

Ασφάλεια και παραβίαση προσωπικών δεδομένων στο διαδίκτυο: τι γνωρίζουν μελλοντικοί εκπαιδευτικοί της Πρωτοβάθμιας Εκπαίδευσης;

Φωτεινή Βαλιμήτη, Ανθή Καρατράντου, Χρήστος Παναγιωτακόπουλος
up1049070@upnet.gr, akarar@upatras.gr, cpanag@upatras.gr
Τμήμα Επιστημών της Εκπαίδευσης και Κοινωνικής Εργασίας, Πανεπιστήμιο Πατρών

Περίληψη

Η παρούσα εργασία αποσκοπεί στη διερεύνηση των γνώσεων μελλοντικών εκπαιδευτικών Πρωτοβάθμιας Εκπαίδευσης σχετικά με θέματα ασφάλειας προσωπικών δεδομένων στο διαδίκτυο. Στην έρευνα χρησιμοποιήθηκε ερωτηματολόγιο το οποίο απαντήθηκε εθελοντικά από φοιτητές Παιδαγωγικού Τμήματος Δημοτικής Εκπαίδευσης. Τα αποτελέσματα έδειξαν ότι η πλειοψηφία των συμμετεχόντων γνωρίζει ποια είναι τα προσωπικά και τα ευαίσθητα προσωπικά δεδομένα, δεν γνωρίζει όμως τι είναι και πως λειτουργούν τα Cookies, το WebCam Hacking και το Phishing. Οι περισσότεροι θεωρούν ότι τα προσωπικά τους δεδομένα δεν είναι ασφαλή στο διαδίκτυο. Παρόλα αυτά δεν διαβάζουν την πολιτική χρήσης των ιστοχώρων που χρησιμοποιούν. Η σχετική πλειοψηφία των συμμετεχόντων στην έρευνα γνωρίζει τι είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων, αναγνωρίζει αρκετές από τις παράνομες ενέργειες στο διαδίκτυο και τους φορείς που μπορεί να απευθυνθεί για βοήθεια, εάν αντιληφθεί ότι συμβαίνει κάτι παράνομο. Το φύλο δεν φαίνεται να επιδρά στις απαντήσεις, ενώ το έτος φοίτησης φάνηκε να επιδρά μόνο στην αναγνώριση των ευαίσθητων προσωπικών δεδομένων και στις γνώσεις σχετικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Λέξεις κλειδιά: Ασφάλεια προσωπικών δεδομένων, Διαδίκτυο, Μελλοντικοί εκπαιδευτικοί

Εισαγωγή

Η τεχνολογία σήμερα έχει αλλάξει δραστικά τη ζωή και την καθημερινότητα των νέων. Τα περισσότερα παιδιά και οι έφηβοι διεθνώς είναι σε καθημερινή βάση συνδεδεμένοι στο διαδίκτυο και αφιερώνουν ένα σημαντικό μέρος του χρόνου τους στις υπηρεσίες που παρέχονται σ' αυτό. Η τεχνολογία δίνει ευκαιρίες στους χρήστες για ψυχαγωγία, επικοινωνία, εκπαίδευση, εργασία και αναζήτηση πληροφοριών για οποιοδήποτε θέμα. Από την άλλη πλευρά, ο ψηφιακός κόσμος κρύβει και πολλούς κινδύνους. Η ασφάλεια των δεδομένων των νέων και ιδιαίτερα των παιδιών, όμως, δεν είναι η μόνη που κινδυνεύει κατά την ενασχόληση τους με τις νέες τεχνολογίες. Έρευνες δείχνουν πως η σωματική και ψυχική τους υγεία μπορεί επίσης να παρουσιάσει διαταραχές (Žumárová et al., 2010).

Παρά τους κινδύνους, τα οφέλη των σύγχρονων ψηφιακών μέσων είναι ιδιαίτερα σημαντικά που κάνουν την ενασχόληση των παιδιών με αυτά, απαραίτητη. Για την ασφαλή χρήση του διαδικτύου είναι απαραίτητες οι γνώσεις που αφορούν στα προσωπικά και ευαίσθητα προσωπικά δεδομένα, στους τρόπους παραβίασης και στους τρόπους προστασίας τους. Τα σχολεία και άλλοι φορείς και οργανώσεις οφείλουν να ενημερώνουν και ενημερώνουν τακτικά τους νέους για τους κινδύνους του διαδικτύου ώστε να ελαχιστοποιήσουν τα ενδεχόμενα προβλήματα και να κάνουν μια ασφαλή και παραγωγική χρήση των εφαρμογών του (LCAH Editorial, 2018).

