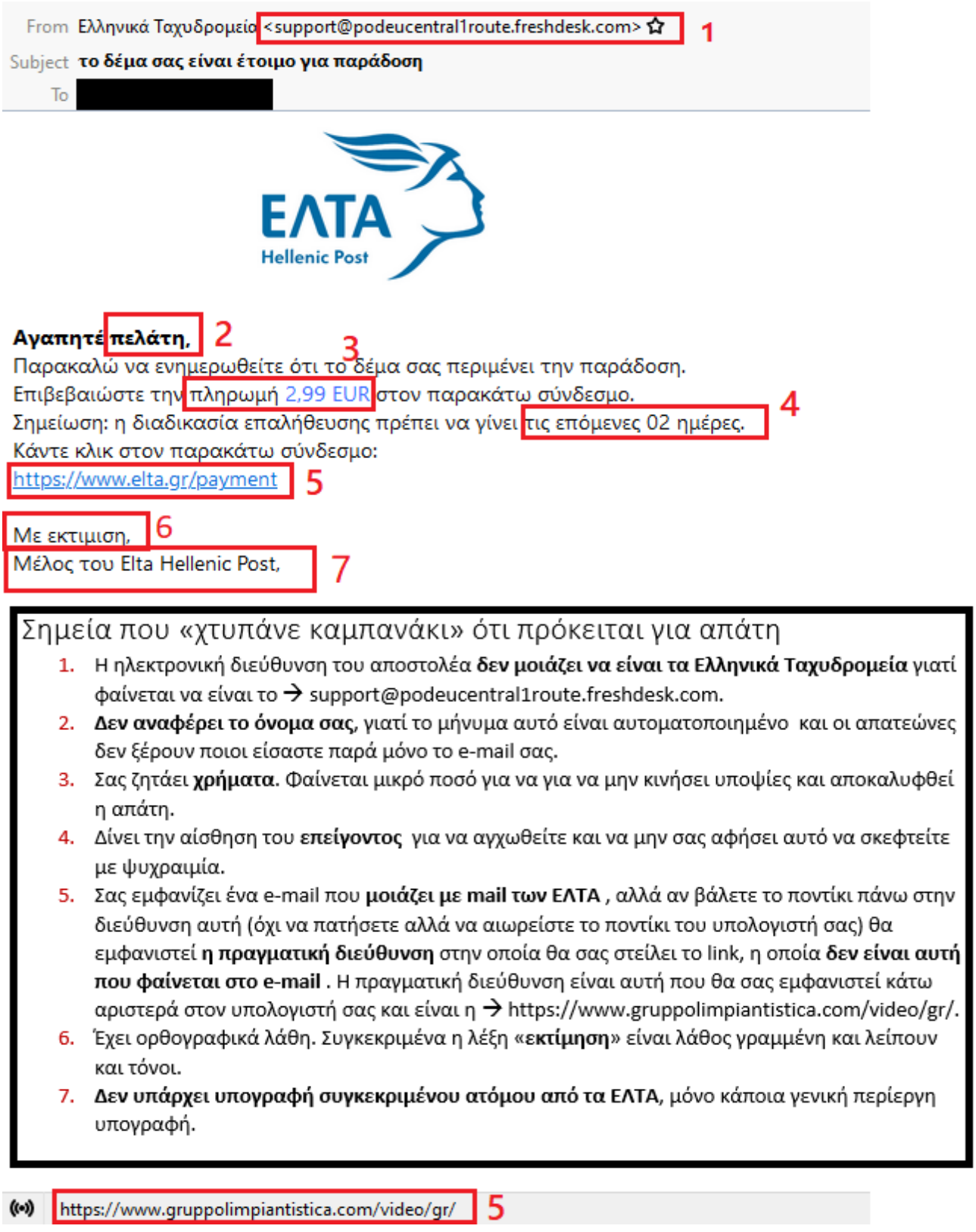
Επαληθεύστε τα στοιχεία σας

Με εκτίμηση,

Αρχή Ανεξάρτητων Δημοσίων Εσόδων (ΑΑΔΕ)

Εικόνα 5Παράδειγμα επιθέσεων ηλεκτρονικού ψαρέματος 2

Πηγή Εικόνας 5: https://xristika.gr/ektakti-eidisi-an-lavete-ayto-to-minym/)



Εικόνα 6 Παράδειγμα επιθέσεων ηλεκτρονικού ψαρέματος 3

(Πηγή Εικόνας 6: https://www.aftodioikisi.gr/koinonia/prosochi-xafrizoyn-chrimata-meso-fake-mail-elta-trapezon-eikones/)

1.3 Αναφορά του εγκλήματος στο κυβερνοχώρο

Στις μέρες μας, τα Πληροφοριακά Συστήματα (ΠΣ) και το διαδίκτυο χρησιμοποιούνται ευρέως και έχουν καλύψει κάθε πτυχή της ζωής μας. Τεράστιος όγκος δεδομένων διακινείται μέσω κινητών συσκευών, ηλεκτρονικών υπολογιστών και το Διαδίκτυο των Πραγμάτων (IoT), το οποίο συνεχίζει να αναπτύσσεται. Για το λόγο αυτό, δημόσιοι και ιδιωτικοί οργανισμοί, εταιρείες και οι άνθρωποι σε όλο τον κόσμο δίνουν μεγαλύτερη έμφαση στον τρόπο αποθήκευσης, επεξεργασίας και προστασίας των δεδομένων. Ωστόσο, πρόσφατες έρευνες έχουν δείξει ότι ένα μεγάλο ποσοστό του εγκλήματος στον κυβερνοχώρο δεν αναφέρεται ούτε εσωτερικά εντός του οργανισμού, σε αρμόδιους για το λόγο αυτό υπαλλήλους ούτε στις Αρχές.

Η αναφορά των περιστατικών είναι πολύ σημαντική προκειμένου να σχεδιαστούν αποτελεσματικές στρατηγικές πρόληψης και αντιμετώπισης του εγκλήματος στον κυβερνοχώρο (van de Weijer et al., 2019; Kemp, 2020; Kemp et al., 2020). Στην πραγματικότητα, το έγκλημα στον κυβερνοχώρο είναι μεταξύ των λιγότερο αναφερόμενων τύπων εγκλήματος (van de Weijer et al., 2019). Για παράδειγμα, τα θύματα στην Ολλανδία, αναφέρουν τα εγκλήματα στον κυβερνοχώρο στην αστυνομία λιγότερο συχνά από τα θύματα των περισσότερων τύπων παραδοσιακών εγκλημάτων (van de Weijer et al., 2019). Επίσης, στην Πορτογαλία, το 86,6% των θυμάτων δεν ανέφεραν στην αστυνομία κάποιο διαδικτυακό συμβάν απάτης (Fonseca et al., 2022). Ομοίως, στην Ισπανία, τα περισσότερα άτομα δεν αναφέρουν απάτες στον κυβερνοχώρο στην αστυνομία, ειδικά εκείνες που σχετίζονται με τραπεζικές απάτες (π.χ. απάτες με πιστωτικές κάρτες) (Kemp, et al. 2020). Σε γενική ομολογία τα θύματα του εγκλήματος στον κυβερνοχώρο είναι λιγότερο πιθανό από εκείνα του παραδοσιακού εγκλήματος να αναφέρουν το περιστατικό στην αστυνομία ή άλλες αρχές (Curtis and Oxburgh, 2022).

Στη βιβλιογραφία υπάρχει πλήθος ερευνών που εντοπίζει το υπάρχον κενό στην αναφορά εγκλημάτων στον κυβερνοχώρο. Σύμφωνα με τον Bidgoli (2021) τα εγκλήματα στον κυβερνοχώρο έχουν ιστορικό μη καταγγελίας από τα θύματα. Όπως υποστηρίζουν οι Tcherni et al., (2015), ένα πολύ μικρότερο ποσοστό θυμάτων του εγκλήματος στον κυβερνοχώρο αναφέρει το συμβάν σε σύγκριση με τα θύματα βίαιων εγκλημάτων και το πραγματικό χάσμα στην αναφορά μπορεί να είναι ακόμη μεγαλύτερο. Σύμφωνα με αυτό, ο Cross (2020) αναγνώρισε τη διαδικτυακή απάτη ως το έγκλημα με ένα από τα χαμηλότερα ποσοστά αναφοράς σε όλους τους τύπους εγκλημάτων. Περαιτέρω, οι Kwak et al. (2020) παρουσίασαν στοιχεία ότι οι χρήστες σπάνια αναφέρουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου και η τάση αυτή είναι επίσης ορατή σε άλλους τύπους εγκλημάτων στον κυβερνοχώρο. Οι Tcherni et al. (2015) διαπίστωσαν ότι το έγκλημα στον κυβερνοχώρο επηρεάζει ένα σημαντικό και

αυξανόμενο ποσοστό νοικοκυριών ετησίως, αλλά τα ποσοστά αναφοράς στην αστυνομία είναι χαμηλά. Δηλώνουν επίσης ότι τα εγκλήματα στον κυβερνοχώρο είναι πιθανό να αυξάνονται και ότι η έκταση του προβλήματος μπορεί να υποτιμάται. Τέλος, η έλλειψη αναφοράς εγκλημάτων στον κυβερνοχώρο στην αστυνομία από θύματα κυβερνοεγκλήματος είναι επίσης, ένα από τα ευρήματα μιας μελέτης στο Ηνωμένο Βασίλειο (Kemp et al., 2023). Τα αποτελέσματα υποδεικνύουν ότι ο τύπος του εγκλήματος στον κυβερνοχώρο σχετίζεται με την απόφαση αναφοράς και ότι η πιθανότητα αναφοράς αυξάνεται όταν τα περιστατικά στον κυβερνοχώρο έχουν αρνητικές επιπτώσεις και όταν η εταιρεία δίνει υψηλή προτεραιότητα στην ασφάλεια στον κυβερνοχώρο.

Ένας καθοριστικός παράγοντας για την αναφορά του εγκλήματος ή όχι είναι το πόσο σοβαρό είναι το αδίκημα. Πιο σοβαρά αδικήματα - περιστατικά εγκλήματος στον κυβερνοχώρο αναφέρονται συχνότερα από άτομα και οργανισμούς στην αστυνομία ή εσωτερικά στον οργανισμό. Επίσης, αναφέρονται λιγότερο συχνά αδικήματα, σε καταστάσεις όπου το θύμα γνωρίζει προσωπικά τον δράστη (Van de Weijer et al., 2020). Ένα άλλο σημαντικό εύρημα που εντοπίζεται στη βιβλιογραφία είναι ότι η αναφορά δεν γίνεται σωστά, ειδικά σε περιπτώσεις όπου τα θύματα είναι ηλικίας 60 ετών και άνω (Karagiannopoulos et al., 2021).

Η έκθεση «ENISA Threat Landscape for Ransomware Attacks» σημειώνει ότι η αναφορά επιθέσεων ransomware γίνεται σπάνια από τους οργανισμούς ή δεν περιλαμβάνει λεπτομέρειες σχετικά με (i) πώς συνέβη η επίθεση, (ii) τον τύπο του κακόβουλου λογισμικού, (iii) λύτρα που ζητήθηκαν και (iv) εάν τα λύτρα τελικά πληρώθηκαν (ENISA, 2022). Η ανεπαρκής αναφορά οδηγεί σε μειωμένη ανταλλαγή πληροφοριών και σε διδάγματα που αποκόμισε ο οργανισμός, καθιστώντας δύσκολο για τους ερευνητές ασφάλειας να εντοπίσουν τους παράγοντες της επίθεσης, να κατανοήσουν τις τακτικές τους και να ανταποκριθούν σε τέτοιες επιθέσεις (ENISA 2022). Επιπρόσθετα, έρευνες έχουν δείξει ότι οι εταιρείες, που δεν λαμβάνουν σοβαρά υπόψη την κυβερνοασφάλειά τους, πιθανότατα δεν αναφέρουν περιστατικά στην αστυνομία (Kemp et al., 2021) και ακόμη κι αν το κάνουν, περιστασιακά, αναφέρουν εγκλήματα στον κυβερνοχώρο που έχουν πολύ υψηλό αρνητικό αντίκτυπο.

Η πρόθεση αναφοράς είναι γενικά ελαφρώς υψηλότερη για περιστατικά που συνέβησαν στον φυσικό κόσμο, σε αντίθεση με το διαδικτυακό. Αυτό συνδέεται και με το γεγονός ότι η πεποίθηση ότι η αστυνομία μπορεί να εντοπίσει και να συλλάβει τον δράστη είναι χαμηλότερη για το έγκλημα στον κυβερνοχώρο σε σύγκριση με το παραδοσιακό έγκλημα (Graham et al., 2019). Ένας άλλος εξίσου σημαντικός παράγοντας που επηρεάζει δυσμενώς τη πρόθεση αναφοράς είναι ο φόβος των εταιρειών και των οργανισμών μήπως χάσουν την εμπιστοσύνη των πολιτών-πελατών τους, αποκτήσουν αρνητική δημοσιότητα, και ανταγωνιστικό μειονέκτημα και αγωγές είναι βασικά κριτήρια που θα αξιολογηθούν για τη λήψη της σχετικής απόφασης (Czekster et al., 2022). Επιπρόσθετα, από έρευνα

της εταιρείας «Kaspersky 2017» προέκυψε ότι πολλοί εργαζόμενοι κρύβουν κρίσιμα περιστατικά ασφάλειας πληροφορικής υπό το φόβο των συνεπειών οι οποίες σε πολλές περιπτώσεις οδηγούν σε απόλυση.

Είναι σημαντικό να αναφερθεί ότι η ελλιπείς γνώσεις σχετικά με τη διαδικτυακή ασφάλεια καθώς και η γνώση του τρόπου αναφοράς ενός εγκλήματος στο κυβερνοχώρο επηρεάζει σημαντικά τη πρόθεση αναφοράς αλλά και το αποτέλεσμα αυτής (Bidgoli et all., 2019). Τα θύματα δεν καταλαβαίνουν πάντα ότι έχουν πέσει πραγματικά θύματα διαδικτυακής απάτης (Button and Cross 2017; Kemp et al. 2020) ή μπερδεύονται σχετικά με το ποιος είναι ο καταλληλότερος φορέας για να αναφέρουν την περίπτωσή τους (Button and Cross 2017; Van de Weijer et al. 2019; Bossler et al. 2020; Karagiannopoulos et al., 2021).

Τέλος, για πολλούς οργανισμούς, η συμμετοχή των αρχών επιβολής του νόμου δεν αποτελεί προτεραιότητα, επειδή το ενδιαφέρον έγκειται στη συνέχεια και την ανάκαμψη των επιχειρησιακών λειτουργιών. Ο οργανισμός ενδιαφέρεται περισσότερο για την επαναφορά των δεδομένων και την λειτουργία των συστημάτων του, οπότε θα προτιμούσε να πληρώσει απλώς τα λύτρα σε μια επίθεση «Ransomware» και να τελειώσει. Η κλήση των αρχών επιβολής του νόμου θα μπορούσε ενδεχομένως να επιβραδύνει την επιστροφή στο φυσιολογικό (Fahmida Y.R, 2020). Οι εταιρείες πιστεύουν ότι μπορούν να επιλύσουν περιστατικά εγκλήματος στον κυβερνοχώρο εσωτερικά ή μέσω εξωτερικού συμβούλου και ότι η αστυνομία και το σύστημα ποινικής δικαιοσύνης δεν θα έδιναν αποτελεσματική λύση στο πρόβλημά τους (Kemp et al., 2021; van de Weijer et al., 2021).

1.4 Κυβερνοέγκλημα και Νομοθεσία

1.4.1 Το διαδίκτυο στον ελληνικό Ποινικό Κώδικα

Προκειμένου να διευθετηθούν τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα στο κυβερνοχώρο δημιουργήθηκε το κείμενο της «Σύμβασης για το Έγκλημα στον Κυβερνοχώρο», το οποίο υπογράφηκε στις 23 Νοεμβρίου 2001, στη Βουδαπέστη, από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου και από τις Ηνωμένες Πολιτείες, τον Καναδά, την Νότιο Αφρική και την Ιαπωνία. Η Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο κυρώθηκε και ενσωματώθηκε στην ελληνική νομοθεσία με τον Νόμο 4411/2016. Με τον ίδιο Νόμο ενσωματώθηκε και η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών που αντικατέστησε την απόφαση-πλαισίο 2005/222/ΔΕΥ του Συμβουλίου. (Σύμβαση για το έγκλημα στον Κυβερνοχώρο, Βουδαπέστη 23.11.2001, Ν.4411/2016)

Στη Σύμβαση προβλέπονται ιδιαίτερα εγκλήματα, όπως: (α) η παράνομη πρόσβαση σε δεδομένα (άρθρο 2), (β) η υποκλοπή διαβιβαζόμενων δεδομένων (άρθρο 3), (γ) η παρέμβαση (διαγραφή-αλλοίωση-βλάβη) σε δεδομένα (άρθρο 4), (δ) η παρέμβαση σε συστήματα υπολογιστών (άρθρο 5), (ε) η κακή χρήση συσκευών με σκοπό την τέλεση εγκλημάτων όπως τα προηγούμενα (άρθρο 6), (στ) η πλαστογραφία που σχετίζεται με Η/Υ (άρθρο 7), (ζ) η απάτη που σχετίζεται με Η/Υ (άρθρο 8), (η) η πορνογραφία ανηλίκων και συναφή εγκλήματα (άρθρο 9), (θ) παραβάσεις σχετικές με την πνευματική ιδιοκτησία (άρθρο 10).

Οι διατάξεις του Ποινικού μας Κώδικα που αποτελούν το ελληνικό ποινικό δίκαιο του διαδικτύου είναι οι: 292Α, 292Β, 292Γ, 292Δ, 292Ε, 370 παρ.2, 370Α, 370Β, 370Γ, 370Δ, 370Ε, 348^{A} παρ. 2, 386^{A} όπως ισχύουν σήμερα μετά το Νόμο 4619/2019 - ΦΕΚ 95/Α/11-6-2019 - Κύρωση του Ποινικού Κώδικα. Τα ανωτέρω άρθρα του Ποινικού Κώδικα καλύπτουν πλέον και τυποποιούν ενδεικτικά περιπτώσεις όπως α) Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών (292Α Π.Κ.), β) Παρακώλυση λειτουργίας πληροφοριακών συστημάτων (292Β Π.Κ.) όπου εντάσσονται και οι περιπτώσεις επιθέσεων τύπου DDoS (Distributed Denial-of-Service Attack), γ) Προσβολές του απορρήτου των τηλεπικοινωνιών του κοινού (292Δ Π.Κ.) και δ) Παρακώλυση των τηλεπικοινωνιών (292Ε Π.Κ).

Επίσης τα αδικήματα της παράνομης πρόσβασης σε σύστημα πληροφοριών ή σε δεδομένα προβλέπονται και τιμωρούνται από τις διατάξεις των άρθρων 370Β, 370Γ, 370Δ και 370Ε του Ποινικού Κώδικα. Στις περιπτώσεις αυτές περιγράφονται αδικήματα που αφορούν για παράδειγμα περιπτώσεις παράνομης πρόσβασης σε λογαριασμούς των μέσων κοινωνικής δικτύωσης ή εταιρικούς λογαριασμούς αλλά και πιο σοβαρές περιπτώσεις παραβίασης δεδομένων, πράξεις που είναι σήμερα γνωστές με τον όρο «Hacking».

Τέλος, το αδίκημα της απάτης (386Π.Κ.) συμπληρώνεται και στον ελληνικό ποινικό κώδικα με το έγκλημα της απάτης με υπολογιστή (386Α Π.Κ.). Στις περιπτώσεις αυτές περιλαμβάνονται μεταξύ άλλων οι οικονομικές απάτες μέσω διαδικτύου οι οποίες λαμβάνουν χώρα κυρίως με τη μορφή διαδικτυακών αγορών, διαδικτυακές επενδύσεις δάνεια κ.α.

1.4.2 Οδηγία της Ε.Ε. 2022/2555 NIS 2

Η Ευρωπαϊκή Ένωση καταβάλλει συνεχείς προσπάθειες για την επίτευξη ανθεκτικότητας ενάντια σε ολοένα και μεγαλύτερες κυβερνοαπειλές, καθώς και για τη διατήρηση της ασφάλειας και της προστασίας της ψηφιακής κοινωνίας και οικονομίας μας. η ΕΕ επιθυμεί μια πιο ολιστική και ομοιόμορφη προσέγγιση όσον αφορά την προστασία στον κυβερνοχώρο σε διαφορετικούς τομείς και αλυσίδες εφοδιασμού που επηρεάζουν τις υποδομές ζωτικής σημασίας, καθώς μια καταστροφική κυβερνοεπίθεση μπορεί να έχει τεράστιο αντίκτυπο στην οικονομία κάθε κράτους μέλους, αλλά και στην υπόλοιπη Ευρώπη. (/www.ot.gr 30-01-2023)

Για το λόγο αυτό η Ε.Ε. έθεσε από το έτος 2023 την οδηγία (ΕΕ) 2022/2555 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS1), η οποία δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης το Δεκέμβριο του 2022. Η νέα νομοθεσία θέτει, μεταξύ άλλων, αυστηρότερες απαιτήσεις για τις επιχειρήσεις, τη δημόσια διοίκηση και τις υποδομές.

Η Οδηγία NIS 2 (Οδηγία 2022/2555) αποτελεί την κύρια ευρωπαϊκή νομοθεσία για την ασφάλεια στον κυβερνοχώρο, παρέχοντας νομικά μέτρα με σκοπό την ενίσχυση του συνολικού επιπέδου ασφάλειας στην ΕΕ. Οι αρχικοί κανόνες για την κυβερνοασφάλεια τέθηκαν σε ισχύ το 2016 και κρίθηκε σκόπιμο να επικαιροποιηθούν, ώστε να συμβαδίζουν με την αυξημένη ψηφιοποίηση και το εξελισσόμενο τοπίο απειλών για την κυβερνοασφάλεια. Ουσιαστικά, η Οδηγία NIS 2 συμπληρώνει και καλύπτει τα κενά της Οδηγίας NIS 1, η οποία δεν ήταν πλέον επαρκής, δεδομένης της εντεινόμενης διασύνδεσης, της διαπιστωμένης ανεπαρκούς ανθεκτικότητας των επιχειρήσεων εντός ΕΕ και της έλλειψης κοινού πλαισίου αντιμετώπισης των κρίσεων (Αλεξιάννα Τσότσου 31 May 2023)

Η Οδηγία NIS 2 απαιτεί από τα κράτη-μέλη να υιοθετήσουν εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο. Τα κράτη-μέλη υποχρεούνται επίσης να ορίσουν ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), οι οποίες είναι υπεύθυνες για τον χειρισμό κινδύνων και περιστατικών, μια αρμόδια εθνική αρχή για την ασφάλεια στον κυβερνοχώρο και ένα ενιαίο σημείο επαφής, το οποίο θα ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας μεταξύ των αρχών του κράτους-μέλους με τις αρμόδιες αρχές άλλων κρατών-μελών και,

κατά περίπτωση, με την Επιτροπή και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

Το προτεινόμενο σχέδιο νόμου του Υπουργείου Ψηφιακής Διακυβέρνησης, προβλέπει τη σύσταση Νομικού Προσώπου Δημοσίου Δικαίου με την επωνυμία "Εθνική Αρχή Κυβερνοασφάλειας". Η νέα Αρχή θα συντονίζει, θα εφαρμόζει και θα ελέγχει το ολοκληρωμένο πλαίσιο στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου Κυβερνοασφάλειας στη χώρα.

