ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

ΤΙΤΛΟΣ

Η κυβερνοασφάλεια ως στρατηγική ανάπτυξης του ψηφιακού μετασχηματισμού στην Δημόσια Διοίκηση

ΛΑΜΠΑΔΑΡΙΟΥ ΕΥΓΕΝΙΑ
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : Δρ ΚΩΝΣΤΑΝΤΙΝΙΔΗΣ ΧΡΗΣΤΟΣ

ΣΕΡΡΕΣ 2023

ΠΕΡΙΛΗΨΗ

Στα πλαίσια του ψηφιακού μετασχηματισμού και της Κοινωνίας της Πληροφορίας, ένα από τα πιο σημαντικά ζητήματα που μελετάται αποτελεί η κυβερνοασφάλεια. Ο σύγχρονος κόσμος και η ανάπτυξη της τεχνολογίας έχουν οδηγήσει στις διαδικτυακές συναλλαγές και τις διαδικτυακές αλληλεπιδράσεις. Στόχος της παρούσας εργασίας αποτελεί η διερεύνηση της σημασίας της κυβερνοασφάλειας ως πρόκληση του ψηφιακού μετασχηματισμού μέσα στα πλαίσια της Δημόσιας Διοίκησης. Η εργασία παρουσιάζει την γνώμη των πολιτών σ ένα δείγμα 107 ατόμων αναφορικά με την κυβερνοασφάλεια και τον ψηφιακό μετασχηματισμό. Η εργασία στηρίζεται στην ποσοτική μέθοδο μέσα από ένα δομημένο ερωτηματολόγιο κλειστών ερωτήσεων. Σύμφωνα με τα δεδομένα της έρευνας, η χρήση του διαδικτύου είναι εκτεταμένη από τους πολίτες τόσο ως επικοινωνιακό μέσο όσο και για την διεκπεραίωση χρηματικών συναλλαγών. Ταυτόχρονα οι πολίτες δεν φαίνεται να είναι πλήρως ενημερωμένοι για τους κανόνες ασφαλείας του διαδικτύου όπως επίσης δεν αισθάνονται ασφαλείς με την παροχή ευαίσθητων δεδομένων στο διαδίκτυο. Τέλος, οι πολίτες ως μέτρο προστασίας επιδιώκουν να μην παρέχουν προσωπικά δεδομένα και να διαγράφουν τις πληροφορίες που συλλέγονται για τους ίδιους. Οι κίνδυνοι της ψηφιακής καινοτομίας είναι αναπόφευκτοι αλλά η αποτελεσματική αξιοποίηση της τεχνολογίας μπορεί να θέσει τα θεμέλια για καινούριες βάσεις ασφάλειας και προστασίας των δεδομένων των πολιτών.

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: κυβερνοασφάλεια, κυβερνοτρομοκρατία, προσωπικά δεδομένα, προστασία, Δημόσια Διοίκηση

ABSTRACT

In the frame of digital transformation and in the Society of Information, one of the most important issues is cybersecurity.Modern world and the evolution of technology have lead to digital transactions and digital interactions. The aim of this paper is the examination of the importance of cybersecurity as a challenge of digital transformation in the frame of Civil Administration. The paper shows the opinion of citizens in a sample of 107 people about cybersecurity and digital transformation. The paper is based on the quantitative method via a structured questionnaire with closed questions. According to the findings of the research, the use of the internet is extensive from the citizens as a communication tool as a way to complete their money exchanges. At the same time, people aren't aware of the internet safety rules as also, don t feel safe with the provision of sensitive data on the internet. Lastly, citizens as a protective measure try no to provide personal data and to delete the information which they collect. The dangers of digital innovations are unavoidable but the effective use of technology may set the base for new safety bases and protection of citizens' data.

KEY WORDS : cybersecurity, cyberterrorism, personal data, protection, Civil Administration

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη της τεχνολογίας και η ανάπτυξη του ψηφιακού κόσμου έχει ως αποτέλεσμα την οργάνωση δικτύων επικοινωνίας και την δημιουργία ηλεκτρονικών υπηρεσιών είτε στον ιδιωτικό είτε στον δημόσιο τομέα. Οι συναλλαγές μέσα από την χρήση των υπολογιστών απλουστεύονται ενώ ταυτόχρονα γίνονται πιο γρήγορα από οποιοδήποτε μέρος κι αν βρίσκεται κάποιος που σημαίνει ότι η αυτοποιημένες μέθοδοι αποτελούν πλέον γεγονός.

Παρόλα αυτά, η εξασφάλιση της κυβερνοασφάλειας συνδυαστικά με την βελτίωση της αποτελεσματικότητας και της ποιοτικότερης παροχής υπηρεσιών αποτελεί το ζητούμενο στο μέλλον του ψηφιακού μετασχηματισμού. Τα ηλεκτρονικά δίκτυα ενέχουν κινδύνους τρωτότητας με βασική απειλή για κάθε κράτος, τις κυβερνοεπιθέσεις ως μια νέα μορφή ηλεκτρονικού εγκλήματος.

Η κυβερνοασφάλεια τείνει να αποτελεί μια πρόκληση που οφείλει το Διαδίκτυο να αντιμετωπίσει μέσα από την ανάπτυξη νέων κατάλληλων στρατηγικών διαχείρισης προκειμένου να εξασφαλιστεί η ασφάλεια των πληροφοριών και των προσωπικών δεδομένων εκατομμυρίων πολιτών που αναλύονται και αποθηκεύονται στον κυβερνοχώρο.

Στόχος της παρούσας εργασίας αποτελεί η διερεύνηση του φαινομένου της κυβερνοασφάλειας μέσα στα πλαίσια του ψηφιακού μετασχηματισμού στην κοινωνία των Πληροφοριών και στα πλαίσια της Δημόσιας Διοίκησης. Ειδικότερα, η εργασία αποβλέπει στην διερεύνηση των επιθέσεων που καλείται να αντιμετωπίσει ο κυβερνοχώρος τόσο από κρατικούς όσο και από μη κρατικούς δράστες ενώ παράλληλα αναλύει τις στρατηγικές καταπολέμησης των επιθέσεων αυτών από την πλευρά της Ευρωπαϊκής ένωσης προκειμένου να προάγει την ελευθερία και τον σεβασμό των δικαιωμάτων όλων των ανθρώπων και του κράτους δικαίου στον οποίο βρίσκονται.

Η εργασία δομικά στηρίζεται στο θεωρητικό και στο εμπειρικό μέρος. Αρχικά το θεωρητικό μέρος περιλαμβάνει συνολικά τρία κεφάλαια. Το πρώτο κεφάλαιο αναλύονται οι απειλές και οι επιθέσεις που δέχεται ο κυβερνοχώρος με συνέπειες την αποδυνάμωση της κοινωνικής συνοχής και δυναμικής ιδιαίτερα της Δημόσιας Διοίκησης. Το δεύτερο κεφάλαιο προσεγγίζει εννοιολογικά και σημασιολογικά την ασφάλεια του κυβερνοχώρου, τους τύπους ασφαλείας και τα οφέλη της κυβερνοασφάλειας. Τέλος, το τρίτο κεφάλαιο του θεωρητικού μέρους σχετίζεται με

την αποτελεσματικότητα της Ευρωπαϊκής Ένωσης αναφορικά με το πολιτικό και το νομοθετικό πλαίσιο για την κυβερνοασφάλεια και γενικότερα με τις στρατηγικές που ακολουθούνται για την δημιουργία ενός ασφαλή κυβερνοχώρου.

Από την άλλη, το εμπειρικό μέρος περιλαμβάνει το κεφάλαιο με την μεθοδολογία καθώς και το κεφάλαιο με την στατιστική ανάλυση των δεδομένων που συλλέχθηκαν για την πραγματοποίηση της έρευνας.

Η εργασία στηρίχθηκε τόσο στην βιβλιογραφική ανασκόπηση για την ανάλυση του θεωρητικού μέρους της εργασίας όσο και στην πρωτογενή έρευνα μέσα από την ποσοτική έρευνα με την χρήση ερωτηματολογίων.

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ: ΑΠΕΙΛΕΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Στο παρόν κεφάλαιο δίνονται οι ορισμοί του κυβερνοχώρου ενώ αναλύονται οι απειλές και οι επιθέσεις που λαμβάνουν χώρα στο διαδίκτυο. Επίσης αναλύεται το ζήτημα της κυβερνοτρομοκρατίας ως πρόκληση των τελευταίων ετών στην Δημόσια Διοίκηση και στην προσπάθεια ψηφιακού μετασχηματισμού όλων των υπηρεσιών.

1.1.Η έννοια του Κυβερνοχώρου

Το περιβάλλον που έχει βασιστεί πάνω σε δίκτυα επικοινωνιών τα οποία χρησιμοποιούν ηλεκτρονικούς υπολογιστές υποδηλώνει τον όρο «κυβερνοχώρος» οποίος επικράτησε έναντι του «κυβερνοδιαστήματος». Αυτά τα δίκτυα μπορούν να είναι είτε τοπικής εμβέλειας (*δίκτυα LANs)* δηλαδή ηλεκτρονικοί υπολογιστές μέσα στο ίδιο δωμάτιο ή κτίριο συνδεδεμένοι μεταξύ τους προκειμένου να μοιράζονται και να επεξεργάζονται οι πληροφορίες είτε ευρείας εμβέλειας (*δίκτυα WANs) τα οποία αφορούν τα διεθνή και παγκόσμια δίκτυα του internet.*

Ο συγγραφέας William Gibson ήταν αυτός που πρότεινε τον όρο κυβερνοχώρος μέσα στο μυθιστόρημά του όπου οι χάκερ του μέλλοντος, εισέβαλλαν στον κυβερνοχώρο με τα κράνη τους και πρόβαλλαν τη συνείδηση τους σε τρισδιάστατα εικονικά περιβάλλοντα. Ο W. Gibson εξέφρασε την ιδέα ότι η ανθρώπινη φαντασία μέσα από την τεχνολογία θα μπορούσε να δημιουργήσει νέες πραγματικότητες (Wertheim,1998).

Επίσης, ο JohnPerryBarlow χρησιμοποίησε εξίσου τον συγκεκριμένο όρο προκειμένου να περιγράψει έναν συνδυασμό της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών σ ένα διαφορετικό επίπεδο ως έναν νέο κόσμο δικτύου πληροφοριών που θα διέπεται από νέους κανόνες και πρότυπα συμπεριφοράς αλλά και νέες μεταφορικές έννοιες (Wertheim,1998).

Σήμερα ο κυβερνοχώρος αναφέρεται σ’ ένα δίκτυο εκατομμυρίων υπολογιστών και ιστοσελίδων ενώ ταυτόχρονα επιβιώνει και βελτιώνεται μέσα από

εκατομμύρια χρήστες του ίντερνετ και εκατομμύρια επενδυτές για την υποδομή και τις διαδικτυακές υπηρεσίες του από μεγάλες εταιρίες του χώρου(Τσέκερης,2009).

Αναμένεται ότι οι χρήστες θα υπερδεκαπλασιαστούν στις επόμενες δεκαετίες ενώ ενισχύεται συνεχώς η ταχύτητα μεταφοράς δεδομένων και η επεξεργαστική ισχύς της ψηφιοποίησης των δικτύων τηλεπικοινωνιών. Επίσης, τα εικονικά περιβάλλοντα είναι ευρέως διαδεδομένα με παιχνίδια ρόλων για τους χρήστες μεταφέροντας το προσωπικό τους Avatar (φανταστική προσωπικότητα0 σε έναν κόσμο που τον δημιουργούν οι ίδιοι με εικονικά αγαθά και οι ανθρώπινες υπάρξεις αλληλεπιδρούν μεταξύ τους μέσα από τις δυνατότητες της φαντασίας των χρηστών (Τσέκερης,2009).

Το Διαδίκτυο αποτελεί τον προτιμώμενο τρόπο επικοινωνίας για την πλειοψηφία του πλανήτη και οι δράσεις στον κυβερνοχώρο είναι καθημερινότητα. Η μείξη της τεχνολογίας και της ανθρώπινης συμπεριφοράς αποτελεί έναν νέο ρεύμα στον σύγχρονο δυτικό πολιτισμό με επιδίωξη την εξισορρόπηση του φυσικού και του εικονικού κόσμου (Τσέκερης,2009).

1.1.1. Ορισμοί του Κυβερνοχώρου

Το εικονικό περιβάλλον μέσα στο οποίο πραγματοποιούνται ηλεκτρονικές επικοινωνίες, εμπορικές συνδιαλλαγές και κοινωνικές αλληλεπιδράσεις νοείται ως κυβερνοχώρος. Σύμφωνα λοιπόν με αυτό τον όρο, ο κυβερνοχώρος αφορά ένα δίκτυο επικοινωνιακών υποδομών και ψηφιακών πληροφοριών τα οποία είναι συνδεδεμένα μεταξύ τους σε παγκόσμιο επίπεδο (Erick, 2012).

Την δεκαετία του 1990 ο ορισμός έγινε γνωστός ευρύτερα καθώς εκείνη την περίοδο υπήρχε σημαντική αύξηση των χρηστών του διαδικτύου οι οποίοι άρχισαν να επικοινωνούν σε ψηφιακό επίπεδο και να δυκτυώνονται ενώ μέσα από τον όρο «κυβερνοχώρος» αντιπροσωπεύτηκαν οι καινούριες ιδέες και τα φαινόμενα που εμφανίστηκαν σχετικά με το διαδίκτυο (Erick, 2012).

Μέχρι σήμερα γίνανε πολλές προσπάθειες ώστε να προσδιοριστεί η έννοια του κυβερνοχώρου και σύμφωνα με τον Erik M. Mudrinich ο κυβερνοχώρος αποτελεί έναν τομέα της επιχείρησης όπου η αρχιτεκτονική του διαμορφώνεται μέσα από την χρήση ηλεκτρονικών μέσων και μέσω ενός ηλεκτρομαγνητικού φάσματος ώστε να δημιουργούνται, να αποθηκεύονται, να μεταβάλλονται, να ανταλλάσσονται και να εκμεταλλεύονται πληροφορίες μέσω διασυνδεδεμένων δικτύων χωρίς γεωγραφικά

και πολιτικά σύνορα τόσο σε λογικό όσο και σε υλικό επίπεδο την ίδια στιγμή (Erick, 2012).

Μετά από τις επιθέσεις από ξηρά, από αέρα, από θάλασσα και από το διάστημα, ο κυβερνοχώρος θεωρείται η πέμπτη πολεμική απειλή με την διαφορά ότι πρόκειται για ανθρώπινο δημιούργημα σε σχέση με τις υπόλοιπες απειλές. Αυτή η διαφορά αποτελεί σημαντικό χαρακτηριστικό καθώς υπάρχει γρήγορη ανάπτυξη της τεχνολογίας (Stephanie, 2012).

Οι πολλοί χρήστες οι οποίοι δρουν μέσα στο εικονικό περιβάλλον του κυβερνοχώρου το καθιστούν ιδιαίτερα επικίνδυνο «χώρο» για την εθνική ασφάλεια ενώ η κάθε απειλή του κυβερνοχώρου μπορεί ανά πάσα στιγμή να μετατρέψει την ψηφιακή εποχή σε σκοτεινή εποχή (Stephanie, 2012).

1.2. Απειλές και επιθέσεις στον Κυβερνοχώρο

Προκειμένου να γίνουν κατανοητές το είδος των απειλών και των επιθέσεων που λαμβάνουν χώρα στον κυβερνοχώρο πρέπει να επισημάνουμε ότι το διαδίκτυο δεν είναι ενιαίος χώρος και διαχωρίζεται σε τρία μέρη (FuandChen, 2010):

1. Στο διαδίκτυο, στο οποίο βρίσκονται τόσο σημαντικές όσο και μη σημαντικές πληροφορίες και ανά πάσα στιγμή μπορεί κάποιος να τις ανακτήσει με ευκολία μέσα από την χρήση μηχανών αναζήτησης όπως το Google, το Yahoo Search, το Mozzillaκ.α. και γι’ αυτό το χρησιμοποιεί η πλειοψηφία των χρηστών.
2. Στο deep web, όπου βρίσκονται πληροφορίες οι οποίες δεν είναι καταχωρημένες σε δημοφιλείς πλατφόρμες.
3. Στο σκοτεινό δίκτυο (dark web), στο οποίο περιλαμβάνεται υλικο το οποίο δεν δημοσιοποιείται ούτε διανέμεται σε νόμιμες ιστοσελίδες και εκεί συμβαίνουν για παράδειγμα παράνομες αγοραπωλησίες, διακίνηση παιδικής πορνογραφίας κ.α. Στο σκοτεινό web οι επικοινωνίες και οι συνδιαλλαγές σε πραγματικό περιβάλλον χαρακτηρίζονται ως κακουργήματα και γίνεται μεγάλη προσπάθεια από όλα τα κράτη να ελεγχθεί και να εκμηδενιστεί.

Οι κυριότερες εγκληματικές δράσεις που συμβαίνουν στο darkweb και ταυτόχρονα αποτελούν απειλή για την ασφάλεια του κυβερνοχώρου είναι οι εξής (ChertoffandSimon,2015).

- Διάφορες παράνομες αγοραπωλησίες και συναλλαγές και χαρακτηρίζονται ως εγκληματικές πράξεις τόσο από το ίδιο το κράτος στο οποίο πραγματοποιούνται όσο και από το διεθνές δίκαιο. Εδώ, περιλαμβάνονται παράνομες ουσίες, όπλα, παράνομα φαρμακευτικά σκευάσματα ακόμη και το εμπόριο λευκής σαρκός και το εμπόριο βρεφών.
- Ανταλλαγή και πώληση αγαθών και πληροφοριών τα οποία είναι αποτέλεσμα υποκλοπής. Τέτοιου είδους αγαθά είναι πελατολόγια, αρχαία αντικείμενα, φωτογραφίες κ.α.
- Στελέχωση παράνομων και εγκληματικών ομάδων. Εδώ, περιλαμβάνονται οι κινήσεις οι οποίες υποστηρίζουν αλλά και υποκινούν τις δραστηριότητες μαφίας και γενικότερα τρομοκρατικών ομάδων.
- Παράνομη διακίνηση υλικού (μουσικής, βίντεο κ.τ.λ.) χωρίς την νόμιμη κατοχύρωση πνευματικών δικαιωμάτων.
- Παράνομα στοιχήματα και χαρτοπαιξία. Στην συγκεκριμένη περίπτωση εξαιρούνται αντίστοιχες ενέργειες για τις οποίες έχει καταβληθεί στο κράτος η νόμιμη εισφορά από την εταιρία στοιχημάτων παρέχοντας ταυτόχρονα προστασία στον χρήστη.
- Οργανωμένες δολοφονικές επιθέσεις καθώς και δράσεις εκφοβισμού σε υψηλά πρόσωπα (FuandChen, 2010).

Εσφαλμένα εμφανίζεται η οι εντύπωση ότι οι δράστες των κυβερνοεπιθέσεων είναι άτομα που δρουν μεμονωμένα ή πρόκειται για ομάδες με εγκληματικό χαρακτήρα. Αντίθετα, οι δράστες των επιθέσεων στον κυβερνοχώρο μπορούν εξίσου να είναι πολυεθνικές εταιρίες οι οποίες πίσω από την θέση υπεροχής που έχουν εκμεταλλεύονται καταστάσεις και υποκλέπτουν στοιχεία είτε από ανταγωνίστριες εταιρίες είτε από άλλα κράτη (ChertoffandSimon,2015).

Οι ομάδες του darkwebλειτουργούν όπως λειτουργούν οι ομάδες σε φυσικό περιβάλλον. Μέσα από το darkweb ελλοχεύει υψηλός κίνδυνος αναφορικά με την διεθνή ασφάλεια και πολλά κράτη εμφανίζουν αδυναμία σύλληψης των παράνομων οργανώσεων και ατόμων. Εμφανίζεται παράλληλα η ιδιαιτερότητα και ο προβληματισμός ότι ο δράστης ή οι δράστες εντοπίζονται σε εικονικό περιβάλλον αλλά η σύλληψή τους γίνεται σε πραγματικό περιβάλλον (ChertoffandSimon,2015).

Τέλος, οι εγκληματικές ενέργειες στον κυβερνοχώρο πέρα από τις συνέπειες που έχουν ως παράνομες πράξεις, είναι πιθανό να επηρεάσουν και το σύνολο των

χρηστών έμμεσα. Προβλήματα στην αγορά και στην παραγωγικότητα μιας χώρας εμφανίζονται εξαιτίας της παραοικονομίας και της μαύρης αγοράς πράγμα που βάζει σε κίνδυνο την εύρυθμη λειτουργία των θεσμών και της κοινωνικής ευημερίας ενώ παράνομα αγαθά που διατίθενται προς πώληση χωρίς τον αντίστοιχο έλεγχο για την ποιότητά τους μπορεί να επιφέρουν μια σειρά από αρνητικές συνέπειες για το άτομο που θα το πάρει εν τέλει(ChertoffandSimon,2015).

1.3. Τύποι απειλών στον Κυβερνοχώρο

Οι απειλές που μπορεί να δεχθεί η ασφάλεια του κυβερνοχώρου μπορούν να ταξινομηθούν ως εξής:

- Cybercrime. Πρόκειται για το κυβερνοέγκλημα με σκοπό την αποδιοργάνωση των συστημάτων των υπολογιστών με στόχο την απόσπαση χρηματικών ποσών από τα θύματα, τις απειλές και την πρόκληση ζημιών.
- Cyberattack. Αφορά την λεγόμενη κυβερνοεπίθεση η οποία σχετίζεται ως επί των πλείστων για συγκέντρωση στοιχείων για πολιτικούς λόγους.
- Cyberterrorism. Αναφέρεται στην κυβερνοτρομοκρατία η οποία προκαλεί πανικό και τρόμο εφόσον επιδιώκει την υπονόμευση των ηλεκτρονικών συστημάτων των εκάστοτε θυμάτων.

Περαιτέρω, οι μέθοδοι που χρησιμοποιούνται από τους δράστες για να απειλήσουν την ασφάλεια στον κυβερνοχώρο είναι οι εξής:

1. Malware.

Πρόκειται για ένα λογισμικό κακόβουλο και είναι η πιο κοινή απειλή στον κυβερνοχώρο. Σκοπός του κυβερνοεγκληματία ή χάκερ που χρησιμοποιεί το συγκεκριμένο λογισμικό είναι να βλάψει τον υπολογιστή του νόμιμου χρήστη. Μέσω του ηλεκτρονικού ταχυδρομείου ή μέσω μιας λήψης η οποία φαίνεται νόμιμη, το malware επιτυγχάνει την διάδοσή του. Οι εγκληματίες που το χρησιμοποιούν το λογισμικό αποβλέπουν στην επίτευξη οικονομικού ή πολιτικού κέρδους. Με τη σειρά του το λογισμικό διακρίνεται σε:

- Ιούς (Virus): «μολύνουν» αρχεία μέσω κακόβουλων κωδικών ενώ αναπαράγονται αυτόματα στο υπολογιστικό σύστημα.

- Δούρειος Ίππος (Trojan Horse): οι εγκληματίες του κυβερνοχώρου εξαπατούν τους νόμιμους χρήστες προωθώντας Trojans στα υπολογιστικά τους συστήματα δημιουργώντας ζημιές και αποσπώντας πληροφορίες και δεδομένα.
- Spyware: προγράμματα τα οποία καταγράφουν κρυφά τις κινήσεις των χρηστών και μ αυτό τον τρόπο αποσπώνται πληροφορίες από τους εγκληματίες του κυβερνοχώρου. Παράδειγμα spywareαποτελεί το λογισμικό υποκλοπής αριθμών πιστωτικών καρτών και κωδικών.
- Ransomware: μέσω του συγκεκριμένου λογισμικού, οι χάκερς κλειδώνουν την πρόσβαση στο σύστημα ηλεκτρονικού υπολογιστή του χρήστη καθώς και κρυποτγραφούν τα δεδομένα έως ότου ο χρήστης να καταβάλλει το αντίτιμο που ζητάνε και παρασχεί νέα άδεια χωρίς όμως να είναι απόλυτα σίγουρος ο χρήστης ότι θα καταφέρει να μπει στο σύστημα του ξανά.
- Adware: προωθεί ένα κακόβουλο λογισμικό μέσω διαφήμισης ενός προϊόντος.
- Botnets: οι εγκληματίες του κυβερνοχώρου εκτελούν διαδικτυακές εργασίες μέσω ενός μολυσμένου δικτύου υπολογιστών χωρίς την συγκατάθεση του χρήστη.

2. SQL injection. Πρόκειται για έναν τύπο επίθεσης στον κυβερνοχώρο με στόχο τον έλεγχο και την υποκλοπή πληροφοριών από διάφορες βάσεις δεδομένων. Οι δράστες εισάγουν ένα κακόβουλο κώδικα εκμεταλλευόμενοι τις ευπάθειες των εφαρμογών διαχείρισης δεδομένων και φέρουν αρνητικές συνέπειες στις βάσεις δεδομένων που επιτίθενται.

3. Ηλεκτρονικό ψάρεμα (Phishing). Το ηλεκτρονικό ψάρεμα ή αλλιώς Phising είναι μια διαδεδομένη μέθοδος κατά την οποία αποστέλλονται ψευδή μηνύματα στους χρήστες ηλεκτρονικών ταχυδρομείων και τα οποία φαίνονται ως κανονικά εισερχόμενα μηνύματα από οικείους και αξιόπιστους αποστολείς. Στόχος του ηλεκτρονικού ψαρέματος είναι η υποκλοπή σημαντικών προσωπικών πληροφοριών και δεδομένων όπως για παράδειγμα αριθμούς τραπεζικών λογαριασμών και καρτών.

4. Επίθεσηαπό Man in the middle. Η συγκεκριμένη επίθεση αφορά την υποκλοπή μιας επικοινωνίας μεταξύ δυο ή περισσότερων συνομιλητών μέσω ενός μη

ασφαλούς Wi-Fi με στόχο την αποκόμιση σημαντικών προσωπικών πληροφοριών από τους χρήστες.

5. Denialofserviceattack. Ηεπίθεση αυτή γίνεται από τους εγκληματίες του κυβερνοχώρου με σκοπό να αχρηστεύσουν δίκτυα και διακομιστές. Βασική συνέπεια της συγκεκριμένης επίθεσης είναι τα συστήματα να μην «υπακούουν» στις νόμιμες εντολές των χρηστών τους και να πρέπει να εκτελεσθούν λειτουργίες ζωτικής φύσης για τον οργανισμό που τα διαθέτει προκειμένου να τα επαναφέρει (Al-Rowailyetal., 2015).

1.4. Η Κυβερνοτρομοκρατία

Σε παγκόσμιο επίπεδο τα τελευταία χρόνια, η τρομοκρατία στον κυβερνοχώρο αποτελεί μια πρόκληση τόσο για την Δημόσια Διοίκηση, όσο και για τις επιχειρήσεις και τους απλούς πολίτες. Στόχος των δραστών δεν αποτελεί ο φυσικός θάνατος ανθρώπων μέσω τρομοκρατικών ενεργειών αλλά η αναταραχή της παγκόσμιας τάξης και ασφάλειας καθώς και η αμφισβήτηση των ικανοτήτων των φορέων που προάγουν και εγγυώνται γι αυτήν(Caruso and Locatelli, 2014).

Στα πλαίσια της τρομοκρατίας περιλαμβάνεται η αγοραπωλησία όπλων τα οποία χρησιμοποιούνται για μαζική καταστροφή αλλά και χημικών ουσιών οι οποίες χρησιμοποιούνται ως πρώτη ύλη για την βάση δημιουργίας βιολογικών όπλων. Για το υπάρχον κλίμα ασφαλείας αυτή η ανικανότητα ελέγχου ενεργεί με πολλαπλασιαστικό τρόπο και ταυτόχρονα με μεγάλη ευκολία ολοκληρώνεται ο στόχος της αποδιοργάνωσης της εξουσίας με συνολικές συνέπειες σε πολιτικό και κοινωνικό επίπεδο (Caruso and Locatelli, 2014).

Οι τρομοκράτες στο διαδίκτυο αποτελούν μια συνεχή απειλή ενώ η «δύναμή» τους αντλείται από την ικανότητά τους να είναι αόρατοι και ταυτόχρονα μονίμως παρόντες. Αυτή η ασαφής εικόνα των τρομοκρατών και το πεδίο που ενεργούν να αυξάνει συνεχώς και ασαφώς αποτελεί έναν δύσκολο και άνισο αγώνα προσπάθειας για δικαιοσύνη και ασφάλεια(Caruso and Locatelli, 2014).