Επειδή, όπως φαίνεται, ο ρόλος του εκπαιδευτικού για την εκπαίδευση σε θέματα ασφαλούς χρήσης του διαδικτύου ιδιαίτερα σε μαθητές μικρής ηλικίας είναι πολύ σημαντικός

(Livingstone et al., 2013; Τσιγκρης, 2014), η έρευνα αυτή στοχεύει να διερευνήσει τι γνωρίζουν για την ασφάλεια των προσωπικών δεδομένων μελλοντικοί εκπαιδευτικοί της πρωτοβάθμιας εκπαίδευσης.

Νέοι και Διαδίκτυο

Ο τρόπος χρήσης του διαδικτύου έχει αλλάξει ριζικά από τη δεκαετία του 1990. Οι χρήστες δημιουργούν ηλεκτρονικά προφίλ συνδεδεμένα με τις προσωπικότητές τους και το διαδίκτυο δεν προσφέρεται πλέον μόνο για επικοινωνία. Οι άνθρωποι αλληλεπιδρούν διαδικτυακά κάθε μέρα, επηρεάζοντας ο ένας τον άλλον. Η ιδιωτικότητα όμως κινδυνεύει καθώς οι χρήστες εκθέτουν πληθώρα προσωπικών στοιχείων τους σε δημόσια θέα. Έτσι, ένας πολύ σημαντικός κίνδυνος που αναδύεται, αφορά στην παραβίαση των προσωπικών δεδομένων και συχνά κατά την πλοήγηση στο διαδίκτυο δεν είμαστε σίγουροι αν τα δεδομένα που έχουμε καταθέσει εκεί, είναι ευάλωτα ή όχι (Zilka, 2017). Το πρόβλημα φαίνεται να είναι εντονότερο στους νέους, οι οποίοι πολλές φορές λειτουργούν χωρίς να ελέγχουν λεπτομερώς το αποτέλεσμα των ενεργειών τους κι έτσι να είναι περισσότερο ευάλωτοι στους κινδύνους που κρύβονται στο διαδίκτυο (Dunkels et al., 2011).

Έρευνες δείχνουν ότι η μεγαλύτερη χρήση του διαδικτύου γίνεται από νέους ηλικίας 16-24 αλλά και μεγαλύτερους, ηλικίας 35-44 ετών και αφορά κυρίως στην κοινωνική δικτύωση. Τα κοινωνικά δίκτυα καλύπτουν διάφορες ανάγκες των ανθρώπων. Η πιο συχνή ανάγκη είναι εκείνη της επικοινωνίας και οι χρήστες μπορούν να βρίσκονται σε επαφή σε όποιο σημείο του πλανήτη κι αν βρίσκονται. Οι νέοι συχνά βρίσκονται μόνιμα συνδεδεμένοι με το διαδίκτυο και περνούν καθημερινά πολλές ώρες σ' αυτό, πραγματοποιώντας διάφορες δραστηριότητες, σχετικές με ψυχαγωγία, συγγραφή εργασιών, ενημέρωση, αγορές κ.ά. Παράλληλα όμως, οι χρήστες είναι εκτεθειμένοι σε διάφορους κινδύνους χωρίς να το έχουν συνειδητοποιήσει και μπορεί να μετατραπούν εύκολα σε θύματα σεξουαλικής ή άλλου είδους παρενόχλησης (grooming & sexting), εκφοβισμού (cyberbullying) αλλά και εξαπάτησης εφόσον δίνουν διάφορες προσωπικές πληροφορίες σε άτομα που δεν γνωρίζουν, τα οποία προσποιούνται ότι ενδιαφέρονται γι' αυτούς (Mason, 2017).