Θα εποπτεύεται από τον Υπουργό Ψηφιακής Διακυβέρνησης και θα αποτελέσει την ενιαία και λειτουργική δομή που θα αναλάβει το σχεδιασμό και την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας σε συνεργασία με άλλες αρμόδιες αρχές. Μεταξύ άλλων αρμοδιοτήτων η Αρχή θα κατέχει τον εποπτικό και επιχειρησιακό ρόλο, στο πλαίσιο της εφαρμογής της Οδηγίας 2022/2555 (Οδηγία NIS2). Σημειώνεται ότι με την ενσωμάτωση της προαναφερόμενης οδηγίας θα αυξηθούν κατακόρυφα οι εποπτευόμενοι φορείς σε δημόσιο και ιδιωτικό τομέα. Οι φορείς που εμπίπτουν στο πεδίο της Οδηγίας NIS 1 είναι περίπου 70, ενώ με την ενσωμάτωση στο ελληνικό Δίκαιο της NIS 2, οι φορείς θα ξεπεράσουν τους 2000 (Υπουργείο Ψηφιακής Διακυβέρνησης 2024).

1.4.3 Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ - GDPR)

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ), γνωστός και ως Γενικός Κανονισμός για την Προστασία των Δεδομένων των Πολιτών (ΓΚΠΔΠ ή GDPR στα αγγλικά), είναι ένας νομοθετικός κανονισμός της Ευρωπαϊκής Ένωσης με άμεση εφαρμογή σε όλα τα Κράτη-Μέλη από 25/05/2018 χωρίς την προϋπόθεση κρατικής νομοθεσίας. Ο στόχος του είναι η προστασία και η ενίσχυση της ιδιωτικής ζωής και των προσωπικών δεδομένων των πολιτών της ΕΕ. Ο ΓΚΠΔ θεσπίζει κανόνες σχετικά με τη συλλογή, την επεξεργασία και την αποθήκευση προσωπικών δεδομένων από επιχειρήσεις και οργανισμούς, είτε βρίσκονται εντός είτε εκτός της ΕΕ, ανεξαρτήτως του αν η επεξεργασία αυτών των δεδομένων πραγματοποιείται από αυτές τις επιχειρήσεις ή οργανισμούς ή από τρίτους εκτελεστές.

Οι κύριες αρχές του GDPR περιλαμβάνουν την αρχή της διαφάνειας, της λογικής επεξεργασίας, της περιορισμένης αποθήκευσης, της ακρίβειας και της ευθύνης. Επιπλέον, εισάγει τα δικαιώματα των ενδιαφερομένων όσον αφορά την πρόσβαση, τη διόρθωση, τη διαγραφή και τη μεταφορά των προσωπικών τους δεδομένων. Οι παραβάσεις του GDPR μπορούν να επιφέρουν σημαντικά πρόστιμα για τις επιχειρήσεις ή τους οργανισμούς που τις διαπράττουν, καθώς και άλλες κυρώσεις όπως απαγόρευση της επεξεργασίας δεδομένων και ανάκληση άδειας λειτουργίας.

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) έχει επιφέρει αρκετές σημαντικές αλλαγές στους οργανισμούς, μερικές από τις οποίες περιλαμβάνουν:

Αυξημένες απαιτήσεις σχετικά με τη συγκατάθεση των ατόμων: Οι οργανισμοί πρέπει να είναι πιο διαφανείς και να λαμβάνουν σαφή συγκατάθεση για τη συλλογή και την επεξεργασία των προσωπικών τους δεδομένων.

Αυξημένα δικαιώματα των ατόμων: Ο GDPR δίνει στα άτομα περισσότερο έλεγχο επί των προσωπικών τους δεδομένων, συμπεριλαμβανομένων των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής και μεταφοράς των δεδομένων τους.

Αυξημένες υποχρεώσεις ασφαλείας δεδομένων: Οι οργανισμοί πρέπει να λάβουν επαρκείς μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων που κατέχουν και να αναφέρουν πιθανές παραβάσεις δεδομένων εντός 72 ωρών. Ο υπεύθυνος επεξεργασίας οφείλει, σε περίπτωση παραβιάσεως και διαρροής δεδομένων, να ενημερώσει εντός 72 ωρών την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και σε ορισμένες περιπτώσεις και το ίδιο το υποκείμενο

Αυστηρότερες κυρώσεις: Ο GDPR θεσπίζει ποινές για τις παραβάσεις, με πρόστιμα που μπορούν να φτάσουν έως και το 4% του ετήσιου παγκόσμιου τζίρου ενός οργανισμού ή έως και 20 εκατομμύρια ευρώ, εξαρτώμενα από το ποιο είναι μεγαλύτερο. (άρ.8, 11, 25 έως 39, 41 παρ. 4, 42 και 43 & αρ.5, 6, 7, 9 Βασικές αρχές).

Αυξημένες απαιτήσεις για τις μεταφορές δεδομένων εκτός της ΕΕ: Οι οργανισμοί που μεταφέρουν προσωπικά δεδομένα εκτός της Ευρωπαϊκής Ένωσης πρέπει να τηρούν αυστηρούς κανόνες που ορίζονται από το GDPR για την προστασία αυτών των δεδομένων.

Οι αλλαγές αυτές απαιτούν από τους οργανισμούς να αναθεωρήσουν τις πρακτικές τους σχετικά με την προστασία των δεδομένων και να εφαρμόσουν νέες διαδικασίες και πολιτικές προκειμένου να συμμορφωθούν με τις απαιτήσεις του κανονισμού. Η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων (GDPR) επηρεάζει επίσης τους οργανισμούς του δημοσίου. Ορισμένες από τις αλλαγές που πρέπει να πραγματοποιήσουν οι δημόσιοι οργανισμοί συμπεριλαμβάνουν:

Εκπαίδευση προσωπικού: Οι δημόσιοι οργανισμοί θα πρέπει να διασφαλίσουν ότι το προσωπικό τους είναι ενημερωμένο και εκπαιδευμένο σχετικά με τις νέες απαιτήσεις του GDPR, καθώς και τις εσωτερικές διαδικασίες για την προστασία των δεδομένων.

Αναθεώρηση διαδικασιών και πολιτικών: Οι οργανισμοί θα πρέπει να επανεξετάσουν και να ενημερώσουν τις πολιτικές τους για την προστασία των δεδομένων, καθώς και τις διαδικασίες για τη συγκέντρωση, την επεξεργασία και τη διατήρηση των προσωπικών δεδομένων.

Επένδυση σε τεχνολογία και υποδομές: Οι οργανισμοί θα πρέπει να επενδύσουν σε τεχνολογία και υποδομές που θα τους επιτρέπουν να προστατεύουν αποτελεσματικά τα προσωπικά δεδομένα που κατέχουν.

Συνεργασία με εξωτερικούς εμπειρογνώμονες: Οι οργανισμοί μπορούν να συνεργαστούν με εξωτερικούς εμπειρογνώμονες για να αξιολογήσουν και να βελτιώσουν τη συμμόρφωσή τους με τον κανονισμό.

Επιβολή κυρώσεων: Στους Δημόσιους οργανισμούς επίσης μπορεί να επιβληθούν κυρώσεις σε περίπτωση παραβίασης του GDPR, συμπεριλαμβανομένων των προστίμων που μπορεί να επιβληθούν από τις εποπτικές αρχές.

Συνολικά, οι δημόσιοι οργανισμοί στην Ελλάδα πρέπει να αναγνωρίσουν τη σημασία της προστασίας των δεδομένων και να λάβουν τα αναγκαία μέτρα για τη συμμόρφωσή τους με το GDPR. (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, Access to Europian Union Law, eur-lex.europa.eu/legal-content), (Εισαγωγή στο νέο Γενικό Κανονισμό Προστασίας Δεδομένων, https://www.gdprgreece.com)

Η Αρχή που είναι υπεύθυνη για την προστασία των προσωπικών δεδομένων και την προώθηση του γενικού κανονισμού περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης (GDPR) στην ελληνική νομοθεσία είναι η συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Η Αρχή ιδρύθηκε με τον νόμο 4624/2019 και αποτελεί έναν ανεξάρτητο οργανισμό που λειτουργεί ως εγγυητής της προστασίας των προσωπικών δεδομένων των πολιτών. Οι βασικές της αρμοδιότητες περιλαμβάνουν την επιβολή των κανόνων προστασίας δεδομένων στην Ελλάδα, την παροχή κατευθυντηρίων οδηγιών, την παρακολούθηση της συμμόρφωσης των οργανισμών με τους νόμους περί προστασίας δεδομένων και τη διεξαγωγή έρευνας και επιβολής κυρώσεων σε περίπτωση παραβίασης των κανονισμών. Η ΑΠΠΔ δραστηριοποιείται σε συνεργασία με άλλες ευρωπαϊκές αρχές προστασίας δεδομένων, όπως ο Ευρωπαίος Επόπτης Προσωπικών Δεδομένων (EDPS), για την εξασφάλιση της συμμόρφωσης με τους ευρωπαϊκούς κανόνες προστασίας δεδομένων.

Κεφάλαιο 2ο Μεθοδολογία έρευνας

2.1 Ειδικό ερευνητικό μέρος

Ο ανθρώπινος παράγοντας στην ασφάλεια των πληροφοριακών συστημάτων όπως αναλύθηκε στο προηγούμενο κεφάλαιο είναι εξαιρετικά κρίσιμος, καθώς οι άνθρωποι συχνά αποτελούν τον αδύναμο κρίκο στην αλυσίδα ασφαλείας. Υπάρχουν διάφορες πτυχές που καθιστούν σημαντικό τον ανθρώπινο παράγοντα με πιο σημαντική την εκπαίδευση και ενημέρωση. Οι χρήστες των πληροφοριακών συστημάτων πρέπει να είναι ενημερωμένοι και εκπαιδευμένοι σχετικά με τις απειλές και τις βέλτιστες πρακτικές ασφάλειας. Η έλλειψη γνώσης μπορεί να οδηγήσει σε αμέλεια ή λανθασμένες αποφάσεις που θέτουν σε κίνδυνο την ασφάλεια του συστήματος. Τα ανθρώπινα λάθη των χρηστών, όπως η χρήση απλών κωδικών πρόσβασης, η απρόσεκτη διαχείριση ευαίσθητων πληροφοριών ή η αποδοχή ύποπτων συνημμένων αρχείων, μπορούν να δώσουν πρόσβαση σε κακόβουλους χρήστες.

Ο δημόσιος τομέας στην Ελλάδα αντιμετωπίζει διάφορες προκλήσεις, όπως η γραφειοκρατία, η διαφθορά, και η ανάγκη για εκσυγχρονισμό και ψηφιοποίηση των υπηρεσιών. Τα τελευταία χρόνια έχουν γίνει αρκετές προσπάθειες μεταρρύθμισης με στόχο την αύξηση της αποδοτικότητας και της διαφάνειας. Μία από τις σημαντικότερες αποτελεί η ψηφιακή διακυβέρνηση, δηλαδή η προώθηση της μεταρρύθμισης και ψηφιοποίησης των δημοσίων υπηρεσιών. Στη κατεύθυνση αυτή σοβαρή πρόκληση αποτελεί η ασφάλεια. Για το λόγο αυτό η παρούσα εργασία εξετάζει το βαθμό ευαισθητοποίησης σε θέματα ασφάλειας των εργαζομένων στο Δημόσιο τομέα της Ελλάδος προκειμένου αφενός να αναδείξει τη σπουδαιότητα της ασφάλειας και του ανθρώπινου παράγοντα και αφετέρου να εντοπίσει τυχών προβληματικές και να παραθέσει προτάσεις προς βελτίωση.

2.2 Επιλογή μεθόδου έρευνας

Η μέθοδος που χρησιμοποιήθηκε είναι η ποσοτική μέθοδος έρευνας. Η συγκεκριμένη μέθοδος επιλέχθηκε ως η πιο κατάλληλη προκειμένου να μελετηθεί και να αναλυθεί ο βαθμός ευαισθητοποίησης των υπαλλήλων στον δημόσιο τομέα σε ζητήματα ασφάλειας των πληροφοριών, καθώς με τη μέθοδο αυτή δύναται να συγκεντρώνονται και να επεξεργάζονται τα δεδομένα. Τα δεδομένα αυτά μπορούν εύκολα να αναλυθούν και να ερμηνευτούν με στατιστικούς ελέγχους, πίνακες και διαγράμματα μέσω της συσχέτισης μεταβλητών.

2.3 Είδος δειγματοληψίας

Το δείγμα της έρευνας επιλέχθηκε με τη στατιστική μέθοδο δειγματοληψίας μη πιθανότητας με δείγμα ευκολίας (Convenience Sampling). Η δειγματοληψία ευκολίας (Convenience Sampling) είναι μια μη-πιθανολογική μέθοδος δειγματοληψίας που βασίζεται στην επιλογή συμμετεχόντων που είναι πιο εύκολο να προσεγγιστούν και να συμμετάσχουν στην έρευνα. Αυτή η μέθοδος συχνά χρησιμοποιείται όταν οι πόροι, ο χρόνος ή η πρόσβαση στον πληθυσμό είναι περιορισμένοι. Συγκεκριμένα το ερωτηματολόγιο απεστάλη μέσω μηνύματος ηλεκτρονικού ταχυδρομείου σε σπουδαστές και απόφοιτους του προγράμματος μεταπτυχιακών Σπουδών «Δημόσια Διοίκηση - Δημόσιο Management» του Τμήματος Διοίκησης Επιχειρήσεων του Πανεπιστημίου Δυτικής Αττικής. Επιπρόσθετα, το ερωτηματολόγιο απεστάλη σε Υπηρεσίες των Υπουργείων, Περιφερειών και Δήμων αλλά και σε Ανεξάρτητες Αρχές, με σκοπό την επιλογή δείγματος από όσο το δυνατόν μεγαλύτερο εύρος υπηρεσιών του Δημοσίου Τομέα.

2.4 Ερευνητικά ερωτήματα

Σκοπός της παρούσας εργασίας είναι η αξιολόγηση του επιπέδου γνώσεων και αντιλήψεων των υπαλλήλων του δημόσιου τομέα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων. Επίσης,

Η ηλικία του εργαζομένου επηρεάζει το βαθμό που αντιλαμβάνονται ότι ο οργανισμός δημιουργεί ευαισθητοποίηση στους εργαζόμενους για θέματα ασφάλειας των πληροφοριακών συστημάτων.
Η ηλικία επηρεάζει την αντίληψη των υπαλλήλων σχετικά με τη σημασία της τήρησης των βασικών αξιών στον οργανισμό.
Η ηλικία επηρεάζει το βαθμό συμφωνίας ότι οι ευαίσθητες πληροφορίες μπορεί να δημιουργήσουν σοβαρά προβλήματα αν διαρρεύσουν.
Το επίπεδο σπουδών επηρεάζει την αντίληψη που έχουν για το πόσο συχνά συνεργάζονται τα διάφορα μέρη του οργανισμού για να δημιουργήσουν αλλαγή.
Το φύλο επηρεάζει το βαθμό που ο εργαζόμενος πιστεύει ότι επιτρέπεται να κάνει «κλικ» σε συνδέσμους που προέρχονται από άγνωστο αποστολέα.
Το φύλο επηρεάζει το βαθμό συμφωνίας ότι επιτρέπεται η αποστολή ευαίσθητων εργασιακών αρχείων μέσω δημόσιου Wi-Fi δικτύου.
Το φύλο του εργαζομένου επηρεάζει το βαθμό που αντιλαμβάνονται ότι ο οργανισμός δημιουργεί ευαισθητοποίηση μεταξύ των εργαζομένων για θέματα ασφάλειας των πληροφοριακών συστημάτων.

Το φύλο του εργαζομένου επηρεάζει την αντίληψή του σχετικά με το βαθμό που η διοίκηση συμμορφώνεται με τους κανόνες.

2.5 Συλλογή δεδομένων και όργανο μέτρησης

Το πρώτο βήμα αυτής της έρευνας είναι η μελέτη της βιβλιογραφίας ώστε να κατανοήσουμε τη σημασία του ανθρώπινου παράγοντα στην ασφάλεια των πληροφοριακών συστημάτων και κατ΄ επέκταση τη σπουδαιότητα της ευαισθητοποίησης των εργαζομένων του οργανισμού σε θέματα ασφάλειας (Information Security Awareness - ISA). Σκοπός της έρευνας είναι η μέτρηση του βαθμού ευαισθητοποίησης του προσωπικού του Δημοσίου Τομέα στην Ελλάδα.

Έπειτα, η έρευνα βασίστηκε στη δημιουργία και διανομή ενός ερωτηματολογίου το οποίο κλήθηκαν να απαντήσουν εργαζόμενοι στο Δημόσιο Τομέα. Το ερωτηματολόγιο, το οποίο αποτελείται συνολικά από πενήντα έξι (56) ερωτήσεις, δημιουργήθηκε μέσω της εφαρμογής «Google Forms» και εστάλη μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η επιλογή των ατόμων έγινε τυχαία και οι απαντήσεις ήταν ανώνυμες ενώ δε προσδιορίζεται ο οργανισμός στον οποίο εργάζεται ο συμμετέχων. Όλα τα προσωπικά δεδομένα των συμμετεχόντων προστατεύονται σύμφωνα με τις διατάξεις του Νόμου 4624/2019 περί προστασίας Προσωπικών Δεδομένων. Συνολικά 172 εργαζόμενοι στον ελληνικό Δημόσιο τομέα συμπλήρωσαν το διαδικτυακό ερωτηματολόγιο. Οι συμμετέχοντες έπρεπε να εργάζονται επί του παρόντος στον Δημόσιο τομέα της Ελλάδας και να είναι τουλάχιστον 18 ετών ηλικίας.

Η πρώτη ενότητα του ερωτηματολογίου, περιλαμβάνει πέντε (5) ερωτήσεις δημογραφικής φύσεως και αφορούν την ηλικία, το φύλο, το επίπεδο σπουδών, το χρόνο εργασίας στο Δημόσιο Τομέα καθώς και το φορέα που εργάζονται, π.χ. Υπουργείο, Τοπική Αυτοδιοίκηση κτλ. χωρίς ωστόσο να προσδιορίζεται καθ' οιονδήποτε τρόπο ο Οργανισμός. Οι λοιπές ερωτήσεις είναι διαμορφωμένες σε κλίμακα τύπου Likert επτά (7) σημείων, που κυμαίνεται από «Διαφωνώ απόλυτα» έως «Συμφωνώ απόλυτα».

Για την έρευνα χρησιμοποιήθηκε τμήμα του ερωτηματολογίου, Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons, K., et. al., 2017). Το ερωτηματολόγιο αυτό αποτελείται από εξήντα τρείς (63) ερωτήσεις ομαδοποιημένο σε επτά τομείς της ασφάλειας των πληροφοριών (Password management, Email use, Internet use, Social media use, Mobile devices, Information handling, Incident report) για κάθε έναν από τους οποίους εξετάζονται τρία (3) στοιχεία (Knowledge, Attitude and Behavior). Ωστόσο, όπως αναφέρουν και οι ερευνητές το ερωτηματολόγιο είναι δυνατό να χρησιμοποιηθεί με τρόπο αρθρωτό, «*we acknowledge that it may not always be viable to use a scale*

of this size. Hence, the HAIS-Q has been designed to be used in a modular fashion». Σε προηγούμενη μελέτη, οι ερευνητές χρησιμοποιήσαν δύο από τα τρία στοιχεία εστίασης «Knowledge and Attitude» (Pattinson, M. et. al., 2016) προκειμένου να μετρήσουν το επίπεδο ωριμότητας υπαλλήλων ενός τραπεζικού ιδρύματος στην Αυστραλία και τη σύγκριση αυτού με το υπόλοιπο εργατικό δυναμικό της χώρας. Για τους σκοπούς της παρούσης έρευνας χρησιμοποιήθηκαν οι τομείς Password management, Email use, Internet use, Mobile devices για κάθε ένα από τα τρία στοιχεία «Knowledge», «Attitude» και «Behaviour» οι οποίοι εξετάζουν κάθε έναν από τους τέσσερις (4) τομείς με τη χρήση τριών (3) ερωτήσεων χρησιμοποιώντας συνολικά τριάντα (36) ερωτήσεις.

Επιπρόσθετα, πέντε (5) ερωτήσεις αντλήθηκαν και τροποποιήθηκαν από το ερωτηματολόγιο μιας έρευνας σχετικά με την αλλαγή κουλτούρας στην ασφάλεια των πληροφοριών «Information Security Culture Change Management (ISCCM)» (Da Veiga, A, 2018). Το εργαλείο αυτό αναφέρεται στη διαδικασία συστηματικής μετατροπής των στάσεων, συμπεριφορών και αντιλήψεων των ατόμων εντός μιας οργάνωσης προς την κατεύθυνση της ασφάλειας των πληροφοριακών συστημάτων. Περιλαμβάνει την εφαρμογή στρατηγικών και πρωτοβουλιών για τη δημιουργία μιας κουλτούρας όπου η ασφάλεια είναι αξιολογημένη, κατανοητή και ενσωματωμένη σε όλες τις πτυχές των λειτουργιών της οργάνωσης. Κύρια στοιχεία της ISCCM μπορεί να περιλαμβάνουν την υποστήριξη της ηγεσίας, την εκπαίδευση και ευαισθητοποίηση του προσωπικού, τη διαφάνεια στην επικοινωνία, τον συμμετοχικό χαρακτήρα, την αναγνώριση και την διαρκή βελτίωση. Μέσω αυτών των μέτρων, η ISCCM στοχεύει στη δημιουργία μιας κουλτούρας όπου η ασφάλεια είναι ενσωματωμένη στο DNA της οργάνωσης, προστατεύοντας ταυτόχρονα τα περιουσιακά στοιχεία της από δυνητικούς κινδύνους.