Για το λόγο αυτό ο μεγαλύτερος αριθμός τρομοκρατικών οργανώσεων έχουν διαφορετικές έδρες-χώρες ενώ το σύστημα ιεραρχίας τους είναι περίπλοκο προκειμένου να μην εντοπίζονται εύκολα. Επίσης η επικοινωνία τους στηρίζεται σε

υβριδικά δίκτυα και σε ανύποπτη στιγμή παραβιάζουν τα συστήματα ασφαλείας, δημοσιοποιούν γραπτές διακηρύξεις και γενικότερα προχωρούν σε απειλές. Η εύρεση και προσέλκυση επιπλέον τρομοκρατών γίνεται μέσω των μέσω της κοινωνικής δικτύωσης ενώ η προπαγάνδα και η πειθώ είναι οι δυο τρόποι που χρησιμοποιούν για να οικειοποιηθούν κι άλλοι αυτή την παράνομη συμπεριφορά(Caruso and Locatelli, 2014).

Όπως συμβαίνει και στο πραγματικό περιβάλλον έτσι και στον κυβερνοχώρο, οι οργανώσεις τρομοκρατίας επιδιώκουν να αρπάζουν τις κατάλληλες ευκαιρίες και εκμεταλλεύονται την κατάλληλη στιγμή προκειμένου να «χτυπήσουν». Έτσι, για παράδειγμα χώρες οι οποίες έχουν πληγεί ή διέπονται από γενικές κρίσεις αυξάνουν τις πιθανότητες κυβερνοεπίθεσης. Το ίδιο ισχύει και τις χώρες που έχουν στρατηγικό ενδιαφέρον ή που αποτελούν την βάση για πολλές και ποικίλες επιχειρηματικές δραστηριότητες. Η ειδοποιός διαφορά και το ζητούμενο είναι να έχουν τις ικανότητες να ενδυναμώνουν τον κυβερνοχώρο διαρκώς μέσα από τους υπεύθυνους φορείς για να μπορούν να αντιμετωπίσουν τις επιθέσεις(Caruso and Locatelli, 2014).

1.5. Αίτια κυβερνοτρομοκρατίας

Βασική πηγή αιτιών για την ύπαρξη και πραγματοποίηση της τρομοκρατίας στον κυβερνοχώρο προέρχεται από τα διάφορα φαινόμενα που συμβαίνουν σε κάθε κοινωνία. Τα κράτη μεταξύ τους αλληλοεξαρτώνται εξαιτίας της παγκοσμιοποιημένης κοινωνίας και μ αυτόν τον τρόπο οι σύγχρονοι άνθρωποι αντιμετωπίζουν όχι απλά κοινά προβλήματα αλλά αλληλοεξαρτώμενα ενώ οι συγκρούσεις και οι προστριβές εκδηλώνονται σε όλα τα επίπεδα. Οι διαφορές μεταξύ αναπτυγμένου και υποανάπτυκτου κόσμου προκύπτουν από τις στερεοτυπικές και παραδοσιακές αντιλήψεις οι οποίες διαταράσσουν το διεθνές σύστημα(Caruso and Locatelli, 2014).

Επομένως, τα προβλήματα που λαμβάνουν χώρα σε κάθε κοινωνία αποτελούν την αιτία για την πραγματοποίηση κυβερνοαπειλών. Η διαρκής αμφισβήτηση για παράδειγμα των δικαιωμάτων διαφόρων μειονοτήτων στις αναπτυγμένες χώρες, ο θρησκευτικός φανατισμός κ.α. έχουν ως συνέπεια εκδηλώσεις ρατσισμού. Οι «θιγμένες» μειονότητες χρησιμοποιούν το διαδίκτυο για να εκφραστούν και μέσα από την ανωνυμία τους προστατεύουν τα προσωπικά τους δεδομένα. Σ αυτό το πλαίσιο, οι

επιθέσεις που εκδηλώνονται στο διαδίκτυο δεν χαρακτηρίζονται πάντα ως εγκλήματα που διώκονται ποινικά γιατί δεν απειλούν άμεσα την ασφάλεια όπως για παράδειγμα την δημοσιοποίηση υλικού και εικόνων με χιουμοριστική διάθεση από μια ομάδα σ έναν ιστότοπο(Bräuchler, 2007).

Παρόλα αυτά, η Ευρωπαϊκή Ένωση επιδιώκει μεταρρυθμίσεις νομικής φύσεως οι οποίες «εμποδίζουν» την ρητορική μίσους έστω και με τρόπο χιουμοριστικό καθώς μπορεί να πραχθεί το μίσος σε εγκληματικές ενέργειες και εκδηλώσεις ρατσιστικής βίας, οι οποίες μπορούν να πραγματοποιηθούν και στον ψηφιακό κόσμο απειλώντας την ανθρώπινη ζωή, προσβάλλοντας την ανθρώπινη αξιοπρέπεια αλλά και την ασφάλειά όλων(Bräuchler, 2007).

Επίσης, βασική επιδίωξη της Ευρωπαϊκής ένωσης αποτελεί η συνεργασία όλων των ευρωπαϊκών χωρών για να συντονιστούν και να περιορίσουν από κοινού όχι μόνο τον ρατσισμό αλλά και τα εγκλήματα που προκύπτουν από αυτήν την ιδέα.

1.6. Κυβερνοεπίθεση και Δημόσια Διοίκηση

Στα πλαίσια της Δημόσιας Διοίκησης, οι κυβερνοεπιθέσεις πλήττουν ηλεκτρονικά συστήματα ζωτικής σημασίας για την κοινωνία. Έτσι σύμφωνα με έρευνες του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), οι τομείς που απειλήθηκαν περισσότερο κατά το 2021 στον τομέα της κυβερνοασφάλειας ήταν οι εξής:

- Δημόσια Διοίκηση και Διακυβέρνηση
- Πάροχοι Ψηφιακών Υπηρεσιών
- Ευρύτερο Δημόσια
- Υγεία
- Χρηματοοικονομικά (http://www.sepe.gr/).

Σε συνέχεια τη έρευνας υπήρξαν 198 περιπτώσεις ψηφιακού εγκλήματος στη δημόσια διοίκηση, 152 περιπτώσεις αναφορικά με τους παρόχους ψηφιακών υπηρεσιών, 143 περιπτώσεις στον τομέα της υγείας, 151 περιπτώσεις στον ευρύτερο δημόσιο και τέλος 97 περιπτώσεις στον χρηματοοικονομικό/τραπεζικό τομέα. (http://www.sepe.gr/).

Σύμφωνα πάλι με τον ENISA, οι Ευρωπαίοι με ποσοστό 76% θεωρούν ότι διατρέχουν υψηλό κίνδυνο να πέσουν θύματα κυβερνοεγκλήματος. Η δημιουργία νέων απειλών κατά της κυβερνοασφάλειας πηγάζει σε μεγάλο βαθμό από την ψηφιακή πρόοδο στα κράτη-μέλη

Το ransomware θεωρείται μια από τις κυριότερες απειλές στην Ευρώπη. Σύμφωνα με στοιχεία της Ευρωπαικής Ένωσης το παγκόσμιο κόστος των ζημιών από επιθέσεις του συγκεκριμένου λογισμικού έφτασε τα €18 δισ., το 2021 σε σχέση με το 2015 όπου ήταν 57 φορές μικρότερο το ποσό (http://www.sepe.gr/).

Επιπλέον, ο μέσος όρος καταβολής λύτρων διπλασιάστηκε από €71.000 το 2019 στα €150.000 το 2021 ενώ κάθε 11 δευτερόλεπτα συνέβαινε επίθεση ransomware έναντι εταιρειών.

Εξίσου σημαντική απειλή είναι οι απειλές ηλεκτρονικού ταχυδρομείου όπου οι επιθέσεις κατά παρόχων υπηρεσιών με στόχο την πρόσβαση σε προσωπικά δεδομένα πολιτών και πελατών ολοένα και αυξάνει (http://www.sepe.gr/).

1.7. Κυβερνοεπιθέσεις και κορονοιός

Η κρίση Covid-19 αποτέλεσε έναν ισχυρό παράγοντα τόσο για την ενεργοποίηση του ψηφιακού μετασχηματισμού σε μεγαλύτερο επίπεδο και την επιτάχυνση των μεταρρυθμίσεων σε σχέση με αυτό όσο και την δημιουργία νέων απειλών στον κυβερνοχώρο. Οι αντιδράσεις των κυβερνήσεων στην πανδημία εστίασαν στην λειτουργία των δημόσιων υπηρεσιών μέσω ηλεκτρονικών υπηρεσιών αλλά και με την χρήση τηλεργασίας για τους εργαζόμενους(https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/).

Η εξ αποστάσεως εργασία κατά την διάρκεια της πανδημίας αλλά πλέον και η καθιέρωσή της ως μορφή εργασίας συμβάλλει στην αύξηση του κινδύνου των απειλών στον κυβερνοχώρο. Οι εγκληματίες του διαδικτύου εκμεταλλεύονται τα μέτρα ασφαλείας του cloud αλλά και το ηλεκτρονικό ταχυδρομείο των υπαλλήλων που εργάζονται από το σπίτι ενώ γίνονται οι ίδιοι επίκεντρο στόχου καθώς διατηρούν παράλληλη σύνδεση με το διαδίκτυο της εταιρίας στην οποία εργάζονται(Bendovschi, 2015).

Την πανδημία του κορονοιού την εκμεταλλεύτηκαν οι κυβερνοεγκληματίες στοχεύοντας σε δημόσιους οργανισμούς και εταιρίες που χρησιμοποιούσαν την τηλεργασία σύμφωνα με το Ευρωπαϊκό Κοινοβούλιο, με αρνητικές συνέπειες σε όλα τα επίπεδα(Bendovschi, 2015).

Πρόσφατα μια από τις μεγαλύτερες κυβερνοεπιθέσεις δέχτηκετο Υπουργείο Ψηφιακής Διακυβέρνησης με επίκεντρο το TAXISnet, του οποίου οι λειτουργίες μπλοκαρίστηκαν για 48 ώρες (https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/).

Έγκυρες πηγές αναφέρουν ότι επρόκειτο για επίθεση τύπου DDoS με στόχο την προσωρινή αναστολή της λειτουργίας 800 ιστοτόπων του Δημοσίου. Οι συγκεκριμένοι ιστόποποι είτε αδυνατούσαν να «ανοίξουν» είτε το «άνοιγμά» τους γινόταν με αργό τρόπο (https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/).

Κατά τις επιθέσεις DDoS, οι δράστες διεισδύουν στην βάση δεδομένων αποκτώντας πρόσβαση σε ευαίσθητες πληροφορίες και εκμεταλλεύονται ευπάθειες ασφαλείας.

Εκατοντάδες υπηρεσίες του GOV.gr λειτουργούν με τη χρήση των κωδικών TAXISnet και έτσι προκλήθηκαν πολλά προβλήματα ανάμεσα σε άλλα να τερματίσει η ηλεκτρονική συνταγογράφηση. Οι γιατροί υποχρεώθηκαν να συνταγογραφούν χειρόγραφα ενώ ταυτόχρονα τα φαρμακεία δεν ήταν σε θέση να εκτελέσουν επείγουσες συνταγές (https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/).

Η Εθνική Αρχή Κυβερνοασφάλειαςανέλαβε δράση μέσω των τεχνικών των πληροφοριακών συστημάτων κάνοντας Geoblocking (γεωγραφικό αποκλεισμό) σε ολόκληρη την Ολλανδία, καθώς διαπιστώθηκε ότι το «μπλοκάρισμα» των ιστοτόπων του Δημοσίου προερχόταν από την Ολλανδία, όπου επίσης «χτυπήθηκε» το δίκτυο Azure της Microsoft (https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/).

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ: Η ΕΝΝΟΙΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Το δεύτερο κεφάλαιο προσεγγίζει την έννοια της κυβερνοασφάλειας ως αντίβαρο στην κυβερνοεπίθεση. Η ασφάλεια του κυβερνοχώρου αποτελεί πρόκληση για τον ψηφιακό μετασχηματισμό καθώς αφορά την προστασία των συστημάτων δικτύου και των χρηστών του από τη στιγμή που σήμερα ο δρόμος για την ψηφιακή αλλαγή είναι ανοιχτός. Το κεφάλαιο προσεγγίζει την έννοια της κυβερνοασφάλειας και τα στοιχεία που την απαρτίζουν, τους τύπους ασφαλείας καθώς και τα πλεονεκτήματα που παρέχονται στο πλαίσιο του ψηφιακού μετασχηματισμού στη Δημόσια Διοίκηση.

2.1. Κυβερνοασφάλεια

Το πρόθεμα «κυβερνό-» εσωκλείει τις έννοιες που έχουν σχέση με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο και καθώς σε ακαδημαϊκό επίπεδο δεν επιτυγχάνεται συμφωνία σε σχέση με την έννοια των όρωνγι αυτό το λόγο αυτό πραγματοποιούνται εναλλακτικές προσεγγίσεις.

Έχουμε ήδη αναφέρει ότι ο κυβερνοχώρος περιλαμβάνει τον ψηφιακό χώρο ο οποίος δημιουργείται από το διαδίκτυο χωρίς όμως να μπορεί να εκφράσει τις άπειρες δυνατότητες του διαδικτύου και για το λόγο αυτό είναι απαραίτητο να διευρυνθεί επιπλέον. Επομένως υιοθετούνται διάφοροι περιγραφικοί όροι ανάλογα την προσέγγιση που επιλέγεται.

Γενικά ο κυβερνοχώρος δεν περιορίζεται και το διαδίκτυο αποτελεί ένα περίπλοκο εικονικό κόσμο. Παρόλα αυτά, η πρόσβαση στο διαδίκτυο από έναν χρήστη δεν προϋποθέτει ειδικές γνώσεις αν και σε εξειδικευμένα μηχανήματα και προγράμματα με μεγάλο εύρος σίγουρα απαιτούνται.

Οι παράνομες δράσεις οι οποίες συμβαίνουν στο ψηφιακό περιβάλλον του διαδικτύου είναι αλληλένδετες και συνδεδεμένες με το πραγματικό περιβάλλον. Οι εγκληματικές οργανώσεις απειλούν τόσο την εθνική όσο και την διεθνήασφάλεια και οι εγκληματικές δραστηριότητες αφορούν το χακάρισμα και την παραβίαση των συστημάτων ασφαλείας είτε ιδιωτών είτε δημόσιων φορέων(https://lawsupport.gr/kivernoasfaleia/).

Η κυβερνοασφάλεια αφορά τη συλλογή λογισμικού, ανθρώπων, διαδικασιών και συστημάτων που προστατεύουν έναν οργανισμό από κυβερνοεπιθέσεις και διασφαλίζουν τη διαθεσιμότητα των πόρων. Επιπλέον, η κυβερνοασφάλεια αποτελεί έναν αυξανόμενο τομέα ανησυχίας, καθώς όλο και περισσότερες εταιρείες και άτομα μπαίνουν στο διαδίκτυο. Η ασφάλεια των πληροφοριών είναι εξίσου στα πλαίσια της κυβερνοασφάλειας. Συντελεί και συμβάλλει στην προστασία των πληροφοριών που έχουμε είτε στα κινητά τηλέφωνα είτε στους υπολογιστές. Εδώ αναφερόμαστε στην ασφάλεια απέναντι σε ιούς ή κακόβουλα λογισμικά ιδίως όταν χρησιμοποιείται ένα δημόσιο Wi-Fi. Σε γενικότερα πλαίσια, η κυβερνοασφάλεια αναφέρεται στην προστασία από χάκερς οι οποίοι θέλουν πρόσβαση σε ευαίσθητα προσωπικά δεδομένα για διάφορους λόγους (https://lawsupport.gr/kivernoasfaleia/).

Το οικονομικό κέρδος αποτελεί τον βασικό στόχο των επιθέσεων του κυβερνοχώρου ενώ οι κρίσεις που μπορεί να διανύουν οι χώρες είτε σε πολιτικό, είτε σε κοινωνικό ή οικονομικό επίπεδο αυξάνουν τις πιθανότητες να παραβιαστούν στα συστήματα ασφαλείας τους (https://lawsupport.gr/kivernoasfaleia/).

Σύμφωνα με έναν νομοθετικό ορισμό κατά την οδηγία της NIS η κυβερνοασφάλεια αφορά την δυνατότητα των συστημάτων δικτύου και πληροφοριών να αμύνονται σε συγκεκριμένο βαθμό αξιοπιστίας απέναντι σε δράσεις οι οποίες πλήττουν την ανθεκτικότητα, την ακεραιότητα, την διαθεσιμότητα και το απόρρητο των δεδομένων που αποθηκεύονται, που μεταφέρονται και επεξεργάζονται μέσα στα συστήματα δικτύου και πληροφοριών (Μήτρου, 2020).

Από ότι φαίνεται η ασφάλεια του κυβερνοχώρου σχετίζεται άμεσα με την πολιτική και την ισχύ. Η δύναμη της πολιτικής αποδίδεται μέσα από το διεθνές σύστημα ποικιλοτρόπως. Πολλές φορές χρησιμοποιείται η διπλωματία κι άλλες φορές χρησιμοποιείτε η ισχύς των ένοπλων δυνάμεων. Από την άλλη ι ισχύς είναι σημαντικά για τα κράτη καθώς ο κυβερνοχώρος είναι ατελείωτος ως περιβάλλον και πολλές φορές οι κανόνες ενός συμβατικού και παραδοσιακού χώρου παύουν να ισχύουν. Η κυβερνοισχύς μπορεί να είναι σκληρή (hardpower), ή ήπια (softpower) και η ανταγωνιστικότητα μεταξύ των κρατών είναι μεγάλη προκειμένου να λάβουν όλα μερίδιο ισχύος στον κυβερνοχώρο.

Το Oxford Dictionary περιγράφει την κυβερνοασφάλεια ως μια κατάσταση η οποία προστατεύει τις χρήσεις ηλεκτρονικών δεδομένων από εγκληματικές και μη εξουσιοδοτημένες χρήσεις.

Παρομοίως σύμφωνα με το Merriam – Webster, η κυβερνοασφάλεια αφορά ένα σύνολο μέτρων τα οποία εφαρμόζονται προκειμένου να προστατέψουν τα άτομα που χειρίζονται τους ηλεκτρονικούς υπολογιστές από κακοβουλες και μη εξουσιοδοτημένες επιθέσεις ή προσβάσεις.

Αναφορικά με τα λειτουργικά λάθη δεν έχει διατυπωθεί ακόμη κάποιος συγκεκριμένος ορισμός. Παρόλα αυτά η έννοια της κυβερνοασφάλειας σχετίζεται με την προστασία από διάφορους κινδύνους κα απειλές για τους ηλεκτρονικούς υπολογιστές και τα δεδομένα που εμπεριέχουν και γι αυτό η κυβερνοασφάλεια ως όρος συχνά αποτελεί συνώνυμο της ασφάλειας των πληροφοριών.

2.2. Τύποι ασφαλείας

Οι τομείς στους οποίες αναφέρεται η ασφάλεια αλλά και η κυβερνοασφάλεια ειδικότερα είναι:

• **Ασφάλεια Επικοινωνιών:** πρόκειται για τα μέτρα εκείνα που προστατεύουν από απειλές τεχνικής φύσης του κυβερνοχώρου και που είναι σε θέση να μεταβάλλουν τα χαρακτηριστικά στοιχεία του με τέτοιο τρόπο ώστε να δραστηριοποιείται σε ενέργειες που δεν είχαν προγραμματιστεί από τον ιδιοκτήτη τους ή τον σχεδιαστή τους και φυσικά ούτε από τον χρήστη του.

• **Ασφάλεια Λειτουργιών:** αφορά τα μέτρα εκείνα που προστατεύουν από την προγραμματισμένη διαφθορά διαδικασιών ή από την προγραμματισμένη ροή της εργασίας με συνέπεια τόσο για τους ιδιοκτήτες, τους σχεδιαστές και τους χρήστες πάνω στον στον προγραμματισμό που είχαν.

Ασφάλεια Πληροφοριών: σχετίζεται με τα μέτρα εκείνα που προστατεύουν από κλοπή, διαγραφή ή μεταβολή των δεδομένων τα οποία έχουν αποθηκευτεί στον κυβερνοχώρο ή απλώς μεταδίδονται.

• **Φυσική ασφάλεια:** όλα τα μέτρα τα οποία προστατεύουν από φυσικούς κινδύνους οι οποίοι έχουν την ικανότητα να επηρεάσουν και να διαταράξουν την ευημερία του κυβερνοχώρου.

• **Δημόσια και Εθνική ασφάλεια:** τα μέτρα που δημιουργούνται για την προστασία από κυβερνοεπιθέσεις οι οποίες αφορούν την φυσική ή κυβερνητική περιουσία προς όφελος του επιτιθέμενου. Ένα παράδειγμα αποτελούν οι επιθέσεις

DOS οι οποίες πραγματοποιήθηκαν σε κοινωφελείς επιχειρήσεις αλλά και σε άλλες διάφορες βασικές υποδομές.

• **Επιχειρησιακή ασφάλεια:**ο κάθε χρήστης κατά την απόκτηση της πρόσβασής του σε κάθε δίκτυο, αποκτά δικαιώματα καθώς επίσης και όρους για το που, με ποιον τρόπο αλλά και από ποιόν μπορούν να χρησιμοποιηθούν δεδομένα και να δημοσιοποιηθούν. Επίσης, εμπεριέχει και τις πρακτικές διασφάλισης της ακεραιότητας των περιουσιακών στοιχείων του εκάστοτε χρήστη.

• **Αποκατάσταση καταστροφών:**περιλαμβάνει τις διαδικασίες προσπάθειας ανταπόκρισης ενός οργανισμού απέναντι σε μια απειλή ασφάλειας του κυβερνοχώρου και στην απειλή απώλειας/διαγραφής των δεδομένων. Κάθε οργανισμός διαθέτει ένα σχέδιο και παρέχει δράσεις που εμπίπτουν στην αποκατάσταση των ζημιών αλλά και στην συνέχεια της λειτουργίας του ακόμη και με καθορισμένους όρους.

• **Εκπαίδευση χρηστών:**πολύ συχνά τα άτομα και περισσότερο οι ιδιώτες που χρησιμοποιούν το διαδίκτυο δεν γνωρίζουν αρκετά για τον συγκεκριμένο τομέα και δρουν με «επικίνδυνο» τρόπο. Χωρίς να το αντιλαμβάνονται οι υπάλληλοι επιχειρήσεων εισάγουν ιούς στον υπολογιστή και στα συστήματα ασφαλείας αφού προσπερνούν ορισμένα στάδια ασφαλείας. Για το λόγο αυτό, η εκπαίδευση των χρηστών κρίνεται αναγκαία και καθοριστική προκειμένου να διασφαλίζεται η ασφάλεια των ενεργειών τους. Η αποφυγή ακατάλληλων ιστοτόπων και το κατέβασμα αρχείων άγνωστης προέλευσης αλλά και η διαγραφή ύποπτων e-mail είναι τακτικές που μπορούν να εξασφαλίσουν σε μεγάλο βαθμό την ασφάλεια του κυβερνοχώρου.

2.3. Οφέλη της Κυβερνοασφάλειας

Σύγχρονες επιχειρήσεις επιδιώκουν να ερμηνεύσουν την νέα πραγματικότητα συνδυάζοντας τις τάσεις που επικρατούν στο εικονικό περιβάλλον με αυτές που επικρατούν στο φυσικό καθώς τα δυο αυτά περιβάλλοντα αναπόφευκτα αλληλοεπηρεάζονται. Προβλήματα που υφίστανται και επηρεάζουν τον πραγματικό κόσμο απασχολούν και εκφράζονται από τους χρήστες των μέσων κοινωνικής δικτύωσης του κυβερνοχώρου. Πολύ συχνά επίσης, απειλές και παράνομες δράσεις

που συμβαίνουν στον κυβερνοχώρο, ξεκινούν από το φυσικό περιβάλλον και ολοκληρώνονται στο εικονικό περιβάλλον και το ανάποδο, αποτελώντας εγκλήματα υβριδικού χαρακτήρα(Panchanatham, 2015).

Επομένως η κυβερνοασφάλεια προσφέρει διεθνή ασφάλεια και ειρήνη απέναντι σε εγκλήματα και απειλές εάν εντοπιστεί η σύνδεση μιας παράνομης ή εγκληματικής δράσης με την τρομοκρατία για παράδειγμα ή επίθεση στο πραγματικό περιβάλλον ενός κράτους(Panchanatham, 2015).

Έχει συνδεθεί ότι η επίθεση στον κυβερνοχώρο αποτελεί απειλή για την διεθνή ασφάλεια του φυσικού περιβάλλοντος με στόχους ανάλογους με αυτούς των τρομοκρατικών επιθέσεων αλλά και την αμφισβήτηση των θεσμών και του συστήματος το οποίο εκφράζεται και μέσα από το διαδίκτυο και επομένως επιδιώκεται η αποδιοργάνωση του(Kumar, & Somani, 2018).

Το θέμα της κυβερνοασφάλειας αφορά ένα πολυδιάστατο ζήτημα στην εποχή μάλιστα του ψηφιακού μετασχηματισμού των ιδιωτικών οργανισμών και της Δημόσιας Διοίκησης αλλά και γενικότερα στην ψηφιακή εποχή. Επιδιώκεται η συνεχή βελτίωσή της μέσα από την διερεύνηση των βασικών εννοιών που την αποτελούν ώστε να διερευνώνται λεπτομερώς και αποτελεσματικά οι στρατηγικές που οφείλει ο κάθε οργανισμός και το κάθε άτομο χωριστά να ακολουθεί καθώς και τους κινδύνους και το κόστος που εμπεριέχονται σ αυτές τις στρατηγικές. Σαφώς η προσέγγιση που υιοθετείται κάθε φορά είναι ανάλογη της οπτικής και των θεωριών που χρησιμοποιούνται κάθε φορά για το παρόν ζήτημα. Επομένως, οι πολιτικές και στρατηγικές για την μεγιστοποίηση της κυβερνοασφάλειας από κράτος σε κράτος διαφέρουν και έτσι διαφέρουν και τα συστήματα ασφαλείας τους(Kumar, & Somani, 2018).

Η ασφάλεια του κυβερνοχώρου που παρέχεται μέσα από την εφαρμογή μέτρων, προσφέρει την απαραίτητη προστασία σε δεδομένα και αρχεία τόσο των μικρών και των μεγάλων επιχειρήσεων ιδιωτικής ή δημόσιας σφαίρας. Η κυβερνοασφάλεια είναι εξαιρετικά σημαντική για την προστασία από επιθέσεις που πιθανό να βλάψουν την ίδια την επιχείρηση αλλά και τον ιδιώτη σε περίπτωση που τα δεδομένα βρεθούν σε κακόβουλα και λάθος χέρια(Grossetal., 2017).

Ιδίως στον τομέα της υγείας, τα ιατρικά δεδομένα τα οποία είναι προσωπικά και ευαίσθητα στοιχεία ασθενών υπό την ευθύνη των ιατρών είναι πολύ σημαντικό να είναι ασφαλή όπως το ίδιο ισχύει και για κυβερνητικά αρχεία τα οποία θα μπορούσαν να «απειλήσουν» ολόκληρα έθνη. Οι κυβερνοεπιθέσεις οι οποίες προσβάλλουν

οικονομικά στοιχεία και αρχεία από επιχειρήσεις αλλά και δημόσιους οργανισμούς του κράτους μέσω υποκλοπής και διαγραφής τους, οδηγούν σε σοβαρές απώλειες και προσβάλλουν την φήμη και την κοινωνική εμπιστοσύνη απέναντί τους(Grossetal., 2017).

Σε προληπτικό επίπεδο η κυβερνοασφάλεια συμβάλλει εξίσου θετικά. Συγκεκριμένα, η κυβερνοασφάλεια βοηθάει στην πρόληψη παραβιάσεων δεδομένων, στην πρόληψη της υποκλοπής προσωπικών δεδομένων και επιθέσεων αλλά και στην ορθή και αποτελεσματική διαχείριση κινδύνων(Grossetal., 2017).

Εάν ο οργανισμός διαθέτει τις κατάλληλες γνώσεις σχετικά με την ασφάλεια των δικτύων συνδυαστικά με ένα ολοκληρωμένο σχέδιο για την αντιμετώπιση τέτοιου είδους περιστατικών τότε έχει περισσότερες πιθανότητες να προλαμβάνει, να συγκρατεί και να διαχειρίζεται τις κυβερνοεπιθέσεις(Grossetal., 2017).