Πολλές ώρες στο διαδίκτυο όμως αφιερώνουν και παιδιά μικρότερης ηλικίας που δέχονται πληθώρα πληροφοριών, αρκετές φορές χωρίς έλεγχο. Από την ηλικία μόλις των 10 ετών, τα παιδιά σήμερα διαθέτουν συσκευή κινητής τηλεφωνίας με πρόσβαση στο διαδίκτυο. Αυτό είναι φυσικό αφού η τεχνολογία έχει εξελιχθεί ραγδαία και αποτελεί αναπόσπαστο κομμάτι της καθημερινότητάς μας, όμως μέσω αυτής τα παιδιά μπορεί πολύ πιο εύκολα να πέσουν θύματα παρενόχλησης και εξαπάτησης. Σε κάθε περίπτωση πρέπει να υπάρχει ένας βαθμός υπευθυνότητας, αλλά και συνειδητοποίησης των κινδύνων που κρύβονται στο διαδίκτυο. Σε σχέση με το φύλο, φαίνεται ότι υπάρχουν μάλλον περισσότερες ομοιότητες παρά διαφορές στη διαδικτυακή συμπεριφορά των μικρών ηλικιών. Πολύ συχνά αυτό αναδεικνύεται μέσα από τη σχετική βιβλιογραφία, αφού οι έρευνες ή οι πρωτοβουλίες που λαμβάνονται αναφέρονται σε «παιδιά» ή σε «μαθητές» και όχι σε κατηγορίες μεταξύ φύλου, ηλικίας, τάξης ή άλλους παράγοντες. Μετά από τα πρώτα μαθητικά χρόνια, οι έρευνες δείχνουν ότι υπάρχουν διαφορές μεταξύ φύλου και προτιμήσεις σε συγκεκριμένο τρόπο διαδικτυακής συμπεριφοράς, όμως οι κίνδυνοι παραμένουν ίδιοι στο διαδίκτυο, ασχέτως φύλου (Weiser, 2004; Livingstone et al., 2013). Ο βαθμός συνειδητοποίησης των κινδύνων φαίνεται να συνδέεται με την ανατροφή των γονιών, αλλά και ο ρόλος του σχολείου και των εκπαιδευτικών φαίνεται να είναι ιδιαίτερα σημαντικός (Ramos-Soler et al., 2018).

Σύμφωνα με τους Livingstone et al. (2013) τα σχολεία είναι ένας από τους κυρίαρχους θεσμούς για τη δημιουργία των «ψηφιακών» πολιτών. Αυτό όμως προϋποθέτει καλά καταρτισμένους εκπαιδευτικούς, το έργο των οποίων είναι δύσκολο. Σημειωτέον, ότι οι

απαγορεύσεις της χρήσης των μέσων κοινωνικής δικτύωσης ή/και των κινητών τηλεφώνων στο σχολείο έχουν φανεί ατελέσφορες.

Ασφάλεια και Παραβίαση Προσωπικών Δεδομένων

Πιο κάτω δίνονται ορισμοί και περιγραφές για έννοιες σχετικές με την ασφάλεια και την παραβίαση των προσωπικών δεδομένων και με τις οποίες ασχολείται η παρούσα έρευνα.

Τα *προσωπικά δεδομένα* σχετίζονται με ονοματεπώνυμο, ηλικία, φυσικά χαρακτηριστικά, μορφωτικά χαρακτηριστικά, επάγγελμα, οικονομική κατάσταση, οικογενειακή κατάσταση, ενδιαφέροντα, δεξιότητες, συνήθειες κ.ά. Τα *ενυπόδητα προσωπικά δεδομένα* σχετίζονται με φυλετική ή εθνική προέλευση, υγεία, πολιτικά φρονήματα, σεξουαλικές συνήθειες και προτιμήσεις, θρησκευτικές - φιλοσοφικές πεποιθήσεις, συνδικαλιστική δραστηριότητα, ποινικές διώξεις ή/και καταδικές, συμμετοχή σε ενώσεις και φορείς, βιομετρικά δεδομένα κ.ά. (Παναγιωτακόπουλος, 2018).

Όταν ένας χρήστης επισκέπτεται μια ιστοσελίδα μέσω του φυλλομετρητή του, τότε ο διακομιστής μπορεί να διαβάσει κάποιες βασικές πληροφορίες που συνδέονται με το προφίλ του επισκέπτη (όπως π.χ. το λειτουργικό σύστημα του χρήστη, το όνομα και την έκδοση του φυλλομετρητή ή τη διεύθυνση σύνδεσης). Ο διακομιστής, εφόσον έχει ρυθμιστεί έτσι, αποστέλλει στον υπολογιστή-επισκέπτη ένα μικρό αρχείο, το *cookie*, το οποίο αποθηκεύεται μέσω του φυλλομετρητή στον υπολογιστή του χρήστη. Αυτό μπορεί να περιέχει τις προηγούμενες πληροφορίες, αλλά και κάποιες ακόμα, όπως π.χ. τις προτιμήσεις της περιήγησης και τις ενέργειες που γίνονται από τον επισκέπτη, τα σχόλια ή τις βαθμολογίες-αξιολογήσεις της ποιότητας κ.ά. (Kurose & Ross, 2004).