Έξι (6) ερωτήσεις αναφέρονται στην οργανωσιακή κουλτούρα του οργανισμού (Detert, et. al., 2000), οι τρείς εκ των οποίων εστιάζουν στη συνέπεια στις βασικές αξίες και κανόνες μιας οργάνωσης σε κάθε επίπεδο, οι οποίες είναι προσανατολισμένες στην ασφάλεια των Π.Σ.. Αυτό δημιουργεί ένα ισχυρό θεμέλιο για την οργανωτική κουλτούρα και βοηθά στην προώθηση της ενότητας, της προβλεψιμότητας και της αξιοπιστίας μέσα στον οργανισμό. Ενώ τρείς (3) ερωτήσεις, οι οποίες ομοίως εστιάζουν στο τομέα της ασφάλειας, αναφέρονται στην ικανότητα του οργανισμού να ανταποκρίνεται και να προσαρμόζεται επιτυχώς σε αλλαγές στο περιβάλλον του. Αυτό σημαίνει ότι ο οργανισμός δεν διατηρεί παθητική στάση απέναντι στις προκλήσεις αλλά αναλαμβάνει ενεργό ρόλο, μέσω της συνεχούς ανανέωσης και βελτίωσης των προσεγγίσεών του. Επίσης, το ερωτηματολόγιο περιέχει τρείς (3) ερωτήσεις που ζητούν τη γνώμη των συμμετεχόντων για το cloud computing στον ελληνικό Δημόσιο Τομέα (Amron, et al., 2019). Τέλος, μία (1) ερώτηση ζητά από τους συμμετέχοντες να δηλώσουν το βαθμό ικανοποίησης για την ενημέρωσή τους σε θέματα ασφάλειας πληροφοριών.

Κεφάλαιο 3ο Στατιστική ανάλυση – Παρουσίαση αποτελεσμάτων

3.1 Περιγραφική στατιστική

3.1.1 Περιγραφή δείγματος

Στην ενότητα αυτή θα παρουσιαστεί το προφίλ των συμμετεχόντων στην έρευνα σύμφωνα με τις απαντήσεις στην ενότητα «Δημογραφικά χαρακτηρίστηκα» του ερωτηματολογίου η οποία περιλαμβάνει πληροφορίες σχετικά την ηλικία, το φύλο, το επίπεδο σπουδών, το χρόνο εργασίας στο Δημόσιο Τομέα καθώς και το φορέα που εργάζονται. Το συνολικό δείγμα το συμμετεχόντων αποτελείται από εκατό εβδομήντα δύο (172) εργαζομένους στο Δημόσιο τομέα της Ελλάδος., τα οποία επελέγησαν με τη χρήση της δειγματοληψίας ευκολίας (Convenience Sampling).

Από τους 172 συμμετέχοντες, η πλειοψηφία είναι γυναίκες σε ποσοστό 69,2% σε αντίθεση με τους άνδρες με ποσοστό 30,8%. Η στήλη Percent (%) και Valid Percent δείχνουν τη σχετική συχνότητα των τιμών της μεταβλητής στο δείγμα, η πρώτη επί του συνόλου των περιπτώσεων και η δεύτερη επί του συνόλου των περιπτώσεων που έδωσαν έγκυρες απαντήσεις

Μεταβλητή		**Συχνότητα**	**Ποσοστό**
Φύλλο Υπαλλήλου	Άνδρας	53	30,8
	Γυναίκα	119	69,2
Ηλικία	18-29	6	3,5
	30-39	24	14
	40-49	61	35,5
	50-59	75	43,6
	>60	6	3,5
Εκπαίδευση	Απόφοιτος Λυκείου	13	7,6
	Απόφοιτος Ανώτερων Σχολών	8	4,7
	Απόφοιτος Πανεπιστημίου	52	30,2
	Απόφοιτος Μεταπτυχιακού Προγράμματος Σπουδών	95	55,2
	Απόφοιτος Διδακτορικού Προγράμματος Σπουδών	4	2,3
Διάρκεια απασχόλησης	<=5	17	9,9
	6-15	35	20,3
	15-25	77	44,8
	>26	43	25
Φορέας εργασίας	Υπουργείο	46	26,7
	ΝΠΔΔ-ΝΠΙΔ	40	23,3
	ΟΤΑ Α' και Β΄ Βαθμού	60	34,9
	λοιποί οργανισμοί δημοσίου, ανεξάρτητες αρχές κ.α.	26	15,1

Πίνακας 1 Δημογραφικά χαρακτηριστηκά δείγματος

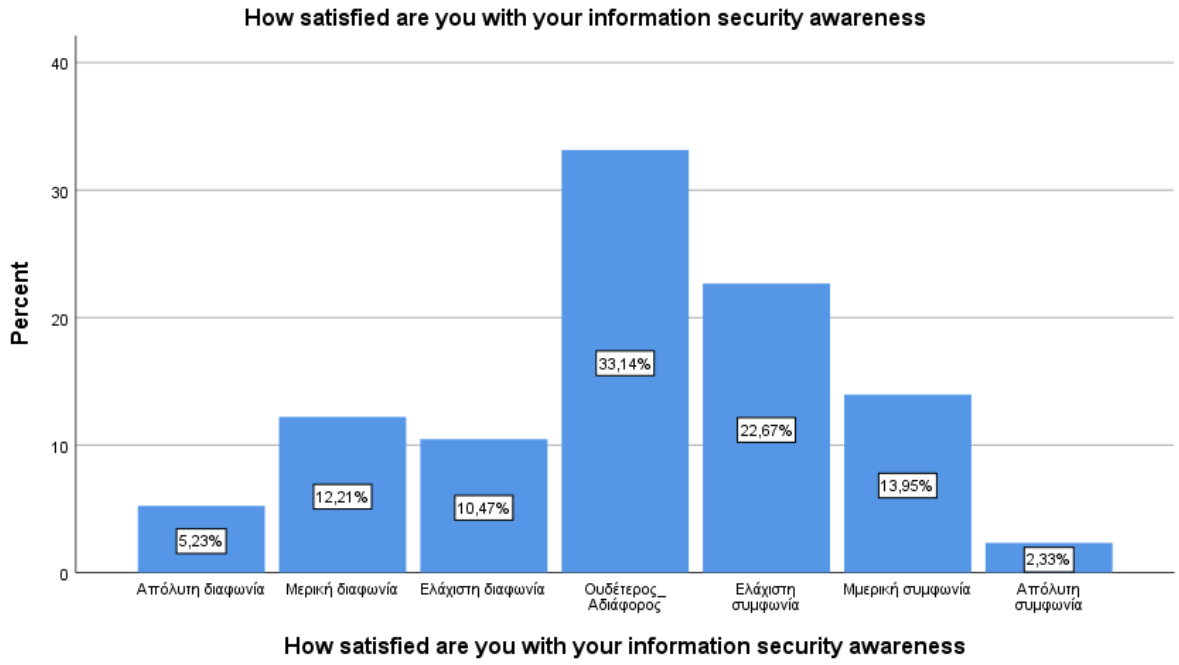
Αναφορικά με την ηλικία, όπως διακρίνεται στον πίνακα 1, η πλειοψηφία των συμμετεχόντων ανήκει στην ηλικιακή μάδα 50-59 ετών με ποσοστό 43,6%, ακολουθεί η ηλικιακή ομάδα 40-49 ετών με ποσοστό 35,5%, ενώ η μειοψηφία ανήκει στις ηλικιακές ομάδες 18-29 ετών και άνω των 60ετών με ποσοστό 3,5% έκαστη.

Η πλειοψηφία των συμμετεχόντων είναι απόφοιτοι Μεταπτυχιακού τίτλου σπουδών (55,2%), απόφοιτοι πανεπιστημίου είναι 30,2% ενώ το μικρότερο ποσοστό των συμμετεχόντων (2,3%) είναι απόφοιτοι διδακτορικού προγράμματος σπουδών.

Για τη διάρκεια απασχόλησης στο Δημόσιο τομέα ορίστηκαν τέσσερις ομάδες. Η πλειοψηφία των συμμετεχόντων εργάζονται στο Δημόσιος Τομέα από 15 έως 25 χρόνια, με ποσοστό 44,8%. Αντίθετα, κάτω από 5 χρόνια εργάζονται 17 άτομα που αντιπροσωπεύουν 9,9% του συνόλου του δείγματος.

Τέλος, σχετικά με το φορέα εργασίας, που αποτελεί τη τελευταία ερώτηση της ενότητας δημογραφικών στοιχείων, προκύπτει ότι οι εργαζόμενοι στη τοπική αυτοδιοίκηση αντιπροσωπεύουν το μεγαλύτερο ποσοστό του δείγματος (34,9%), έναντι των εργαζομένων στους λοιπούς οργανισμούς του Δημοσίου όπως Ανεξάρτητες Αρχές, Σώματα Ασφαλείας κ.α. που αντιπροσωπεύουν το 15,1% του συνόλου του δείγματος.

3.1.2 Ικανοποίηση Εργαζομένων σχετικά με την Πληροφόρηση τους για την Ασφάλεια των Πληροφοριακών Συστημάτων



Διάγραμμα 1 ικανοποίηση από την ενημέρωσή σε θέματα ασφάλειας πληροφοριών

Το διάγραμμα δείχνει τα ποσοστά των απαντήσεων στην ερώτηση "Πόσο ικανοποιημένοι είστε με την επίγνωση σας για την ασφάλεια των πληροφοριών;"

Το μεγαλύτερο ποσοστό των συμμετεχόντων (33,14%) δήλωσε ουδέτεροι ή αδιάφοροι. Η ελάχιστη συμφωνία και η μερική συμφωνία αθροιστικά ανέρχονται σε 36,62%, υποδεικνύοντας ότι αρκετοί συμμετέχοντες έχουν κάποια θετική άποψη για την επίγνωση τους στην ασφάλεια των πληροφοριών. Ένα σημαντικό ποσοστό των συμμετεχόντων (27,91%) ανέφερε κάποιο βαθμό δυσαρέσκειας (απόλυτη, μέτρια ή ελάχιστη). Γενικά, οι απόψεις των συμμετεχόντων φαίνονται να είναι αρκετά διαμοιρασμένες σχετικά με τα επίπεδα ενημέρωσής τους.

3.1.3 Organisational Security Culture Measure

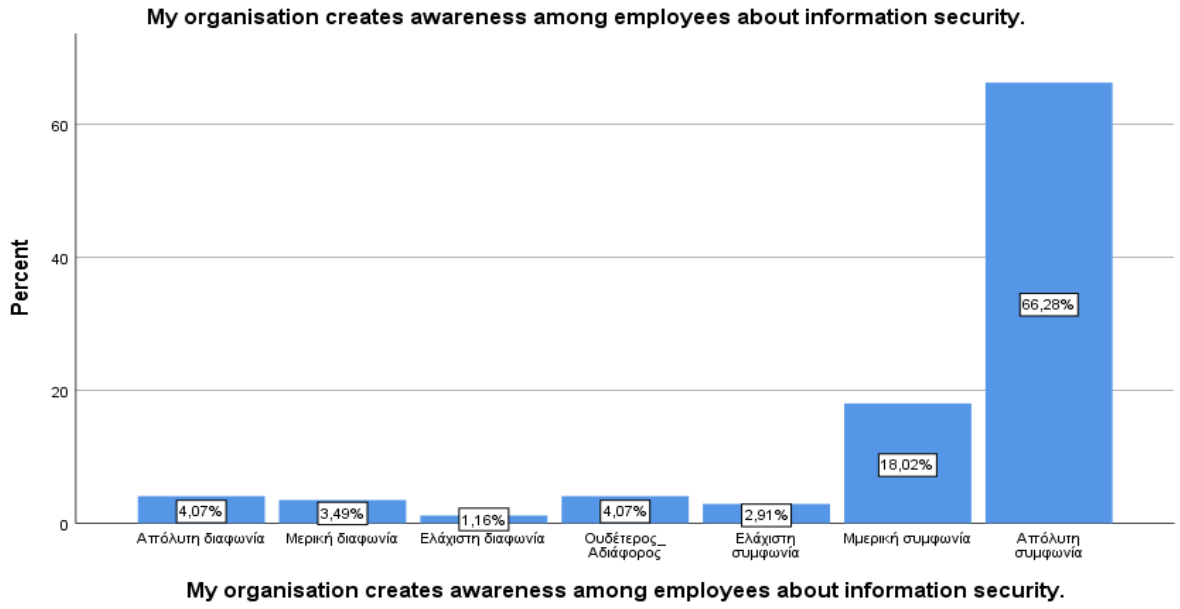
Στην ενότητα αυτή παρουσιάζονται τα αποτελέσματα που προέκυψαν από πέντε (5) ερωτήσεις που τέθηκαν και προσανατολίζονται στην οργανωσιακή κουλτούρα του οργανισμού με κατεύθυνση την ασφάλεια.

Ερώτηση	Μέσος Όρος	Τυπική Απόκλιση	Ελάχιστο	Μέγιστο
Ο οργανισμός μου ενημερώνει τους υπαλλήλους για την ασφάλεια των πληροφοριών.	6,1744	1,58717	1	7
Πιστεύω ότι οι πληροφορίες στον οργανισμό μου προστατεύονται επαρκώς.	3,7093	2,06257	1	7
Πιστεύω ότι όλοι στον οργανισμό μου θέλουν να προστατεύσουν τις οργανωτικές πληροφορίες.	4,9302	1,69823	1	7
Οι νέοι υπάλληλοι στον οργανισμό μου παρακολουθούν εκπαίδευση κατά την ένταξη όπου συζητείται η ασφάλεια των πληροφοριών.	4,4709	1,93287	1	7
Ο οργανισμός μου έχει θέσει σε εφαρμογή μια πολιτική ασφάλειας πληροφοριών (αναφέρεται επίσης ως Πολιτική Αποδεκτής Χρήσης).	4,9651	1,66103	1	7

Πίνακας 2 Organisational Security Culture Measure

Ερώτηση 1: Ο οργανισμός μου ενημερώνει τους υπαλλήλους για την ασφάλεια των πληροφοριών.

Ο υψηλός μέσος όρος (6,1744) υποδηλώνει ότι οι περισσότεροι υπάλληλοι αισθάνονται ότι ο οργανισμός τους ενημερώνει επαρκώς για θέματα ασφάλειας πληροφοριών. Η τυπική απόκλιση 1,58717 δείχνει κάποια ποικιλία στις απόψεις, αλλά γενικά οι απαντήσεις συγκλίνουν προς την υψηλή ενημέρωση. Συμπερασματικά οι οργανισμού του Δημοσίου Τομέα φαίνεται να καταβάλλουν αξιόλογες προσπάθειες για την ενημέρωση των υπαλλήλων τους σχετικά με την ασφάλεια των πληροφοριών, κάτι που είναι θετικό για την καλλιέργεια ενός περιβάλλοντος ασφαλείας.



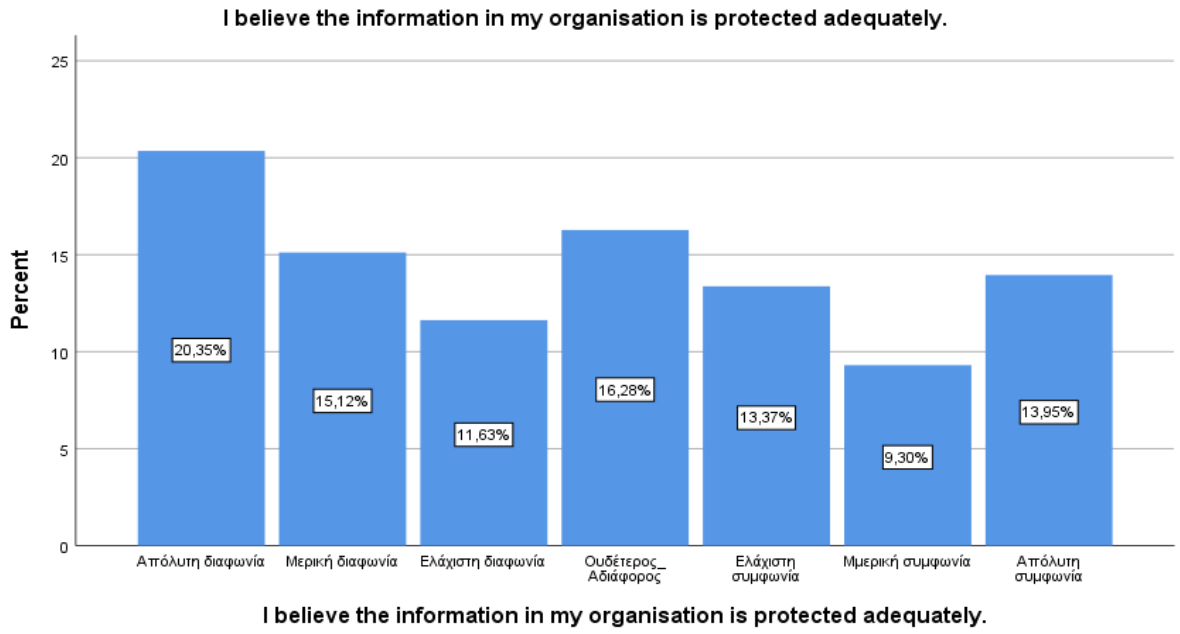
Διάγραμμα 2 Ο οργανισμός μου δημιουργεί ευαισθητοποίηση μεταξύ των εργαζομένων σχετικά με την ασφάλεια των πληροφοριών

Ερώτηση 2: Πιστεύω ότι οι πληροφορίες στον οργανισμό μου προστατεύονται επαρκώς.

Ο μέσος όρος 3,7093 δείχνει ότι οι υπάλληλοι είναι αβέβαιοι ή διχασμένοι ως προς την επάρκεια της προστασίας των πληροφοριών στον οργανισμό τους. Η υψηλή τυπική απόκλιση

(2,06257) υποδηλώνει σημαντική διαφοροποίηση στις απόψεις, με κάποιους υπαλλήλους να νιώθουν αρκετά ασφαλείς και άλλους όχι.

Υπάρχει ανάγκη βελτίωσης στην προστασία των πληροφοριών ή στην επικοινωνία αυτής της προστασίας προς τους υπαλλήλους, ώστε να μειωθεί η αβεβαιότητα και να ενισχυθεί η εμπιστοσύνη.



Διάγραμμα 3Πιστεύω ότι οι πληροφορίες στον οργανισμό μου προστατεύονται επαρκώς

Ερώτηση 3: Πιστεύω ότι όλοι στον οργανισμό μου θέλουν να προστατεύσουν τις πληροφορίες του οργανισμού.

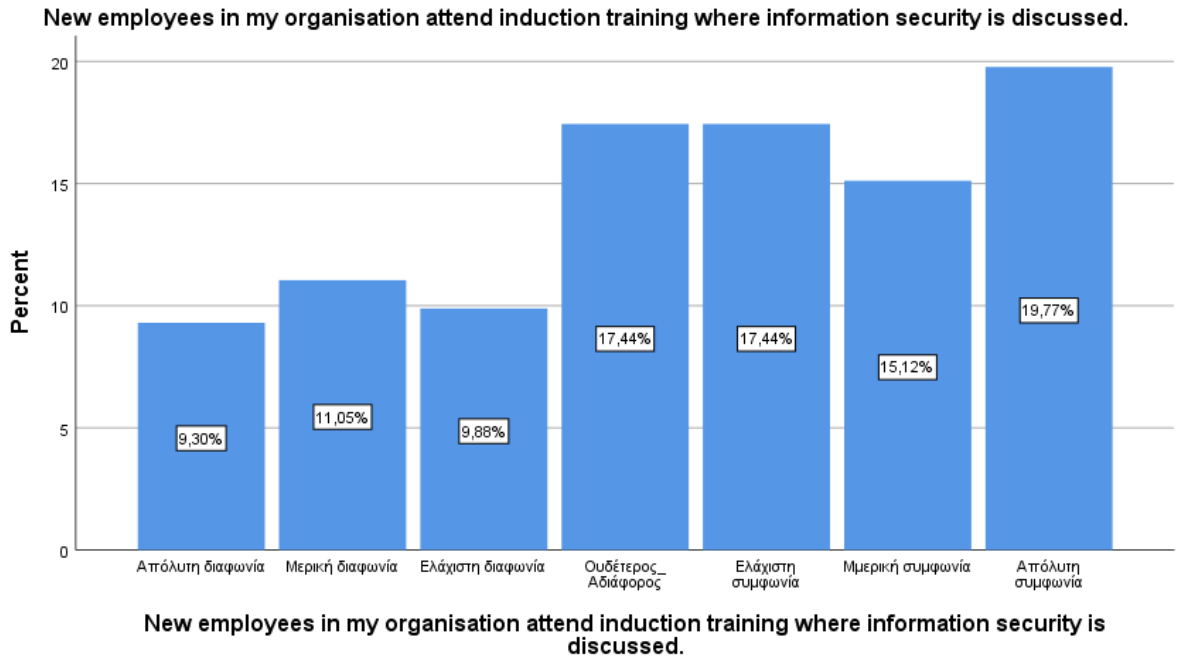
Ο μέσος όρος 4,9302 είναι θετικός, δείχνοντας ότι γενικά υπάρχει η αντίληψη ότι οι υπάλληλοι θέλουν να προστατεύσουν τις πληροφορίες. Η τυπική απόκλιση 1,69823 υποδηλώνει κάποια διακύμανση στις απόψεις, αλλά γενικά υπάρχει μια κοινή αντίληψη περί της επιθυμίας για προστασία.

Διάγραμμα 4Πιστεύω ότι όλοι οι εργαζόμενοι στον οργανισμό μου θέλουν να προστατεύσουν τις πληροφορίες του οργανισμού

Ερώτηση 4: Οι νέοι υπάλληλοι στον οργανισμό μου παρακολουθούν εκπαίδευση κατά την ένταξη όπου συζητείται η ασφάλεια των πληροφοριών.

Ο μέσος όρος 4,4709 δείχνει ότι οι νέοι υπάλληλοι λαμβάνουν κάποια εκπαίδευση σχετικά με την ασφάλεια των πληροφοριών, αλλά αυτό δεν είναι καθολικό ή επαρκές για όλους τους υπαλλήλους. Η τυπική απόκλιση 1,93287 υποδηλώνει ότι οι απόψεις ποικίλουν σημαντικά.