Το θέμα της κυβερνοασφάλειας έχει οφέλη τόσο σε ατομικό επίπεδο όσο και σε κοινωνικό και διεθνές ενώ ταυτόχρονα η διαδικασία είναι δύσκολη καθώς η συνεχής εξέλιξη της τεχνολογίας απαιτεί εγρήγορση και αντίληψη των απειλών.

2.4. Κυβερνοασφάλεια και Τεχνολογία

Η προστασία του κυβερνοχώρου τόσο αναφορικά με τα συστήματα, τα δίκτυα και τον εξοπλισμό παρέχεται τόσο από τεχνολογικά όσο και από ανθρώπινα μέσα. Η φύση και το πρόσωπο της ασφάλειας στον κυβερνοχώρο εξελίσσεται με ραγδαίους ρυθμούς και είναι το άμεσο αποτέλεσμα των διαφόρων τεχνικών που έχουν αναπτυχθεί μέχρι σήμερα.

Το πεδίο της τεχνολογίας διαδραματίζει καθοριστικό ρόλο στην ασφάλεια του κυβερνοχώρου ενώ η διασφάλιση της ασφάλειας των πληροφοριών αποτελεί μια από τις μεγαλύτερες προκλήσεις που αντιμετωπίζουν τα άτομα σήμερα. Καλούνται μάλιστα οι άνθρωποι να είναι σε θέση να αναγνωρίζουν, να γνωρίζουν και να προετοιμάζονται όσο το δυνατό καλύτερα σε σχέση για τις νέες απειλές του κυβερνοχώρου και να προστατεύονται.

Ο κλάδος του Διαδικτύου των Πραγμάτων (Internet of Things- IoT) αποτελεί για τους εγκληματίες του κυβερνοχώρου, στόχο πρώτης προτεραιότητας. Μέχρι το 2017 σύμφωνα με την πρόβλεψη του Business Insider θα υπάρχουν περισσότερες από

41 δισεκατομμύρια διαδικτυακές και συνδεδεμένες συσκευές Internet of Things (IoT) (Dileketal., 2015).

Ο συγκεκριμένος κλάδος σχετίζεται με την ανάπτυξη της τεχνητής νοημοσύνης και προϋποθέτει ένα υψηλό επίπεδο δυσκολίας και κατ' επέκταση τεχνογνωσίας.

Ολοένα και πιο έντονα τα τελευταία χρόνια η τεχνητή νοημοσύνη χρησιμοποιείται όλο και περισσότερο και τείνει να υποκαταστήσει την ανθρώπινη δραστηριότητα όπως για παράδειγμα αναφορικά με την ανάπτυξη αυτοματοποιημένων συστημάτων ασφαλείας που προορίζονται να αντικαταστήσουν τον άνθρωπο καθώς η ανάλυση μεγάλων όγκων δεδομένων κινδύνου γίνεται πολύ πιο γρήγορα (Dileketal., 2015).

Η Τεχνητή Νοημοσύνη φαίνεται να συμβάλει ουσιαστικά στην αναγνώριση των κινδύνων μεταξύ των οργανισμών αλλά ταυτόχρονα και στην διεύρυνση των εγκληματικών δικτύων. Οι κυβερνοεπιθέσεις είναι αυτοματοποιημένες και τα δίκτυα στρέφονται σε τακτικές κλοπής μοντέλων και δηλητηρίασης επιθέσεων. Οι ρυθμοί ανάπτυξης κινδύνων συμβαδίζουν με την ανάπτυξη της τεχνολογίας ενώ οι μέθοδοι που υιοθετούν οι εγκληματίες γίνονται ολοένα και πιο εξελιγμένοι. Τέτοιες μέθοδοι είναι το ransomware το οποίο αναζητά συγκεκριμένους τύπους αρχείων έχοντας την δυνατότητα να κρυπτογραφεί shadow files, αντίγραφα ασφαλείας και ονόματα αρχείων, πράγμα που δυσκολεύει την ανάκτησή τους. Οι χάκερς δε αποζητούν λύτρα ως απάντηση και αντίδοτο της πρόσβασης στα κλεμμένα αρχεία και η λήψη πληρωμών πραγματοποιείται μέσω κρυπτονομισμάτων τα οποία δεν μπορούν να εντοπιστούν.

Υπάρχουν εικονικά ιδιωτικά δίκτυα γνωστά ως VPN και τα οποία χρησιμοποιούνται παγκόσμια από επιχειρήσεις και τμήματα πληροφορικής ως ασπίδα προστασίας στο εσωτερικό δίκτυο των εταιρειών από απομακρυσμένους χρήστες καθώς και το πρόγραμμα Zero-Trust Network Access (ZTNA).

Ένα καθοριστικό μέτρο ασφαλείας, ιδίως για τις εταιρίες, είναι η ορθή αξιολόγηση της ταυτότητας των ατόμων με άξονα την κατάλληλη πρόσβαση στα κατάλληλα άτομα την κατάλληλη στιγμή προκειμένου να προστατεύονται τα δίκτυα των εταιριών (Bendovschi, 2015).

2.4.1. Χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων

Ως αξιόπιστο και δοκιμασμένο πρότυπο στον τομέα της ασφάλειας της τεχνολογίας των πληροφοριών αποτελούν οι κωδικοί πρόσβασης. Πρόκειται για τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA), του οποίου η χρήση δίνει εξουσιοδότηση στους χρήστες λαμβάνοντες υπόψη δυο ή περισσότερους διαφορετικούς παράγοντες προκειμένου να έχουν πρόσβαση σε ευαίσθητα δεδομένα παρέχοντας ένα πρόσθετο επίπεδο προστασίας έναντι των παραβάσεων των δεδομένων και των κακόβουλων επιθέσεων.

Τα αρχικά MFA αποτελούν συντομογραφία της λέξης «έλεγχος ταυτότητας πολλαπλών παραγόντων» και έχει να κάνει με την χρήση πολλαπλών μεθόδων ελέγχου ταυτότητας την ίδια στιγμή. Στους χρήστες προτείνεται να αλλάζουν τις μεθόδους αυθεντικοποίησης πολλαπλών παραγόντων σε αυθεντικοποιητές που στηρίζονται σε εφαρμογές και όχι σε φωνητικά ή γραπτά μηνύματα καθώς ορισμένα είδη πιστοποιήσεων η χάκερς τα παρακάμπτουν.

Οι πρόσφατες εξελιγμένες επιθέσεις έχουν ως στόχο την παράκαμψη του MFA και

οι οργανισμοί πρέπει να λαμβάνουν επιπλέον προφυλάξεις όπως:

- Στο Active Directory παρακολούθηση της δραστηριότητας σύνδεσης και των συμβάντων
- Μείωση των λογαριασμών και των υπηρεσιών που χρησιμοποιούν MFA και περαιτέρω ανάλυσή τους
- Τακτική επικαιροποίηση των στοιχείων των χρηστών και όλων των επιδιορθώσεων
- Ελεγχο ταυτότητας όχι πολλαπλών ταυτοτήτων αλλά μόνο δύο παραγόντων (2FM) με την αρχιτεκτονική μηδενικής εμπιστοσύνης τους.

2.4.2. Απόρρητα Δεδομένα

Οι σύγχρονες επιχειρήσεις καλούνται να προχωρούν σε επιπλέον προφυλάξεις όπως την κρυπτογράφηση των δεδομένων τους, την διασφάλιση των δικτύων τους και την χρήση κωδικών πρόσβασης. Μάλιστα, οι σύγχρονες επιχειρήσεις καλούν τους υπαλλήλους τους να διαφυλάξουν τα στοιχεία τους και τις προσωπικές πληροφορίες με ανεξάρτητες προσπάθειες. Είναι πολύ σημαντικό να αντιλαμβάνεται κανείς ότι οι πληροφορίες και τα δεδομένα μεταφέρονται μέσα από κανάλια επικοινωνίας τα οποία συνδέονται με

δίκτυα υπολογιστών διακλαδισμένα. Επειτα επεξεργάζονται μέσα από μια μεγάλη ποικιλία εφαρμογών και στη συνέχεια αποθηκεύονται. Παράλληλα, τα πληροφοριακά συστήματα υφίστανται διαρκώς αλλαγές και αυτό καθιστά τη διαδικασία διασφάλισης της ασφάλειας ως μια διαδικασία επ' αόριστον η οποία χρειάζεται να προσεγγίζεται συνεχώς (Dileketal., 2015).

Αναζητούνται και διερευνούνται τεχνολογίες που εξασφαλίζουν συνεπή και αξιόπιστα κανάλια επικοινωνίας και όλα τα μέτρα προστασίας που εφαρμόζονται ενισχύονται με πρόσθετα μέτρα ασφαλείας όπως για παράδειγμα την εφαρμογή νέων γενιών τειχών προστασίας και την επιβολή χαρακτηριστικών, τακτικών και μεθόδων ασφαλείας για όλους τους χρήστες ανεξαρτήτου τοποθεσίας (Dileketal., 2015).

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ: Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

Το τρίτο και τελευταίο κεφάλαιο της βιβλιογραφικής ανασκόπησης έχει ως στόχο την ανάλυση της κυβερνοασφάλειας σε σχέση με την Ευρωπαϊκή Ενωση. Ειδικότερα, το παρόν κεφάλαιο εστιάζει στον τρόπο αντιμετώπισης των κυβερνοαπειλών μέσα από την προώθηση της κυβερνοασφάλειας και της κυβερνοανθεκτικότητας. Επίσης, αναλύεται η διεθνής στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο καθώς και οι βασικές προτεραιότητες των στρατηγικών αυτών.

3.1. Ευρωπαϊκή Ένωση και Κυβερνοασφάλεια

Σε θέματα βελτίωσης της προστασίας των πολιτών και των επιχειρήσεων από το ηλεκτρονικό έγκλημα, η Ευρωπαϊκή Ένωση σημειώνει αλματώδη πρόοδο. Έχει ιδρύσει το ευρωπαϊκό κέντρο για εγκλήματα στον κυβερνοχώρο (IP/13/13), το οποίο προτείνει αντίστοιχη νομοθεσία αναφορικά με τις επιθέσεις κατά των συστημάτων

πληροφοριών (IP/10/1239) όπως επίσης και την πρόταση μιας παγκόσμιας συμμαχίας με στόχο την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών στο διαδίκτυο (IP/12/1308).

Επίσης, η Ευρωπαϊκή Ένωση έχει δημιουργήσει έναν οργανισμό για την προστασίας της κυβερνοασφάλειας ο λεγόμενος ENISA και ο οποίος είναι προσηλωμένος στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρώπη.

Ο συγκεκριμένος οργανισμός έχει συνεργασία με επιχειρήσεις και οργανώσεις με στόχο την ενίσχυση της εμπιστοσύνης στην ψηφιακή οικονομία και την ψηφιακή ασφάλεια για τους πολίτες της Ευρωπαικής Ένωσης καθώς και την τόνωση της ανθεκτικότητας των υποδομών της Ευρωπαϊκής Ένωσης (https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_el).

Η ανταλλαγή γνώσεων και η ανάπτυξη του προσωπικού και των δομών βοηθά στην διατήρηση και εξέλιξη της κυβερνοασφάλειας ενώ ο ENISA επιδιώκει μέσα από την κατάρτιση συστημάτων πιστοποίησης της κυβερνοασφάλειας να ενισχύσει την αξιοπιστία των ψηφιακών προιόντων και υπηρεσιών. Για τον λόγο αυτό συνεργάζεται με φορείς και χώρες της Ευρωπαϊκής Ένωσης και συμβάλλει στην προετοιμασία αντιμετώπισης των μελλοντικών προκλήσεων στον κυβερνοχώρο (https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_el).

Τέλος, ο ENISAλειτουργεί αφενός προς όφελος των δημόσιων οργανισμών αναφορικά με τα θεσμικά όργανα και τα αποκεντρωμένα όργανα των χωρών της Ε.Ε. ενώ επίσης βοηθά τον κλάδο των τηλεπικοινωνιών, την επιχειρηματική κοινότητα τόσο μικρές όσο και μεσαίες επιχειρήσεις, την ακαδημαική κοινότητα, τους εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας αλλά και το κοινό (https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_el).

3.2.Νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης

Η οδηγία NIS (NetworkInformationSystems) του 2016,αποτελεί μια νομοθετική πράξη σχετική με την ασφάλεια των δικτύων και πληροφοριών από την Ευρωπαϊκή Ένωση. Σύμφωνα με αυτήν την νομοθεσία τα κράτη μέλη δημιουργούν σχέσεις συνεργασίας και επιδιώκουν να συντονίσουν τις προσπάθειες τους για την ικανότητές τους να εξελιχθούν στην κυβερνοάμυνά τους. η Ευρωπαική Ένωση μάλιστα επιδιώκει την ενσωμάτωση του ρυθμιστικού αυτού πλαισίου στο εθνικό δίκαιο κάθε κράτους μέλους (NIS, 2021).

Επίσης, η παραπάνω οδηγία της Ευρωπαϊκής Ένωσης, θεσπίζει νομικά μέτρα τα οποία ενισχύουν την κυβερνοασφάλεια σε ολικό επίπεδο. Τα κράτη μέλη ήταν υποχρεωμένα να ενσωματώσουν στην εθνική τους νομοθεσία την οδηγία έως το 2018 και στη συνέχεια να καθορίσουν τους φορείς που αναλάμβαναν τις βασικές υπηρεσίες (Γενικός Κανονισμός, 2018).

Η Ελλάδα συμπεριέλαβε την παρούσα οδηγία το 2018 με τον νόμο 4577/2018 ενώ με την υπουργική απόφαση 1027/2019 διευθετήθηκαν και όσα ζητήματα προέκυψαν σε σχέση με την εφαρμογή της σε εθνικό επίπεδο.

Μέσω του προγράμματος «Συνδέοντας την Ευρώπη» και με χορηγία 38 εκατομμύρια ευρώ, το κάθε κράτος μέλος ενδυναμώνεται εθνικά με ομάδες οι οποίες διαχειρίζονται τα περιστατικά ασφαλείας σε ψηφιακά συστήματα Computer Security Incident Response Team (CSIRT) προκειμένου να εφοδιαστεί η Ευρώπη με εργαλεία και μηχανισμούς που θα είναι σε θέση να αντιμετωπίζουν τις κυβερνοεπιθέσεις (Γενικός Κανονισμός, 2018).

Επιπλέον, υπάρχει ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) ο οποίος είναι μια ακόμη πράξη νομοθετικού περιεχομένου και ισχύει και αυτή από το 2016 και εφαρμόζεται για κάθε κράτος μέλος. Πρόκειται για ένα αυστηρό θεσμικό πλαίσιο που αφορά την επεξεργασία και την προστασία των προσωπικών δεδομένων εισάγοντας την αρχή της Λογοδοσίας (Accountability Principle), στην εθνική νομοθεσία κάθε κράτους μέλους ώστε οι επιχειρήσεις να διαχειρίζονται τις διαδικασίες και τα συστήματά τους με εναρμονισμένο τρόπο με τα δεδομένα του νέου Κανονισμού όταν συλλέγουν και επεξεργάζονται προσωπικές πληροφορίες (Γενικός Κανονισμός, 2018).

Ο Κανονισμός αυτός επιβαρύνει με διοικητικά πρόστιμα τις περιπτώσεις παράβασης των διατάξεών του, εφόσον δεν θεσπίζονται άλλα μέτρα. Μάλιστα τα

πρόστιμα αυτά φτάνουν τα 10.000.000 ευρώ ή μπορεί να φτάσει το 2% του ολικού παγκόσμιου κύκλου εργασιών της προηγούμενης οικονομικής χρονιάς ένα αφορά επιχειρήσεις (Γενικός Κανονισμός, 2018).

3.3. Στόχοι και Γενικές Αρχές

Βασικός πυλώνας της οικονομίας της Ελλάδας αποτελεί η ανάπτυξη αι η ενδυνάμωση των ψηφιακών υπηρεσιών αλλά και των αγορών προκειμένου να παρέχει το ανταγωνιστικό πλεονέκτημα τόσο στην Ελλάδα αλλά και στην υπόλοιπη Ευρώπη. Η ανάγκη για Εθνική Στρατηγική Κυβερνοασφάλειας είναι μεγάλη καθώς η Ελλάδα συνεχίζει να προσπαθεί να αναπτυχθεί και επενδύει τόσο σε ιδιωτικούς όσο και σε Δημόσιους φορείς στον τομέα των ψηφιακών δικτύων, υπηρεσιών και αγορών. Οι αρχές που διέπουν την συγκεκριμένη Στρατηγική είναι(NIS, 2021) :

- Η δημιουργία και η εξέλιξη ενός κυβερνοχώρου οποίος θα είναι ασφαλής και ανθεκτικός και θα λειτουργεί σύμφωνα με κανόνες, πρότυπα και ορθές πρακτικές βασισμένες είτε σε εθνικό είτε σε ευρωπαϊκό επίπεδο.
- Οι πολίτες, οι επιχειρήσεις αλλά και οι φορείς θα δραστηριοποιούνται και θα αλληλεπιδρούν μεταξύ τους με ασφάλεια σύμφωνα με τις αξίες κάθε κράτους δικαίου και στόχο την ελευθερία, την διαφάνεια και την δικαιοσύνη.
- Δημιουργία κρίσιμων υποδομών και η εξασφάλιση της επιχειρησιακής συνέχειας για την διαρκή βελτίωση της παρεχόμενης προστασίας από διάφορες επιθέσεις στον κυβερνοχώρο.
- Η ενδυνάμωση του εθνικού πλαισίου της ασφάλειας του κυβερνοχώρου προκειμένου να μειώνονται όσο το δυνατό περισσότερο οι συνέπειες από τις κυβερνοαπειλές και να αντιμετωπίζονται αποτελεσματικά οι κυβερνοεπιθέσεις.
- Η δημιουργία και η ενίσχυση μιας κουλτούρας ασφαλείας στους πολίτες του ιδιωτικού και του δημόσιου φορέα σε συνδυασμό με την ακαδημαϊκή κοινότητα και άλλων ανάλογων φορέων και την αξιοποίηση των δυνατοτήτων τους.

Από την άλλη, οι στόχοι της Εθνικής Στρατηγικής Κυβερνοασφάλειας είναι (NIS, 2020) :

- Ενδυνάμωση των ικανοτήτων των δημόσιων και ιδιωτικών φορέων αναφορικά με την πρόβλεψη, την πρόληψη και την καταπολέμηση των συμβάντων κυβερνοασφάλειας με στόχο την ανάπτυξη της αντοχής και της αποκατάστασης των συστημάτων ΤΠΕ μετά από κυβερνοεπιθέσεις.
- Διαμόρφωση και ανάπτυξη ενός αποδοτικού πλαισίου που θα προωθεί τον συντονισμό και την συνεργασία προσδιορίζοντας τα επιμέρους καθήκοντα των εμπλεκόμενων μερών για την υιοθέτηση της Εθνικής Στρατηγικής της Κυβερνοασφάλειας.
- Συμμετοχή της χώρας σε δράσεις και πρωτοβουλίες σε εθνικό επίπεδο αναφορικά με την κυβερνοασφάλεια των οργανισμών προκειμένου να προάγεται η εθνική ασφάλεια.
- Συμμετοχή και συμβολή όλων των κοινωνικών φορέων και ενημέρωση και πληροφόρηση για την ασφάλεια και την προστασία των χρηστών από τις κυβερνοαπειλές.
- Συνεχής προσαρμογή του θεσμικού πλαισίου της χώρας στις νέες τεχνολογικές απαιτήσεις και καινοτομίες.
- Προαγωγή της καινοτομίας, της ανάπτυξης, της ανάλυσης θεμάτων σε σχέση με την ασφάλεια του κυβερνοχώρου.
- Ορθή αξιοποίηση βέλτιστων πρακτικών σε επίπεδο διεθνές.

Ο πυλώνας της Εθνικής Στρατηγικής Κυβερνοασφάλειας βοηθάει στην δημιουργία ενός ισχυρού κράτους δικαίου το οποίο διαθέτει ένα υψηλό επίπεδο ασφαλείας και ανθεκτικότητας απέναντι στις απειλές του κυβερνοχώρου με σεβασμό προς τα ευαίσθητα προσωπικά δεδομένα και τα κοινωνικά και ατομικά δικαιώματα. Τέλος, η Εθνική Στρατηγική Κυβερνοασφάλειας αποτελεί μοχλό ανάπτυξης της οικονομίας καθώς επιδιώκει την ασφάλεια όλων των οργανισμών, των επιχειρήσεων και όλων των φορέων που εμπλέκονται (NIS, 2021).

3.4.Νέα στρατηγική για την Κυβερνοασφάλεια

Τον Δεκέμβριο του 2020, η Ευρωπαϊκή Ένωση παρουσίασε μια νέα στρατηγική αναφορικά με την κυβερνοασφάλεια. Σύμφωνα με την συγκεκριμένη στρατηγική, η βελτίωση του ψηφιακού μέλλοντος της Ευρώπης, το σχέδιο ανάπτυξής

της και της στρατηγικής για την Ένωση Ασφάλειας είναι οι άξονες πάνω στους οποίους στηρίζεται(https://eur-lex.europa.eu/legalcontent/el/ALL/?uri=CELEX:32016L1148).

Η ενίσχυση της συνολικής ανθεκτικότητας απέναντι στις απειλές του κυβερνοχώρου και η διασφάλιση των πολιτών και των επιχειρήσεων για αξιόπιστες υπηρεσίες και ψηφιακά εργαλεία είναι μέρος της Νέας Στρατηγικής για την Κυβερνοασφάλεια στην Ευρώπη. Η Ευρώπη «παλεύει» για προστασία στον κυβερνοχώρο για όλους τους Ευρωπαίους που χρησιμοποιούν τις συνδεδεμένες συσκευές και το διαδίκτυο σε όλα τα επίπεδα είτε σε τράπεζες, είτε στις υγειονομικές δομές, τις δημόσιες υπηρεσίες κ.α. Παράλληλα, η Ευρωπαϊκή Ένωση μ αυτόν τον τρόπο επιδιώκει να ενισχύσει την ηγετική θέση αναφορικά με τους κανόνες και τα πρότυπα ασφαλείας που διέπουν τον κυβερνοχώρο καθώς και να προωθήσει συνεργασίες σε όλο τον κόσμο (https://eur-lex.europa.eu/legalcontent/el/ALL/?uri=CELEX:32016L1148).

Ένας διεθνής, ελεύθερος, σταθερός και ασφαλής κυβερνοχώρος είναι ο στόχος της Ευρωπαϊκής Ένωσης ο οποίος θα λειτουργεί βάσει δικαιοσύνης, σεβασμού, ατομικών ελευθεριών και δημοκρατίας. Για την επίτευξη ενός τέτοιου πλαισίου από την πλευρά του ανθρώπινου δυναμικού είναι η συμμετοχή του ανθρώπινου δυναμικού στη λήψη αποφάσεων και στην στοχοθέτηση. Η συμμετοχή στις αποφάσεις δημιουργεί έναν πιο ενεργό ρόλο των εργαζομένων και τους οδηγεί σε μια δέσμευση απέναντι στην εργασία τους και μια προθυμία για αφοσίωση, καινοτομία και δημιουργικότητα. Τέτοιου είδους αξίες συνεισφέρουν σε μια ασφαλή διοίκηση ανάμεσα στους εργαζόμενους και στον τρόπο λειτουργίας τους προκειμένου να προστατεύουν το χώρο στον οποίο βρίσκονται τόσο πραγματικά όσο και ψηφιακά (Konstantinidisetal., 2023).

Η νέα στρατηγική ανάπτυξη έχει ως αρχή να αξιολογεί τους παράγοντες εκείνους που επηρεάζουν την προθυμία του ανθρώπινου δυναμικού του εκάστοτε οργανισμού για την δέσμευσή τους απέναντι στις προαναφερθείσες αξίες με στόχο την ποιοτικότερη λειτουργία της Διοίκησης συμπεριλαμβανομένου και της κυβερνοασφάλειας (Konstantinidisetal., 2023).

Αξίζει να επισημανθεί ότι ανταμοιβές όπως το αίσθημα της ασφάλειας και η διατήρηση ενός ασφαλούς περιβάλλοντος στους εργαζόμενους, δημιουργεί ένα

αίσθημα επιτεύγματος καθώς και πρόκλησης στα πλαίσια της εργασίας τους ενώ ταυτόχρονα αυξάνει τα επίπεδα αποδοτικότητας (Kirkpatrick, 2009).

Για όλους τους παραπάνω λόγους η Ευρωπαϊκή Ένωση προτείνει οδηγίες που περιέχουν μέτρα τα οποία θα είναι κοινά για όλα τα κράτη-μέλη της Ευρώπης ώστε να εξασφαλιστεί ένα υψηλό επίπεδο ασφάλειας στον κυβερνοχώρο. Επίσης, κατέθεσε και μια οδηγία η οποία θα προωθεί την ανάλυση της ανθεκτικότητας των κρίσιμων οντοτήτων με στόχο την κάλυψη ενός μεγάλου ποσοστού καταπολέμησης των κινδύνων του διαδικτύου που υπάρχουν όσο και των εν δυνάμει. Με άλλα λόγια, η αξιολόγηση των κινδύνων σε επίπεδο επιχειρήσεων θα οδηγούν στην λήψη τεχνικών ή οργανικών μέτρων αλλά και στην δημοσιοποίηση περιστατικών για προληπτικούς λόγους(https://eur-lex.europa.eu/legalcontent/el/ALL/?uri=CELEX:32016L1148).

Τόσο το Συμβούλιο όσο και το Ευρωπαϊκό Κοινοβούλιο είναι υπεύθυνοι για την εξέταση και την εφαρμογή της οδηγίας NIS 2.

3.5. Ελλάδα και Κυβερνοασφάλεια

Αναφορικά με την Ελληνική Δημόσια Διοίκηση, η επίτευξη των στόχων τόσο της Ελληνικής Επικράτειας όσο και ευρύτερα της Ευρωπαϊκής Ένωσης αποτελεί μια δύσκολη κατάσταση, γεγονός που καθιστά απαραίτητη τη αξιοποίηση και την εφαρμογή μεθόδων και τακτικών παρακίνησης του ανθρώπινου δυναμικού προκειμένου να αυξηθεί η αποδοτικότητα και η αποτελεσματικότητα του. Σύμφωνα με τους Konstantinidisetal., 2023 οι εργαζόμενοι σε ελληνικές δασικές υπηρεσίες στην περιοχή Μακεδονίας και Θράκης θεωρούν ως πιο σημαντικό παράγοντα κινήτρων την ανάγκη των εργαζομένων να εργάζονται για το κοινό καλό και να μπορούν να πάρουν ενεργό μέρος σ' ένα σημαντικό όραμα πράγμα που πραγματοποιείται μέσα από την αναγνώριση της συνεισφοράς τους. Αυτά τα ευρήματα αποτελούν σημαντικές πληροφορίες και εργαλείο για όσους παρέχουν χάραξη πολιτικής προκειμένου όχι μόνο να είναι οι εργαζόμενοι αποδοτικοί αλλά και να παρέχουν ποιοτικές υπηρεσίες μέσα στα πλαίσια της τεχνολογικής ανάπτυξης.

Για την ψηφιακή ανάπτυξη της Ελλάδας φαίνεται ότι προϋπόθεση αποτελεί η δημιουργία και η διατήρηση ενός υψηλού επίπεδο ασφάλειας του κυβερνοχώρου τόσο των ψηφιακών υπηρεσιών όσο και των συστημάτων της. Η εμπιστοσύνη των

χρηστών στις ψηφιακές υπηρεσίες και τις εφαρμογές των νέων τεχνολογιών μπορεί να επέλθει μέσα από την βελτίωση της ασφάλειας του κυβερνοχώρου και την σταθερότητα αυτής της κατάστασης (Υπουργείο Ψηφιακής Διακυβέρνησης, 2021).

Παράλληλα, η ανάπτυξη των νέων τεχνολογιών και εφαρμογών έχει ταυτόχρονα ως αποτέλεσμα και περισσότερες ευκαιρίες για επιθέσεις στον κυβερνοχώρο. Λαμβάνοντας σοβαρά αυτή την σκέψη, η στρατηγική προσέγγιση οφείλει να είναι σφαιρική και μέσα από αυτή να καθορίζονται τα εξής:

- Καθορισμός των αξόνων παρέμβασης
- Καθορισμός στόχων
- Δημιουργία ενός πλαισίου δράσεων με ολιστική προσέγγιση
- Ενεργοποίηση και συντονισμός όλων των εμπλεκόμενων φορέων

(Υπουργείο Ψηφιακής Διακυβέρνησης, 2021).

Η ανατροφοδότηση σαφώς διαδραματίζει σημαντικό ρόλο σε όλη την διαδικασία της κυβερνοασφάλειας ενώ σε επίπεδο Ευρωπαϊκής Ένωσης, έχει εκδοθεί η Στρατηγική για την Ένωση Ασφάλειας 2020 -2025 (COM(2020) 605 final), όπου αναλύεται ο ρόλος της κυβερνοασφάλειας η Ελλάδα συμμετέχει κανονικά. Στο κοινό πλαίσιο που καθιερώνεται, η Ελλάδα αναγνωρίζει υπηρεσίες όπως αυτή των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) και των Παρόχων Ψηφιακών Υπηρεσιών (Π.Ψ.Υ.) καθώς επίσης υπάρχει συνεργασία με τον Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια (ENISA) με έδρα στην Ελλάδα προσφέροντας τεχνογνωσία, συμβουλές και πρακτικές για ενιαία

στρατηγική προς αντιμετώπιση των κινδύνων (Υπουργείο Ψηφιακής Διακυβέρνησης, 2021).

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ: ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ

Το παρακάτω κεφάλαιο προσδιορίζει την μεθοδολογία έρευνας που χρησιμοποιεί η παρούσα εργασία. Ειδικότερα, το τέταρτο κεφάλαιο αναλύει τον στόχο της έρευνας και τις επιμέρους ερευνητικές υποθέσεις, το δείγμα και την επιλογή της δειγματοληψίας. Επίσης, αναλύεται το ερωτηματολόγιο καθώς και ηεπιλογή της ποσοτικής έρευνας ως καταλληλότερης για την παρούσα έρευνα. Τέλος, προσδιορίζεται η εγκυρότητα και η αξιοπιστία της έρευνας προκειμένου να συνεισφέρει θετικά προς την υπόλοιπη επιστημονική βιβλιογραφία.

4.1. Ποσοτική Μέθοδος

Για την διεξαγωγή ερευνών χρησιμοποιούνται τόσο οι ποιοτικές όσο και οι ποσοτικές έρευνες και κατά βάση χρησιμοποιούνται τρία εργαλεία για την συλλογή των δεδομένων: το ερωτηματολόγιο, η συνέντευξη και η παρατήρηση. Σαφώς η κάθε μέθοδος παρουσιάζει πλεονεκτήματα αλλά και μειονεκτήματα (Παρασκευόπουλος, 1993).

Ως καταλληλότερη μέθοδος για την συλλογή πληροφοριών αναφορικά με τις απόψεις και τις αντιλήψεις των συμμετεχόντων στην έρευνα σε σχέση με την κυβερνοασφάλεια στα πλαίσια του ψηφιακού μετασχηματισμού της Δημόσιας Διοίκησης αλλά και τον βαθμό χρήσης του Διαδικτύου θεωρήθηκε η ποσοτική μέθοδος.

Παράλληλα, η παρούσα έρευνα χρησιμοποίησε την ποσοτική μέθοδο για διάφορους λόγους. Αρχικά, επεδίωξε τον έλεγχο περισσότερων από μια υποθέσεων, πράγμα που ενδείκνυται από την συγκεκριμένη μέθοδο. Επίσης, επεδίωξε να έχει μεγάλο δείγμα δεδομένων, τυχαίων δεδομένων αλλά και να προσδιορίσει στατιστικές σχέσεις ανάμεσα σε μεταβλητές, κάτι το οποίο το εξασφαλίζει η ποσοτική επίσης μέθοδος(Παρασκευόπουλος, 1993).

Ένα ακόμη βασικό πλεονέκτημα για την επιλογή της ποσοτικής μεθόδου αποτέλεσε η ανωνυμία των συμμετεχόντων και κατ’ επέκταση μειώνεται το επίπεδο προκαταλήψεων και ο ερευνητής αναλύει εξ ολοκλήρου τα στατιστικά στοιχεία που διαθέτει από την συλλογή των δεδομένων (Παρασκευόπουλος, 1993).

Η ποσοτική μέθοδος δίνει την δυνατότητα διερεύνησης μεταξύ των μεταβλητών, παρέχει αριθμητική απεικόνιση του υπό μελέτη δείγματος του πληθυσμού καθώς επίσης και την σχηματική απεικόνισή του (Creswell, 2014).

Τέλος, η ποσοτική μέθοδος προσέφερε την γρήγορη και ανέξοδη συλλογή των δεδομένων μέσω του ερωτηματολογίου ενώ επίσης η συμπλήρωσή του ήταν σχετικά εύκολη (Παρασκευόπουλος, 1993).

4.2. Σκοπός της έρευνας

Στόχος της παρούσας έρευνας καθώς και αντικείμενο μελέτης αποτελεί η διερεύνηση της έννοιας και της σημασίας της κυβερνοασφάλειας ως πρόκληση στα πλαίσια του ψηφιακού μετασχηματισμού στη Δημόσια Διοίκηση. Με άλλα λόγια, η εργασία εξετάζει τις απόψεις και τις στάσεις των πολιτών αναφορικά με την κυβερνοασφάλεια και την εκτίμηση της προστασίας τους κατά την χρήση του διαδικτύου και ιδιαίτερα των ηλεκτρονικών υπηρεσιών που αφορούν την Δημόσια Διοίκηση.

Σε θεωρητικό επίπεδο επιδιώκεται μια περιγραφή των πιθανών κινδύνων στο ψηφιακό πλαίσιο το οποίο λειτουργεί η Δημόσια Διοίκηση καθώς και η προσπάθεια προστασίας των πολιτών και των προσωπικών τους δεδομένων στα πλαίσια της κυβερνοασφάλειας ενώ σε πρακτικό επίπεδο εξετάζονται οι απόψεις των πολιτών σε σχέση με τα παραπάνω.

Επιμέρους ερευνητικά ερωτήματα που διερευνώνται μέσα από την έρευνα είναι τα εξής:

- Οι δημογραφικοί και κοινωνικοί παράγοντες όπως το φύλο, η ηλικία, το εκπαιδευτικό επίπεδο και η εργασιακή κατάσταση.
- Η αξιολόγηση του συνολικού βαθμού χρήσης του διαδικτύου από τους πολίτες.
- Τους παράγοντες εκείνους που βοηθούν να αισθανθούν ασφάλεια οι πολίτες από το διαδίκτυο
- Το φύλο, την ηλικία και το εκπαιδευτικό επίπεδο ως ποσοστιαίες διαφοροποιήσεις σε σχέση με την συνολική εικόνα της κυβερνοασφάλειας ανάμεσα στου πολίτες

- Την συζήτηση για μελλοντικές προτάσεις προς διερεύνησημε στόχο την βελτίωση της προστασίας της ασφάλειας των πολιτών από τους κινδύνους του διαδικτύου και των εφαρμογών της Δημόσιας Διοίκησης.

4.3. Δείγμα

Οι συμμετέχοντες της παρούσας έρευνας είναι ενήλικές και η συγκεκριμένη δειγματοληψία πηγάζει από τον γενικό πληθυσμό του Δήμου Σερρών. Συνολικά το δείγμα αποτέλεσαν 107 άτομα (N=107).

Το δείγμα είναι δείγμα ευκολίας καθώς υπήρξε η εύκολη και άμεση πρόσβαση με τα συγκεκριμένα άτομα.

4.4. Ερευνητικό Εργαλείο

Στην παρούσα εργασία χρησιμοποιήθηκε ως ερευνητικό εργαλείο το δομημένο ερωτηματολόγιο βασισμένο σε κλειστού τύπου ερωτήσεις. Πρόκειται για απλές και κατανοητές ερωτήσεις που διευκολύνουν το ερωτώμενο και εξασφαλίζουν την σαφήνεια και την αξιοπιστία του εργαλείου.

Ειδικότερα, το ερωτηματολόγιο είναι χωρισμένο σε 5 θεματικές και περιλαμβάνει συνολικά 27 ερωτήσεις. Η πρώτη θεματική αφορά τα δημογραφικά χαρακτηριστικά του δείγματος όπως το φύλο, την ηλικία, το εκπαιδευτικό επίπεδο και την εργασιακή κατάσταση. Στην συνέχεια, η δεύτερη θεματική σχετίζεται με την χρήση των ηλεκτρονικών υπηρεσιών και περιλαμβάνει 6 ερωτήσεις ενώ η τρίτη θεματική απαρτίζεται από 4 ερωτήσεις σχετικά με τους λόγους χρήσης του διαδικτύου. Στην τέταρτη θεματική το ερωτηματολόγιο εξετάζει μέσα από 7 ερωτήσεις, την ασφάλεια των ηλεκτρονικών υπηρεσιών και τέλος η πέμπτη θεματική με άλλες 7 ερωτήσεις εστιάζει στα μέτρα προστασίας των πολιτών απέναντι στους κινδύνους του διαδικτύου ως τρόπος αντιμετώπισης τους.

Οι απαντήσεις των ερωτήσεων βασίζονται τόσο σε τετραβάθμια όσο και σε πενταβάθμια κλίμακα Likert.

Αρχικά δηλώνοντας τον βαθμό συχνότητας από:

- Πολύ συχνά

- Συχνά
- Σπάνια
- Ποτέ

Δηλώνοντας τον βαθμό συμφωνίας/διαφωνίας:

- Συμφωνώ Απόλυτα
- Συμφωνώ
- Ούτε συμφωνώ/ούτε διαφωνώ
- Διαφωνώ
- Διαφωνώ απόλυτα

και τέλοστον ποσοτικό βαθμό :

- Πάρα πολύ
- Πολύ
- Αρκετά
- Λίγο
- Καθόλου

Το ερευνητικό εργαλείο δημιουργήθηκε ηλεκτρονικά με την βοήθεια του διαδικτυακού εργαλείου Google Forms ενώ στάλθηκε μέσω ηλεκτρονικού ταχυδρομείου όπως επίσης συλλέχθηκαν οι απαντήσεις με τον ίδιο τρόπο.

4.5. Ερευνητική διαδικασία

Η παρούσα έρευνα έλαβε χώρα στο Νομό Σερρών και η διαδικασία της έρευνας από τον διαμερισμό των ερωτηματολογίων έως την συλλογή των δεδομένων διήρκησε ένα μήνα, από τον Μάρτιο του 2023 έως τον Απρίλιο του 2023.

Το ερωτηματολόγιο χορηγήθηκε ηλεκτρονικά προς τους συμμετέχοντες ώστε να έχουν γρήγορη, άμεση και εύκολη πρόσβαση. Το ερωτηματολόγιο συμπληρωνόταν σε ατομικό επίπεδο μέσω εφαρμογής ερωτηματολογίου αυτοαναφοράς με συμπλήρωση ενώ υπήρξε συνοδευτικό εισαγωγικό σημείωμα στην αρχή του ερωτηματολογίου από την ερευνήτρια προκειμένου να διευκρινίζει τον σκοπό της έρευνας αλλά και να τονίσει την εμπιστευτικότητα, την ανωνυμία των προσωπικών δεδομένων των συμμετεχόντων αλλά και την εθελοντική τους συμμετοχή. Ταυτόχρονα, το εισαγωγικό σημείωμα τόνιζε την συμβολή της συμμετοχής των

ερωτηθέντων στην έρευνα καθώς και την προτροπή για αυθόρμητες και ειλικρινείς απαντήσεις.

Η ερευνητική διαδικασία ολοκληρώθηκε μέσα από την συλλογή, την ταξινόμηση και την κωδικοποίηση των πρωτογενών δεδομένων ενώ η στατιστική τους επεξεργασία πραγματοποιήθηκε μέσω του στατιστικού πακέτου JASP (Jeffreys'sAmazingStatisticsProgram).

4.6. Εγκυρότητα και αξιοπιστία της έρευνας

Όπως σε κάθε έρευνα έτσι και στην παρούσα, οφείλει ο ερευνητής να εξασφαλίσει την εγκυρότητα και την αξιοπιστία της έρευνας προκειμένου να διαθέσει και να συμβάλλει στην βιβλιογραφία αποδεκτά και αξιόπιστα αποτελέσματα.

Προκειμένου επομένως, η ερευνήτρια να ενισχύσει την διαφάνεια των στοιχείων που συνέλλεξε, επιβεβαίωσε αρχικά τους συμμετέχοντες για το ερευνητικό εμπιστευτικό και την διατήρηση της ανωνυμίας όλων των συμμετεχόντων (Cohen etal., 2000).

Επίσης, το ερωτηματολόγιο το οποίο ήταν εύκολο, απλό και αποτυπωμένο στην ελληνική γλώσσα επιτυγχάνοντας ότι το δείγμα κατανοεί καλά και επαρκώς τις ερωτήσεις, συνέβαλε στην εξασφάλιση της εγκυρότητας της έρευνας (Cohen etal., 2000).

Η παρούσα έρευνα θέλοντας να επιβεβαιώσει την αξιοπιστία εσωτερικής συνοχής μεταξύ των συσχετίσεων που εξετάζονται μέσα στο ερωτηματολόγιο χρησιμοποιεί τον δείκτη a του AlphaCronbach, σύμφωνα με τον οποίο οι τιμές που είναι μεγαλύτερες του 0,7 ή 0,8 θεωρούνται ικανοποιητικές. Η μέτρηση του δείκτη a έγινε με την βοήθεια του Jasp(Zikmundetal., 2011). Ειδικότερα ισχύει:

Cronbach'sAlpha	**Εσωτερική συνοχή**
$\alpha \geq 0.9$	Εξαιρετική
$0.9 > \alpha \geq 0.8$	Καλή
$0.8 > \alpha \geq 0.7$	Αποδεκτή

$0.7 > \alpha \geq 0.6$	Αμφισβητήσιμη
$0.6 > \alpha \geq 0.5$	Κακή
$0.5 > \alpha$	Μη αποδεκτή

Επομένως, προκειμένου να πραγματοποιηθεί έλεγχος της εσωτερικής συνέπειας των τιμών χρησιμοποιήθηκε ο συντελεστής αξιοπιστίας Cronbacha. Σε όσες μεταβλητές ο συντελεστής αξιοπιστίας είναι μικρότερος του 0,70 πρέπει να απορριφθούν.

Από τα παραπάνω φαίνεται ότι ο συντελεστής αξιοπιστίας είναι 0,74 >0,70 επομένως οι ερωτήσεις έχουν σωστό βαθμό αξιοπιστίας, πάνω από 70% και γι' αυτό δε χρειάζεται να απορριφθούν.

Frequentist Scale Reliability Statistics

Estimate	Cronbach's α
Point estimate	0.747
95% CI lower bound	0.682
95% CI upper bound	0.813

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ: ΣΤΑΤΙΣΤΙΚΗ ΑΝΑΛΥΣΗ ΔΕΔΟΜΕΝΩΝ

Το παρακάτω κεφάλαιο αναλύει στατιστικά τα δεδομένα που συλλέχθηκαν για την υλοποίηση της παρούσας έρευνας. Ακολουθούν τόσο περιγραφική ανάλυση όσο και στατιστική με την βοήθεια των πινάκων και των διαγραμμάτων. Τέλος, ακολουθούν συσχετίσεις αναφορικά με τις μεταβλητές.

5.1. ΔΗΜΟΓΡΑΦΙΚΑ ΣΤΟΙΧΕΙΑ

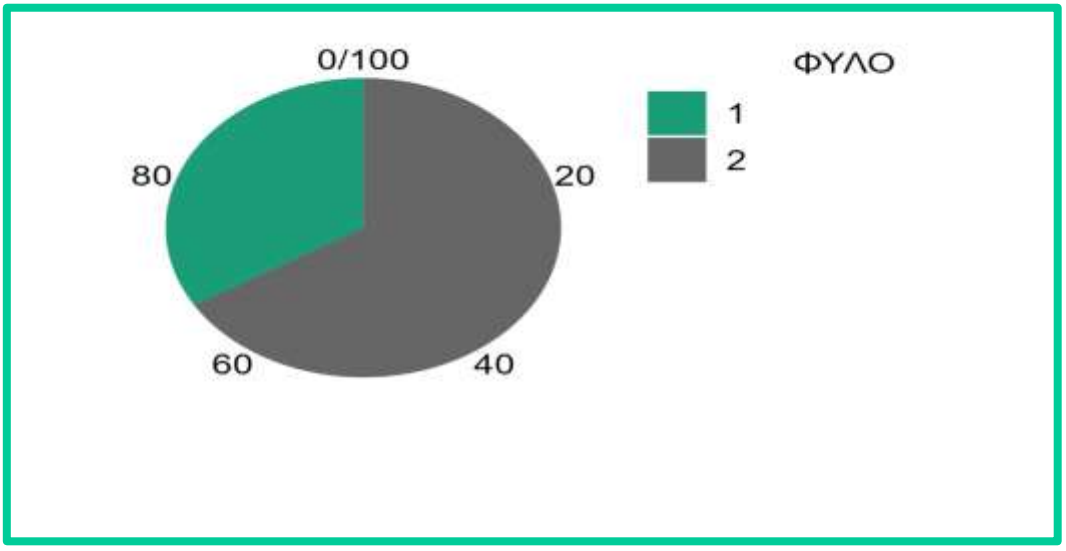
1. ΦΥΛΟ

Σύμφωνα με την ανάλυση των δεδομένων, το δείγμα μας αποτελείται από 71 γυναίκες το οποίο αντιστοιχεί σε ποσοστό 66,3% έναντι των ανδρών που είναι 36 με ποσοστό 33,6%.

Όπου 1= Άνδρας, 2=Γυναίκα

Πίνακας 1.

ΦΥΛΟ	Frequency	Percent	Valid Percent	Cumulative Percent
1	36	33.645	33.645	33.645
2	71	66.355	66.355	100.000
Missing	0	0.000		
Total	107	100.000		



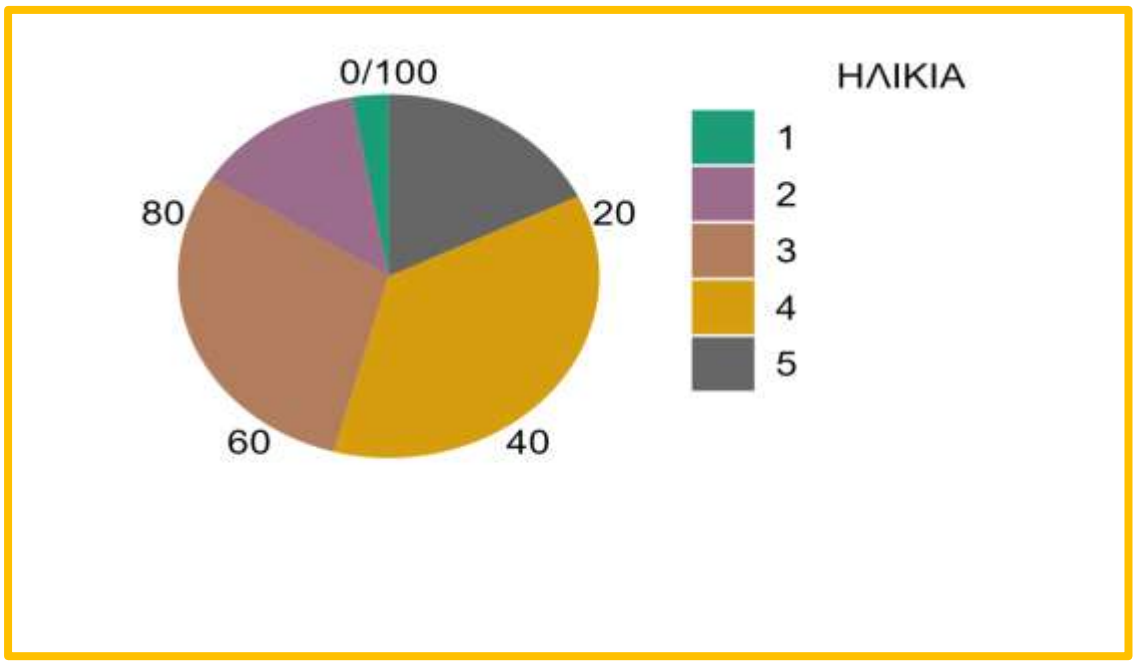
2. ΗΛΙΚΙΑ

Το δείγμα μας στην πλειοψηφία του ανήκει στην ηλικιακή ομάδα μεταξύ 41-50 ετών με ποσοστό 36,4% και ακολουθεί με ποσοστό 29,9% η ηλικιακή ομάδα των 31-40 ετών. Άνω των 50 ετών εμφανίζονται 19 άτομα που αντιστοιχούν σε ποσοστό 17,7% και 14 άτομα μεταξύ 21-30 ετών που αντιστοιχούν σε 13%. Τέλος μόλις τρία άτομα δηλώνουν μικρότερα των 20 ετών.

Όπου 1=<20, 2=21-30, 3=31-40, 4=41-50, 5=>50

Πίνακας 2.

ΗΛΙΚΙΑ	Frequency	Percent	Valid Percent	Cumulative Percent
1	3	2.804	2.804	2.804
2	14	13.084	13.084	15.888
3	32	29.907	29.907	45.794
4	39	36.449	36.449	82.243
5	19	17.757	17.757	100.000
Missing	0	0.000		
Total	107	100.000		



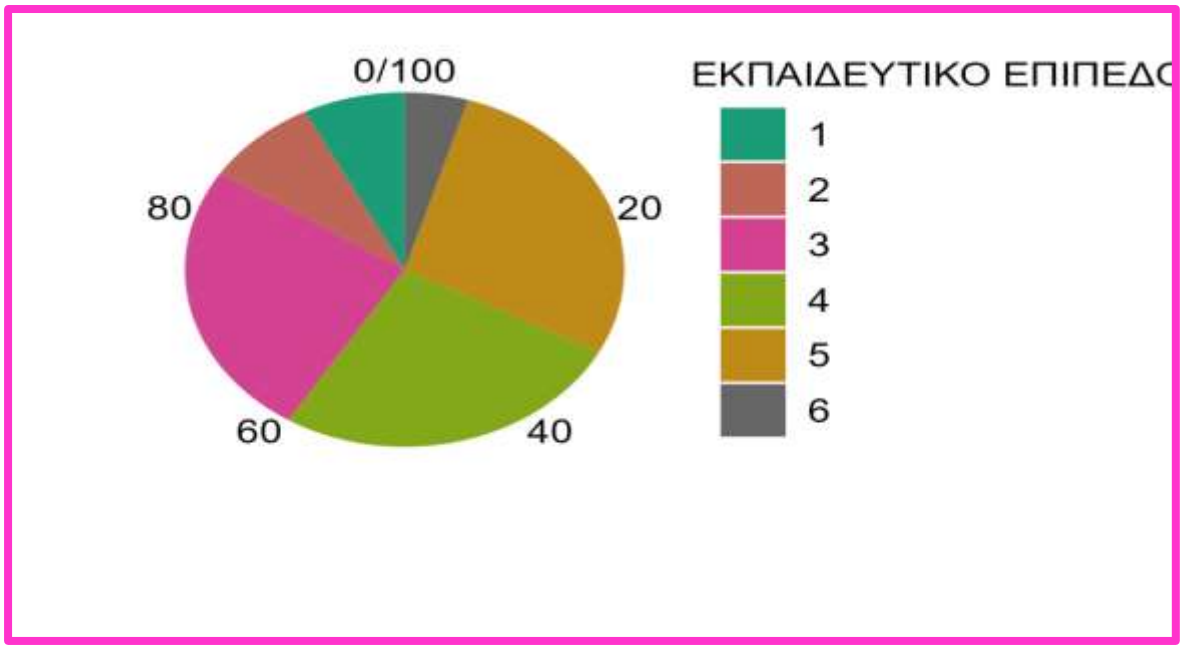
3. ΕΚΠΑΙΔΕΥΤΙΚΟ ΕΠΙΠΕΔΟ

Το εκπαιδευτικό επίπεδο της πλειοψηφίας των συμμετεχόντων στην έρευνα, δηλώνουν κάτοχοι μεταπτυχιακού (28%) και ακολουθούν οι απόφοιτοι ΑΤΕΙ με ποσοστό (26,1%). Επίσης, το 25,2% είναι απόφοιτοι ΑΕΙ ενώ το 8,4% είναι απόφοιτοι Λυκείου. Από τα 107 άτομα τα 8 δηλώνουν ότι έχουν τελειώσει την Βασική Εκπαίδευση (7,4%) και 5 άτομα κατέχουν διδακτορικό τίτλο σπουδών (4,6%).

Όπου 1= Βασική Εκπαίδευση(Δημοτικό/Γυμνάσιο), 2=Δευτεροβάθμια Εκπαίδευση(Λύκειο), 3= Απόφοιτος/η ΑΕΙ, 4= Απόφοιτος/η ΑΤΕΙ, 5=Κάτοχος Μεταπτυχιακού, 6= Κάτοχος Διδακτορικού

Πίνακας 3.

ΕΚΠΑΙΔΕΥΤΙΚΟ ΕΠΙΠΕΔΟ	Frequency	Percent	Valid Percent	Cumulative Percent
1	8	7.477	7.477	7.477
2	9	8.411	8.411	15.888
3	27	25.234	25.234	41.121
4	28	26.168	26.168	67.290
5	30	28.037	28.037	95.327
6	5	4.673	4.673	100.000
Missing	0	0.000		
Total	107	100.000		



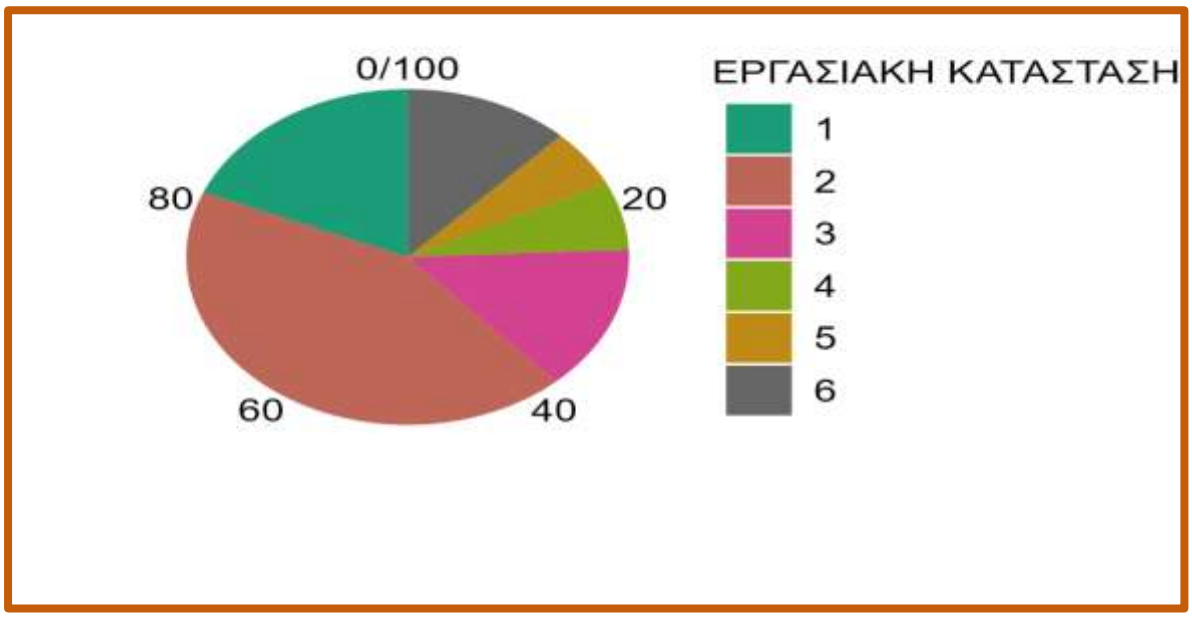
4. ΕΡΓΑΣΙΑΚΗ ΚΑΤΑΣΤΑΣΗ

Αναφορικά με την εργασιακή κατάσταση των συμμετεχόντων, η πλειοψηφία του δείγματος απασχολείται στον ιδιωτικό τομέα με ποσοστό 42,9% ενώ ακολουθούν με ποσοστό 18,6% τα άτομα που απασχολούνται στον δημόσιο τομέα. Επιπλέον, το 14% του δείγματος δηλώνει ότι είναι εκπαιδευτικοί. Το 6,5% δηλώνουν άνεργοι και 5,6% δηλώνουν συνταξιούχοι. Τέλος, υπάρχουν 13 άτομα από τους συμμετέχοντες οι οποίοι δηλώνουν ότι δεν ανήκουν σε καμία από τις προαναφερθείσες περιπτώσεις.