Η εκπαίδευση των νέων υπαλλήλων μπορεί να ενισχυθεί για να διασφαλιστεί ότι όλοι λαμβάνουν επαρκή γνώση σχετικά με την ασφάλεια των πληροφοριών από την αρχή.



Διάγραμμα 5 Οι νέοι υπάλληλοι στον οργανισμό μου παρακολουθούν εισαγωγική εκπαίδευση μέρος της οποίας αποτελεί η ασφάλεια των πληροφοριών

Ερώτηση 5: Ο οργανισμός μου έχει θέσει σε εφαρμογή μια πολιτική ασφάλειας πληροφοριών (αναφέρεται επίσης ως Πολιτική Αποδεκτής Χρήσης).

Διάγραμμα 6 Ο οργανισμός μου έχει θέσει σε εφαρμογή μια πολιτική ασφάλειας πληροφοριών.

Ο μέσος όρος 4,9651 υποδηλώνει ότι υπάρχει γενική αντίληψη ότι ο οργανισμός έχει θέσει σε εφαρμογή πολιτική ασφάλειας πληροφοριών, αλλά ίσως αυτή δεν είναι πλήρως κατανοητή ή εφαρμοσμένη από όλους. Η τυπική απόκλιση 1,66103 δείχνει κάποια ποικιλία στις απαντήσεις.

Ο οργανισμός θα πρέπει να συνεχίσει να ενισχύει και να επικοινωνεί την πολιτική ασφάλειας πληροφοριών, διασφαλίζοντας ότι όλοι οι υπάλληλοι είναι ενήμεροι και κατανοούν τις πρακτικές ασφαλείας που εφαρμόζονται.

Ο Δημόσιος Τομέας φαίνεται να έχει καλή βάση στις προσπάθειες ασφάλειας πληροφοριών, αλλά υπάρχουν περιθώρια βελτίωσης στην εκπαίδευση και την επικοινωνία των πολιτικών ασφάλειας. Η ενίσχυση της προστασίας των πληροφοριών και η συνεπής ενημέρωση των υπαλλήλων θα βελτιώσει την εμπιστοσύνη και την αντίληψη ασφάλειας στον οργανισμό.

3.1.4 Consistency Core Values

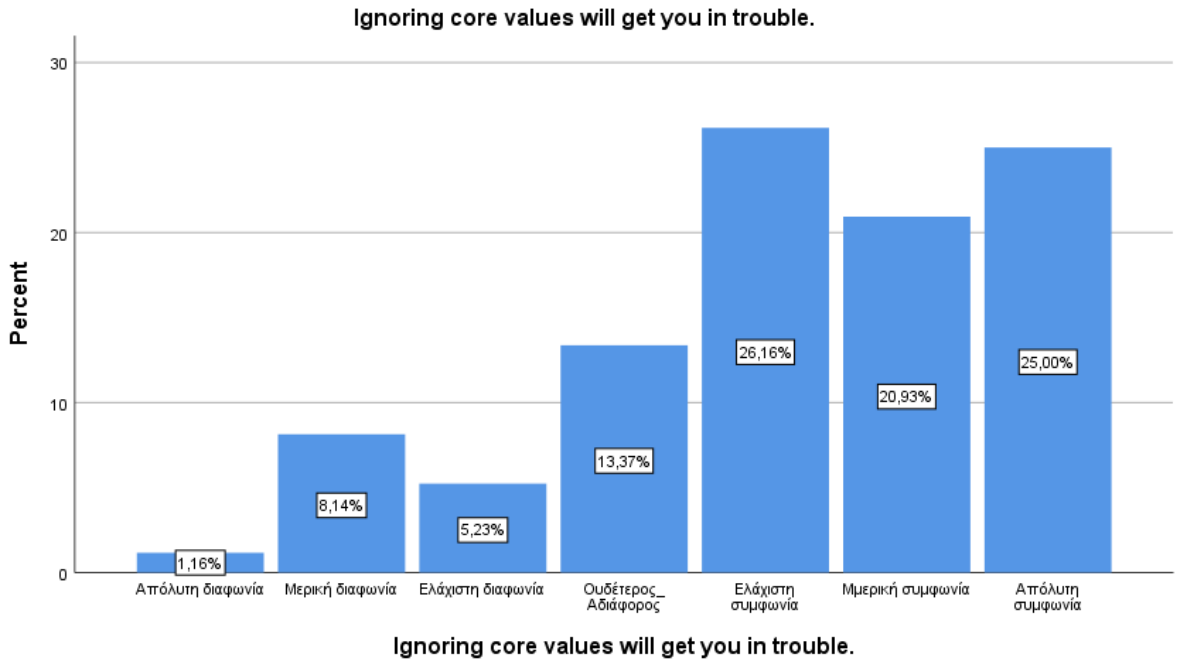
Ο παρακάτω πίνακας παρουσιάζει τα αποτελέσματα της αξιολόγησης τριών σημείων σχετικά με την ασφάλεια των πληροφοριών και την ηθική στον οργανισμό. Η ανάλυση βασίζεται σε μέσο όρο, τυπική απόκλιση, ελάχιστη και μέγιστη τιμή.

Κατηγορία	Μέσος Όρος	Τυπική Απόκλιση	Ελάχιστο	Μέγιστο
Η αγνόηση των βασικών κανόνων μπορεί να έχει δυσμενής συνέπειες	5,1802	1,56611	1	7
Η ηγεσία του Οργανισμού συμμορφώνεται και ακολουθεί τους κανόνες (προς τη κατεύθυνση της ασφάλειας των πληροφοριών) που επιβάλει στον οργανισμό	5,3605	1,6643	1	7
Υπάρχει ένας κώδικας ηθικής όπου καθοδηγεί τη συμπεριφορά μας και μας διαχωρίζει το σωστό από το λάθος.	4	1,61499	1	7

Πίνακας 3 Consistency Core Values

1. **Αγνόηση Βασικών Κανόνων**:

   Ο μέσος όρος 5,18 υποδηλώνει ότι οι περισσότεροι θεωρούν ότι η αγνόηση των βασικών κανόνων έχει σοβαρές συνέπειες. Η τυπική απόκλιση 1,57 δείχνει μια σχετική ποικιλία στις απαντήσεις, με κάποιους να αντιλαμβάνονται την κατάσταση πιο έντονα από άλλους.



Διάγραμμα 7 Η αγνόηση των βασικών κανόνων μπορεί να έχει δυσμενής συνέπειες

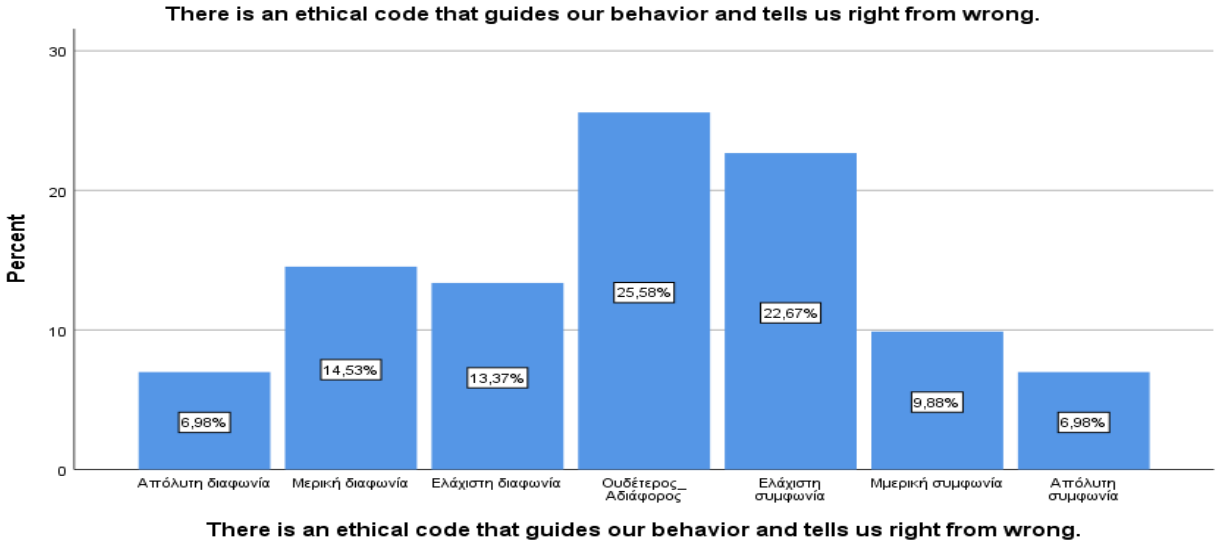
2. **Συμμόρφωση της Ηγεσίας**:

   Με μέσο όρο 5,36, φαίνεται ότι οι συμμετέχοντες γενικά συμφωνούν ότι η ηγεσία τηρεί τους κανόνες που θέτει για την ασφάλεια των πληροφοριών. Η τυπική απόκλιση 1,66 υποδηλώνει ότι υπάρχει σημαντική διαφοροποίηση στις απόψεις για τη συμμόρφωση της ηγεσίας.

Διάγραμμα 8 Η ηγεσία του Οργανισμού συμορφώνεται και ακολουθεί τους κανόνες που επιβάλει στον οργανισμό

3. **Κώδικας Ηθικής**:

   Ο μέσος όρος 4 δείχνει ότι οι απόψεις για την ύπαρξη και εφαρμογή ενός κώδικα ηθικής είναι ουδέτερες έως θετικές, αλλά δεν είναι τόσο ισχυρές όσο οι άλλες κατηγορίες. Η τυπική απόκλιση 1,61 υποδηλώνει ότι υπάρχει διαφοροποίηση στις απόψεις σχετικά με τον κώδικα ηθικής.



Διάγραμμα 9 Υπάρχει ένας κώδικας ηθικής όπου καθοδηγεί τη συμπεριφορά μας και μας διαχωρίζει το σωστό από το λάθος

Συνολικά, τα δεδομένα υποδεικνύουν ότι ενώ υπάρχει γενική συμφωνία για τη σημασία της τήρησης των κανόνων και της ηγεσίας που δείχνει το καλό παράδειγμα, υπάρχει μεγαλύτερη αβεβαιότητα σχετικά με την ύπαρξη και την αποτελεσματικότητα ενός κώδικα ηθικής στον οργανισμό. Οι ελάχιστες και μέγιστες τιμές υποδεικνύουν ότι υπάρχουν ακραίες απόψεις και στα τρία θέματα, δείχνοντας ότι οι απόψεις των εργαζομένων ποικίλλουν σημαντικά.

3.1.5 Adaptability Creating Change

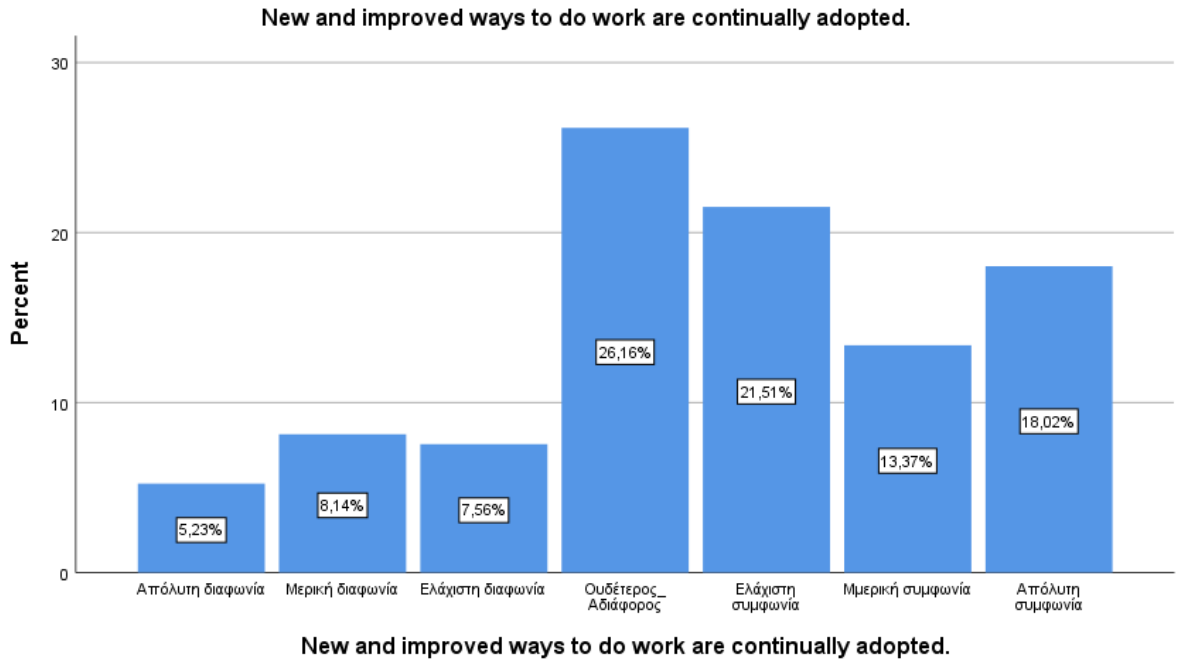
Ο παρακάτω πίνακας παρουσιάζει τα αποτελέσματα της αξιολόγησης τριών βασικών πτυχών σχετικά με την υιοθέτηση νέων τρόπων εργασίας, τις προσπάθειες για αλλαγή και τη συνεργασία μεταξύ των μερών του οργανισμού. Η ανάλυση βασίζεται σε μέσο όρο, τυπική απόκλιση, ελάχιστη και μέγιστη τιμή.

Κατηγορία	Μέσος Όρος	Τυπική Απόκλιση	Ελάχιστο	Μέγιστο
Νέοι και βελτιωμένοι τρόποι εργασίας υιοθετούνται συνεχώς.	4,6279	1,69310	1.00	7.00
Οι προσπάθειες για αλλαγή είναι συνήθως εύκολες.	3,9767	1,46680	1.00	7.00
Διάφορα μέρη του οργανισμού συνεργάζονται συχνά για τη δημιουργία αλλαγής.	3,7616	1,75590	1.00	7.00

Πίνακας 4 Adaptability Creating Change

1. **Υιοθέτηση Νέων Τρόπων Εργασίας**:

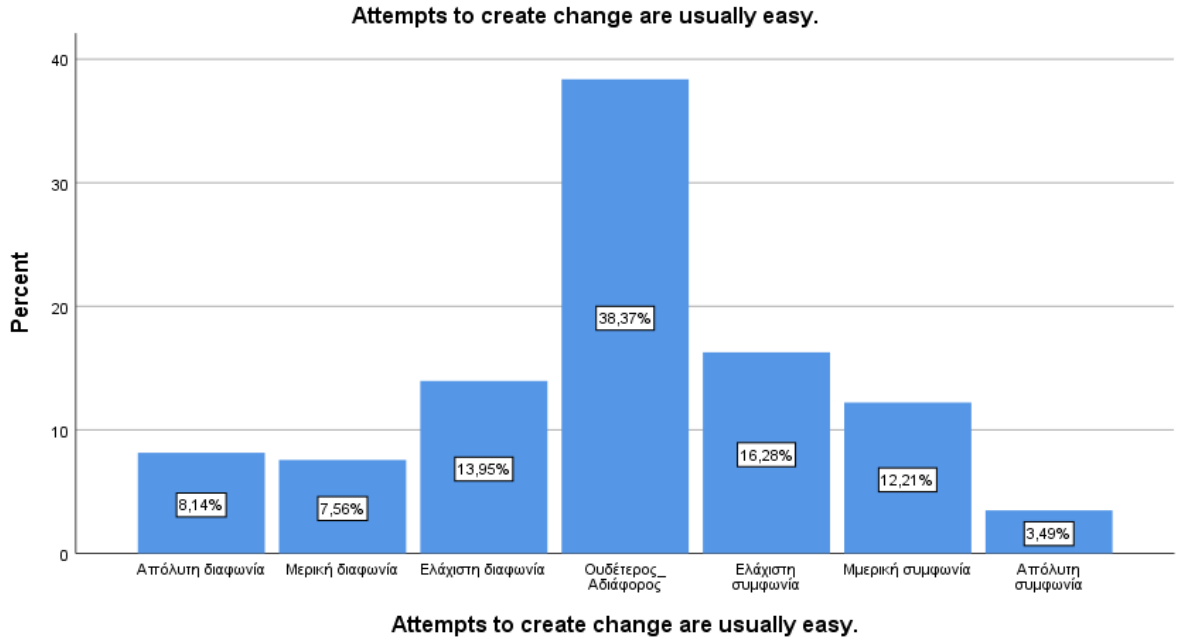
   Ο μέσος όρος 4,63 δείχνει ότι γενικά οι εργαζόμενοι πιστεύουν πως ο οργανισμός υιοθετεί νέους και βελτιωμένους τρόπους εργασίας. Η τυπική απόκλιση 1,69 υποδηλώνει ότι υπάρχουν διαφοροποιήσεις στις απόψεις των εργαζομένων. Οι ελάχιστες και μέγιστες τιμές (1 και 7 αντίστοιχα) δείχνουν ότι υπάρχουν πολύ διαφορετικές απόψεις, με κάποιους να είναι απόλυτα αρνητικοί και άλλους απόλυτα θετικοί.



Διάγραμμα 10 Υιοθετούνται συνεχώς νέες και βελτιομένες μέθοδοι εργασίας

2. **Προσπάθειες για Αλλαγή**:

Με μέσο όρο 3,98, η αντίληψη των εργαζομένων είναι κάπως ουδέτερη σχετικά με τη δήλωση αν οι προσπάθειες για αλλαγή είναι συνήθως εύκολες. Η τυπική απόκλιση 1,47 δείχνει ότι υπάρχει μια σημαντική ποικιλία στις απόψεις των εργαζομένων. Οι ελάχιστες και μέγιστες τιμές (1 και 7) δείχνουν ότι οι απόψεις ποικίλουν από πολύ αρνητικές έως πολύ θετικές.



Διάγραμμα 11 Οι προσπάθειες για αλλαγή στην ασφάλεια των πληροφοριών συνήθως γίνονται εύκολα.

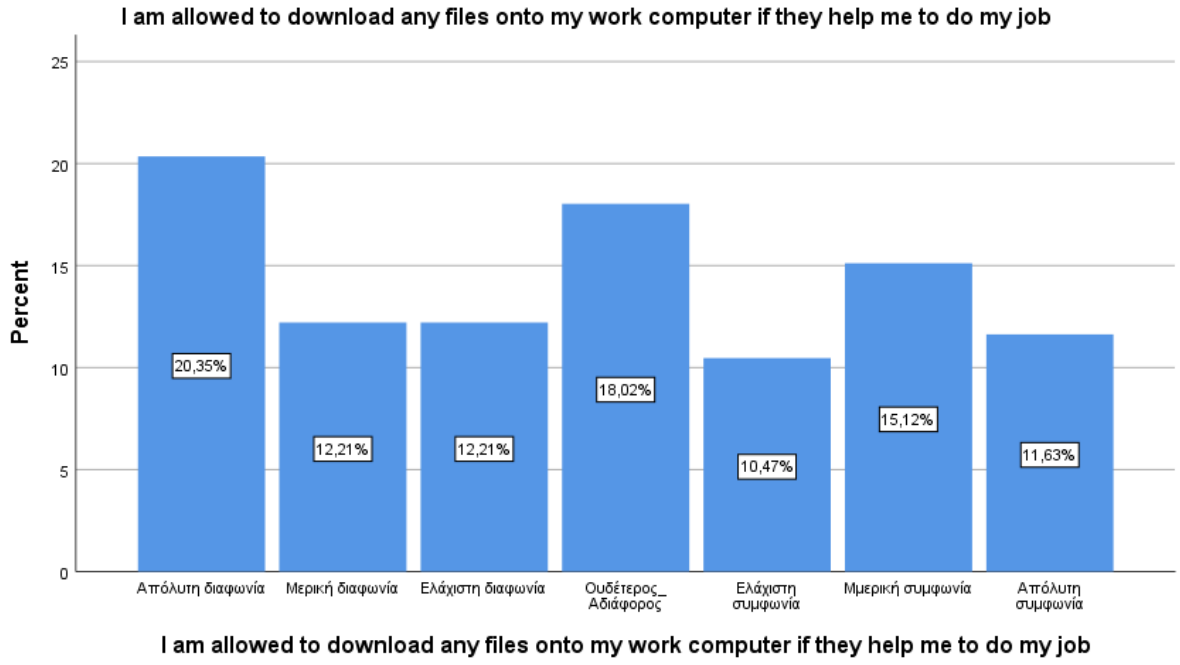
3. **Συνεργασία για Δημιουργία Αλλαγής**:

Ο μέσος όρος 3,76 υποδηλώνει ότι οι εργαζόμενοι είναι κάπως ουδέτεροι σχετικά με το αν τα διάφορα μέρη του οργανισμού συνεργάζονται συχνά για τη δημιουργία αλλαγής. Η τυπική απόκλιση 1,76 υποδηλώνει μια ακόμα μεγαλύτερη διαφοροποίηση στις απόψεις σε σχέση με τις άλλες κατηγορίες. Οι ελάχιστες και μέγιστες τιμές (1 και 7) δείχνουν ότι οι απόψεις διαφέρουν πολύ, με μερικούς να είναι απόλυτα αρνητικοί και άλλους απόλυτα θετικοί.