Όπου 1= Δημόσιος Υπάλληλος, 2= Ιδιωτικός Υπάλληλος, 3= Εκπαιδευτικός, 4=Άνεργος, 5= Συνταξιούχος, 6=Τίποτα από τα παραπάνω

Πίνακας 4.

ΕΡΓΑΣΙΑΚΗ ΚΑΤΑΣΤΑΣΗ	Frequency	Percent	Valid Percent	Cumulative Percent
1	20	18.692	18.692	18.692
2	46	42.991	42.991	61.682
3	15	14.019	14.019	75.701
4	7	6.542	6.542	82.243
5	6	5.607	5.607	87.850
6	13	12.150	12.150	100.000
Missing	0	0.000		
Total	107	100.000		



5.2. ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

5. Πόσο χρησιμοποιείται το διαδίκτυο

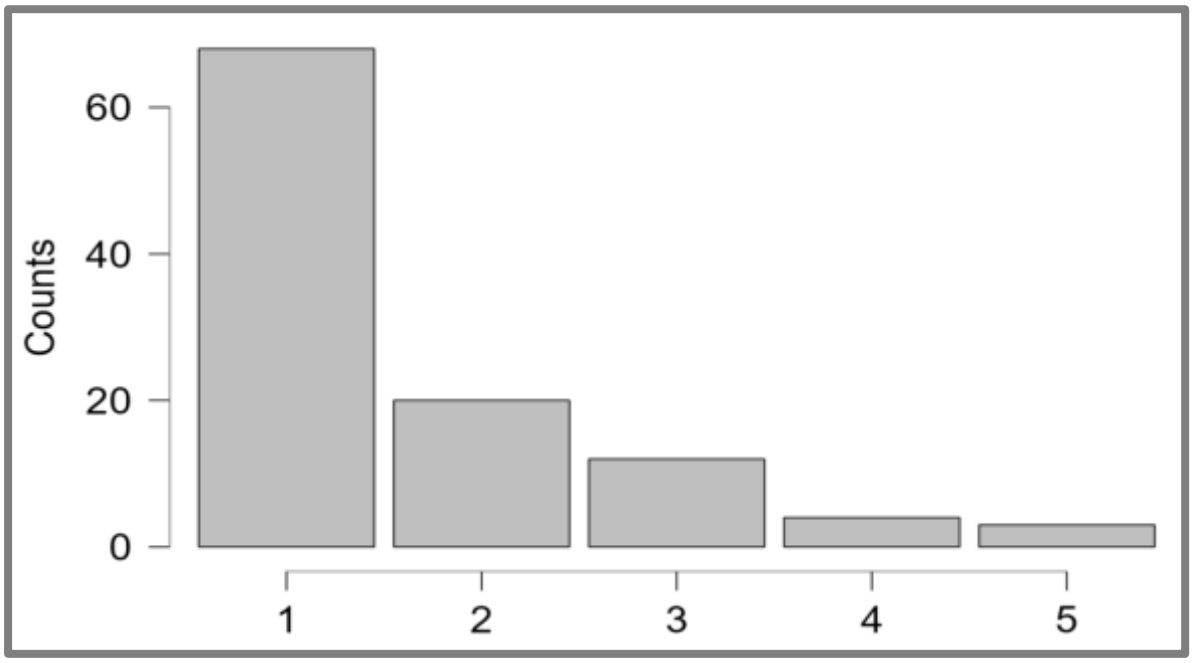
Στην συνέχεια του ερωτηματολογίου διερευνάται ο βαθμός χρήσης των ηλεκτρονικών υπηρεσιών. Ειδικότερα, η συντριπτική πλειοψηφία του δείγματος με ποσοστό 63,5% δηλώνει ότι χρησιμοποιεί το διαδίκτυο «πάρα πολύ» και ακολουθούν με 18,6% αυτοί που το χρησιμοποιούν «πολύ». Το 11,2% δηλώνει ότι το

χρησιμοποιεί «αρκετά» ενώ 3,7% δηλώνει «λίγο». Τέλος, υπάρχουν 3 άτομα που δηλώνουν ότι δεν το χρησιμοποιούν «καθόλου».

Όπου 1=Πάρα πολύ, 2= Πολύ, 3= Αρκετά, 4=Λίγο, 5=Καθόλου

Πίνακας 5.

ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Πόσο χρησιμοποιείτε το διαδίκτυο]	Frequency	Percent	Valid Percent	Cumulative Percent
1	68	63.551	63.551	63.551
2	20	18.692	18.692	82.243
3	12	11.215	11.215	93.458
4	4	3.738	3.738	97.196
5	3	2.804	2.804	100.000
Missing	0	0.000		
Total	107	100.000		



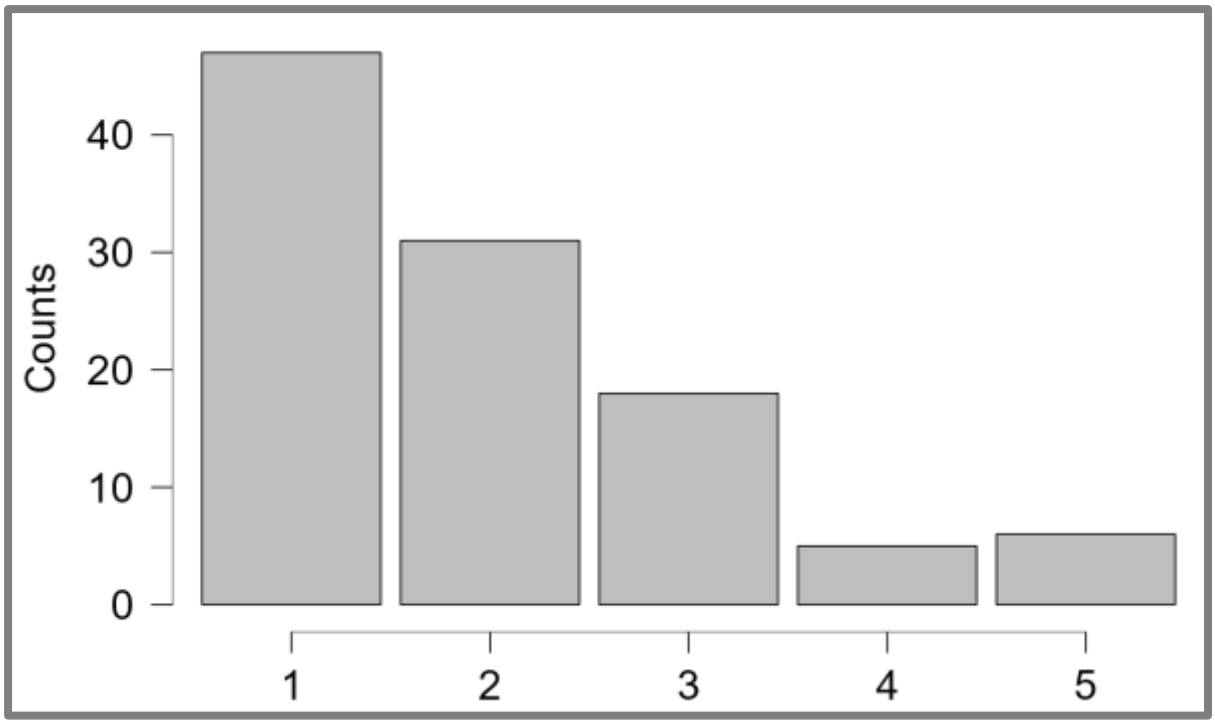
6. Πόσο χρησιμοποιείται τις ηλεκτρονικές συναλλαγές

Οι συμμετέχοντες σε μεγάλο βαθμό χρησιμοποιούν τις ηλεκτρονικές τραπεζικές συναλλαγές με ποσοστό 43,9% να δηλώνει «πάρα πολύ» και 28,9% να δηλώνει «πολύ». Επίσης, το 16,8% δηλώνει «αρκετά» ενώ το 4,6% δηλώνει «λίγο». Από τα 107 άτομα του δείγματος υπάρχουν 6 άτομα τα οποία δηλώνουν ότι δεν χρησιμοποιούν καθόλου τις ηλεκτρονικές τραπεζικές συναλλαγές.

Όπου 1=Πάρα πολύ, 2= Πολύ, 3= Αρκετά, 4=Λίγο, 5=Καθόλου

Πίνακας 6.

ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Πόσο χρησιμοποιείτε τις ηλεκτρονικές τραπεζικές συναλλαγές]	Frequency	Percent	Valid Percent	Cumulative Percent
1	47	43.925	43.925	43.925
2	31	28.972	28.972	72.897
3	18	16.822	16.822	89.720
4	5	4.673	4.673	94.393
5	6	5.607	5.607	100.000
Missing	0	0.000		
Total	107	100.000		



7. Πόσο εύκολη είναι η πρόσβαση στις ηλεκτρονικές υπηρεσίες

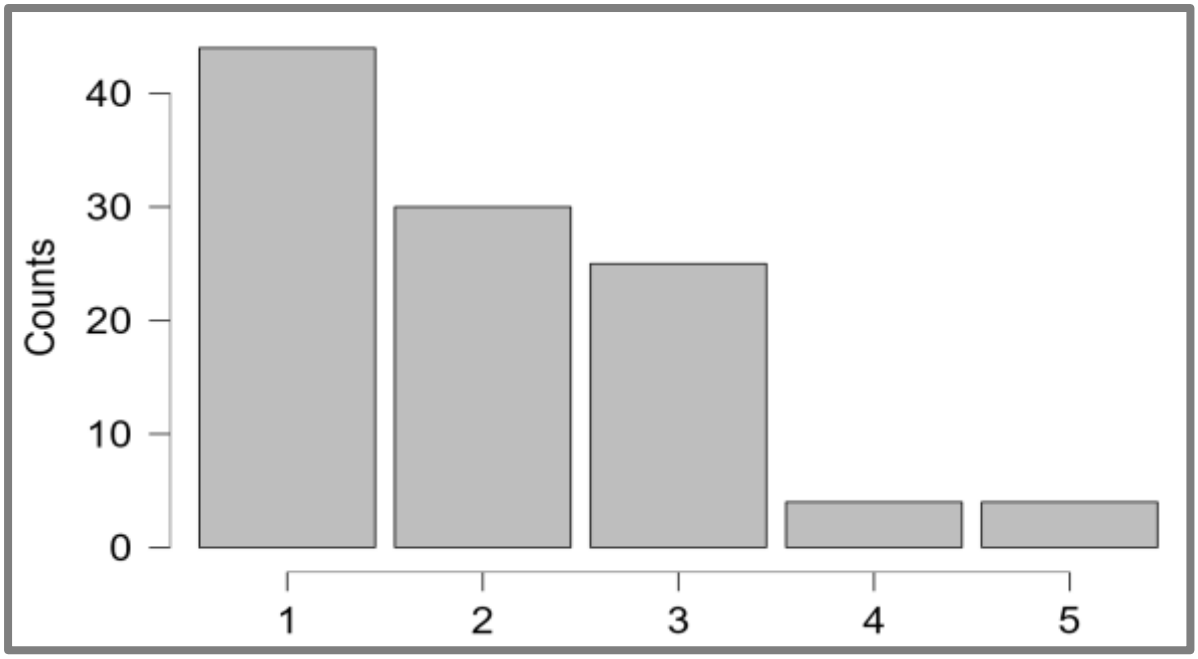
Αναφορικά με τον βαθμό ευκολίας της πρόσβασης στις ηλεκτρονικές υπηρεσίες, το δείγμα απαντά ότι είναι «πάρα πολύ» εύκολη σε ποσοστό 41,1% και «πολύ» εύκολη σε ποσοστό 28%. Ακολουθούν αυτοί που απαντούν «αρκετά» με ποσοστό 23,3% ενώ ισοβαθμούν με ποσοστό 3,7% οι απαντήσεις «λίγο» και «καθόλου». Συμπερασματικά

η πλειοψηφία δεν αντιμετωπίζει προβλήματα προσβασιμότητας στις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί.

Όπου 1=Πάρα πολύ, 2= Πολύ, 3= Αρκετά, 4=Λίγο, 5=Καθόλου

Πίνακας 7.

ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Πόσο εύκολη είναι η πρόσβαση στις ηλεκτρονικές υπηρεσίες]	Frequency	Percent	Valid Percent	Cumulative Percent
1	44	41.121	41.121	41.121
2	30	28.037	28.037	69.159
3	25	23.364	23.364	92.523
4	4	3.738	3.738	96.262
5	4	3.738	3.738	100.000
Missing	0	0.000		
Total	107	100.000		



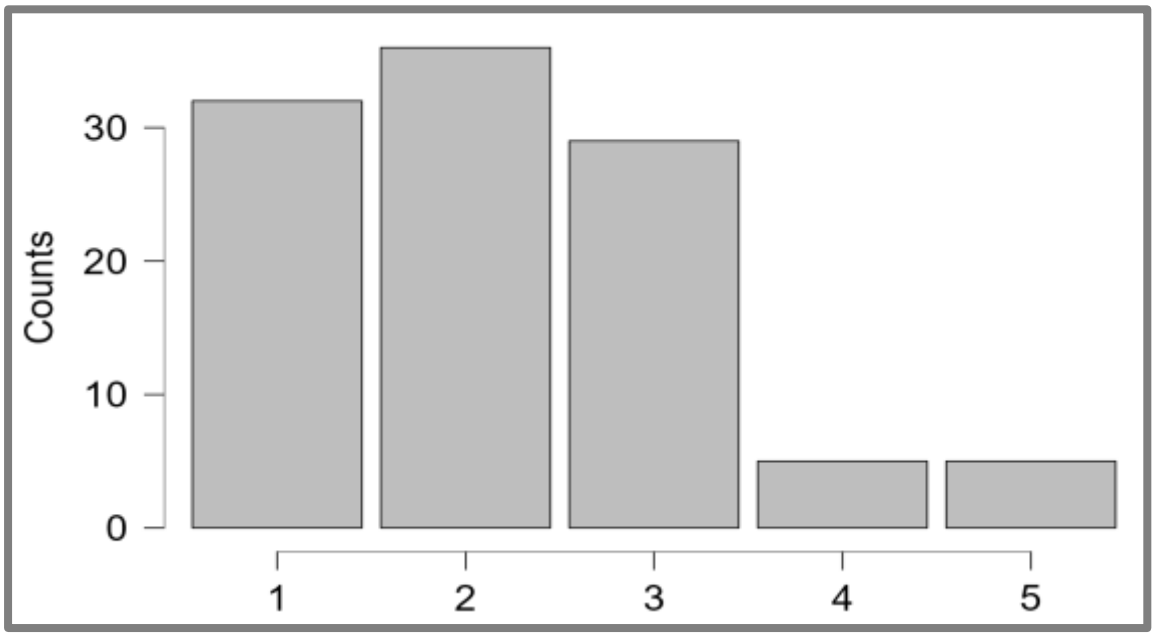
8. Πόσο εύκολες και κατανοητές είναι οι ψηφιακές πλατφόρμες που χρησιμοποιείτε

Από τους 107 συμμετέχοντες στην έρευνα, οι 32 δηλώνουν ότι είναι «πάρα πολύ» εύκολες και κατανοητές οι ψηφιακές πλατφόρμες που χρησιμοποιούν και οι 36 δηλώνουν «πολύ». Επίσης, 29 από αυτούς δηλώνουν «αρκετά» ενώ αντίστοιχα 5 άτομα δηλώνουν «λίγο» και 5 άτομα δηλώνουν «καθόλου» εύκολες και κατανοητές.

Όπου 1=Πάρα πολύ, 2= Πολύ, 3= Αρκετά, 4=Λίγο, 5=Καθόλου

Πίνακας 8.

ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Πόσο εύκολες και κατανοητές	Frequency	Percent	Valid Percent	Cumulative Percent
1	32	29.907	29.907	29.907
2	36	33.645	33.645	63.551
3	29	27.103	27.103	90.654
4	5	4.673	4.673	95.327
5	5	4.673	4.673	100.000
Missing	0	0.000		
Total	107	100.000		



9. Πόσο ικανοποιημένοι είστε από τις ηλεκτρονικές υπηρεσίες που προσφέρονται από την Δημόσια Διοίκηση

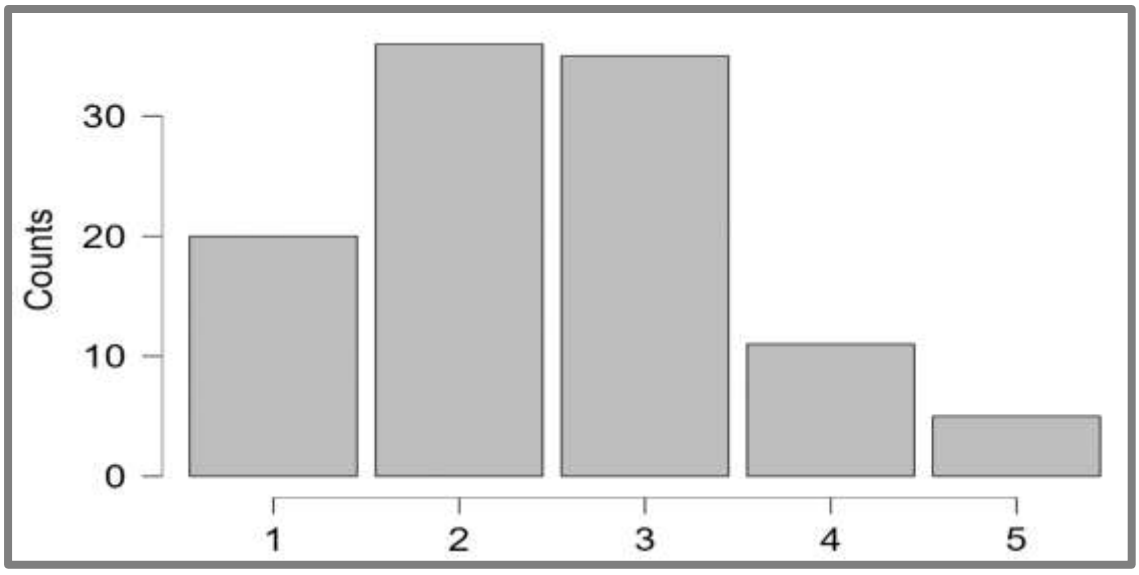
Η πλειοψηφία του δείγματος δηλώνει ότι είναι «πολύ» ικανοποιημένη με τις ηλεκτρονικές υπηρεσίες της Δημόσιας Διοίκησης (33,6%) ενώ ακολουθούν με 32,7% αυτοί που δηλώνουν «αρκετά». Από τα 107 άτομα οι 20 (18,6%) δηλώνουν «πολύ» ικανοποιημένοι και 11 άτομα (10,2%) δηλώνουν «λίγο». Τέλος, σε σταθερή βάση

εμφανίζονται 5 άτομα (4,6%) τα οποία δηλώνουν ότι δεν είναι καθόλου ικανοποιημένοι.

Όπου 1=Πάρα πολύ, 2= Πολύ, 3= Αρκετά, 4=Λίγο, 5=Καθόλου

Πίνακας 9.

ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Πόσο ικανοποιημένοι είστε από τις ηλεκτρονικές υπηρεσίες που προσφέρονται από την Δημόσια Διοίκηση]	Frequency	Percent	Valid Percent	Cumulative Percent
1	20	18.692	18.692	18.692
2	36	33.645	33.645	52.336
3	35	32.710	32.710	85.047
4	11	10.280	10.280	95.327
5	5	4.673	4.673	100.000
Missing	0	0.000		
Total	107	100.000		



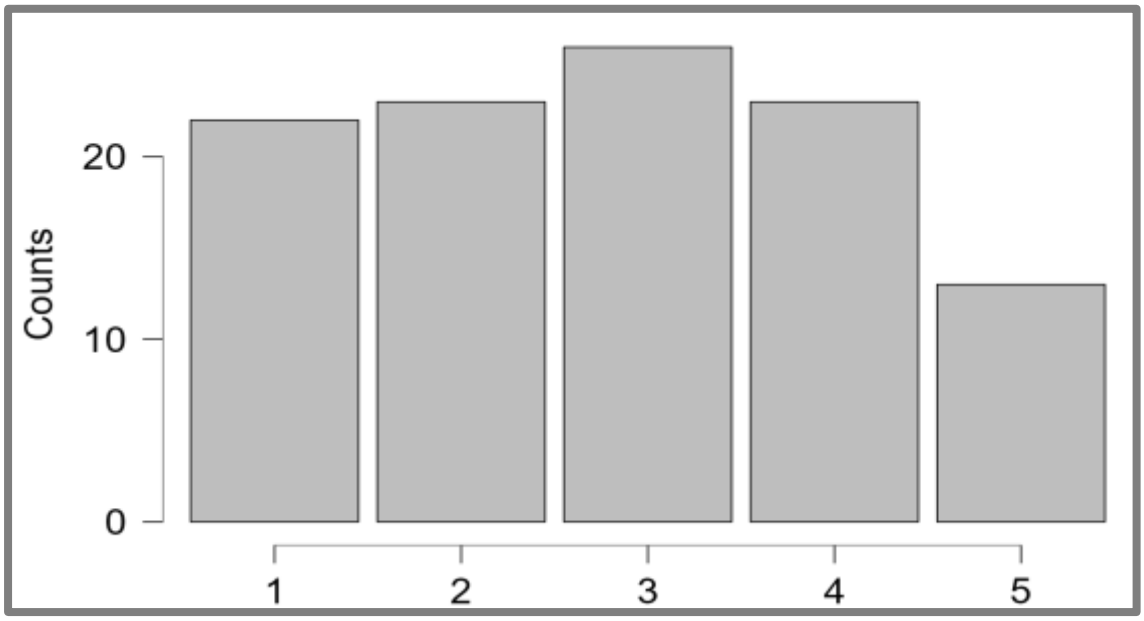
10. Έχω αυξανόμενες ανησυχίες για την επιτήρηση από την κυβέρνηση

Στην παρούσα ερώτηση οι απαντήσεις είναι ισόποσα μοιρασμένες . Ειδικότερα, το 20,5% δηλώνει «πάρα πολύ», το 21,4% δηλώνει «πολύ» ενώ το 24,2% δηλώνει «αρκετά». Επίσης το 21,4% δηλώνει «λίγο» ενώ το 12,1% δηλώνει «καθόλου».

Όπου 1=Πάρα πολύ, 2= Πολύ, 3= Αρκετά, 4=Λίγο, 5=Καθόλου

Πίνακας 10.

ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Έχω αυξανόμενες ανησυχίες για την επιτήρηση από την κυβέρνηση]	Frequency	Percent	Valid Percent	Cumulative Percent
1	22	20.561	20.561	20.561
2	23	21.495	21.495	42.056
3	26	24.299	24.299	66.355
4	23	21.495	21.495	87.850
5	13	12.150	12.150	100.000
Missing	0	0.000		
Total	107	100.000		



5.3. ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

11. Χρησιμοποιείτε το διαδίκτυο για διεκπεραίωση εργασιών

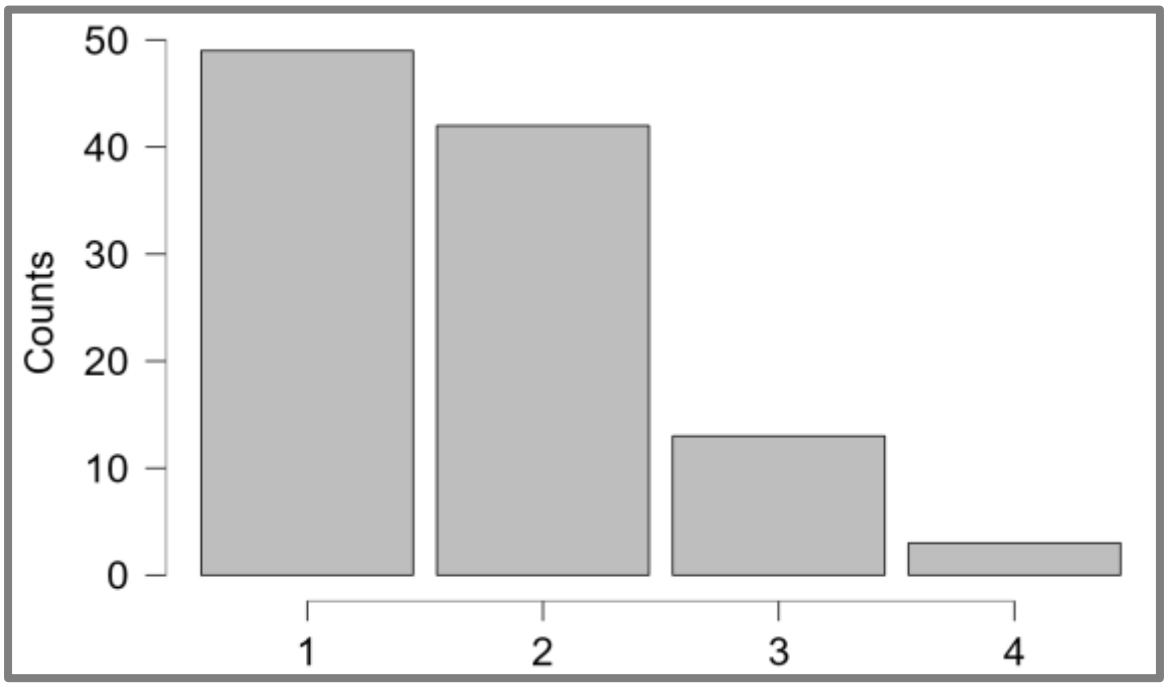
Ο πίνακας 11 δείχνει ότι οι ερωτηθέντες στην πλειοψηφία τους χρησιμοποιούν το διαδίκτυο για διεκπεραίωση εργασιών «πολύ συχνά» με ποσοστό 45,7% και «συχνά»

με ποσοστό 39,2 ενώ «σπάνια» απαντούν το 12,1% . Τέλος υπάρχουν 3 άτομα από τα 107 τα οποία δεν χρησιμοποιούν «ποτέ» το διαδίκτυο για αυτό το λόγο.

Όπου 1= Πολύ Συχνά , 2= Συχνά, 3= Σπάνια, 4= Ποτέ

Πίνακας 11.

ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ[Χρησιμοποιείτε το διαδίκτυο για διεκπεραίωση εργασιών]	Frequency	Percent	Valid Percent	Cumulative Percent
1	49	45.794	45.794	45.794
2	42	39.252	39.252	85.047
3	13	12.150	12.150	97.196
4	3	2.804	2.804	100.000
Missing	0	0.000		
Total	107	100.000		



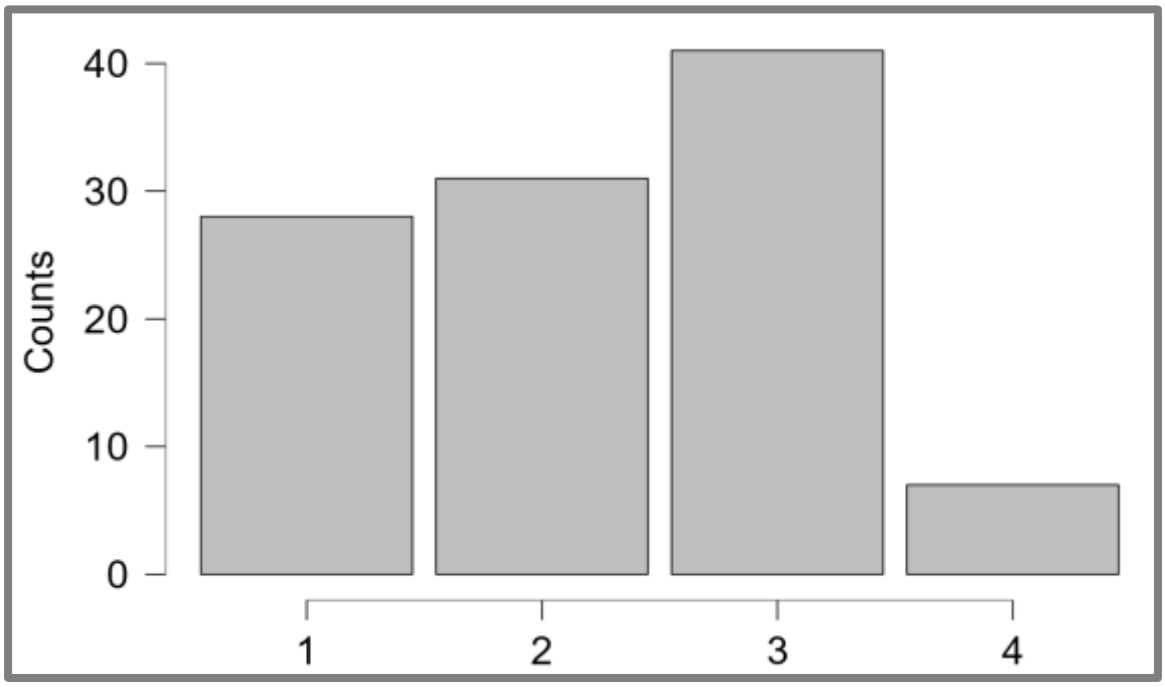
12. Χρησιμοποιείτε το διαδίκτυο για να κατεβάσετε αρχεία (μουσική, ταινίες κ.α.)

Με 38,3% οι ερωτηθέντες απαντούν ότι «σπάνια» κατεβάζουν αρχεία όπως για παράδειγμα μουσική ή ταινίες όπως δείχνει και ο πίνακας 12 παρακάτω. Επίσης, το 28,9% απαντά με «συχνά» ενώ 26,1% απαντά «πολύ συχνά». Τέλος, «ποτέ» δηλώνει το 6,5% των ερωτηθέντων.

Όπου 1= Πολύ Συχνά , 2= Συχνά, 3= Σπάνια, 4= Ποτέ

Πίνακας 12.

ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ[Χρησιμοποιείτε το διαδίκτυο για να κατεβάσετε αρχεία (μουσική, ταινίες κ.α.)]	Frequency	Percent	Valid Percent	Cumulative Percent
1	28	26.168	26.168	26.168
2	31	28.972	28.972	55.140
3	41	38.318	38.318	93.458
4	7	6.542	6.542	100.000
Missing	0	0.000		
Total	107	100.000		



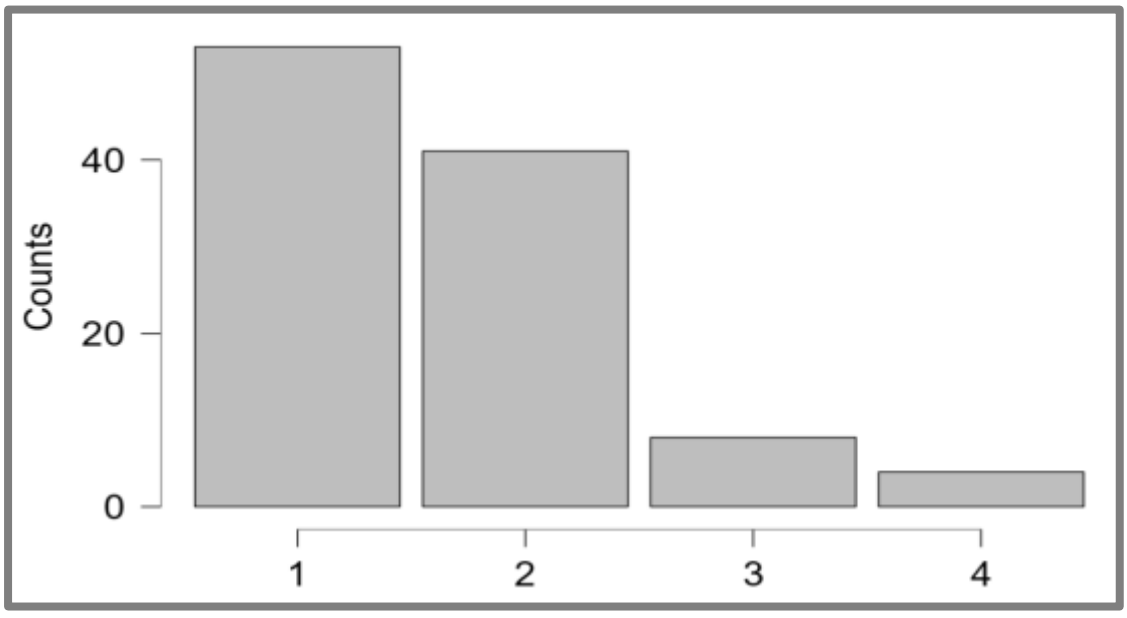
13. Χρησιμοποιείτε το διαδίκτυο για χρηματικές συναλλαγές

Σαφώς και η συντριπτική πλειοψηφία φαίνεται ότι χρησιμοποιεί το διαδίκτυο για χρηματικές συναλλαγές και δηλώνει με 49,5% «πολύ συχνά» και 38,3% «συχνά». Παράλληλα, «σπάνια» απαντά το 7,4% και «ποτέ» απαντά το 3,7% όπως δείχνει και ο πίνακας 13.

Όπου 1= Πολύ Συχνά , 2= Συχνά, 3= Σπάνια, 4= Ποτέ

Πίνακας 13.

ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ[Χρησιμοποιείτε το διαδίκτυο για χρηματικές συναλλαγές]	Frequency	Percent	Valid Percent	Cumulative Percent
1	53	49.533	50.000	50.000
2	41	38.318	38.679	88.679
3	8	7.477	7.547	96.226
4	4	3.738	3.774	100.000
Missing	1	0.935		
Total	107	100.000		



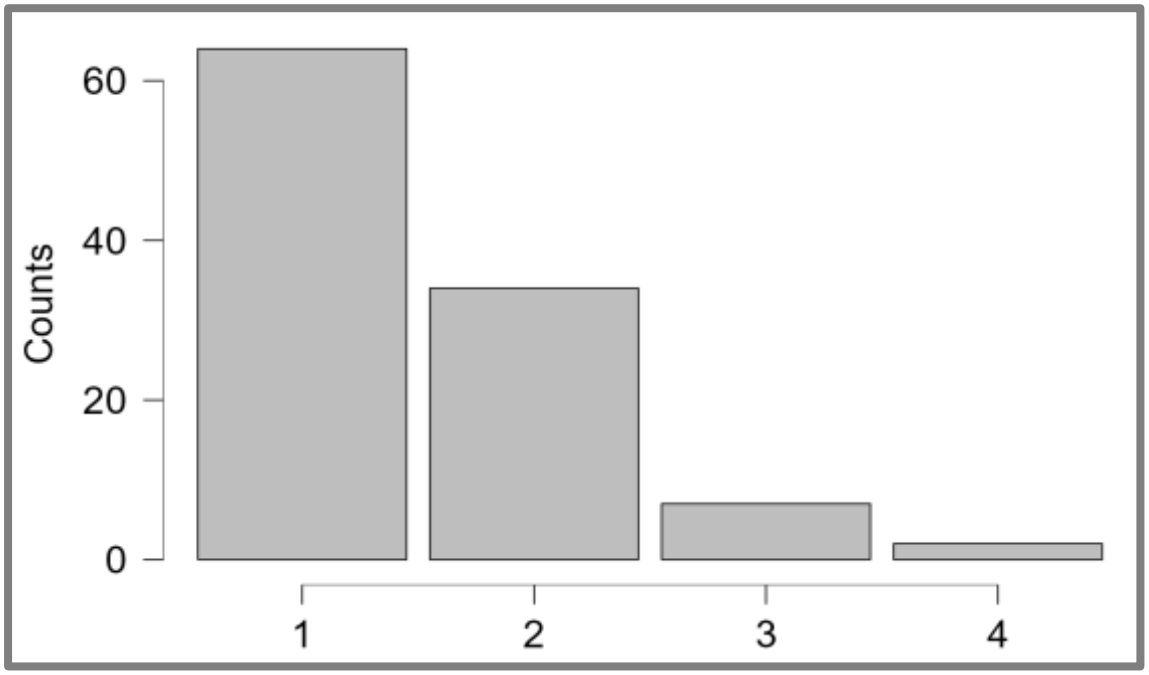
14. Χρησιμοποιείται το διαδίκτυο για να ανταλλάσσετε μηνύματα με φίλους

Σύμφωνα με τον πίνακα 14, οι συμμετέχοντες «πολύ συχνά» χρησιμοποιούν το διαδίκτυο για να ανταλλάξουν μηνύματα με φίλους με ποσοστό 59,8% και «συχνά» με ποσοστό 31,7%. Ταυτόχρονα «σπάνια» δηλώνει το 6,5% στην συγκεκριμένη ερώτηση ενώ μόλις 2 άτομα από τα 107 απαντούν «ποτέ».

Όπου 1= Πολύ Συχνά , 2= Συχνά, 3= Σπάνια, 4= Ποτέ

Πίνακας 14.

ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ[Χρησιμοποιείται το διαδίκτυο για να ανταλλάσσετε μηνύματα με φίλους]	Frequency	Percent	Valid Percent	Cumulative Percent
1	64	59.813	59.813	59.813
2	34	31.776	31.776	91.589
3	7	6.542	6.542	98.131
4	2	1.869	1.869	100.000
Missing	0	0.000		
Total	107	100.000		



5.4. ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

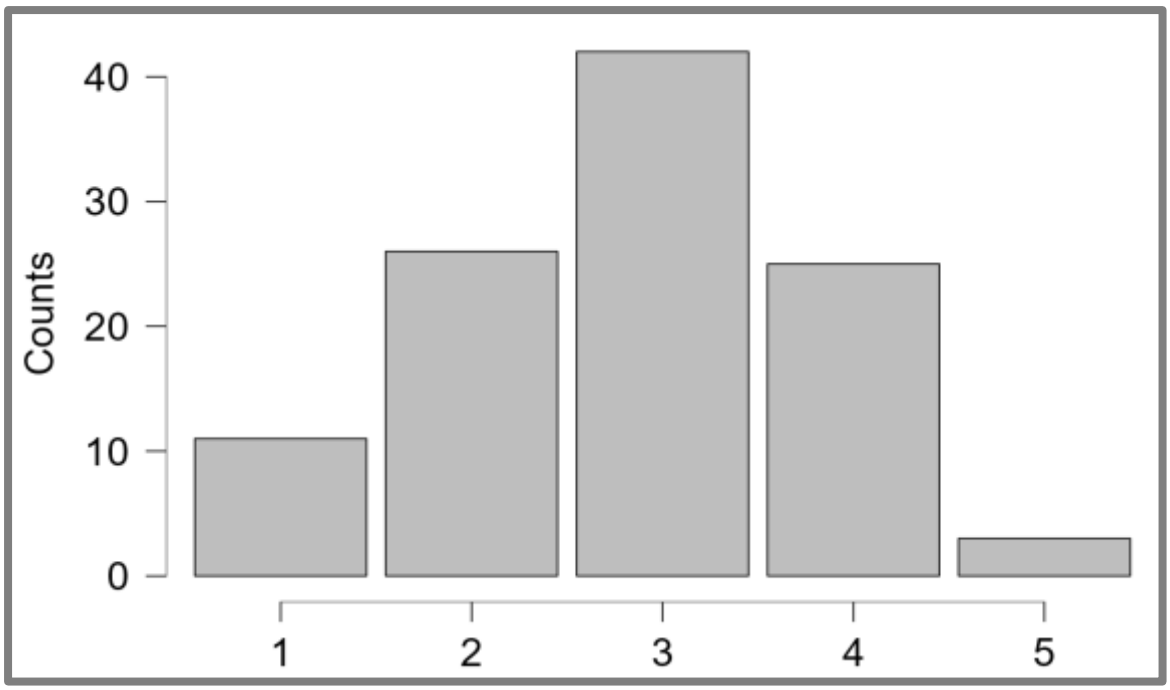
15. Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής

Διερευνώντας την ασφάλεια των ηλεκτρονικών υπηρεσιών, το δείγμα δηλώνει ουδέτερη στάση και απαντά με 39,2% ότι ούτε συμφωνεί/ούτε διαφωνεί με την παραπάνω δήλωση. Από την άλλη, το 24,2% δηλώνει ότι συμφωνεί και 10,2% συμφωνεί απόλυτα. Τέλος, 23,3% διαφωνεί με αυτό ενώ 2,8% διαφωνεί απόλυτα.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 15.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής]	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	11	10.280	10.280	10.280
2	26	24.299	24.299	34.579
3	42	39.252	39.252	73.832
4	25	23.364	23.364	97.196
5	3	2.804	2.804	100.000
Missing	0	0.000		
Total	107	100.000		



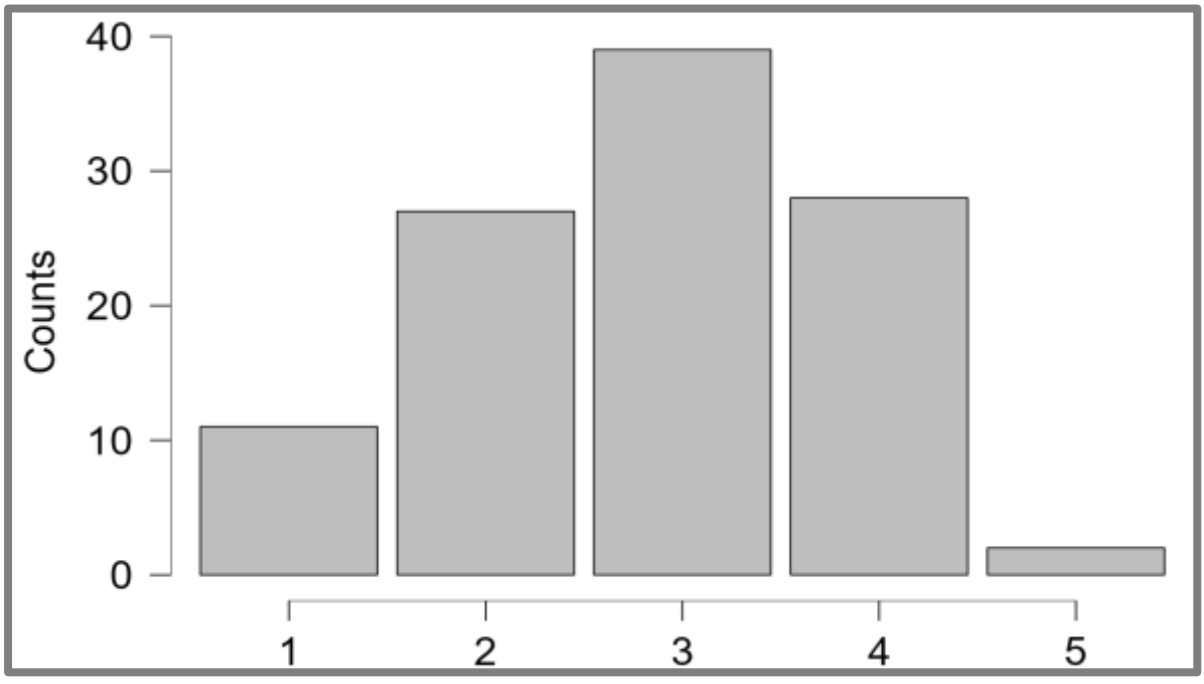
16. Αισθάνεστε ότι έχετε τον έλεγχο στις πληροφορίες που παρέχετε σε απευθείας σύνδεση

Ο πίνακας 16 παρουσιάζει το 36,4% του δείγματος ούτε να συμφωνεί/ούτε να διαφωνεί με την παραπάνω δήλωση. Από την άλλη, το 35,4% συνολικά είτε συμφωνεί είτε συμφωνεί απόλυτα ενώ μικρότερο εμφανίζεται το ποσοστό (27,9%) το οποίο είτε διαφωνεί είτε διαφωνεί απόλυτα.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 16.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Αισθάνεστε ότι έχετε τον έλεγχο στις πληροφορίες που παρέχετε σε απευθείας σύνδεση]	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	11	10.280	10.280	10.280
2	27	25.234	25.234	35.514
3	39	36.449	36.449	71.963
4	28	26.168	26.168	98.131
5	2	1.869	1.869	100.000
Missing	0	0.000		
Total	107	100.000		



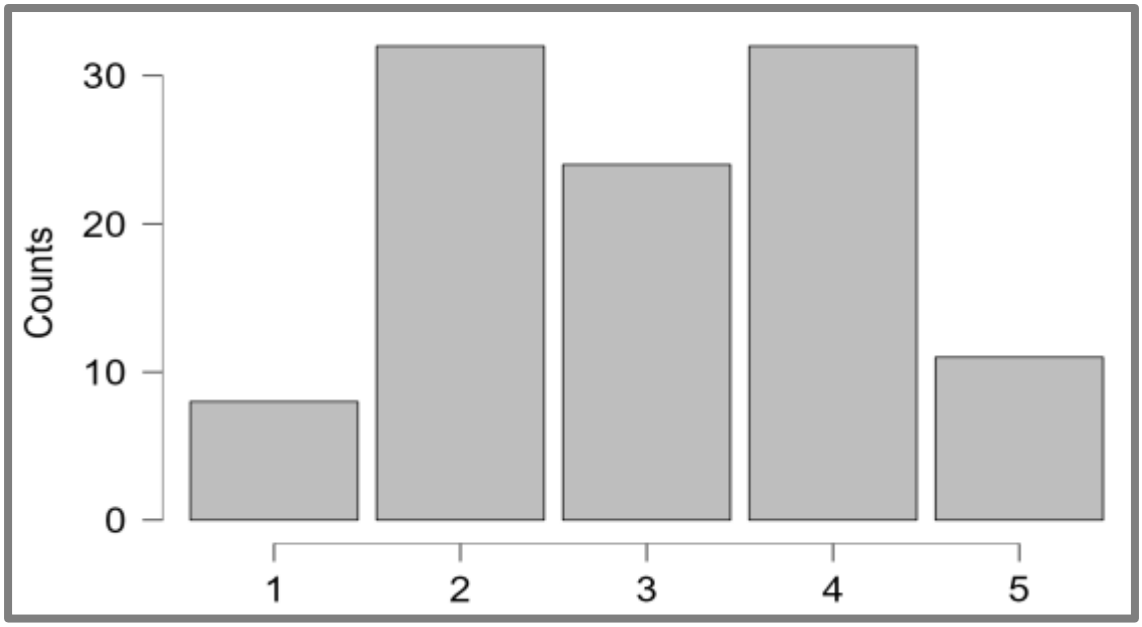
17. Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη

Το 40% περίπου διαφωνεί ή διαφωνεί απόλυτα με την παραπάνω δήλωση έναντι του 37,% το οποίο συμφωνεί ή συμφωνεί απόλυτα. Αντίστοιχα, το 22,4% ούτε συμφωνεί/ούτε διαφωνεί εκφράζοντας ουδέτερη στάση.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 17.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη]	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	8	7.477	7.477	7.477
2	32	29.907	29.907	37.383
3	24	22.430	22.430	59.813
4	32	29.907	29.907	89.720
5	11	10.280	10.280	100.000
Missing	0	0.000		
Total	107	100.000		



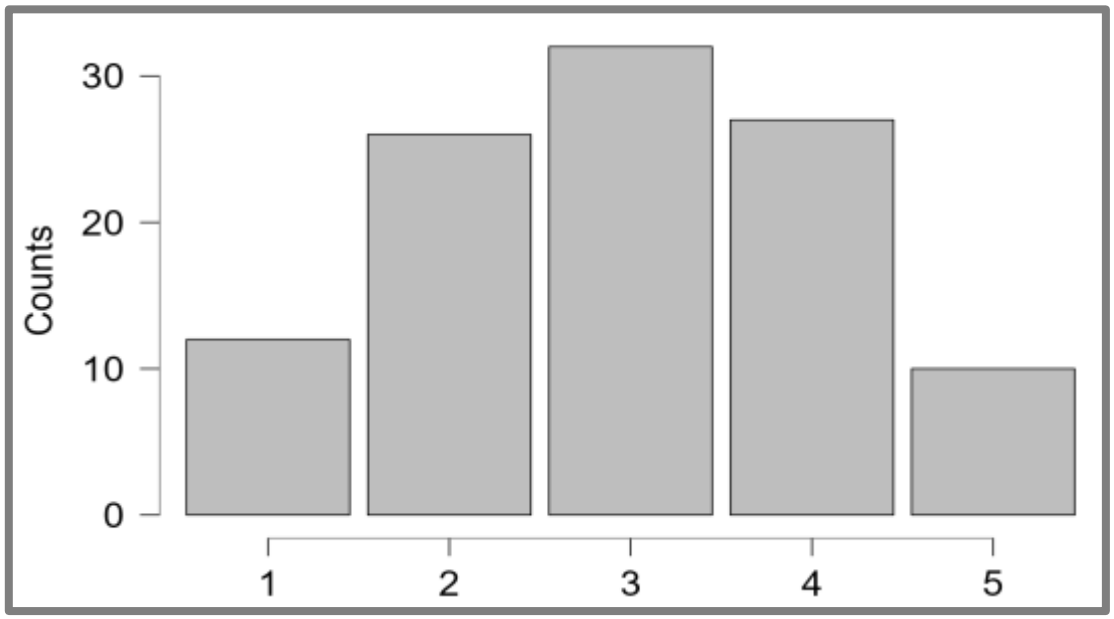
18. Έχω εμπιστοσύνη στην τεχνολογία που χρησιμοποιούν οι κυβερνητικοί φορείς

Στον πίνακα 18 οι απόψεις των συμμετεχόντων στην έρευνα είναι ισόποσα μοιρασμένες αναφορικά με την εμπιστοσύνη στην τεχνολογία που χρησιμοποιούν οι κυβερνητικοί φορείς καθώς το 35,4% συνολικά συμφωνεί με την δήλωση έναντι του 34,5% συνολικά που διαφωνεί. Το 29,9% ούτε συμφωνεί ούτε διαφωνεί με αυτό. Συμπερασματικά δεν προκύπτει συγκεκριμένη τάση που να διαφοροποιεί τα άτομα του δείγματος μεταξύ τους.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 18.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Έχω εμπιστοσύνη στην τεχνολογία που χρησιμοποιούν οι κυβερνητικοί φορείς]	Frequency	Percent	Valid Percent	Cumulative Percent
1	12	11.215	11.215	11.215
2	26	24.299	24.299	35.514
3	32	29.907	29.907	65.421
4	27	25.234	25.234	90.654
5	10	9.346	9.346	100.000
Missing	0	0.000		
Total	107	100.000		



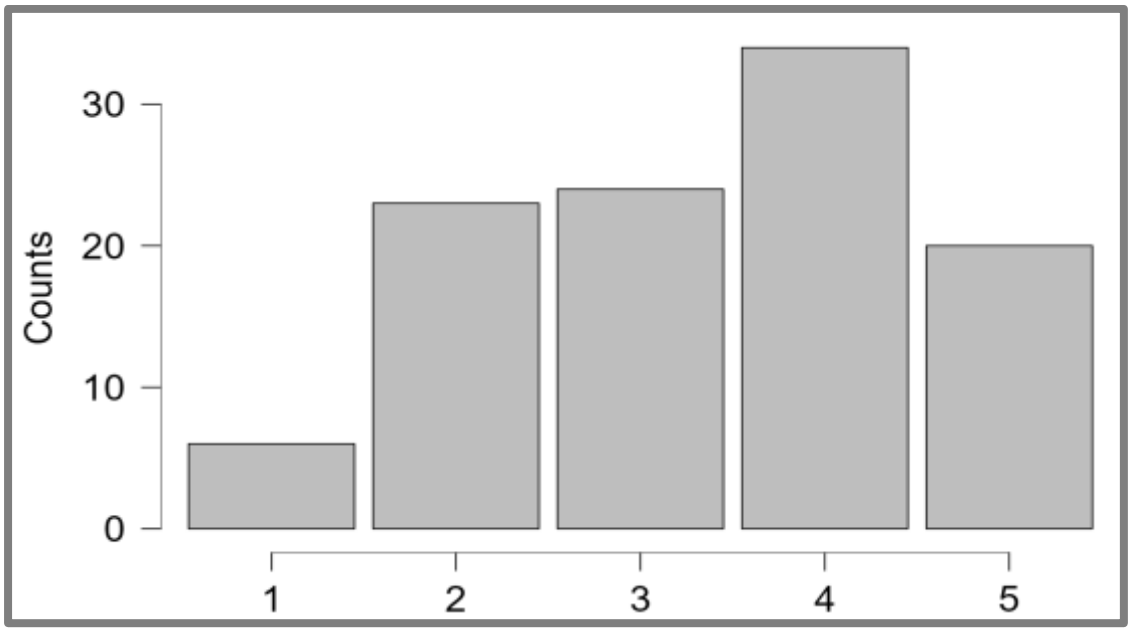
19. Νοιώθω ασφαλής να παρέχω ευαίσθητες πληροφορίες στο διαδίκτυο (π.χ. αριθμό πιστωτικής κάρτας

Η πλειοψηφία του δείγματος της έρευνας με ποσοστό συνολικά 50,2% δηλώνει ότι δεν νοιώθει ασφαλής να παρέχει ευαίσθητες πληροφορίες στο διαδίκτυο ενώ 27% δηλώνει ασφαλής. Υψηλό εμφανίζεται το ποσοστό (22,4%) το οποίο δηλώνει ότι ούτε συμφωνεί/ούτε διαφωνεί με την παραπάνω δήλωση.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 19.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Νοιώθω ασφαλής να παρέχω ευαίσθητες πληροφορίες στο διαδίκτυο (π.χ. αριθμό πιστωτικής κάρτας)]	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	6	5.607	5.607	5.607
2	23	21.495	21.495	27.103
3	24	22.430	22.430	49.533
4	34	31.776	31.776	81.308
5	20	18.692	18.692	100.000
Missing	0	0.000		
Total	107	100.000		



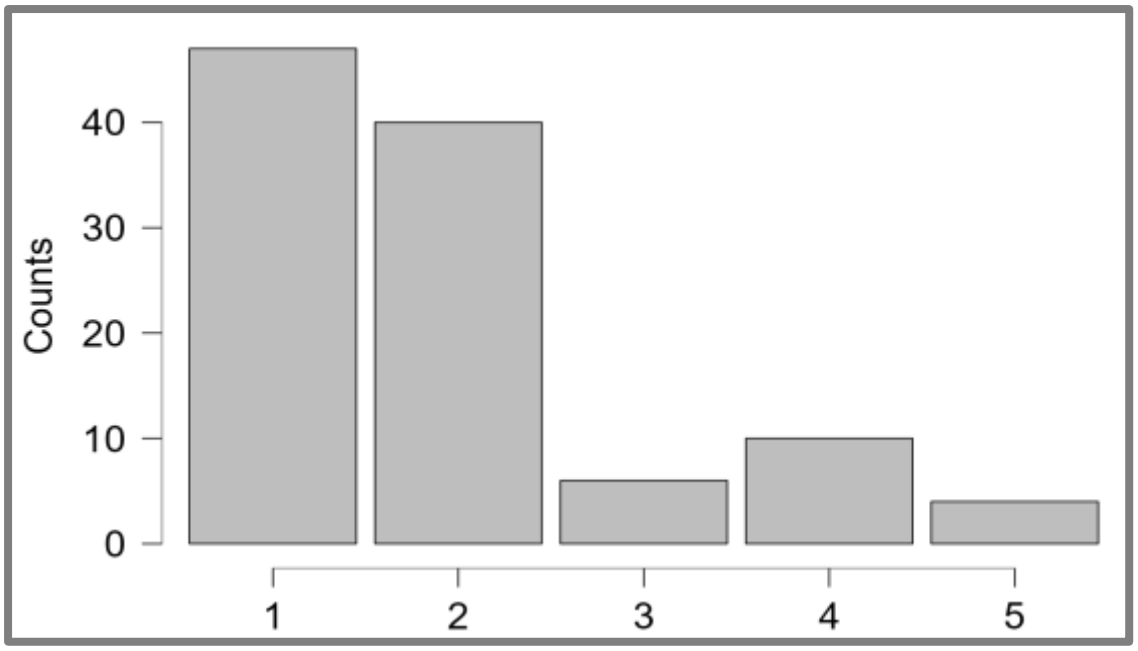
20. Είναι απαραίτητη η ενημέρωση των χρηστών για τους κανόνες ασφάλειας του διαδικτύου

Η συντριπτική πλειοψηφία του δείγματος της έρευνας συμφωνεί ή συμφωνεί απόλυτα με ποσοστό 81% ότι πρέπει να ενημερώνονται οι χρήστες για τους κανόνες ασφαλείας του διαδικτύου ενώ το 13% διαφωνεί ή διαφωνεί απόλυτα. Το 5,6% ούτε συμφωνεί/ ούτε διαφωνεί.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 20.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Είναι απαραίτητη η ενημέρωση των χρηστών για τους κανόνες ασφάλειας του διαδικτύου]	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	47	43.925	43.925	43.925
2	40	37.383	37.383	81.308
3	6	5.607	5.607	86.916
4	10	9.346	9.346	96.262
5	4	3.738	3.738	100.000
Missing	0	0.000		
Total	107	100.000		



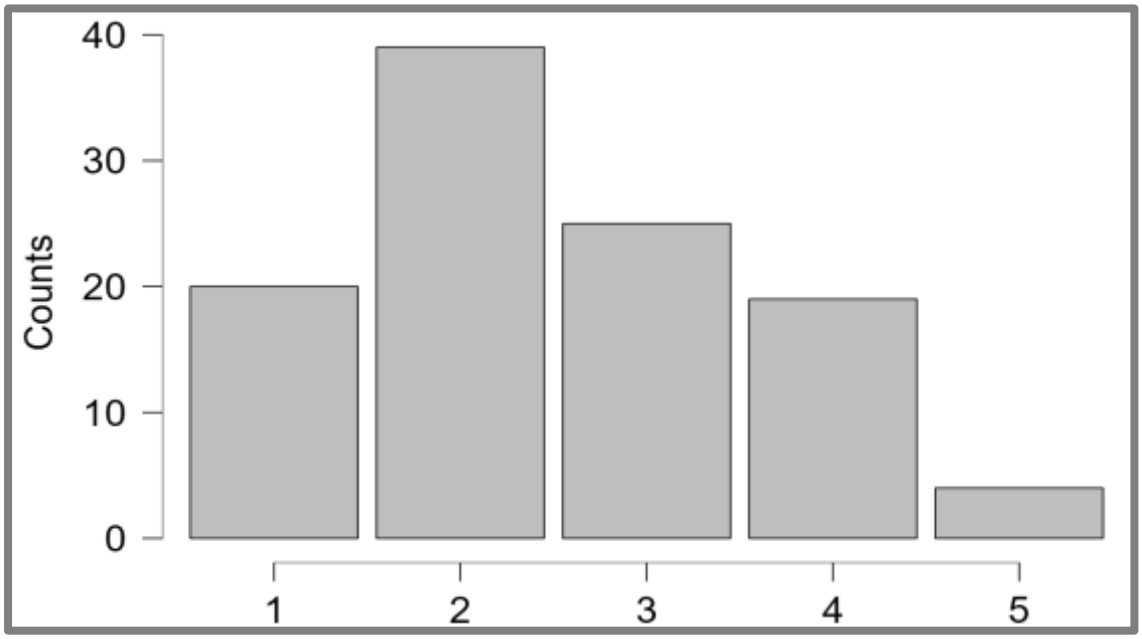
21. Είμαι πλήρως και ορθώς ενημερωμένος/η για την ασφάλεια και τους κινδύνους του διαδικτύου

Ο πίνακας 21 αποτυπώνει ότι το γεγονός ότι 55% των ερωτηθέντων υποστηρίζει ότι είναι πλήρως και ορθώς ενημερωμένο για την ασφάλεια και τους κινδύνους του διαδικτύου έναντι του 21,4% το οποίο δηλώνει ότι δεν είναι ενημερωμένο. Τέλος, το 23,3% ούτε συμφωνεί/ούτε διαφωνεί με την παραπάνω δήλωση.