Διάγραμμα 12 Διαφορετικά μέρη του οργανισμού συχνά συνεργάζονται για να δημιουργήσουν αλλαγές

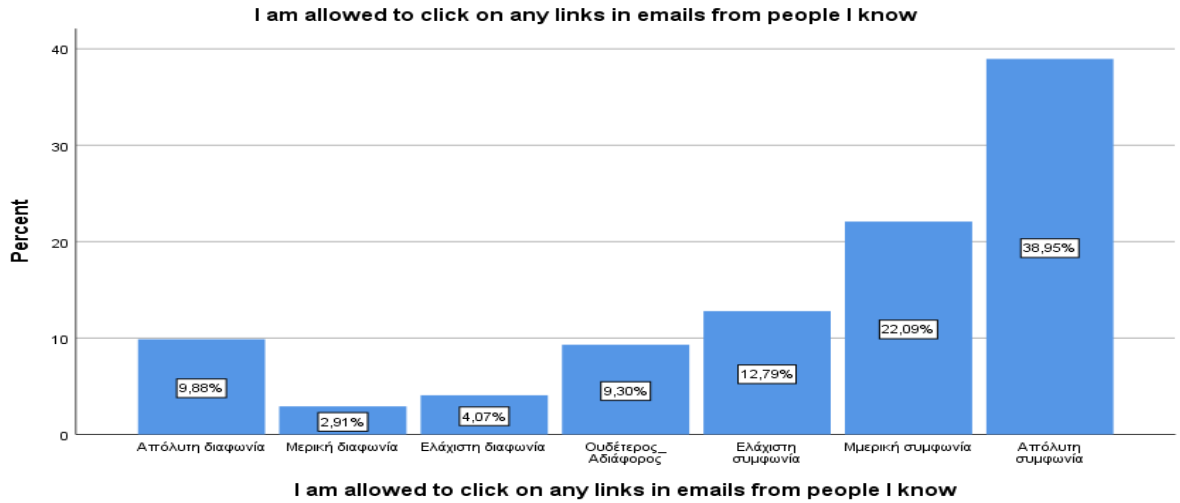
Συνολικά, τα δεδομένα υποδεικνύουν ότι υπάρχει μια σχετική ποικιλία στις απόψεις των εργαζομένων σχετικά με την υιοθέτηση νέων τρόπων εργασίας, την ευκολία των αλλαγών και τη συνεργασία μεταξύ των διαφόρων μερών του οργανισμού. Η μεγάλη τυπική απόκλιση και οι ελάχιστες και μέγιστες τιμές δείχνουν ότι οι απόψεις είναι αρκετά πολωμένες.

3.1.6 Ανάλυση συμπεριφοράς



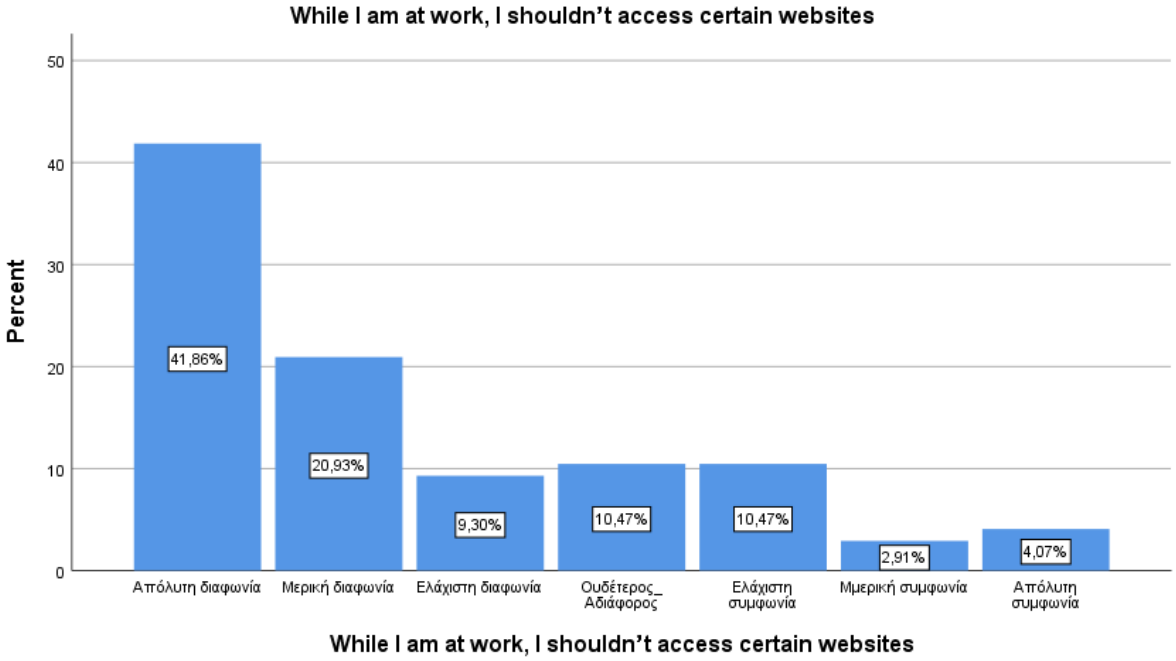
Διάγραμμα 13 Επιτρέπεται να κάνω λήψη οποιωνδήποτε αρχείων στον υπολογιστή εργασίας μου, εάν με βοηθούν να κάνω τη δουλειά μου

Το διάγραμμα 13 παρουσιάζει τις αντιδράσεις των ερωτηθέντων στη δήλωση "Μου επιτρέπεται να κατεβάζω οποιαδήποτε αρχεία στον υπολογιστή της εργασίας μου εάν με βοηθούν στη δουλειά μου." Διαπιστώνεται μια ποικιλία απόψεων σχετικά με τη λήψη αρχείων στον εργασιακό υπολογιστή. Παρόλο που το μεγαλύτερο ποσοστό των ερωτηθέντων διαφωνεί (20,35%) με την ιδέα, υπάρχει ένα σημαντικό μέρος που συμφωνεί ή είναι ουδέτερο (55,24%).



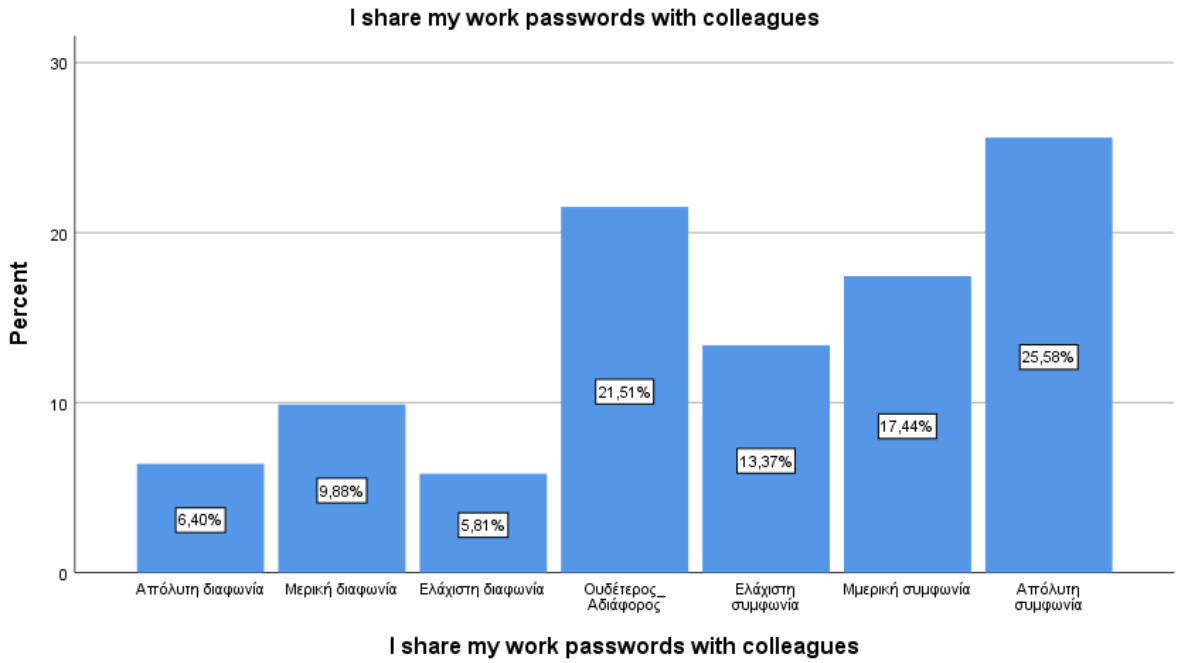
Διάγραμμα 14 Επιτρέπεται να κάνω κλικ σε συνδέσμους που εμπεριέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου από άτομα που γνωρίζω

Το διάγραμμα 14 παρουσιάζει τις αντιδράσεις των ερωτηθέντων στη δήλωση "Μου επιτρέπεται να κάνω κλικ σε οποιονδήποτε σύνδεσμο σε email από άτομα που γνωρίζω.". Το διάγραμμα δείχνει ότι ένα μεγάλο ποσοστό των ερωτηθέντων έχει υψηλή εμπιστοσύνη στα email από γνωστά άτομα, με το 38.95% να συμφωνεί απόλυτα και το 22.09% να συμφωνεί μερικώς με την ιδέα ότι επιτρέπεται να κάνουν κλικ σε οποιονδήποτε σύνδεσμο σε τέτοια email.



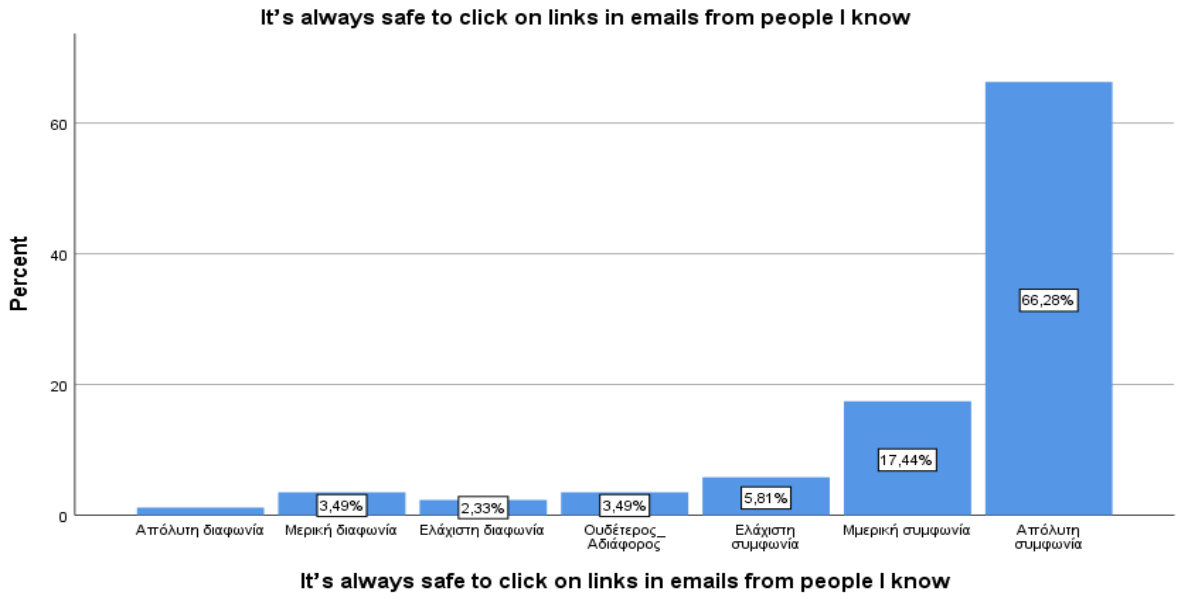
Διάγραμμα 15 Δεν πρέπει να επισκέπτομαι οποιονδήποτε ιστότοπο από τον υπολογιστή που εργάζομαι

Το διάγραμμα 15 παρουσιάζει τις άποψη των ερωτηθέντων στη δήλωση "Όταν είμαι στη δουλειά, δεν πρέπει να έχω πρόσβαση σε οποιονδήποτε ιστότοπο". Το μεγαλύτερο ποσοστό των ερωτηθέντων (41,86%) διαφωνεί απόλυτα με τη δήλωση ότι δεν πρέπει να έχουν πρόσβαση σε συγκεκριμένες ιστοσελίδες κατά τη διάρκεια της εργασίας τους. Αυτό μπορεί να υποδηλώνει ότι θεωρούν σημαντικό να έχουν πλήρη πρόσβαση στο διαδίκτυο για να εκτελούν τις εργασίες τους αποτελεσματικά.



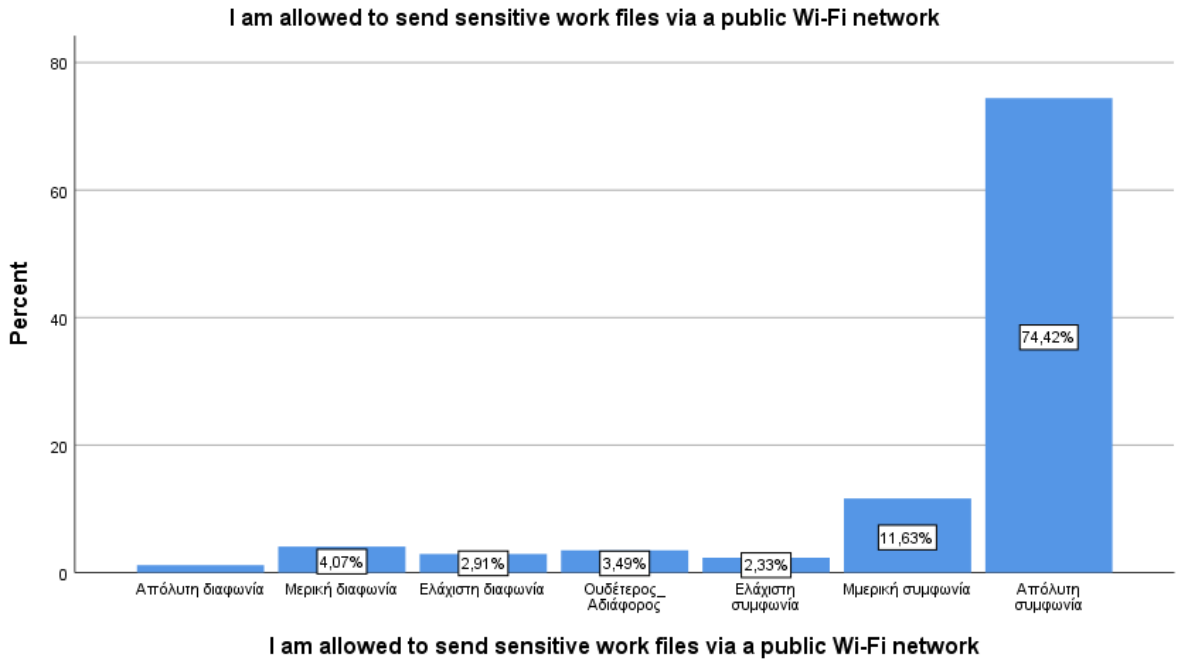
Διάγραμμα 16 Μοιράζομαι τους κωδικούς μου σε λογαριασμούς εργασίας μου με συναδέλφους

Σύμφωνα με τα αποτελέσματα του διαγράμματος 16 η πλειονότητα των ερωτηθέντων έχει θετική στάση προς την κοινοποίηση των κωδικών πρόσβασης με συναδέλφους. Το συνολικό ποσοστό των ερωτηθέντων που συμφωνούν (ελαφριά, μερική και απόλυτη συμφωνία) είναι υψηλό, υποδεικνύοντας ότι πολλοί θεωρούν ότι η κοινοποίηση των κωδικών είναι αποδεκτή ή ακόμη και αναγκαία σε συγκεκριμένες περιπτώσεις.



Διάγραμμα 17 Είναι πάντα ασφαλές να κάνω "κλικ" σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου από αποστολέα που γνωρίζω

Το διάγραμμα 17 παρουσιάζει τις αντιδράσεις των ερωτηθέντων στη δήλωση "Είναι πάντα ασφαλές να κάνετε κλικ σε συνδέσμους σε emails από άτομα που γνωρίζω". Το μεγαλύτερο ποσοστό των ερωτηθέντων, 66,28%, συμφωνεί απόλυτα με την ιδέα ότι είναι πάντα ασφαλές να κάνουν κλικ σε συνδέσμους σε emails από γνωστά άτομα. Ένα πολύ μικρό ποσοστό των ερωτηθέντων διαφωνεί απόλυτα με την ιδέα.



Διάγραμμα 18 Επιτρέπεται να χρησιμοποιώ δημόσιο δίκτυο Wi-Fi για την αποστολή ευαίσθητων αρχείων ή για πρόσβαση σε σημαντικούς λογαριασμούς

Σύμφωνα με τα δεδομένα του διαγράμματος 18, το οποίο αναλύει τις αντιδράσεις των ερωτηθέντων στη δήλωση "Επιτρέπεται να στέλνω ευαίσθητα εργασιακά αρχεία μέσω δημόσιου δικτύου Wi-Fi." Διαπιστώνεται ότι ένα πολύ μικρό ποσοστό των ερωτηθέντων διαφωνεί απόλυτα με την ιδέα να στέλνουν ευαίσθητα εργασιακά αρχεία μέσω δημόσιου δικτύου Wi-Fi, κατανοώντας τους κινδύνους που σχετίζονται με την ασφάλεια αυτής της πρακτικής. Το μεγαλύτερο ποσοστό των ερωτηθέντων, 74,42%, συμφωνεί απόλυτα με την ιδέα να στέλνουν ευαίσθητα αρχεία μέσω δημόσιου δικτύου Wi-Fi, υποδηλώνοντας μια ισχυρή πεποίθηση ότι αυτή η πρακτική είναι ασφαλής

3.2 Επαγωγική στατιστική

Ερευνητική υπόθεση 1: Η ηλικία του εργαζομένου επηρεάζει το βαθμό που αντιλαμβάνονται ότι ο οργανισμός δημιουργεί ευαισθητοποίηση στους εργαζόμενους για θέματα ασφάλειας των πληροφοριακών συστημάτων.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
My organization creates awareness among employees about information security.	**18-29**	**6**	**6.1667**	**1.16905**	**.47726**	**4.9398**	**7.3935**	**4.00**	7.00
	30-39	**24**	**5.0833**	**2.35753**	**.48123**	**4.0878**	**6.0788**	**1.00**	7.00
	40-49	**61**	**6.0492**	**1.75524**	**.22474**	**5.5996**	**6.4987**	**1.00**	7.00
	50-59	**75**	**6.6133**	**.89885**	**.10379**	**6.4065**	**6.8201**	**2.00**	7.00
	>60	**6**	**6.3333**	**1.21106**	**.49441**	**5.0624**	**7.6043**	**4.00**	7.00
	Total	**172**	**6.1744**	**1.58717**	**.12102**	**5.9355**	**6.4133**	**1.00**	7.00

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
My organisation creates awareness among employees about information security.	Between Groups	44.128	4	11.032	4.765	.001
	Within Groups	386.639	167	2.315		
	Total	430.767	171			

Πίνακας 5 ANOVA - ερευνητική υπόθεση 1η

Bonferroni

Dependent Variable	(I) Ηλικία	(J) Ηλικία	Mean Difference (I-J)	Sig.
My organisation creates awareness among employees about information security.	18-29	30-39	1.08333	1.000
		40-49	.11749	1.000
		50-59	-.44667	1.000
		>60	-.16667	1.000
	30-39	18-29	-1.08333	1.000
		40-49	-.96585	.092
		50-59	-1.53000*	.000
		>60	-1.25000	.737

Στη διερεύνηση των αντιλήψεων όσων συμμετείχαν στην έρευνα καταλήξαμε στα ακόλουθα: σχετικά με την ερώτηση: My organization creates awareness among employees about information security:

Το F στατιστικό F(4, 167) = 4.765, είναι στατιστικά σημαντικό με επίπεδο σημαντικότητας (p = .001), και ελέγχουμε τα αποτελέσματα διορθωμένα με πολλαπλές συγκρίσεις σύμφωνα με τη διόρθωση Bonferroni, φαίνεται ότι υπάρχει στατιστικά σημαντική διαφορά ανάμεσα σε διαφορετικές ηλικιακές ομάδες ως προς την ευαισθητοποίηση των υπαλλήλων σχετικά με την ασφάλεια των πληροφοριών. Η μέση διαφορά (-1,5300, p=0.000) υποδεικνύει ότι οι εργαζόμενοι που ανήκουν στην ηλικιακή ομάδα 50-59 ετών (mean=6.6133) αντιλαμβάνονται ότι ο οργανισμός τους δημιουργεί μεγαλύτερη ευαισθητοποίηση στους εργαζόμενους σχετικά με εργαζόμενους που ανήκουν στην ηλικιακή ομάδα 30-39 (mean=5.08330 σχετικά με την ασφάλεια των πληροφοριακών συστημάτων.

Ερευνητική υπόθεση 2: Η ηλικία επηρεάζει την αντίληψη των υπαλλήλων σχετικά με τη σημασία της τήρησης των βασικών αξιών στον οργανισμό.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Ignoring core values will get you in trouble.	**18-29**	**6**	**5.0000**	**1.41421**	**.57735**	**3.5159**	**6.4841**	3.00	7.00
	30-39	**24**	**4.0000**	**1.56038**	**.31851**	**3.3411**	**4.6589**	2.00	7.00
	40-49	**61**	**5.1475**	**1.61076**	**.20624**	**4.7350**	**5.5601**	1.00	7.00
	50-59	**75**	**5.5600**	**1.39729**	**.16135**	**5.2385**	**5.8815**	2.00	7.00
	>60	**6**	**5.6667**	**1.21106**	**.49441**	**4.3957**	**6.9376**	4.00	7.00
	Total	**172**	**5.1802**	**1.56611**	**.11941**	**4.9445**	**5.4159**	1.00	7.00

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Ignoring core values will get you in trouble.	Between Groups	45.927	4	11.482	5.134	.001
	Within Groups	373.485	167	2.236		
	Total	419.413	171			

Πίνακας 6 ANOVA - ερευνητική υπόθεση 2η

Ignoring core values will get you in trouble.	18-29	30-39	1,00000
		40-49	-,14754
		50-59	-,56000
		>60	-,66667
	30-39	18-29	-1,00000
		40-49	-1,14754*
		50-59	-1,56000*
		>60	-1,66667
	40-49	18-29	,14754
		30-39	1,14754*
		50-59	-,41246

Η ανάλυση ANOVA δείχνει ότι υπάρχουν στατιστικά σημαντικές διαφορές στις αντιλήψεις των εργαζομένων σχετικά με την πρόταση "Ignoring core values will get you in trouble" (p = .001). Συγκεκριμένα, οι αντιλήψεις ανάμεσα διαφέρουν στατιστικά σημαντικά ως προς το πώς αντιλαμβάνονται τη σημασία της τήρησης των βασικών αξιών.

Συγκεκριμένα, η ανάλυση με πολλαπλές συγκρίσεις (post hoc analysis) με την διόρθωση bonferoni δείχνει ότι η μέση διαφορά (1,14754, p=0.00) στις αντιλήψεις των υπάλληλων ηλικίας 30-39 ετών (mean= 4.000) διαφέρουν στατιστικά σημαντικά από τις αντιλήψεις των εργαζομένων ηλικιακής ομάδας 40-49 (mean=5.1475). Άρα, οι νεότεροι εργαζόμενοι δεν θεωρούν ότι η αδιαφορία ως προς τη χρήση πληροφοριακών συστημάτων μπορεί να προκαλέσει προβλήματα στη λειτουργία του οργανισμού.