Όπου 1= Συμφωνώ απόλυτα, 2= Συμφωνώ, 3=Ούτε Συμφωνώ/Ούτε Διαφωνώ, 4= Διαφωνώ, 5= Διαφωνώ Απόλυτα

Πίνακας 21.

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Είμαι πλήρως και ορθώς ενημερωμένος/η	Frequency	Percent	Valid Percent	Cumulative Percent
1	20	18.692	18.692	18.692
2	39	36.449	36.449	55.140
3	25	23.364	23.364	78.505
4	19	17.757	17.757	96.262
5	4	3.738	3.738	100.000
Missing	0	0.000		
Total	107	100.000		



5.5. ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

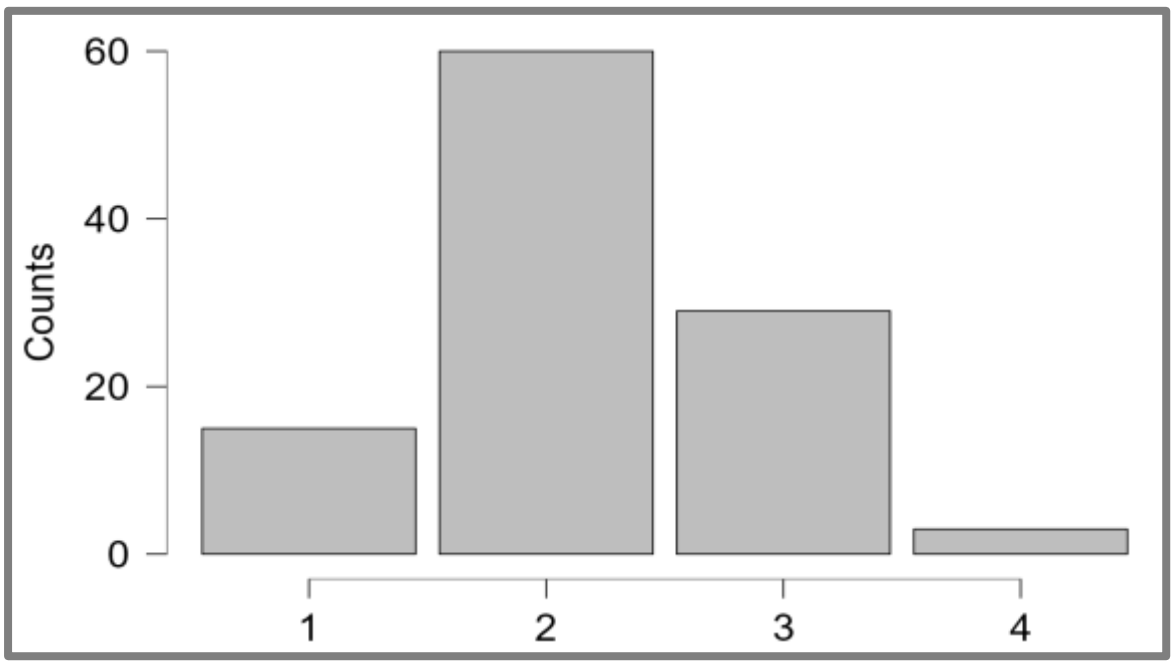
22. Αποχωρώ από τη συλλογή δεδομένων

Ως μέτρο προστασίας η συντριπτική πλειοψηφία με 56% απαντά ότι «συχνά» αποχωρούν από τη συλλογή δεδομένων ενώ το 14% απαντούν «πάντα». Από την άλλη, το 27% απαντά «σπάνια» και μόλις τρία άτομα από τα 107 απαντούν «ποτέ».

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Πίνακας 22.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Αποχωρώ από τη συλλογή δεδομένων]	Frequency	Percent	Valid Percent	Cumulative Percent
1	15	14.019	14.019	14.019
2	60	56.075	56.075	70.093
3	29	27.103	27.103	97.196
4	3	2.804	2.804	100.000
Missing	0	0.000		
Total	107	100.000		



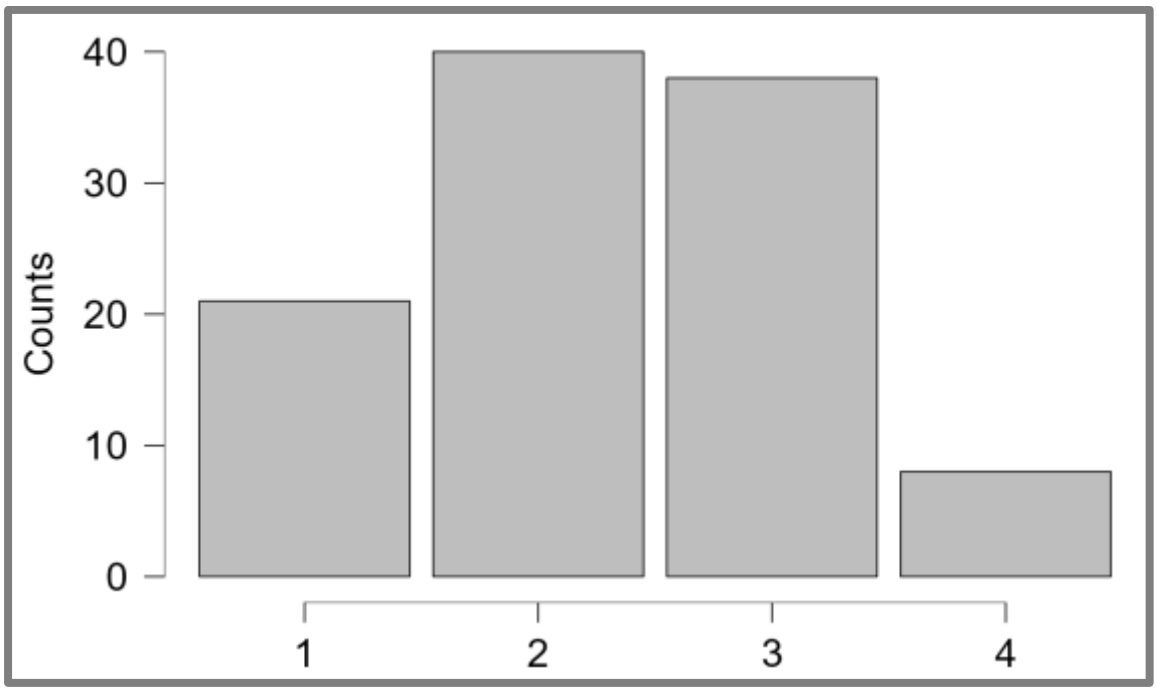
23. Διαγράφω οποιαδήποτε πληροφορία που συλλέγονται για μένα

Ο πίνακας 23 αποτυπώνει ότι το 37,3% των ερωτηθέντων απαντά «συχνά» σε σχέση με το παραπάνω μέτρο προστασίας ενώ το 35,5% απαντά «σπάνια». Το 19,6% απαντά «πάντα» και το 7,4% απαντά ότι «ποτέ» δεν διαγράφει τις πληροφορίες που συλλέγοντα για το άτομό του.

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Πίνακας 23.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Διαγράφω οποιαδήποτε πληροφορία που συλλέγονται για μένα]	Frequency	Percent	Valid Percent	Cumulative Percent
1	21	19.626	19.626	19.626
2	40	37.383	37.383	57.009
3	38	35.514	35.514	92.523
4	8	7.477	7.477	100.000
Missing	0	0.000		
Total	107	100.000		



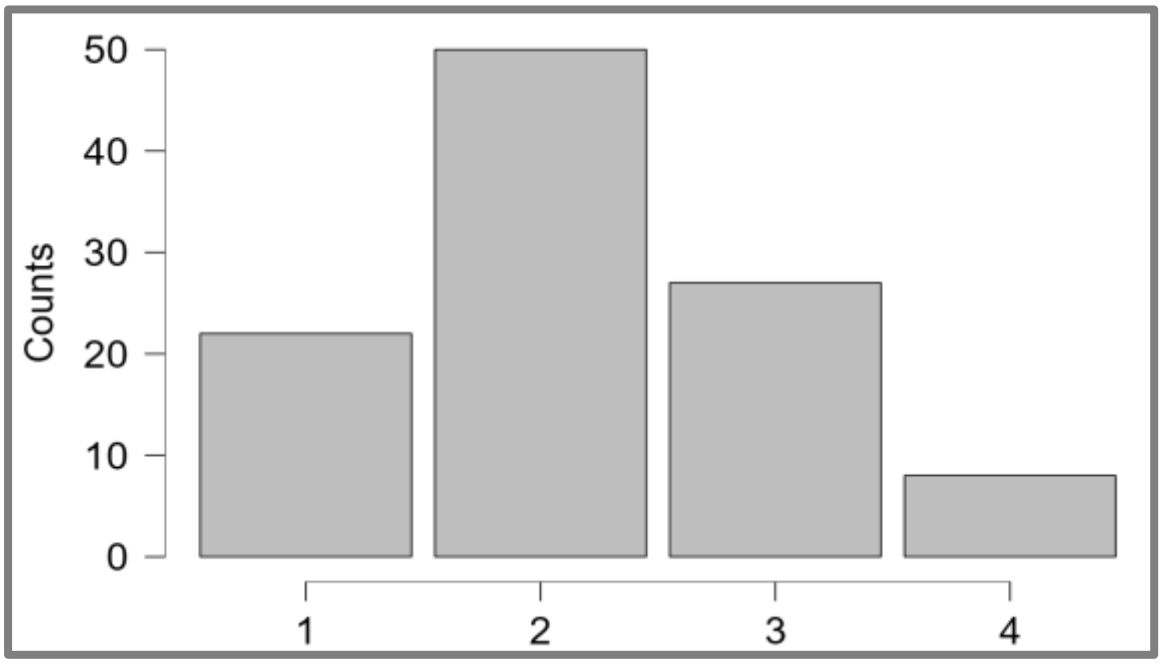
24. Η συσκευή που χρησιμοποιώ παρέχει ισχυρό έλεγχο ταυτότητας

Σύμφωνα με τον πίνακα 24 οι ερωτηθέντες χρησιμοποιούν «συχνά» (46,7%) συσκευή με ισχυρό έλεγχο ταυτότητας και το 20,5% χρησιμοποιούν «πάντα». Από την άλλη, το 25,2% απαντά «σπάνια και το 7,4% απαντά «ποτέ».

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Πίνακας 24.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Η συσκευή που χρησιμοποιώ παρέχει ισχυρό έλεγχο ταυτότητας]	Frequency	Percent	Valid Percent	Cumulative Percent
1	22	20.561	20.561	20.561
2	50	46.729	46.729	67.290
3	27	25.234	25.234	92.523
4	8	7.477	7.477	100.000
Missing	0	0.000		
Total	107	100.000		



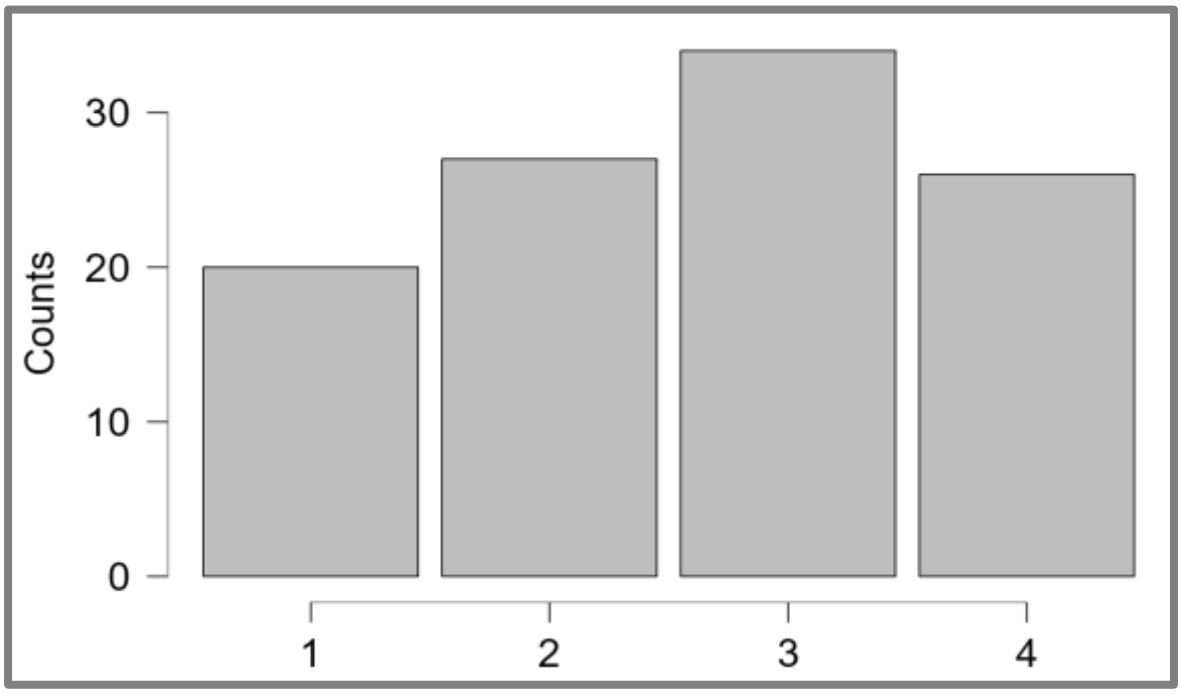
25. Μπορώ εξ αποστάσεως να απενεργοποιήσω τη συσκευή, εάν χαθεί ή κλαπεί

Βάσει των απαντήσεων στον πίνακα 25, φαίνεται ότι το 31,7% το οποίο αντιστοιχεί και στην πλειοψηφία του δείγματος, «σπάνια» μπορεί να απενεργοποιήσει εξ αποστάσεως την συσκευή ένα χαθεί ή αν κλαπεί και 24,2% δηλώνει «ποτέ». από την άλλη, το 25,2% δηλώνει «συχνά» ενώ το 18,6% δηλώνει «πάντα». Μια πιθανή αιτιολογία για τις συγκεκριμένες απαντήσεις είναι ότι οι νέες «έξυπνες» συσκευές κοστίζουν πολλά χρήματα τα οποία δεν είναι σε θέση όλοι να τα διαθέσουν και γι' αυτό δεν έχουν την αντίστοιχη δυνατότητα.

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Πίνακας 25.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Μπορώ εξ αποστάσεως να απενεργοποιήσω τη συσκευή, εάν χαθεί ή κλαπεί]	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	20	18.692	18.692	18.692
2	27	25.234	25.234	43.925
3	34	31.776	31.776	75.701
4	26	24.299	24.299	100.000
Missing	0	0.000		
Total	107	100.000		



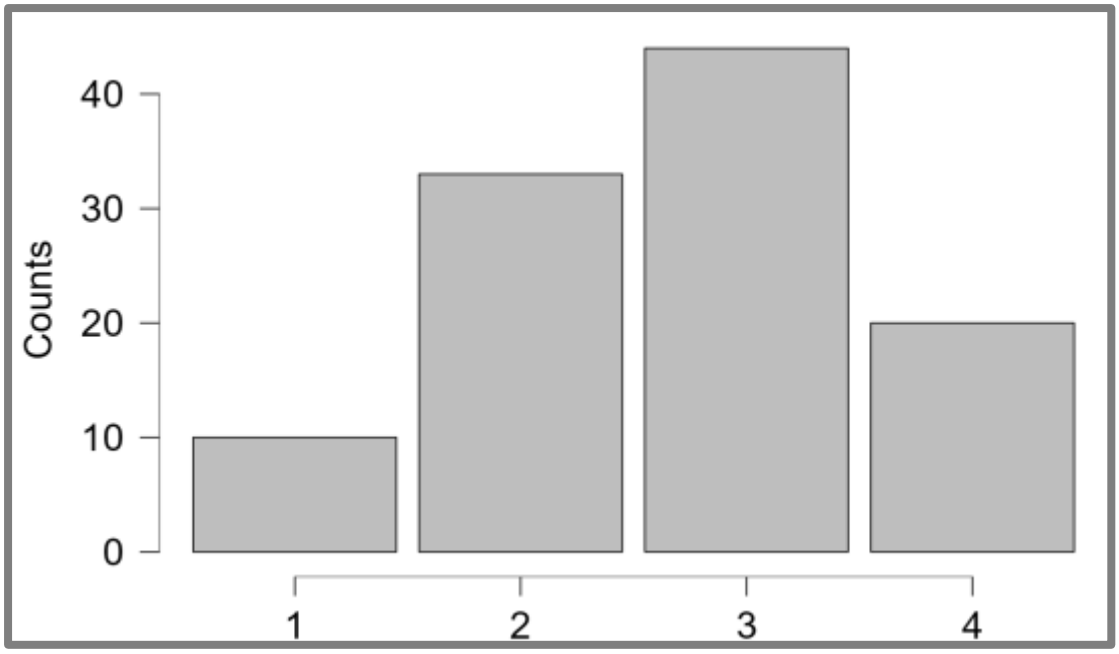
26. Δεν χρησιμοποιώ κυβερνητικές ηλεκτρονικές πλατφόρμες

Από ότι φαίνεται στον πίνακα 26, το δείγμα με 41,1% «σπάνια» δεν χρησιμοποιεί κυβερνητικές ηλεκτρονικές πλατφόρμες και 18,6% «ποτέ». Η πλειοψηφία δηλώνει ότι χρησιμοποιεί «συχνά» κυβερνητικές ηλεκτρονικές πλατφόρμες με ποσοστό 30,8% και «πάντα» με 9,3%.

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Πίνακας 26.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Δεν χρησιμοποιώ κυβερνητικές ηλεκτρονικές πλατφόρμες]	Frequency	Percent	Valid Percent	Cumulative Percent
1	10	9.346	9.346	9.346
2	33	30.841	30.841	40.187
3	44	41.121	41.121	81.308
4	20	18.692	18.692	100.000
Missing	0	0.000		
Total	107	100.000		



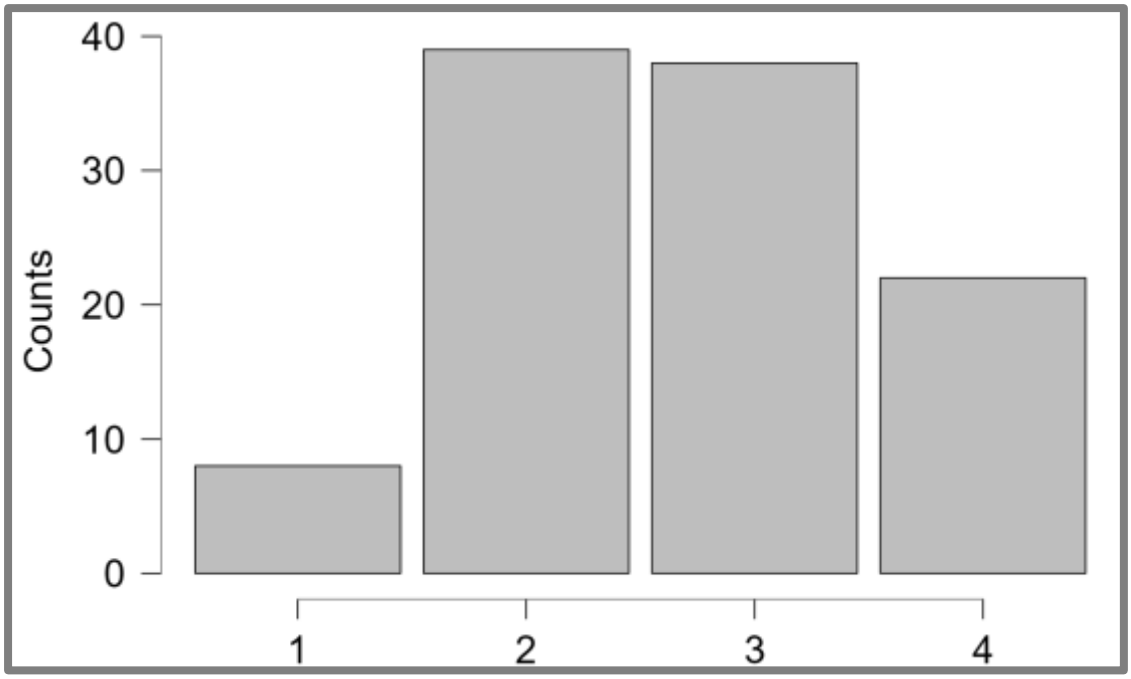
27. Χρησιμοποιώ ανώνυμη περιήγηση στο διαδίκτυο

Από τους 107 συμμετέχοντες στην έρευνα, οι 39 δηλώνουν ότι «συχνά» χρησιμοποιούν ανώνυμη περιήγηση στο διαδίκτυο καθώς 8 από αυτούς δηλώνουν «πάντα» όπως δείχνει και ο πίνακας 27. Αντίθετα, οι 38 από τους 107 δηλώνουν «σπάνια» και οι 22 δηλώνουν «ποτέ».

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Πίνακας 27.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Χρησιμοποιώ ανώνυμη περιήγηση στο διαδίκτυο]	Frequency	Percent	Valid Percent	Cumulative Percent
1	8	7.477	7.477	7.477
2	39	36.449	36.449	43.925
3	38	35.514	35.514	79.439
4	22	20.561	20.561	100.000
Missing	0	0.000		
Total	107	100.000		



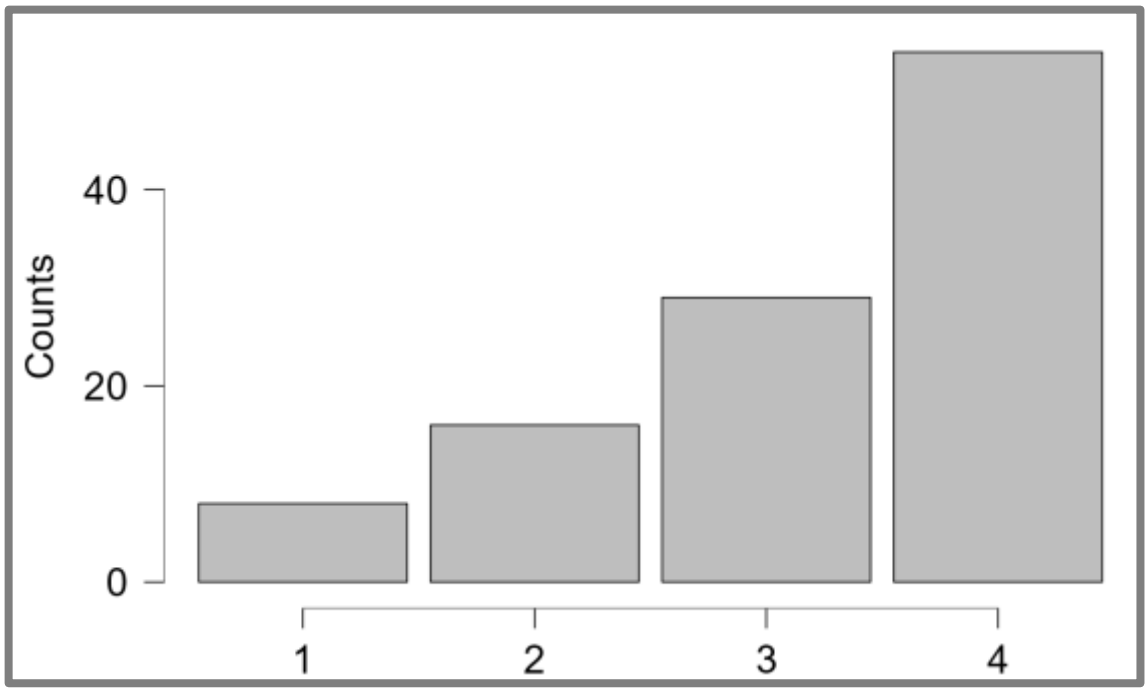
28. Δίνω προσωπικά στοιχεία σε συνομιλία στο διαδίκτυο

Στην τελευταία ερώτηση του ερωτηματολογίου, οι ερωτηθέντες δηλώνουν ότι «ποτέ» δίνουν προσωπικά στοιχεία σε συνομιλία τους στο διαδίκτυο σε ποσοστό 50,4% καθώς και το 27,1% δηλώνουν «σπάνια». Τέλος, το 14,9% δίνει στοιχεία προσωπικά «συχνά» ενώ το 7,4% δίνει «πάντα».

Όπου 1=Πάντα, 2=Συχνά, 3=Σπάνια, 4=Ποτέ

Frequencies for ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Δίνω

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ [Δίνω	Frequency	Percent	Valid Percent	Cumulative Percent
1	8	7.477	7.477	7.477
2	16	14.953	14.953	22.430
3	29	27.103	27.103	49.533
4	54	50.467	50.467	100.000
Missing	0	0.000		
Total	107	100.000		



5.6. ΣΥΣΧΕΤΙΣΕΙΣ

1. Φύλο και «Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής»

Contingency Tables

ΦΥΛΟ		ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής]					Total
		1	2	3	4	5	
1	Count	4.000	11.000	13.000	8.000	0.000	36.000
	% within row	11.111 %	30.556 %	36.111 %	22.222 %	0.000 %	100.000 %
	% within column	36.364 %	42.308 %	30.952 %	32.000 %	0.000 %	33.645 %
	% of total	3.738 %	10.280 %	12.150 %	7.477 %	0.000 %	33.645 %
2	Count	7.000	15.000	29.000	17.000	3.000	71.000
	% within row	9.859 %	21.127 %	40.845 %	23.944 %	4.225 %	100.000 %
	% within column	63.636 %	57.692 %	69.048 %	68.000 %	100.000 %	66.355 %
	% of total	6.542 %	14.019 %	27.103 %	15.888 %	2.804 %	66.355 %
Total	Count	11.000	26.000	42.000	25.000	3.000	107.000
	% within row	10.280 %	24.299 %	39.252 %	23.364 %	2.804 %	100.000 %
	% within column	100.000 %	100.000 %	100.000 %	100.000 %	100.000 %	100.000 %
	% of total	10.280 %	24.299 %	39.252 %	23.364 %	2.804 %	100.000 %

Στον παραπάνω πίνακα ελέγχουμε αν οι μεταβλητές φύλο και «Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής»είναι ανεξάρτητες. Βλέπουμε πως από το σύνολο των 107 ερωτηθέντων, το 34,57% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 26,16% του δείγματος βρίσκεται στο διαφωνώ έως διαφωνώ απόλυτα. Τέλος το 39,25% τείνει στο ούτε συμφωνώ ούτε διαφωνώ. Πιο συγκεκριμένα το 20,5% του συνόλου των γυναικών συμφωνούν έως συμφωνούν

απόλυτα με την άποψη αυτή, ενώ το 27,1% βρίσκεται στο ούτε συμφωνώ ούτε διαφωνώ. Μικρότερα ποσοστά στο διαφωνώ έως διαφωνώ απόλυτα. Όσον αφορά τους άνδρες, το 14,01% συμφωνεί έως συμφωνεί απόλυτα με την άποψη αυτή, ενώ μικρότερα ποσοστά είτε τείνουν στο ούτε συμφωνώ ούτε διαφωνώ είτε στο διαφωνώ έως διαφωνώ απόλυτα.