Τα αποτελέσματα αυτά υποδεικνύουν ότι η ηλικία επηρεάζει την αντίληψη των υπαλλήλων σχετικά με τη σημασία της τήρησης των βασικών αξιών στον οργανισμό. Οι μεγαλύτερης ηλικίας υπάλληλοι τείνουν να συμφωνούν περισσότερο ότι η αγνόηση των βασικών αξιών θα δημιουργήσει προβλήματα, ενώ οι νεότεροι υπάλληλοι είναι λιγότερο πιθανό να συμφωνούν με αυτήν την πρόταση.

Ερευνητική υπόθεση 3: Η ηλικία επηρεάζει το βαθμό συμφωνίας ότι οι ευαίσθητες πληροφορίες μπορεί να δημιουργήσουν σοβαρά προβλήματα αν διαρρεύσουν.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
It's risky to access sensitive work files on a laptop if strangers can see my screen	**18-29**	**6**	**5.0000**	**1.54919**	**.63246**	**3.3742**	**6.6258**	4.00	7.00
	30-39	**24**	**3.5417**	**1.76879**	**.36105**	**2.7948**	**4.2886**	1.00	7.00
	40-49	**61**	**4.4754**	**1.63917**	**.20987**	**4.0556**	**4.8952**	1.00	7.00
	50-59	**75**	**4.9333**	**1.75787**	**.20298**	**4.5289**	**5.3378**	1.00	7.00
	>60	**6**	**6.5000**	**.54772**	**.22361**	**5.9252**	**7.0748**	6.00	7.00
	Total	**172**	**4.6337**	**1.76702**	**.13473**	**4.3678**	**4.8997**	1.00	7.00

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
It's risky to access sensitive work files on a laptop if strangrers can see my screen	Between Groups	58.586	4	14.647	5.146	.001
	Within Groups	475.338	167	2.846		
	Total	533.924	171			

Πίνακας 7 ANOVA - ερευνητική υπόθεση 3η

Dependent Variable	(I) Ηλικία	(J) Ηλικία	Mean Difference (I-J)	Sig.
It's risky to access sensitive work files on a laptop if strangers can see my screen	**18-29**	**30-39**	**1.45833**	**.600**
		40-49	**.52459**	**1.000**
		50-59	**.06667**	**1.000**
		>60	**-1.50000**	**1.000**
	30-39	**18-29**	**-1.45833**	**.600**
		40-49	**-.93374**	**.229**
		50-59	**-1.39167***	**.006**
		>60	**-2.95833***	**.002**
	40-49	**18-29**	**-.52459**	**1.000**
		30-39	**.93374**	**.229**
		50-59	**-.45792**	**1.000**
		>60	**-2.02459**	**.056**

Η ανάλυση ANOVA δείχνει ότι υπάρχει στατιστικά σημαντική διαφορά (p=.001) στην αντίληψη των διαφορετικών ηλικιακών ομάδων σχετικά με το πόσο επικίνδυνο θεωρούν την πρόσβαση σε ευαίσθητα αρχεία σε έναν φορητό υπολογιστή όταν οι ξένοι μπορούν να δουν την οθόνη τους.

Η ηλικιακή ομάδα εργαζομένων 18-29 ετών και η ηλικιακή ομάδα μεγαλύτερη των 60 ετών, δείχνουν υψηλότερη ανησυχία (μέσες τιμές 5.0000 και 6.5000 αντίστοιχα). Η ομάδα 30-39 δείχνει τη χαμηλότερη ανησυχία με μέση τιμή 3.5417. Οι ομάδες 40-49 και 50-59 βρίσκονται σε ενδιάμεσο επίπεδο ανησυχίας (μέσες τιμές 4.4754 και 4.9333 αντίστοιχα).

Συγκεκριμένα, η ανάλυση με πολλαπλές συγκρίσεις (post hoc analysis) με την διόρθωση bonferroni δείχνει ότι η μέση διαφορά (2.95833, p=.002) στις αντιλήψεις των υπάλληλων ηλικίας 30-39 ετών (mean= 3.5417) διαφέρουν στατιστικά σημαντικά από τις αντιλήψεις των εργαζομένων ηλικιακής ομάδας >60 (mean=6.500). Αρα, οι νεότεροι εργαζόμενοι έχουν χαμηλότερη αντίληψη σχετικά με το βαθμό επικινδυνότητας αυτής της συμπεριφοράς.

Τα αποτελέσματα αυτά υποδεικνύουν και σε αυτή τη περίπτωση ότι η ηλικία επηρεάζει την αντίληψη των υπαλλήλων. Οι μεγαλύτερης ηλικίας υπάλληλοι τείνουν να συμφωνούν περισσότερο ότι οι ευαίσθητες πληροφορίες μπορεί να δημιουργήσουν σοβαρά προβλήματα αν διαρρεύσουν, ενώ οι νεότεροι υπάλληλοι είναι λιγότερο πιθανό να συμφωνούν με αυτήν την πρόταση.

Ερευνητική υπόθεση 4: Το επίπεδο σπουδών επηρεάζει την αντίληψη που έχουν για το πόσο συχνά συνεργάζονται τα διάφορα μέρη του οργανισμού για να δημιουργήσουν αλλαγή.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Different parts of the organization often cooperate to create change.	Απόφοιτος Λυκείου	13	5.3077	1.25064	.34687	4.5519	6.0634	3.00	7.00
	Απόφοιτος Ανώτερων Σχολών	8	4.7500	1.90863	.67480	3.1543	6.3457	2.00	7.00
	Απόφοιτος Πανεπιστημίου	52	3.7308	1.77251	.24580	3.2373	4.2242	1.00	7.00
	Απόφοιτος Μεταπτυχιακού Προγράμματος Σπουδών	95	3.4947	1.68771	.17316	3.1509	3.8385	1.00	7.00
	Απόφοιτος Διδακτορικού Προγράμματος Σπουδών	4	3.5000	1.73205	.86603	.7439	6.2561	2.00	6.00
	Total	172	3.7616	1.75590	.13389	3.4973	4.0259	1.00	7.00

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Different parts of the organization often cooperate to create change.	Between Groups	45.979	4	11.495	3.989	.004
	Within Groups	481.247	167	2.882		
	Total	527.227	171			

Πίνακας 8 ANOVA ερευνητική υπόθεση 4η

	(I) Εκπαίδευση	(J) Εκπαίδευση	Mean Difference (I-J)	Sig.
Different parts of the organization often cooperate to create change.	Απόφοιτος Μεταπτυχιακού Προγράμματος Σπουδών	**Απόφοιτος Λυκείου**	**-1.81296***	**.004**
		Απόφοιτος Ανώτερων Σχολών	**-1.25526**	**.462**
		Απόφοιτος Πανεπιστημίου	**-.23603**	**1.000**
		Απόφοιτος Διδακτορικού Προγράμματος Σπουδών	**-.00526**	**1.000**

Η τιμή Sig. (p-value) είναι 0.004, είναι μικρότερη από το επίπεδο σημαντικότητας 0.05. Αυτό δείχνει ότι υπάρχει στατιστικά σημαντική διαφορά μεταξύ των διαφορετικών ομάδων σχετικά με την αντίληψη που έχουν για το πόσο συχνά συνεργάζονται τα διάφορα μέρη του οργανισμού για να δημιουργήσουν αλλαγή.

Συγκεκριμένα, η ανάλυση με πολλαπλές συγκρίσεις (post hoc analysis) με την διόρθωση bonferoni δείχνει ότι η μέση διαφορά (1.81296, p=.004) στις αντιλήψεις των υπάλληλων που είναι απόφοιτοι Λυκείου (mean= 5.3077) διαφέρουν στατιστικά σημαντικά από τις αντιλήψεις των εργαζομένων που είναι απόφοιτοι μεταπτυχιακού προγράμματος σπουδών (mean=3.4947). Επίσης, παρόμοια διαφορά παρατηρούμε και με τους υπαλλήλους οι οποίοι είναι κάτοχοι διδακτορικού τίτλου σπουδών (mean=3.5000).

Οι απόφοιτοι λυκείου και ανώτερων σχολών τείνουν να θεωρούν ότι υπάρχει μεγαλύτερη συνεργασία εντός του οργανισμού για τη δημιουργία αλλαγών σε σύγκριση με τους αποφοίτους διδακτορικού και μεταπτυχιακών προγραμμάτων.

Ερευνητική υπόθεση 5: Το φύλο επηρεάζει το βαθμό που ο εργαζόμενος πιστεύει ότι επιτρέπεται να κάνει «κλικ» σε συνδέσμους που προέρχονται από άγνωστο αποστολέα.

Group Statistics

	Φύλλο Υπαλλήλου	N	Mean	Std. Deviation	Std. Error Mean
I am not permitted to click on a link in an email from an unknown sender	**Άνδρας**	**53**	**5.4906**	**2.21553**	**.30433**
	Γυναίκα	**119**	**6.0000**	**1.69246**	**.15515**

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference Lower	Upper
I am not permitted to click on a link in an email from an unknown sender	**Equal variances assumed**	**12.237**	**.001**	**-1.651**	**170**	.101	-.50943	.30849	-1.11840	.09954
	Equal variances not assumed			**-1.491**	**80.156**	.140	-.50943	.34159	-1.18920	.17034

*Πίνακας **9** Independent Samples Test ερευνητική υπόθεση 5η*

Σύμφωνα με τον έλεγχο Levene δεν παρατηρείται ομοιογένεια διακυμάνσεων (F = 12.237, Sig. = .001) και δεν παρατηρείται στατιστικά σημαντική διαφορά ανάμεσα στους μέσους των ανδρών και των γυναικών ως προς την αντίληψη τους για τη πρόταση «I am not permitted to click on a link in an email from an unknown sender».

Ερευνητική υπόθεση 6: Το φύλο επηρεάζει το βαθμό συμφωνίας ότι επιτρέπεται η αποστολή ευαίσθητων εργασιακών αρχείων μέσω δημόσιου Wi-Fi δικτύου.

Group Statistics

	Φύλλο Υπαλλήλου	N	Mean	Std. Deviation	Std. Error Mean
I am allowed to send sensitive work files via a public Wi-Fi network	**Άνδρας**	**53**	**5.9623**	**1.74270**	**.23938**
	Γυναίκα	**119**	**6.5126**	**1.21338**	**.11123**

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference Lower	Upper
I am allowed to send sensitive work files via a public Wi-Fi network	**Equal variances assumed**	**12.280**	**.001**	**-2.386**	**170**	.018	-.55034	.23066	-1.00567	-.09501
	Equal variances not assumed			**-2.085**	**75.331**	.040	-.55034	.26396	-1.07614	-.02455

Πίνακας 10 Independent Samples Test ερευνητική υπόθεση 6η

Σύμφωνα με τον έλεγχο Levene δεν παρατηρείται ομοιογένεια διακυμάνσεων (F = 12.280**,** Sig. = .001) και παρατηρείται στατιστικά σημαντική διαφορά στους μέσους των ανδρών και των γυναικών ως προς την αντίληψη τους για **I am allowed to send sensitive work files via a public Wi-Fi network.** Συγκεκριμένα, t=-2.085, df(75.331) p=0.40<0.05.

Τα αποτελέσματα της ανάλυσης δείχνουν ότι υπάρχει στατιστικά σημαντική διαφορά μεταξύ των μέσων όρων των ανδρών (mean=**5.9623)** και των γυναικών (mean=**6.5126)** σχετικά με τη δήλωση "I am allowed to send sensitive work files via a public Wi-Fi network". Οι γυναίκες έχουν σημαντικά υψηλότερο μέσο όρο σε σχέση με τους άνδρες, υποδηλώνοντας ότι οι γυναίκες είναι πιθανότερο να θεωρούν ότι επιτρέπεται η αποστολή ευαίσθητων εργασιακών αρχείων μέσω δημόσιου Wi-Fi δικτύου.

Ερευνητική υπόθεση 7: Το φύλο του εργαζομένου επηρεάζει το βαθμό που αντιλαμβάνονται ότι ο οργανισμός δημιουργεί ευαισθητοποίηση μεταξύ των εργαζομένων για θέματα ασφάλειας των πληροφοριακών συστημάτων.

Group Statistics

Φύλλο Υπαλλήλου	N	Mean	Std. Deviation	Std. Error Mean
Άνδρας	**53**	**5.3962**	**2.33979**	**.32139**
Γυναίκα	**119**	**6.5210**	**.91918**	**.08426**

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference Lower	Upper
My organisation creates awareness among employees about information security.	**Equal variances assumed**	**101.749**	**.000**	**-4.530**	**170**	.000	-1.12478	.24832	-1.61496	-.63460
	Equal variances not assumed			**-3.385**	**59.271**	.001	-1.12478	.33226	-1.78956	-.46000

Πίνακας 11 Independent Samples Test ερευνητική υπόθεση 7η

Σύμφωνα με τον έλεγχο Levene δεν παρατηρείται ομοιογένεια διακυμάνσεων (F = 101.749**,** Sig. = .000) και παρατηρείται στατιστικά σημαντική διαφορά στους μέσους των ανδρών και των γυναικών ως προς την αντίληψη τους για **τη δημιουργία ευαισθητοποίησης που δημιουργεί ο οργανισμός για την ασφάλεια των πληροφοριακών συστημάτων.** Συγκεκριμένα, t=-3385, df (59271) p=0.001.

Τα αποτελέσματα της ανάλυσης δείχνουν ότι υπάρχει στατιστικά σημαντική διαφορά μεταξύ των μέσων όρων των ανδρών (mean=**5.3962)** και των γυναικών (mean=**6.5210)** σχετικά με τη δήλωση "Ο οργανισμός μου δημιουργεί ευαισθητοποίηση μεταξύ των εργαζομένων σχετικά με την ασφάλεια των πληροφοριών". Επίσης, η τυπική απόκλιση για τους άνδρες είναι μεγαλύτερη, υποδεικνύοντας μεγαλύτερη διακύμανση στις απαντήσεις τους σε σύγκριση με τις γυναίκες. Οι αντιλήψεις για την ευαισθητοποίηση σχετικά με την ασφάλεια πληροφοριών διαφέρουν σημαντικά ανάμεσα στα φύλα, με τις γυναίκες να έχουν πιο θετική αξιολόγηση σε σύγκριση με τους άνδρες.

Ερευνητική υπόθεση 8: Το φύλο του εργαζομένου επηρεάζει την αντίληψη του σχετικά με το βαθμό που η διοίκηση συμμορφώνεται με τους κανόνες.

Group Statistics

	Φύλλο Υπαλλήλου	N	Mean	Std. Deviation	Std. Error Mean
The leaders and managers "practice what they preach".	**Άνδρας**	**53**	**4.6415**	**2.04840**	**.28137**
	Γυναίκα	**119**	**5.6807**	**1.35254**	**.12399**

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference Lower	Upper
The leaders and managers "practice what they preach".	**Equal variances assumed**	**20.987**	**.000**	**-3.938**	**170**	.000	-1.03916	.26388	-1.56006	-.51827
	Equal variances not assumed			**-3.380**	**72.943**	.001	-1.03916	.30748	-1.65197	-.42636

Πίνακας 12 Independent Samples Test ερευνητική υπόθεση 8η

Σύμφωνα με τον έλεγχο Levene δεν παρατηρείται ομοιογένεια διακυμάνσεων (F = 101.749**,** Sig. = .000) και παρατηρείται στατιστικά σημαντική διαφορά στους μέσους των ανδρών και των γυναικών ως προς την αντίληψη σχετικά με το βαθμό συμμόρφωσης της ηγεσίας με τους κανόνες προς τη κατεύθυνση της ασφάλειας των πληροφοριών. Συγκεκριμένα, t=-3.380, df(72943), p=0.001.

Τα αποτελέσματα της ανάλυσης δείχνουν ότι υπάρχει στατιστικά σημαντική διαφορά μεταξύ των μέσων όρων των ανδρών (mean=**4.6415)** και των γυναικών (mean=**5.6807)** σχετικά με τη δήλωση **"**η ηγεσία του Οργανισμού συμμορφώνεται και ακολουθεί τους κανόνες (προς τη κατεύθυνση της ασφάλειας των πληροφοριών) που επιβάλει στον οργανισμό". Επίσης, η τυπική απόκλιση για τους άνδρες είναι μεγαλύτερη, υποδεικνύοντας μεγαλύτερη διακύμανση στις απαντήσεις τους σε σύγκριση με τις γυναίκες.

Κεφάλαιο 4ο Συζήτηση - Συμπεράσματα – Περιορισμοί - Προτάσεις

Στη παρούσα έρευνα, σε θεωρητικό επίπεδο έγινε μία προσπάθεια να κατανοήσουμε τον καθοριστικό ρόλο που διαδραματίζει ο ανθρώπινος παράγοντας στην ασφάλεια των πληροφοριακών συστημάτων. Αν και η τεχνολογία μπορεί να παρέχει ισχυρά εργαλεία για την προστασία δεδομένων και συστημάτων, η ανθρώπινη συμπεριφορά και οι αποφάσεις αποτελούν τον πλέον κρίσιμο παράγοντα.

Στο ερευνητικό μέρος αξιολογήθηκαν οι γνώσεις και η συμπεριφορά ενός δείγματος 172 υπαλλήλων του δημοσίου τομέα, σε ορισμένους τομείς σχετικά με την ασφάλεια των πληροφοριακών συστημάτων. Επιπρόσθετα, σκοπός του ερωτηματολογίου είναι να αξιολογήσει την άποψη των εργαζομένων για θέματα όπως η οργάνωση εκπαιδεύσεων, η συμπεριφορά της διοίκησης και η δημιουργία κουλτούρας προσανατολισμένης στην ασφάλεια.

Το προφίλ των συμμετεχόντων στην έρευνα είναι στη πλειοψηφία τους γυναίκες με ποσοστό 69.2%, όπου το 44.8% εργάζεται στο δημόσιο τομέα περισσότερα από 15 χρόνια και το 25% πλέον των 26 ετών ενώ λιγότερο από 5 χρόνια εργάζεται το μικρότερο ποσοστό (9.9%). Το μεγαλύτερο ποσοστό είναι ηλικίας 50-59 ετών (43.6%), αντίθετα μόλις το 3.5% είναι στην ηλικιακή ομάδα 18-29 ετών. Απόφοιτοι Λυκείου είναι το 7.6% των συμμετεχόντων ενώ περισσότεροι από τους μισούς είναι απόφοιτοι μεταπτυχιακού προγράμματος σπουδών (55.2%) και το 2.3% κατέχει διδακτορικό δίπλωμα. Τέλος, οι συμμετέχοντες προέρχονται από διάφορους φορείς του ελληνικού δημοσίου με το 34.9% να εργάζεται στη τοπική αυτοδιοίκηση, το 26.7% σε Υπουργεία και τις υπηρεσίες αυτών, 23.3% σε Νομικά Πρόσωπα Δημοσίου Δικαίου και σε δημόσια Νομικά Πρόσωπα Ιδιωτικού Δικαίου ενώ το μικρότερο ποσοστό (15.1%) σε λοιπούς οργανισμούς και Ανεξάρτητες Αρχές.

Αναφορικά με το βαθμό ικανοποίησης των υπαλλήλων σχετικά με την ευαισθητοποίησή τους για την ασφάλεια των πληροφοριακών συστημάτων, παρατηρείται (Διάγραμμα 1) ότι η πλειοψηφία των υπαλλήλων είναι είτε ουδέτερη είτε δεν είναι απόλυτα ικανοποιημένη με την ευαισθητοποίησή τους για την ασφάλεια των πληροφοριακών συστημάτων. Μόλις το 2.33% των ερωτηθέντων δηλώνει απόλυτα ικανοποιημένο, δείχνοντας ότι υπάρχει σημαντικό περιθώριο για βελτίωση και ενίσχυση των σχετικών εκπαιδευτικών προγραμμάτων.

Η οργανωτική κουλτούρα του οργανισμού αξιολογήθηκε μέσα από πέντε ερωτήσεις οι οποίες εξετάζουν τις πιο σημαντικές πτυχές που περιγράφουν μια κουλτούρα τμήμα της οποίας αποτελεί η ασφάλεια των πληροφοριών. Στην ερώτηση «Ο οργανισμός μου ενημερώνει τους υπαλλήλους για την ασφάλεια των πληροφοριών» ο μέσος όρος των απαντήσεων δείχνει ότι οι υπάλληλοι γενικά συμφωνούν ότι ο οργανισμός τους ενημερώνει για την ασφάλεια των πληροφοριών, δείχνοντας ότι οι οργανισμοί προσπαθούν να ευαισθητοποιήσουν τους εργαζομένους προς τη κατεύθυνση αυτή.

Ωστόσο, στη δήλωση «Πιστεύω ότι οι πληροφορίες στον οργανισμό μου προστατεύονται επαρκώς» ο μέσος όρος (3,7093) είναι ιδιαίτερα χαμηλός, υποδεικνύοντας ότι οι υπάλληλοι έχουν αμφιβολίες σχετικά με την επάρκεια προστασίας των πληροφοριών. Στη τρίτη ερώτηση, «Πιστεύω ότι όλοι στον οργανισμό μου θέλουν να προστατεύσουν τις οργανωτικές πληροφορίες» σύμφωνα με το μέσο όρο (4,9302) οι υπάλληλοι γενικά πιστεύουν ότι υπάρχει διάθεση για προστασία των πληροφοριών, αλλά όχι με μεγάλη βεβαιότητα. Διαπιστώνουμε αυξημένη προθυμία των υπαλλήλων να προστατεύσουν τις πληροφορίες, αλλά ο οργανισμός θα πρέπει να ενισχύσει τις προσπάθειες για να ευθυγραμμίσει όλα τα μέρη προς αυτόν τον στόχο. Αναφορικά με την εισαγωγική εκπαίδευση των νέων υπαλλήλων, ο μέσος όρος (4,4709) δείχνει ότι η εκπαίδευση για την ασφάλεια των πληροφοριών κατά την ένταξη δεν είναι τόσο ισχυρή και δε πραγματοποιείται πάντα εκπαίδευση, δηλώντας απόλυτη συμφωνία μόλις το 19.8%. Επιπρόσθετα, η υψηλή τυπική απόκλιση υποδεικνύει μεγάλη ποικιλία στις εμπειρίες των υπαλλήλων σχετικά με αυτό το θέμα. Αναφορικά με την ύπαρξη πολιτικής ασφαλείας παρατηρούμε (Διάγραμμα 6) ότι η πλειοψηφία των υπαλλήλων έχει θετική άποψη για την ύπαρξη και εφαρμογή μιας πολιτικής ασφάλειας πληροφοριών στον οργανισμό τους, με τις μεγαλύτερες κατηγορίες να βρίσκονται στις ομάδες της ελάχιστης, μερικής και απόλυτης συμφωνίας. Ωστόσο, υπάρχει και ένα ποσοστό που είτε είναι αδιάφορο είτε διαφωνεί, υποδεικνύοντας την ανάγκη για περαιτέρω ενημέρωση σχετικά με τη πολιτική ασφαλείας, η οποία θα πρέπει να είναι γνωστή σε όλο το προσωπικό.

Σχετικά με την αντίληψη των συμμετεχόντων στην έρευνα, ότι η αγνόηση των βασικών κανόνων μπορεί να έχει δυσμενείς συνέπειες, ο μέσος όρος (5,1802) δείχνει ότι οι υπάλληλοι γενικά συμφωνούν, αλλά δεν είναι απόλυτα πεπεισμένοι. Η τυπική απόκλιση υποδεικνύει ότι υπάρχει κάποια ποικιλία στις απαντήσεις, με μερικούς να μην αναγνωρίζουν την σοβαρότητα των συνεπειών και άλλους να συμφωνούν πλήρως. Επίσης, οι υπάλληλοι έχουν μια θετική αντίληψη για τη συμμόρφωση της ηγεσίας με τους κανόνες ασφαλείας των πληροφοριών με μέσο όρο (5,3605) ενώ και στη περίπτωση αυτή η τυπική απόκλιση δείχνει ότι υπάρχει αρκετή ποικιλία. προκύπτει ότι υπάρχει μια ποικιλία απόψεων σχετικά με τον κώδικα ηθικής στον οργανισμό. Τα αποτελέσματα σχετικά με την ύπαρξη κώδικα ηθικής στον οργανισμό, η μεγαλύτερη ομάδα υπαλλήλων είναι ουδέτερη (25.59%), ενώ υπάρχει επίσης ένα σημαντικό ποσοστό που αναγνωρίζει την ύπαρξη του κώδικα με θετικό τρόπο (ελάχιστη και μερική συμφωνία – 31.55%). Ωστόσο, υπάρχουν και σημαντικά ποσοστά υπαλλήλων που εκφράζουν διαφωνία, υποδεικνύοντας την ανάγκη για βελτίωση και ενίσχυση της κατανόησης και εφαρμογής του κώδικα ηθικής που προσανατολίζεται στην ασφάλεια στον οργανισμό.

Για την αξιολόγηση της ικανότητας του οργανισμού να προβαίνει σε αλλαγές, μελετήθηκαν τρείς βασικές πτυχές που αφορούν την υιοθέτηση νέων τρόπων εργασίας, τις προσπάθειες για αλλαγή και τη συνεργασία μεταξύ των μερών του οργανισμού. Συγκεκριμένα, τα δεδομένα καταδεικνύουν ότι

ενώ υπάρχει μια τάση για υιοθέτηση νέων και βελτιωμένων τρόπων εργασίας (4,6279), οι υπάλληλοι βρίσκουν τις προσπάθειες για αλλαγή μέτρια έως δύσκολες (3,9767) ενώ μέσος όρος (3,7616) δείχνει ότι οι υπάλληλοι είναι κάπως ουδέτεροι ή ελαφρώς θετικοί σχετικά με τη συνεργασία των διάφορων μερών του οργανισμού για τη δημιουργία αλλαγής και έχουν ανάμεικτες απόψεις για τη συνεργασία μεταξύ των διάφορων μερών του οργανισμού με τη τυπική απόκλιση είναι υψηλή (1,75590), υποδεικνύοντας μεγάλη ποικιλία στις απόψεις,. Αυτό υποδηλώνει την ανάγκη για καλύτερη επικοινωνία και υποστήριξη κατά τη διαδικασία αλλαγής, καθώς και την ενίσχυση της συνεργασίας μεταξύ των τμημάτων του οργανισμού.

Εν συνεχεία, η έρευνα ασχολήθηκε με ορισμένες συμπεριφορές των εργαζομένων οι οποίες ενδέχεται να είναι επικίνδυνες για την ασφάλεια των πληροφοριακών συστημάτων και εν γένει τις πληροφορίες που διαχειρίζεται ο οργανισμός. Στην ερώτηση αν επιτρέπεται να κατεβάζουν οποιαδήποτε αρχεία στον υπολογιστή τους στη δουλειά, αν αυτά τους βοηθούν να ολοκληρώσουν την εργασία τους, οι ανάλυση των δεδομένων δείχνει ότι η μεγαλύτερη ομάδα υπαλλήλων φαίνεται να διαφωνεί (44,77%) με την ιδέα, υποδεικνύοντας ότι πιθανώς υπάρχουν αυστηροί περιορισμοί στην πολιτική του οργανισμού, ενώ ένα σημαντικό ποσοστό συμφωνεί (37,22%), είτε μερικώς είτε απόλυτα, δείχνοντας ότι η πολιτική μπορεί να είναι πιο ευέλικτη ή να εφαρμόζεται διαφορετικά σε διάφορα τμήματα του οργανισμού. Στη δήλωση αν οι υπάλληλοι επιτρέπεται να κλικάρουν σε οποιοδήποτε σύνδεσμο σε email από άτομα που γνωρίζουν, σύμφωνα με τις απαντήσεις η μεγαλύτερη ομάδα υπαλλήλων φαίνεται να συμφωνεί (73,83%) με αυτό, υποδεικνύοντας ότι η ενημέρωσή τους στο τομέα αυτό είναι ελλιπείς καθιστώντας τους σχετικά ευάλωτους σε επιθέσεις κοινωνικής μηχανικής. Το αποτέλεσμα αυτό επιβεβαιώνεται και από τα αποτελέσματα της δήλωσης "Είναι πάντα ασφαλές να κάνετε κλικ σε συνδέσμους σε emails από άτομα που γνωρίζω"», με τη μεγάλη πλειοψηφία των υπαλλήλων (88,37%) να θεωρεί ότι είναι πάντα ή γενικά ασφαλές να κλικάρουν σε συνδέσμους σε email από άτομα που γνωρίζουν. Συμπληρωματικά, προβληματική δημιουργεί και το γεγονός ότι η πλειοψηφία των υπαλλήλων φαίνεται να διαφωνεί (72,09%) με την ιδέα ότι δεν πρέπει να έχουν πρόσβαση σε συγκεκριμένους ιστότοπους κατά τη διάρκεια της εργασίας, με μόλις ένα μικρό ποσοστό (17,45%) να συμφωνεί με την πολιτική αυτή.

Επιπρόσθετα, προέκυψε ότι μια σημαντική ομάδα υπαλλήλων (56,39% ελάχιστη + μερική + απόλυτη) συμφωνεί με την ιδέα να μοιράζονται τους κωδικούς πρόσβασης της δουλειάς τους με συναδέλφους, υποδεικνύοντας ότι η πρακτική αυτή είναι αρκετά διαδεδομένη. Ωστόσο, υπάρχει ένα ποσοστό (22,09%) που διαφωνεί με την πρακτική αυτή, δείχνοντας ότι μπορεί να υπάρχουν πολιτικές που το απαγορεύουν ή ανησυχίες σχετικά με το κίνδυνο μη εξουσιοδοτημένης πρόσβασης σε δεδομένα. Τέλος, σύμφωνα με τα αποτελέσματα του διαγράμματος 18, η μεγάλη πλειοψηφία των υπαλλήλων (86,305% μερική + απόλυτη) θεωρεί ότι είναι πάντα ή γενικά ασφαλές να στέλνουν

ευαίσθητα αρχεία εργασίας μέσω δημόσιου δικτύου Wi-Fi, υποδεικνύοντας ότι υπάρχει υψηλή εμπιστοσύνη στη χρήση των δημόσιων δικτύων, εκθέτοντας τον οργανισμό σε κίνδυνο διαρροής δεδομένων μέσω μη ασφαλών δικτύων.

Προέκυψε ότι η ηλικία του εργαζομένου επηρεάζει το βαθμό που αντιλαμβάνονται ότι ο οργανισμός δημιουργεί ευαισθητοποίηση στους εργαζόμενους για θέματα ασφάλειας των πληροφοριακών συστημάτων. Όμοια συμπεράσματα προέκυψαν και από άλλη έρευνα (Branley-Bell, D. et. al., 2022) σύμφωνα με την οποία πολλοί άνθρωποι μεγαλύτερης ηλικίας επιδεικνύουν υψηλά επίπεδα ευαισθητοποίησης και ικανότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο σε αντίθεση με στερεότυπες απόψεις που υποστηρίζουν το αντίθετο.

Επιβεβαιώθηκε επίσης η δεύτερη ερευνητική υπόθεση ότι **η ηλικία επηρεάζει την αντίληψη των υπαλλήλων σχετικά με τη σημασία της τήρησης των βασικών αξιών στον οργανισμό.** Οι μεγαλύτερης ηλικίας υπάλληλοι τείνουν να συμφωνούν περισσότερο ότι η αγνόηση των βασικών αξιών θα δημιουργήσει προβλήματα, ενώ οι νεότεροι υπάλληλοι είναι λιγότερο πιθανό να συμφωνούν με αυτήν την πρόταση**.** Οι μεγαλύτερης ηλικίας εργαζόμενοι τείνουν να έχουν μεγαλύτερη εμπειρία και μακροχρόνια σχέση με τον οργανισμό, γεγονός που τους καθιστά πιο ευαισθητοποιημένους και δεσμευμένους στις οργανωτικές αξίες. Μελέτες έχουν δείξει ότι οι μεγαλύτερης ηλικίας υπάλληλοι εκτιμούν περισσότερο τις ηθικές και πολιτισμικές αξίες του οργανισμού και αντιλαμβάνονται τη συμμόρφωση με αυτές ως κρίσιμη για την επιτυχία και τη συνοχή του οργανισμού (Che, Y., Zhu, J., & Huang, H., 2022) (Chua, J., & Ayoko, O. B. 2021)

Η ηλικία επηρεάζει το βαθμό συμφωνίας ότι οι ευαίσθητες πληροφορίες μπορεί να δημιουργήσουν σοβαρά προβλήματα αν διαρρεύσουν. Υπάρχει στατιστικά σημαντική διαφορά (p=.001) στην αντίληψη των διαφορετικών ηλικιακών ομάδων σχετικά με το πόσο επικίνδυνο θεωρούν την πρόσβαση σε ευαίσθητα αρχεία σε έναν φορητό υπολογιστή όταν οι ξένοι μπορούν να δουν την οθόνη τους. Η ηλικιακή ομάδα 18-29 και η ομάδα >60 δείχνουν υψηλότερη ανησυχία (μέσες τιμές 5.0000 και 6.5000 αντίστοιχα). Η ομάδα 30-39 δείχνει τη χαμηλότερη ανησυχία με μέση τιμή 3.5417. Οι ομάδες 40-49 και 50-59 βρίσκονται σε ενδιάμεσο επίπεδο ανησυχίας. Μια μελέτη βρήκε ότι οι διαφορετικές ομάδες ηλικιών αντιλαμβάνονται και εκτιμούν τον κίνδυνο διαρροής πληροφοριών διαφορετικά (Huang, L., Zhou, J., Lin, J., & Deng, S. 2022). Για παράδειγμα, οι μεγαλύτεροι σε ηλικία είναι πιο πιθανό να ανησυχούν για τις συνέπειες της διαρροής ευαίσθητων πληροφοριών και να υποστηρίζουν αυστηρότερα μέτρα προστασίας σε σύγκριση με τους νεότερους, οι οποίοι ενδέχεται να είναι πιο ανεκτικοί ή να μην αντιλαμβάνονται τον ίδιο βαθμό κινδύνου

Το επίπεδο σπουδών επηρεάζει την αντίληψη που έχουν για το πόσο συχνά συνεργάζονται τα διάφορα μέρη του οργανισμού για να δημιουργήσουν αλλαγή. Προέκυψε ότι οι απόφοιτοι λυκείου και ανώτερων σχολών τείνουν να θεωρούν ότι υπάρχει μεγαλύτερη συνεργασία εντός του οργανισμού

για τη δημιουργία αλλαγών σε σύγκριση με τους αποφοίτους διδακτορικού και μεταπτυχιακών προγραμμάτων. Οι απόφοιτοι μεταπτυχιακού ή και διδακτορικού προγράμματος είναι πιο πιθανό να κατέχουν υψηλότερη θέση στην ιεραρχία του οργανισμού. Κατά συνέπεια λόγω της θέσης ο βαθμός εμπλοκής τους στις διαδικασίες αλλαγής είναι υψηλότερος με αποτέλεσμα να αντιλαμβάνονται διαφορετικά το επίπεδο συνεργασίας των μερών του οργανισμού (Jones, L., et. al., 2008).

Το φύλο επηρεάζει το βαθμό που ο εργαζόμενος πιστεύει ότι επιτρέπεται να κάνει «κλικ» σε συνδέσμους που προέρχονται από άγνωστο αποστολέα. δεν παρατηρείται στατιστικά σημαντική διαφορά στους μέσους των ανδρών και των γυναικών ως προς την αντίληψη τους για τη πρόταση. Η υπόθεση δεν επαληθεύεται.

Το φύλο επηρεάζει το βαθμό συμφωνίας ότι επιτρέπεται η αποστολή ευαίσθητων εργασιακών αρχείων μέσω δημόσιου Wi-Fi δικτύου. Οι γυναίκες έχουν σημαντικά υψηλότερο μέσο όρο σε σχέση με τους άνδρες, υποδηλώνοντας ότι οι γυναίκες είναι πιθανότερο να θεωρούν ότι επιτρέπεται η αποστολή ευαίσθητων εργασιακών αρχείων μέσω δημόσιου Wi-Fi δικτύου. Αυτό ωστόσο έρχεται σε αντίθεση με την υφιστάμενη βιβλιογραφία (Kaleta, J. P., & Mahadevan, L., 2020) (Harris, C. R., & Jenkins, M., 2006) σύμφωνα με την οποία οι γυναίκες έχουν μεγαλύτερη επίγνωση των θεμάτων ιδιωτικότητας και των κινδύνων, γεγονός που τις καθιστά πιο πιθανό να αποφεύγουν την αποστολή ευαίσθητων πληροφοριών μέσω αυτών των δικτύων.

Το φύλο του εργαζομένου επηρεάζει το βαθμό που αντιλαμβάνονται ότι ο οργανισμός δημιουργεί ευαισθητοποίηση μεταξύ των εργαζομένων για θέματα ασφάλειας των πληροφοριακών συστημάτων. Οι αντιλήψεις για την ευαισθητοποίηση σχετικά με την ασφάλεια πληροφοριών διαφέρουν σημαντικά ανάμεσα στα φύλα, με τις γυναίκες να έχουν πιο θετική αξιολόγηση σε σύγκριση με τους άνδρες. Μελέτη επισημαίνει ότι οι γυναίκες αντιλαμβάνονται τις εταιρικές πρωτοβουλίες για ασφάλεια με μεγαλύτερη σοβαρότητα και τείνουν να συμμετέχουν πιο ενεργά σε προγράμματα ευαισθητοποίησης, κάτι που μπορεί να επηρεάσει θετικά την αντίληψή τους για τις προσπάθειες του οργανισμού (Cuesta, A., et. al., 2022).

Το φύλο του εργαζομένου επηρεάζει την αντίληψη που έχει σχετικά με το βαθμό που η διοίκηση συμμορφώνεται με τους κανόνες. Τα αποτελέσματα της ανάλυσης δείχνουν ότι υπάρχει στατιστικά σημαντική διαφορά μεταξύ των μέσων όρων των ανδρών (mean=**4.6415)** και των γυναικών (mean=**5.6807)** σχετικά με τη δήλωση **"**η ηγεσία του Οργανισμού συμμορφώνεται και ακολουθεί τους κανόνες (προς τη κατεύθυνση της ασφάλειας των πληροφοριών) που επιβάλει στον οργανισμό". Δεν επιβεβαιώνεται από υφιστάμενη βιβλιογραφία.

Ο ανθρώπινος παράγοντας στην ασφάλεια πληροφοριακών συστημάτων είναι ζωτικής σημασίας, καθώς οι άνθρωποι συχνά αποτελούν τον πιο αδύναμο κρίκο σε ένα σύστημα ασφάλειας. Οι εργαζόμενοι μπορούν ακούσια να εκθέσουν τα συστήματα σε κινδύνους μέσω πράξεων όπως η χρήση

αδύναμων κωδικών πρόσβασης, η μη τήρηση των πρωτοκόλλων ασφαλείας, ή η απερισκεψία στην ανταλλαγή ευαίσθητων πληροφοριών. Επιπλέον, οι επιθέσεις κοινωνικής μηχανικής, όπως το phishing, εκμεταλλεύονται την ανθρώπινη ψυχολογία και μπορούν να παρακάμψουν ακόμα και τα πιο προηγμένα τεχνολογικά μέτρα ασφάλειας. Συνεπώς, η εκπαίδευση και η ευαισθητοποίηση των χρηστών, η ανάπτυξη μιας κουλτούρας ασφάλειας και η συνεχής αναβάθμιση των γνώσεων τους σχετικά με τις νέες απειλές και τις βέλτιστες πρακτικές, είναι απαραίτητα στοιχεία για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων (Parsons, K., et. al, 2014).

Η εκπαίδευση των χρηστών θα πρέπει να περιλαμβάνει τακτικά σεμινάρια και εκπαιδευτικά προγράμματα που επικεντρώνονται στην αναγνώριση και αντιμετώπιση των κυβερνοαπειλών. Αυτά τα σεμινάρια θα μπορούσαν να περιλαμβάνουν πρακτικές ασκήσεις για την αναγνώριση phishing emails, την αποφυγή κακόβουλων ιστοσελίδων και την ασφαλή διαχείριση κωδικών πρόσβασης. Η συχνότητα της εκπαίδευσης θα πρέπει να είναι τουλάχιστον ετήσια, με επιπλέον εκπαιδευτικές συνεδρίες όταν προκύπτουν νέες απειλές ή τεχνολογίες. Η ενημέρωση πρέπει να παρέχεται μέσω διαδραστικών πλατφορμών, όπως webinars και online μαθήματα, καθώς και μέσω ενημερωτικών δελτίων που αναλύουν τις τελευταίες εξελίξεις στις κυβερνοεπιθέσεις και τις μεθόδους αντιμετώπισής τους. Τα ενημερωτικά δελτία θα μπορούσαν να περιλαμβάνουν πραγματικά παραδείγματα επιθέσεων και συμβουλές για την προστασία από αυτές, ενώ οι διαδραστικές πλατφόρμες θα επιτρέπουν στους χρήστες να θέτουν ερωτήσεις και να λαμβάνουν άμεσες απαντήσεις από ειδικούς. Η αναθεώρηση των εκπαιδευτικών προγραμμάτων και των ενημερωτικών υλικών πρέπει να γίνεται τακτικά, ώστε να διασφαλίζεται ότι οι πληροφορίες παραμένουν επίκαιρες και σχετικές με τις νέες απειλές και τεχνολογίες. (Alshaikh, M., 2020), (Sommestad, T. et.al, 2020) and (Torten, R., et.al, 2018)

Επιπλέον, η καθιέρωση αυστηρών πολιτικών και διαδικασιών που περιλαμβάνουν σαφείς οδηγίες για την ασφαλή χρήση των συστημάτων και την ανταπόκριση σε περιστατικά ασφάλειας είναι κρίσιμη (AlHogail, A., 2015). Επιπρόσθετα, η καθιέρωση αυστηρών κανόνων για τη διαχείριση των κωδικών πρόσβασης με σκοπό την αποτροπή πρακτικών όπως ο διαμοιρασμός μεταξύ των εργαζομένων (Tarwireyi P. et.al, 2011). Οι οργανισμοί πρέπει να ενθαρρύνουν την αναφορά ύποπτων δραστηριοτήτων και να διασφαλίζουν ότι όλοι οι εργαζόμενοι γνωρίζουν πώς να αντιδράσουν σε περίπτωση κυβερνοεπίθεσης. Οι τακτικές εκπαιδευτικές συνεδρίες και οι προσομοιώσεις επιθέσεων μπορούν να βοηθήσουν στην προετοιμασία των εργαζομένων και στη μείωση του κινδύνου ανθρώπινων λαθών.

Είναι επίσης σημαντικό να αναγνωρίσουμε τον ρόλο της ανώτερης διοίκησης στην προώθηση της ασφάλειας πληροφοριακών συστημάτων (Ifinedo, P., 2012). Οι ηγέτες των οργανισμών πρέπει να επιδεικνύουν δέσμευση στην ασφάλεια, παρέχοντας τους απαραίτητους πόρους και υποστήριξη για την εφαρμογή και τη διατήρηση αποτελεσματικών πρακτικών ασφάλειας (Xue, B., et.al., 2021). Με

αυτόν τον τρόπο, δημιουργείται μια κουλτούρα όπου η ασφάλεια θεωρείται συλλογική ευθύνη και κάθε εργαζόμενος αισθάνεται υπεύθυνος για την προστασία των πληροφοριών και των συστημάτων του οργανισμού.

Τέλος, η συνεχής παρακολούθηση και αναθεώρηση των μέτρων ασφαλείας είναι απαραίτητη για την προσαρμογή σε νέες απειλές και την αντιμετώπιση των αναδυόμενων κινδύνων (Bauer S. et al., 2017). Η συνεργασία μεταξύ ανθρώπων και τεχνολογίας μπορεί να προσφέρει ένα αποτελεσματικότερο και πιο ανθεκτικό σύστημα ασφάλειας πληροφοριών.

Περιορισμοί της έρευνας

Στους περιορισμούς της έρευνας συγκαταλέγεται το γεγονός ότι παρόλη την προσπάθεια που έγινε το εύρος του ερωτηματολογίου να είναι σύντομο για να μη προκαλέσει την δυσανασχέτηση των ερωτηθέντων υπάρχει πιθανότητα να δημιούργησε κόπωση σε κάποιους συμμετέχοντες. Επίσης, στη προσπάθεια αυτή από το ερωτηματολόγιο αφαιρέθηκαν οι τομείς “Social media use”, “Information handling” και “Incident report” οι οποίες είναι πολύ σημαντικές για τη κατανόηση του βαθμού ευαισθητοποίησης των εργαζομένων. Ο Δημόσιος τομέας αποτελείται από δεκάδες οργανισμούς, αρχές και υπηρεσίες που παρουσιάζουν έντονες διαφορές στην οργάνωση, τη δομή και τις διαδικασίες τους. Ως εκ τούτου, για την εξαγωγή αποτελεσμάτων που θα αντιπροσωπεύουν με μεγαλύτερη ασφάλεια το δημόσιο τομέα, απαιτείται η διεξαγωγή της έρευνας με ανάλογο δείγμα από κάθε έναν οργανισμό, μια διαδικασία που απαιτεί χρόνο και πόρους.