Chi-Squared Tests

	Value	df	P
X^2	2.598	4	0.627
N	107		

Στο παραπάνω πινακάκι παρουσιάζονται τα αποτελέσματα ελέγχου χ^2

Για τον παραπάνω έλεγχο θα πρέπει να καθοριστούν τα εξής:

H_0:Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής και το φύλο είναι ανεξάρτητες μεταβλητές

Η1:Η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής και το φύλο δεν είναι ανεξάρτητες μεταβλητές

Το κριτήριο απόφασης είναι:

Εάν p>a, η H_0 είναι αποδεκτή.

Η απόφαση

Αν α=0,05, τότε p=0,62 >0,05, άρα η H_0 είναι δεκτή.

Επομένως για α=0,05 το φύλο και η τήρηση των προσωπικών δεδομένων στο διαδίκτυο είναι ασφαλής είναι ανεξάρτητες μεταβλητές.

2. Εκπαιδευτικό Επίπεδο και «Είμαι πλήρως και ορθώς ενημερωμένος/η

Contingency Tables

ΕΚΠΑΙΔΕΥΤΙΚΟ ΕΠΙΠΕΔΟ		ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Είμαι πλήρως και ορθώς ενημερωμένος/η					
		1	2	3	4	5	Total
1	Count	1.000	0.000	1.000	3.000	3.000	8.000
	% within row	12.500 %	0.000 %	12.500 %	37.500 %	37.500 %	100.000 %
	% within column	5.000 %	0.000 %	4.000 %	15.789 %	75.000 %	7.477 %
	% of total	0.935 %	0.000 %	0.935 %	2.804 %	2.804 %	7.477 %
2	Count	2.000	5.000	1.000	1.000	0.000	9.000
	% within row	22.222 %	55.556 %	11.111 %	11.111 %	0.000 %	100.000 %
	% within column	10.000 %	12.821 %	4.000 %	5.263 %	0.000 %	8.411 %
	% of total	1.869 %	4.673 %	0.935 %	0.935 %	0.000 %	8.411 %
3	Count	5.000	9.000	8.000	5.000	0.000	27.000
	% within row	18.519 %	33.333 %	29.630 %	18.519 %	0.000 %	100.000 %
	% within column	25.000 %	23.077 %	32.000 %	26.316 %	0.000 %	25.234 %
	% of total	4.673 %	8.411 %	7.477 %	4.673 %	0.000 %	25.234 %
4	Count	3.000	13.000	7.000	5.000	0.000	28.000
	% within row	10.714 %	46.429 %	25.000 %	17.857 %	0.000 %	100.000 %
	% within column	15.000 %	33.333 %	28.000 %	26.316 %	0.000 %	26.168 %
	% of total	2.804 %	12.150 %	6.542 %	4.673 %	0.000 %	26.168 %
5	Count	6.000	11.000	8.000	4.000	1.000	30.000

2. Εκπαιδευτικό Επίπεδο και «Είμαι πλήρως και ορθώς ενημερωμένος/η

Contingency Tables

ΕΚΠΑΙΔΕΥΤΙΚΟ ΕΠΙΠΕΔΟ		ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Είμαι πλήρως και ορθώς ενημερωμένος/η					
		1	2	3	4	5	Total
6	% within row	20.000 %	36.667 %	26.667 %	13.333 %	3.333 %	100.000 %
	% within column	30.000 %	28.205 %	32.000 %	21.053 %	25.000 %	28.037 %
	% of total	5.607 %	10.280 %	7.477 %	3.738 %	0.935 %	28.037 %
	Count	3.000	1.000	0.000	1.000	0.000	5.000
	% within row	60.000 %	20.000 %	0.000 %	20.000 %	0.000 %	100.000 %
	% within column	15.000 %	2.564 %	0.000 %	5.263 %	0.000 %	4.673 %
	% of total	2.804 %	0.935 %	0.000 %	0.935 %	0.000 %	4.673 %
Total	Count	20.000	39.000	25.000	19.000	4.000	107.000
	% within row	18.692 %	36.449 %	23.364 %	17.757 %	3.738 %	100.000 %
	% within column	100.000 %	100.000 %	100.000 %	100.000 %	100.000 %	100.000 %
	% of total	18.692 %	36.449 %	23.364 %	17.757 %	3.738 %	100.000 %

Στον παραπάνω πίνακα ελέγχουμε αν οι μεταβλητές εκπαίδευσηκαι «Είμαι πλήρως και ορθώς ενημερωμένος/η για την ασφάλεια και τους κινδύνους του διαδικτύου»είναι ανεξάρτητες. Βλέπουμε πως από το σύνολο των 107 ερωτηθέντων, το 55,13% συμφωνεί έως συμφωνεί απόλυτα με την άποψη αυτή ενώ το 21,48% διαφωνεί. Σύμφωνα με την πρώτη κλίμακα εκπαίδευσης (Δημοτικό/Γυμνάσιο), το 0,93% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 5,6% του δείγματος βρίσκεται στο διαφωνώ. Σύμφωνα με τη δεύτερη κλίμακα εκπαίδευσης (Δευτεροβάθμια), το

6,53% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 0,93% του δείγματος βρίσκεται στο διαφωνώ έως διαφωνώ απόλυτα. Στην κλίμακα πτυχιούχοι ΑΕΙ, το 13,07% είναι στο συμφωνούν έως συμφωνούν απόλυτα,ενώ το 4,67% του δείγματος βρίσκεται στο διαφωνώ έως διαφωνώ απόλυτα. Στην κλίμακα πτυχιούχοι ΑΤΕΙ, το 14,95% είναι στο συμφωνούν έως συμφωνούν απόλυτα,ενώ το 4,67% του δείγματος βρίσκεται στο διαφωνώ έως διαφωνώ απόλυτα. Στην κλίμακα των κατόχων τίτλο Μεταπτυχιακού, το 15,88% συμφωνούν έως συμφωνούν απόλυτα. Τέλος στην κλίμακα κατόχων Διδακτορικού το 3,73% είναι συμφωνούν έως συμφωνούν απόλυτα.

Chi-Squared Tests

	Value	df	p
X^2	42.891	20	0.002
N	107		

Στο παραπάνω πινακάκι παρουσιάζονται τα αποτελέσματα ελέγχου χ^2

Για τον παραπάνω έλεγχο θα πρέπει να καθοριστούν τα εξής:

H_0: Είμαι πλήρως και ορθώς ενημερωμένος/η για την ασφάλεια και τους κινδύνους του διαδικτύου και ηεκπαίδευση είναι ανεξάρτητες μεταβλητές

Η1: Είμαι πλήρως και ορθώς ενημερωμένος/η για την ασφάλεια και τους κινδύνους του διαδικτύου και ηεκπαίδευση δεν είναι ανεξάρτητες μεταβλητές

Το κριτήριο απόφασης είναι:

Εάν p>a, η H_0 είναι αποδεκτή.

Η απόφαση

Αν α=0,05, τότε p=0,002 < 0,05, άρα ηH_0δεν είναι δεκτή.

Επομένως για α=0,05 ηεκπαίδευση και είμαι πλήρως και ορθώς ενημερωμένος/η για την ασφάλεια και τους κινδύνους του διαδικτύου δεν είναι ανεξάρτητες μεταβλητές.

3. Ηλικία και «Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη

Contingency Tables

ΗΛΙΚΙΑ		ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη]					
		1	**2**	**3**	**4**	**5**	**Total**
1	Count	0.000	0.000	0.000	2.000	1.000	3.000
	% within row	0.000 %	0.000 %	0.000 %	66.667 %	33.333 %	100.000 %
	% within column	0.000 %	0.000 %	0.000 %	6.250 %	9.091 %	2.804 %
	% of total	0.000 %	0.000 %	0.000 %	1.869 %	0.935 %	2.804 %
2	Count	1.000	6.000	1.000	3.000	3.000	14.000
	% within row	7.143 %	42.857 %	7.143 %	21.429 %	21.429 %	100.000 %
	% within column	12.500 %	18.750 %	4.167 %	9.375 %	27.273 %	13.084 %
	% of total	0.935 %	5.607 %	0.935 %	2.804 %	2.804 %	13.084 %
3	Count	4.000	9.000	11.000	6.000	2.000	32.000
	% within row	12.500 %	28.125 %	34.375 %	18.750 %	6.250 %	100.000 %
	% within column	50.000 %	28.125 %	45.833 %	18.750 %	18.182 %	29.907 %
	% of total	3.738 %	8.411 %	10.280 %	5.607 %	1.869 %	29.907 %
4	Count	3.000	14.000	9.000	11.000	2.000	39.000
	% within row	7.692 %	35.897 %	23.077 %	28.205 %	5.128 %	100.000 %
	% within column	37.500 %	43.750 %	37.500 %	34.375 %	18.182 %	36.449 %
	% of total	2.804 %	13.084 %	8.411 %	10.280 %	1.869 %	36.449 %
5	Count	0.000	3.000	3.000	10.000	3.000	19.000
	% within row	0.000 %	15.789 %	15.789 %	52.632 %	15.789 %	100.000 %

3. Ηλικία και «Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη

Contingency Tables

		ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ [Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη]					
ΗΛΙΚΙΑ		**1**	**2**	**3**	**4**	**5**	**Total**
	% within column	0.000 %	9.375 %	12.500 %	31.250 %	27.273 %	17.757 %
	% of total	0.000 %	2.804 %	2.804 %	9.346 %	2.804 %	17.757 %
	Count	8.000	32.000	24.000	32.000	11.000	107.000
	% within row	7.477 %	29.907 %	22.430 %	29.907 %	10.280 %	100.000 %
Total	% within column	100.000 %	100.000 %	100.000 %	100.000 %	100.000 %	100.000 %
	% of total	7.477 %	29.907 %	22.430 %	29.907 %	10.280 %	100.000 %

Στον παραπάνω πίνακα ελέγχουμε αν οι μεταβλητέςηλικίακαι «Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη»είναι ανεξάρτητες. Βλέπουμε πως από το σύνολο των 107 ερωτηθέντων, το 37,37% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 40,18% του δείγματος βρίσκεται στο διαφωνώ έως διαφωνώ απόλυτα. Τέλος ένα 22,43% τείνει στο ούτε συμφωνώ ούτε διαφωνώ. Πιο συγκεκριμένα η ηλικιακή ομάδα κάτω των 20 βρίσκεται στο καθόλου. Στην ηλικιακή ομάδα κάτω των 20 ετών, το 2,69 διαφωνούν έως διαφωνούν απόλυτα. Στην ηλικιακή ομάδα των 21-30 ετών, το 6,53 συμφωνούν έως συμφωνούν απόλυτα,ενώ το 0,93% του δείγματος βρίσκεται στο ούτε συμφωνώ ούτε διαφωνώ. Στην ηλικιακή ομάδα των 31-40 ετών, το 12,14% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 10,28% του δείγματος βρίσκεται στο ούτε συμφωνώ ούτε διαφωνώ. Έπειτα στην ηλικιακή ομάδα των 41-50 ετών, το 15,88% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 8,41% του δείγματος βρίσκεται στο ούτε συμφωνώ ούτε διαφωνώ. Τέλος στην ηλικιακή ομάδα άνω των 50 ετών 2,8% συμφωνούν έως συμφωνούν απόλυτα,ενώ το 12,14% του δείγματος βρίσκεται στο διαφωνώ έως διαφωνώ απόλυτα.

Chi-Squared Tests

	Value	df	p
X^2	22.387	16	0.131
N	107		

Στο παραπάνω πινακάκι παρουσιάζονται τα αποτελέσματα ελέγχου χ^2

Για τον παραπάνω έλεγχο θα πρέπει να καθοριστούν τα εξής:

H_0: Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη και η ηλικία είναι ανεξάρτητες μεταβλητές

Η1: Η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητη και ηηλικία δεν είναι ανεξάρτητες μεταβλητές

Το κριτήριο απόφασης είναι:

Εάν p>a, η H_0 είναι αποδεκτή.

Η απόφαση

Αν α=0,05, τότε p=0,13 > 0,05, άρα η H_0είναι δεκτή.

Επομένως για α=0,05 ηηλικία και η λήψη cookies κατά την είσοδο σας στις ιστοσελίδες είναι απαραίτητηείναι ανεξάρτητες μεταβλητές.

ΚΕΦΑΛΑΙΟ ΕΚΤΟ

6.1. ΣΥΜΠΕΡΑΣΜΑΤΑ-ΣΥΖΗΤΗΣΗ

Σύμφωνα με τα δημογραφικά αποτελέσματα της έρευνας, η συντριπτική πλειοψηφία του δείγματος είναι γυναίκες ενώ το μεγαλύτερο μέρος του δείγματος ανήκει στο ηλικιακό γκρουπ των 41-50 και ακολουθεί το ηλικιακό γκρουπ των 31-40 διαπιστώνοντας ότι η πλειοψηφία ανήκει στην μέση ηλικία. Μεγάλο επίσης είναι το ποσοστό των συμμετεχόντων οι οποίοι δηλώνουν κάτοχοι μεταπτυχιακού τίτλου αναφορικά με το εκπαιδευτικό επίπεδο του δείγματος καθώς εξίσου υψηλό είναι το ποσοστό αυτών που είναι απόφοιτοι Πανεπιστημίου. Τα συγκεκριμένα ευρήματα δείχνουν το εκπαιδευτικό επίπεδο των ερωτηθέντων είναι αρκετά υψηλό. Τέλος, σύμφωνα με τα δημογραφικά στοιχεία η πλειοψηφία του δείγματος εργάζεται στον ιδιωτικό τομέα ενώ μεγάλο ποσοστό εμφανίζεται να δηλώνει ότι δεν ανήκει σε καμία από τις αναφερθείσες κατηγορίες του ερωτηματολογίου.

Βάσει ανάλυσης του ερωτηματολογίου, τα 2/3 του δείγματος χρησιμοποιούν πάρα πολύ συχνά το διαδίκτυο όπως επίσης χρησιμοποιούν παρά πολύ τις ηλεκτρονικές τραπεζικές συναλλαγές. Τόσο η πρόσβαση στις ηλεκτρονικές υπηρεσίες όπως επίσης οι ίδιες οι ψηφιακές πλατφόρμες θεωρούνται εύκολες από την πλειοψηφία του δείγματος. Παρόλο που σε μεγάλο ποσοστό το δείγμα είναι ικανοποιημένο από τις ηλεκτρονικές υπηρεσίες της Δημόσιας Διοίκησης, το δείγμα δηλώνει ανησυχία για την επιτήρηση από την κυβέρνηση αναφορικά με το διαδίκτυο.

Σε συνέχεια του ερωτηματολογίου, οι συμμετέχοντες στην έρευνα χρησιμοποιούν το διαδίκτυο σε μεγαλύτερο ποσοστό για ανταλλαγή μηνυμάτων με φίλους και στη συνέχεια για χρηματικές συναλλαγές. Τέλος, άλλος σημαντικός λόγος χρήσης του διαδικτύου αποτελεί η διεκπεραίωση διαφόρων εργασιών.

Από το μέρος του ερωτηματολογίου το οποίο εξετάζει την ασφάλεια του διαδικτύου, οι απαντήσεις δεν είναι τόσο ξεκάθαρος. Μεγάλο ποσοστό του δείγματος κρατάει ουδέτερη στάση δηλώνοντας «ούτε διαφωνώ/ ούτε συμφωνώ», στο ότι η τήρηση των προσωπικών δεδομένων είναι ασφαλής στο διαδίκτυο όπως επίσης στο ότι αισθάνονται ότι έχουν τον έλεγχο στις πληροφορίες που παρέχουν σε απευθείας σύνδεση. Επιπλέον, το δείγμα δηλώνει ότι δεν έχει εμπιστοσύνη στην τεχνολογία που χρησιμοποιούν οι κυβερνητικοί φορείς καθώς επίσης δεν νοιώθει ασφάλεια όταν παρέχει ευαίσθητες πληροφορίες στο διαδίκτυο. Τέλος, η ενημέρωση

για τους κανόνες ασφαλείας του διαδικτύου κρίνεται απαραίτητη για το δείγμα ενώ η πλειοψηφία του δηλώνει ότι είναι ορθά ενήμερη.

Τέλος, σύμφωνα με την έρευνα οι συμμετέχοντες επιλέγουν συχνά να αποχωρήσουν από την συλλογή δεδομένων και ταυτόχρονα οι συσκευές τους διαθέτουν έναν ισχυρό έλεγχο ταυτότητας ως μέτρα προστασίας από απειλές του διαδικτύου. Επίσης οι συμμετέχοντες της έρευνας, διαγράφουν οποιαδήποτε πληροφορία συλλέγεται για αυτούς και ταυτόχρονα δεν δίνουν προσωπικές πληροφορίες σε συνομιλίες τους στο διαδίκτυο. Τέλος, χρησιμοποιούν ανώνυμη περιήγηση στο διαδίκτυο ως μέτρο προστασίας στον κυβερνοχώρο.

Γίνεται λοιπόν, αντιληπτό ότι η ασφάλεια στο διαδίκτυο αποτελεί ένα θέμα που απασχολεί και προβληματίζει τους πολίτες που αναπόφευκτα το χρησιμοποιούν και μάλιστα διεκπεραιώνουν πολλές συναλλαγές κυρίως χρηματικές.

Η τεχνολογία έχει μεταμορφώσει τις καθημερινές διαδικασίες και μάλιστα με υψηλή αποτελεσματικότητα αλλά ταυτόχρονα δημιούργησε και πολλούς κινδύνους. Τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο γίνεται συνεχής προσπάθεια για προστασία των πολιτών και των οργανώσεων από τις κυβερνοαπειλές οι οποίες είτε σε επίπεδο ατομικό είτε σε επίπεδο επιχειρήσεων μπορεί να έχει άσχημες και αρνητικές συνέπειες σε κοινωνικό επίπεδο.

Από την έρευνα προκύπτει ότι η προσπάθεια για προστασία της ασφάλειας γίνεται περισσότερο σε ατομικό επίπεδο και ο κάθε πολίτης επιδιώκει με δικούς του τρόπους να ακολουθεί ορισμένα βήματα προκειμένου να καλύψει τα ευαίσθητα προσωπικά δεδομένα που κοινοποιεί στο διαδίκτυο.

Επίσης η ενημέρωση και η εκπαίδευση των πολιτών αναφορικά με τη σωστή χρήση και την ορθή προστασία των πολιτών από τις κυβερνοαπειλές αποτελεί το σημαντικότερο μέτρο προστασίας τους.

Η Ευρωπαϊκή Ένωση στο σύνολό της αλλά και οι κυβερνήσεις ξεχωριστά οφείλουν να παρέχουν ενημέρωση στις επιχειρήσεις τόσο του ιδιωτικού τομέα όσο και του δημοσίου αλλά και να αναβαθμίζουν συνεχώς τις μεθόδους προστασίας τους έναντι των κυβερνοαπειλών καθώς ο ψηφιακός μετασχηματισμός αποτελεί πλέον πραγματικότητα. η τήρηση της σχετικής νομοθεσίας για την ακριβή ταυτοποίηση και την παροχή ευθύνης σε περιπτώσεις κυβερνοεγκλήματος.

6.2. ΠΕΡΙΟΡΙΣΜΟΙ ΤΗΣ ΕΡΕΥΝΑΣ

Όπως όλες οι έρευνες έτσι και η συγκεκριμένη έρευνα υπόκειται στους μεθοδολογικούς περιορισμούς οι οποίοι έχουν να κάνουν με ορισμένες αδυναμίες κατά την διεξαγωγή της έρευνας.

Στην παρούσα έρευνα οι περιορισμοί της σχετίζονται αρχικά με το μέγεθος του δείγματος καθώς και με τον τόπο και το εύρος της. Αρχικά το δείγμα της έρευνας είναι σχετικά μικρό για την συλλογή δεδομένων αναφορικά με το υπό εξέταση θέμα. Επίσης, το γεωγραφικό μέρος το οποίο επιλέχθηκε να διεξαχθεί η έρευνα και να αποτυπωθεί το δείγμα είναι εξίσου συγκεκριμένο και στοχευμένο. Ως συνέπεια αυτών, η έρευνα δεν είναι σε θέση γενικεύσει τα αποτελέσματά της στον γενικότερο πληθυσμό και να αναδείξει την γενικότερη τάση των πολιτών σε σχέση με την κυβερνοασφάλεια στον τομέα της Δημόσιας Διοίκησης.

Επίσης το δείγμα που χρησιμοποιήθηκε στην έρευνα ήταν δείγμα ευκολίας καθώς υπήρχε ευκολότερη πρόσβαση σε αυτό αλλά ταυτόχρονα πρόκειται για μια σοβαρή απειλή της έρευνας και έναν σοβαρό περιορισμό για την αντιπροσωπευτικότητα των αποτελεσμάτων.

Το ίδιο το ερευνητικό εργαλείο που χρησιμοποιήθηκε από μόνο του παρουσιάζει ορισμένους περιορισμούς. Οι κλειστού τύπου ερωτήσεις δεν αφήνουν περιθώρια βάθους των πληροφοριών που συλλέγονται αλλά αντίθετα υπάρχει απώλεια λεπτομερειών στις απαντήσεις και πιθανή δικαιολόγηση των συγκεκριμένων απαντήσεων που δίνονται.

Τέλος, τόσο η έλλειψη ελέγχου της ακρίβειας των απαντήσεων όσο και η έλλειψη ελέγχου της ειλικρίνειας των ερωτηθέντων αποτελούν δυο επιπλέον περιορισμούς τόσο της παρούσας έρευνας όσο και των ερευνών στο σύνολό τους.

6.3. ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΕΡΕΥΝΑ

Η παρούσα εργασία προσπάθησε να αναδείξει την σημασία της κυβερνοασφάλειας ως μια νέα πλευρά του ψηφιακού μετασχηματισμού στον σύγχρονο κόσμο της Δημόσιας Διοίκησης.

Ως βασική μελλοντική πρόταση για έρευνα πάνω στο συγκεκριμένο θέμα θα μπορούσε να είναι η επανάληψη της ίδιας της έρευνας με πολύ μεγαλύτερο δείγμα και μεγαλύτερο γεωγραφικό εύρος προκειμένου τα αποτελέσματα να μπορούν να αντιπροσωπεύσουν τον γενικό πληθυσμό της Ελλάδας.

Επίσης η έρευνα θα μπορούσε να διεξαχθεί συνδυαστικά με ποιοτική έρευνα προκειμένου να αναλύονται περαιτέρω οι απαντήσεις και να πραγματοποιείται μια εις βάθος ανάλυση των δεδομένων για την διεξαγωγή επιπλέον συμπερασμάτων.

Στο ίδιο πλαίσιο θα μπορούσε να διεξαχθεί η έρευνα και σε άλλους τομείς πέρα από τη Δημόσια Διοίκηση όπως για παράδειγμα στον ιδιωτικό τομέα ή στον τραπεζικό κλάδο.

Τέλος, η έρευνα μπορεί να διεξαχθεί σε μελλοντικό χρόνο εφόσον τόσο οι κρατικοί μηχανισμοί όσο και η Ευρωπαϊκή ένωση αλλά και η εκπαίδευση των πολιτών σε σχέση με την κυβερνοασφάλεια θα έχει εξελιχθεί και αναπτυχθεί, προκειμένου να διαπιστωθούν τυχόν διαφορές στις απόψεις των πολιτών αναφορικά με το συγκεκριμένο ζήτημα μέσα από συγκριτική μελέτη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (GDPR) (2018). Διαθέσιμο στο: https://www.taxheaven.gr/circulars/28194/arora-o-neos-genikos-kanonismos-giathn-prostasia-dedomenwn-proswpikoy-xarakthra-gdpr.

Creswell, J. (2014). *Εκπαιδευτική έρευνα. Σχεδιασμός, διεξαγωγή και αξιολόγηση της ποσοτικής και ποιοτικής έρευνας.* Αθήνα: εκδόσεις Έλλην.

Παρασκευόπουλος, Ι. (1993). Μεθοδολογία Επιστημονικής Έρευνας. Αθήνα: εκδόσεις Πολιτεία.

Τσέκερης, Χ.(2009). Η Κοινωνιολογία του Κυβερνοχώρου, στο Κ. Κοσκινάς & Σ. Αρσένης (επιμ.) *Δυνητικές Κοινότητες και Διαδίκτυο: Κοινωνιο-Ψυχολογικές Προσεγγίσεις και Τεχνικές Εφαρμογές*. Αθήνα: Εκδόσεις Κλειδάριθμος.

ΥπουργείοΨηφιακήςΔιακυβέρνησης. (2021). *Κυβερνοασφάλεια.* Διαθέσιμο στο:http://www.opengov.gr/digitalandbrief/?p=2123.

ΞΕΝΟΓΛΩΣΣΗ

Al-Rowaily, K., Abulaish, M. Al-HasanHaldar , N. andAl-Rubaian, M. (2015). BiSAL– A bilingual sentiment analysis lexicon to analyze Dark Web forums for cyber security, *Digital Investigation*, vol. 14, pp. 53-62. Διαθέσιμοστο: 10.1016/j.diin.2015.07.006.

Bräuchler, B. (2007). Religious Conflicts in Cyberage", *Citizenship Studies*, vol. 11, no. 4, pp. 329-347. Διαθέσιμοστο : 10.1080/13621020701476012.

Caruso, R. and Locatelli, A. (2014). *Understanding terrorism*. Bingley: Emerald Group Publishing Limited.

Chertoff, M. and Simon, T. (2015). *The impact of the dark web on internet goverannce and cyber security.*

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber-crimes: A review. arXiv preprint arXiv:1502.03552.

Erik M. (2012). Cyber 3.0: The Department of Defense strategy for operating in cyberspace and the attribution problem, *Air Force Law Review*, vol. 68.

Fu, A. Abbasi and Chen, H. (2010). A focused crawler for Dark Web forums. *Journal of the American Society for Information Science and Technology.* Διαθέσιμοστο: 10.1002/asi.21323.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, 3(1), 49–58. Διαθέσιμοστο: doi:10.1093/cybsec/tyw018.

Hongthong, W. (2017). Preventative Measures Against On-Line Hate Speech: A Case Study of Thailand Political Conflict, 2005-2014. *RSU International Journal of College of Government (RSUIJCG)*, vol. 4, no.1.

Kirkpatrick, D. L. (2009). *Managing change effectively*. Boston, MA: Routledge.

Konstaninidis, C., Ntonti, M., Zografou, S. &Kourtesi, S. (2023). Work motivation as a strategic development tool for the Greek forest service departments:Evidence from the region of Macedonia and Thrace. *International Journal of Applied Economics, Finance and Accounting*,16 (2), pp. 297-307. DOI: 10.33094/ijaefa.v16i2.982.

Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. *International Journal of Advance Research in Computer Science and Management*, 4(4), pp. 125-129.

NIS Directive in Greece (2021). *Shaping Europe's digital future.* Διαθέσιμο στο:https://digital-strategy.ec.europa.eu/en/policies/nis-directive-greece

Panchanatham, D. N. (2015). *A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology*.

Stephanie G., (2012). The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. *Stanford Journal of International Law*, vol. 48 (1).

Wertheim, M.(1998). *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet*, Norton, New York.

ΔΙΑΔΙΚΤΥΟ

http://www.sepe.gr/

https://www.tovima.gr/2022/11/14/society/epithesi-xaker-sto-yp-psifiakis-diakyvernisis-epixeirisan-na-riksoun-800-istotopous-tou-dimosiou/.

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_el.

https://eur-lex.europa.eu/legalcontent/el/ALL/?uri=CELEX:32016L1148