Προτάσεις

Η παρούσα έρευνα συμβάλλει σημαντικά στην κατανόηση του βαθμού ευαισθητοποίησης των υπαλλήλων στον ελληνικό δημόσιο τομέα σε θέματα ασφάλειας πληροφοριακών συστημάτων. Τα ευρήματα της έρευνας παρέχουν πολύτιμες πληροφορίες για την τρέχουσα κατάσταση και τις ανάγκες εκπαίδευσης των υπαλλήλων, επιτρέποντας στους οργανισμούς να εντοπίσουν αδυναμίες και να λάβουν μέτρα βελτίωσης. Επιπλέον, η έρευνα αυτή μπορεί να βοηθήσει στη διαμόρφωση πολιτικών και στρατηγικών που θα ενισχύσουν την ασφάλεια των πληροφοριακών συστημάτων και θα μειώσουν τον κίνδυνο παραβιάσεων.

Τα αποτελέσματα της έρευνας μπορούν να χρησιμοποιηθούν από τους φορείς του δημόσιου τομέα για την ανάπτυξη και εφαρμογή αποτελεσματικών προγραμμάτων εκπαίδευσης και ευαισθητοποίησης. Επιπλέον, η έρευνα μπορεί να χρησιμεύσει ως βάση για την αξιολόγηση της αποτελεσματικότητας των τρεχουσών πρακτικών και να καθοδηγήσει την ανάπτυξη νέων προσεγγίσεων για την αντιμετώπιση των εξελισσόμενων απειλών στις οποίες ο ανθρώπινος

παράγοντας διαδραματίζει καίριο ρόλο. Τονίζεται ότι κάθε οργανισμός έχει διαφορετικές ανάγκες και απαιτήσεις οι οποίες ποικίλουν αναλόγως της δομής, της οργάνωσης αλλά και του υφιστάμενου επιπέδου σε θέματα ασφάλειας των υπαλλήλων του. Για το λόγο αυτό απαιτείται κάθε οργανισμός να διεξάγει περιοδικά εσωτερική έρευνα, βασιζόμενη στη παρούσα, προσαρμοζόμενη στις απαιτήσεις του.

Για την περαιτέρω ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων στον δημόσιο τομέα, προτείνεται η διεξαγωγή μελλοντικών ερευνών που θα εξετάζουν πιο εξειδικευμένα θέματα, όπως η αξιολόγηση ειδικών εκπαιδευτικών προγραμμάτων που ενδεχομένως έχουν ήδη εφαρμοστεί στον ελληνικό δημόσιο τομέα όπως η μελέτη της αποτελεσματικότητας διαφόρων τύπων εκπαιδευτικών προγραμμάτων και εργαλείων (π.χ. gamification, simulations) στην αύξηση της ευαισθητοποίησης και στην αλλαγή συμπεριφοράς των υπαλλήλων.

Η μέτρηση του βαθμού ευαισθητοποίησης των υπαλλήλων στον δημόσιο τομέα σε θέματα ασφάλειας πληροφοριακών συστημάτων αποτελεί κρίσιμο παράγοντα για την ενίσχυση της συνολικής ασφάλειας των οργανισμών. Η συνεχής εκπαίδευση, η σαφής και αυστηρή και συνεχόμενη εφαρμογή πολιτικών, η καλλιέργεια μιας κουλτούρας ασφάλειας, και η τεχνολογική υποστήριξη των χρηστών αποτελούν βασικά συστατικά μιας επιτυχημένης οργανωσιακής στρατηγικής. Με τη δέουσα υποστήριξη από τη διοίκηση και την ενσωμάτωση καινοτόμων πρακτικών, είναι δυνατόν να δημιουργηθεί ένα περιβάλλον όπου οι υπάλληλοι είναι πλήρως ενημερωμένοι και ευαισθητοποιημένοι σχετικά με την ασφάλεια των πληροφοριών, συμβάλλοντας ουσιαστικά στην προστασία των πληροφοριακών συστημάτων και την αποτροπή απειλών.

References

Ξενόγλωσση βιβλιογραφία

1. Al-Izki, F. and Weir, G. R. (2016, August). Management attitudes toward information security in Omani public sector organisations. In 2016 Cybersecurity and Cyberforensics Conference (CCC) (pp. 107-112). IEEE
2. Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R. and Ismail, A. (2022). Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees. International Journal of Advanced Computer Science and Applications (IJACSA).
3. Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A. and Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. International journal of communication networks and information security, 12(3), 326-337.
4. AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567-575.
5. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. DOI: 10.1016/j.cose.2020.102003
6. Alzubaidi A., Kalita J., Authentication of smartphone users using behavioral biometrics, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1998–2026.
7. Amron, M. T., Ibrahim, R., Bakar, N. A. A., & Chuprat, S. (2019). Development and validation of a questionnaire to measure the acceptance of cloud computing in public sectors. *Open International Journal of Informatics*, *7*(Special Issue 2), 85-95
8. Andrew Valentine, 2006, 'Enhancing the employee security awareness model', Cybertrust's ICSA Labs, p.17-19
9. Aslan, Ö. A. and Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE access, 8, 6249-6271.
10. Atzori L., Iera A., Morabito G., The Internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
11. Back, S. and Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. Journal of contemporary criminal justice, 37(3), 427-451.
12. Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *computers & security*, *68*, 145-159.

13. Bekkers, L., van't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R. and Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers and Security, 127, 103099
14. Bhuvana, A. Bhat, T. Shetty and M. Naik, "A Study on Various Phishing Techniques and Recent Phishing Attacks", International Journal of Advanced Research in Science, Communication and Technology, pp. 142-148, 2021.
15. Bidgoli, M. (2021). If You See Something Suspicious Online, Report It: An Investigation into Addressing and Overcoming the Challenges in Cybercrime Reporting. The Pennsylvania State University.
16. Bidgoli, M., Knijnenburg, B. P., Grossklags, J. and Wardman, B. (2019, November). Report now. Report effectively. Conceptualizing the industry practice for cybercrime reporting. In 2019 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-10). IEEE.
17. Bossler A., Holt T., Cross C., Burruss G., "Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness." Security Journal 33, no. 2, 2020: 311-328.
18. Bountakas, P. and Xenakis, C. (2023). HELPHED: Hybrid Ensemble Learning PHishing Email Detection. Journal of Network and Computer Applications, 210, 103545.
19. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, *2022*.
20. Buckley, J., Lottridge, D., Murphy, J. G. and Corballis, P. M. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention and email typology. International Journal of Human-Computer Studies, 172, 102996.
21. Button, M. and Cross, C. (2017). Cyber frauds, scams and their victims. Taylor and Francis.
22. Che, Y., Zhu, J., & Huang, H. (2022). How does employee–organization relationship affect work engagement and work well-being of knowledge-based employees?. *Frontiers in psychology*, *13*, 814324.
23. Chua, J., & Ayoko, O. B. (2021). Employees' self-determined motivation, transformational leadership and work engagement. *Journal of Management & Organization*, *27*(3), 523-543.
24. Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminology and Criminal Justice, 20(3), 358-375.
25. Cuesta, A., Alvear, D., Carnevale, A., & Amon, F. (2022). Gender and public perception of disasters: a multiple hazards exploratory study of EU citizens. *Safety*, *8*(3), 59.

26. Curtis, J. and Oxburgh, G. (2022). Understanding cybercrime in 'real world'policing and law enforcement. The Police Journal, 0032258X221107584.
27. Czekster, R. M., Metere, R. and Morisset, C. (2022). cyberaCTIve: a STIX-based Tool for Cyber Threat Intelligence in Complex Models. arXiv preprint arXiv:2204.03676.
28. Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security*, *26*(5), 584-612.
29. Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework for linking culture and improvement initiatives in organizations. *Academy of management Review*, *25*(4), 850-863.
30. Drivas, G., Maglaras, L., Janicke, H. and Ioannidis, S. (2020). Assessing Cyber Security Threats and Risks in the Public Sector of Greece. Journal of Information Warfare, 19(1), 96-112.
31. ENISA, Threat Landscape for Ransomware Attacks, 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
32. Evans, M., He, Y., Maglaras, L., Yevseyeva, I. and Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International journal of medical informatics, 127, 109-119.
33. Filippidis, A. P., Hilas, C. S., Filippidis, G. and Politis, A. (2018, May). Information security awareness of Greek higher education students—preliminary findings. In 2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST) (pp. 1-4). IEEE.
34. Fiona Carroll1, John Ayooluwa Adejobi, Reza Montasari (2022) How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society https://link.springer.com/article/10.1007/s42979-022-01069-1
35. Fonseca C., Moreira S and Inês Guedes., "Online Consumer Fraud Victimization and Reporting: A Quantitative Study of the Predictors and Motives." Victims and Offenders 17, no. 5 (2022): 756-780
36. Fusi, F., Jung, H. and Welch, E. (2023). Technological vulnerability and knowledge of cyber-incidents: threats to innovativeness in local governments?. Public Management Review, 1-27.
37. Graham, A., Kulig, T. C. and Cullen, F. T. (2019). Willingness to report crime to the police: Traditional crime, cybercrime and procedural justice. Policing: An International Journal, 43(1), 1-16.
38. Harris, C. R., & Jenkins, M. (2006). Gender differences in risk assessment: why do women take fewer risks than men?. *Judgment and Decision making*, *1*(1), 48-63.
39. Hillman, D., Harel, Y. and Toch, E. (2023). Evaluating Organizational Phishing Awareness Training on an Enterprise Scale. Computers and Security, 103364.

40. Homburg, V. and Kokje, J. (2020). Information policy security compliance in Dutch local government.
41. Huang, L., Zhou, J., Lin, J., & Deng, S. (2022). View analysis of personal information leakage and privacy protection in big data era—based on Q method. *Aslib Journal of Information Management*, *74*(5), 901-927.
42. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
43. Jampen, D., Gür, G., Sutter, T. and Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences, 10(1), 1-41.
44. Jones, L., Watson, B., Hobman, E., Bordia, P., Gallois, C., & Callan, V. J. (2008). Employee perceptions of organizational change: impact of hierarchical level. *Leadership & Organization Development Journal*, *29*(4), 294-316.
45. Kaleta, J. P., & Mahadevan, L. (2020). Examining differences in perceptions of trust, privacy and risk in home and public Wi-Fi internet channels. *Journal of systems and information technology*, *22*(3), 265-287.
46. Karagiannopoulos, V., Kirby, A., Ms, S. O. M. and Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. Computer Law and Security Review, 43, 105615.
47. Kemp, S., Buil-Gil, D., Miró-Llinares, F. and Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. Criminology and Criminal Justice, 23(3), 468-489.
48. Kemp S, Miró-Llinares F., Moneva A.. "The dark figure and the cyber fraud rise in Europe: evidence from Spain." European Journal on Criminal Policy and Research 26, no. 3 2020: 293-312.
49. Kemp S., "Fraud reporting in Catalonia in the Internet era: Determinants and motives." European Journal of Criminology,2020, doi: 1477370820941405.
50. Kostas Papagiannakis, 2011, An overview of the current level of Security Awareness in Greek companies,
51. Kwak, Y., Lee, S., Damiano, A. and Vishwanath, A. (2020). Why do users not report spear phishing emails?. Telematics and Informatics, 48, 101343.
52. Lang, M., Connolly, L., Taylor, P. and Corner, P. J. (2023). The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. Digital Threats: Research and Practice, 4(4), 1-22.

53. Loukis, E. and Spinellis, D. (2001). Information systems security in the Greek public sector. Information management and computer security, 9(1), 21-31.
54. Masilela, L. and Nel, D. (2021). The role of data and information security governance in protecting public sector data and information assets in national government in South Africa. Africa's Public Service Delivery and Performance Review, 9(1), 385.
55. Mohanty, K., Bopche, G. S., Brahnam, S. and Dash, S. R. (2023). Ransomware-as-a-Weapon (RaaW): A Futuristic Approach for Understanding Malware as a Social Weapon. In Contemporary Challenges for Cyber Security and Data Privacy (pp. 247-266). IGI Global.
56. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S. and Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. Computers and Security, 103387.
57. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.
58. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.
59. Pattinson, M. R., Butavicius, M. A., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The Information Security Awareness of Bank Employees. In *HAISA* (pp. 189-198)
60. Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C. and Assi, C. (2023). The Age of Ransomware: A Survey on the Evolution, Taxonomy and Research Directions. IEEE Access.
61. Safi, A. and Singh, S. (2023). A systematic literature review on phishing website detection techniques. Journal of King Saud University-Computer and Information Sciences.
62. Salloum, S., Gaber, T., Vadera, S. and Shaalan, K. (2021). Phishing email detection using natural language processing techniques: a literature survey. Procedia Computer Science, 189, 19-28.
63. Sharma, P., Dash, B. and Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber Defense Mechanisms. International Journal of Advanced Research in Computer and Communication Engineering ISO, 3297, 2007.
64. Sommestad, T., Karlzén, H., & Hallberg, J. (2020). The sufficiency of the Theory of Planned Behavior for explaining information security policy compliance. *Information & Computer Security, 28*(2), 217-233.
65. Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T. and Klepacki, B. (2020). Information security assessment in public administration. Computers and Security, 90, 101709.

66. Tally, A. C., Abbott, J., Bochner, A. M., Das, S. and Nippert-Eng, C. (2023, April). Tips, Tricks and Training: Supporting Anti-Phishing Awareness among Mid-Career Office Workers Based on Employees' Current Practices. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-13).
67. Tarwireyi, P.; Flowerday, S.; Bayaga, A. Information security competence test with regards to password management. In Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 1–7.
68. Tcherni, M., Davies, A., Lopes, G. and Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave?. Justice Quarterly, 33(5), 890-911.
69. Teichmann, F., Boticiu, S. R. and Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?. International Cybersecurity Law Review, 4(3), 259-280.
70. Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of organizational learning culture on information security compliance and cultural values. *Journal of Information System Security, 14*(3), 103-123.Van Boven, L. S., Kusters, R. W., Tin, D., van Osch, F. H., De Cauwer, H., Ketelings, L., . and Barten, D. G. (2023). Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals. Annals of Emergency Medicine.
71. Van Veenstra, A. F. and Ramilli, M. (2011). Exploring information security issues in public sector inter-organizational collaboration. In Electronic Government: 10th IFIP WG 8.5 International Conference, EGOV 2011, Delft, The Netherlands, August 28–September 2, 2011. Proceedings 10 (pp. 355-366). Springer Berlin Heidelberg.
72. Van de Weijer, S., Leukfeldt, R. and Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives and previous experiences. Policing: An International Journal, 43(1), 17-34.
73. Van de Weijer, Steve GA, Rutger Leukfeldt and Sophie van der Zee. "Cybercrime reporting behaviors among small-and medium-sized enterprises in the Netherlands." In Cybercrime in Context, pp. 303-325. Springer, Cham, 2021
74. Van de Weijer, Steve GA, Rutger Leukfeldt and Wim Bernasco. "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud and hacking." European Journal of Criminology 16, no. 4, 2019, : 486-508
75. Wilson, M., McDonald, S., Button, D. and McGarry, K. (2023). It won't happen to me: Surveying sme attitudes to cyber-security. Journal of Computer Information Systems, 63(2), 397-409.
76. Xue, B., Xu, F., Luo, X., & Warkentin, M. (2021). Ethical leadership and employee information security policy (ISP) violation: exploring dual-mediation paths. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 5-23.

77. Yilmaz, Y., Cetin, O., Arief, B. and Hernandez-Castro, J. (2021). Investigating the impact of ransomware splash screens. Journal of Information Security and Applications, 61, 102934
78. Young, J. A. and Farshadkhah, S. (2023). Teaching Tip: Hook, Line and Sinker–The Development of a Phishing Exercise to Enhance Cybersecurity Awareness. Journal of Information Systems Education, 34(4), 347-359.

Ελληνόγλωσση βιβλιογραφία

1. Γέρμανος Γεώργιος και Γεωργίου Νικόλαος (2021), «κυβερνέγκλημα», 141-147

Ιστοσελίδες

1. Chebac A., (2023), What Is Cybercrime-as-a-Service (CaaS), accessible at: Cybercrime-as-a-service (CaaS): Deffinition, Types and Threaths? (heimdalsecurity.com) (Accessed 09 November 2023)
2. Cost of a data breach Report 2023 | IBM, accessible at: https://www.ibm.com/reports/data-breach
3. Data Breach Investigations Report 2023, accessible at: 2023 Data Breach Investigations Report | Verizon (Accessed 09 November 2023)
4. ENISA, malware 2022, accessible at: https://www.enisa.europa.eu/topics/incident-response/glossary/malware (Accessed 06 December 2023)
5. European Union Agency for Criminal Justice Cooperation, Annual Report 2021, 6.3. Tackling 'Cybercrime as a Service', accessible at: 6.3. Tackling 'Cybercrime as a Service' | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu) (Accessed 09 November 2023)
6. European Union Agency for Cybersecurity (ENISA), accessible at Ransomwarehttps://www.enisa.europa.eu/topics/incident-response/glossary/ransomware (Accessed 07 December 2023)
7. Europol, High-Tech crime, 2022 accessible at: https://www.europol.europa.eu/crime-areas/cybercrime/high-tech-crime (Accessed 06 December 2023)
8. Europol, Tips and advice to prevent ransomware from infecting your electronic devices, accessible at:https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices (Accessed 07 December 2023)
9. Fahmida Y. Rashid, Cybercrime victims are not calling the police, 2020 available: https://duo.com/decipher/cybercrime-victims-are-not-calling-the-police (Accessed at 18 December 2023)
10. Greek Cyber Crime Center online accessible at: https://www.cybercc.gr/el/ (Accessed 09 November 2023)
11. Institute for Defense and Business, (2022) Top 5 Cyber Threats Facing the Public Sector accessible at https://www.idb.org/top-5-cyberthreats-facing-the-public-sector/ (Accessed 09 November 2023)
12. Internet World Stats: Usage and Population Statistics, accessible at: https://www. internetworldstats.com/stats.htm. (Accessed 9 November 2023).

13. Kaspersky, Ransomware protection: How to keep your data safe in 2023, accessible at: https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware (Accessed 07 December 2023)
14. Kaspersky Lab survey, 10 July 2017, "One-in-Four Hide Cybersecurity Incidents From Their Employers" https://usa.kaspersky.com/about/press-releases/2017_kaseprsky-lab-survey-one-in-four-hide-cybersecurity-incidents-from-their-employers
15. Michelle Davidson, 2022, 11 Tips on Spotting Malicious Emails, accessible at: https://www.globalsign.com/en/blog/how-to-spot-a-phishing-email (Accessed 11 December 2023)
16. Microsoft, Protect your PC from ransomware, accessible at: https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3 (Accessed 07 December 2023)
17. Microsoft, "Protect yourself from phishing" accessible at: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44 (Accessed 11 December 2023)
18. National Cyber Security Centre, Phishing attacks, 2023: defending your organization accessible at https://www.ncsc.gov.uk/guidance/phishing (Accessed 08 December 2023)
19. State of Malware, 2023 accessible at: https://go.malwarebytes.com/rs/805-USG-300/images/MWB_State_of_Malware_Report_2023.pdf (Accessed 09 November 2023)
20. TrendLabs The Global Technical Support and R&D Center of TREND MICRO, Ransomware Past, Present and Future, 2017 accessible at: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf (Accessed 07 December 2023)
21. UpGuard, Erward Kost, 15 Nov. 2023, accessible at: https://www.upguard.com/blog/protecting-employee-credentials-from-ransomware-compromise (Accessed 07 December 2023)
22. UpGuard, Kely Chin, 15 Nov. 2023, How to Prevent Ransomware Attacks: Top 10 Best Practices in 2023 accessible at: https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks (Accessed 07 December 2023)
23. Έκθεση απειλών ESET 1ο εξάμηνο 2023 | ESET accessible at: https://www.eset.com/int/business/resource-center/reports/eset-threat-report-h1-2023/ (Accessed 09 November 2023)
24. Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, "Ανακοίνωση από την Εθνική Αρχή Κυβερνοασφάλειας" 15 Ιουλίου 2023, accessible at: https://mindigital.gr/archives/5310 (Accessed 11 December 2023)

25. Νικολέτα Αρκολάκη, ¨Αυτοδιοίκση¨ https://www.aftodioikisi.gr/koinonia/prosochi-xafrizoyn-chrimata-meso-fake-mail-elta-trapezon-eikones/ (Accessed 11 December 2023)
26. Πανεπιστήμιο Δυτικής Αττικής, Συμβουλές για αναγνώριση κακόβουλων/παραπλανητικών μηνυμάτων, 2022 accessible at: https://wiki.noc.uniwa.gr/doku.php?id=spamdetectionadvices (Accessed 11 December 2023)
27. Ελενόπουλος Π., 2023, Έκτακτη είδηση: Αν λάβετε αυτό το μήνυμα καλέστε αμέσως την Αστυνομία, accessible at: https://xristika.gr/ektakti-eidisi-an-lavete-ayto-to-minym/ (Accessed 11 December 2023)
28. Οικονομικός Ταχυδρόμος, 2023, Κυβερνοασφάλεια: Τι σηματοδοτεί η οδηγία NIS2 για τις επιχειρήσεις, accessible at: https://www.ot.gr/2023/01/30/texnologia/kyvernoasfaleia-ti-simatodotei-i-odigia-nis2-gia-tis-epixeiriseis/ (Accessed 20 February 2024)
29. Αλεξιάννα Τσότσου 31 May 2023, «Η κυβερνοασφάλεια στο επίκεντρο: Το νέο νομοθετικό πλαίσιο στην ΕΕ που αλλάζει τα δεδομένα», accessible at: https://lawyermagazine.gr/ (Accessed 20 February 2024)
30. Υπουργείο Ψηφιακής Διακυβέρνησης, Δικτυακός Τόπος Διαβουλεύσεων, accessible at: http://www.opengov.gr/digitalandbrief/?p=3131, (Accessed 20 February 2024)
31. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, Access to Europian Union Law, eur-lex.europa.eu/legal-content (Accessed 05 April 2024)
32. Εισαγωγή στο νέο Γενικό Κανονισμό Προστασίας Δεδομένων, https://www.gdprgreece.com (Accessed 05 April 2024)