Το *WebCam hacking* είναι ένας πολύ συνηθισμένος τρόπος για την υποκλοπή των προσωπικών δεδομένων μέσω της κάμερας είτε του ηλεκτρονικού υπολογιστή, είτε του κινητού τηλεφώνου. Οι *hackers* μέσω διαφόρων ηλεκτρονικών μηνυμάτων ή διαφημίσεων που αποστέλλουν στους χρήστες ή σπάζοντας κωδικούς πρόσβασης αποκτούν πρόσβαση στον ηλεκτρονικό υπολογιστή, tablet ή smartphone των χρηστών. Έτσι, έχοντας αποκτήσει πρόσβαση μπορούν να παρακολουθούν τους χρήστες μέσω εικόνες βίντεο ή να υποκλέπτουν έγγραφα που υπάρχουν αποθηκευμένα στις συσκευές τους. Με τον τρόπο αυτό, όλα τα δεδομένα των χρηστών καθίστανται ευάλωτα (Mateiu, 2017).

Το *Phishing*, αφορά σε μία μέθοδο υποκλοπής που συχνά χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο μέσω του οποίου οι χρήστες λαμβάνουν δελεαστικά μηνύματα (κλήρωση δώρων, ταξιδιών κ.ά.) ή μηνύματα επιβεβαίωσης κωδικών. Αν ενδώσουν στις προτροπές γίνεται δυνατή η υποκλοπή προσωπικών τους δεδομένων, όπως π.χ. ο αριθμός του κινητού τηλεφώνου, οι κωδικοί πρόσβασης σε e-mail ή σε τραπεζικό λογαριασμό, με απρόβλεπτες συνέπειες (Παναγιωτακόπουλος, 2018).

Ως *παράνομες πράξεις* με βάση την Ελληνική νομοθεσία, ορίζονται η πορνογραφία ανηλικών, ο ρατσισμός, η βία και η τρομοκρατία, η οικονομική απάτη μέσω διαδικτύου και η παραβίαση προσωπικών δεδομένων. Έχουν θεσπιστεί σχετικοί νόμοι με τις ανάλογες κυρώσεις για όποιον τους παραβιάσει. Οι νόμοι αυτοί πρέπει να λαμβάνονται υπόψη από όλους τους χρήστες του διαδικτύου (Saferinternet, n.d.).

Τα *πνευματικά δικαιώματα* είναι τα δικαιώματα που κατέχουν οι δημιουργοί για λογοτεχνικά έργα (μυθιστορήματα, βιβλία, ταινίες, μουσικές, κ.ά.) και καλλιτεχνικά έργα (πίνακες ζωγραφικής, χάρτες, φωτογραφίες, γλυπτά, διαφημίσεις, κ.ά.) (Παναγιωτακόπουλος, 2018).

Ο *Γενικός Κανονισμός της Προστασίας Δεδομένων* (General Data Protection Regulation/GDPR) είναι ο κανονισμός (Ε.Ε.) 2016/679 του Ευρωπαϊκού Κοινοβουλίου, ο οποίος ρυθμίζει την επεξεργασία από άτομο, εταιρεία ή οργανισμό των δεδομένων προσωπικού χαρακτήρα που αφορούν πολίτες στην Ε.Ε. Η εφαρμογή του έχει ως στόχο να πληροφορείται αναλυτικά

ο επισκέπτης ενός δικτυακού χώρου για το ποια προσωπικά δεδομένα αποθηκεύονται στο διακομιστή, ώστε να μη γίνεται εν αγνοία του καμία ενέργεια. Απαγορεύει τη συλλογή προσωπικών δεδομένων από παιδιά με ηλικία μικρότερη των 13 χρονών, χωρίς να υπάρχει άδεια από τους κηδεμόνες τους. Δίνει τη δυνατότητα στον χρήστη να διαγράψει τα προσωπικά του δεδομένα και υποχρεώνει τους φορείς συλλογής να θέτουν πρότυπα ασφαλείας για την αποφυγή διαρροής (Schulz & Hennis-Plasschaert, 2016).

Ερευνητικά Ερωτήματα

Με δεδομένο ότι πρόκειται για μελλοντικούς εκπαιδευτικούς Πρωτοβάθμιας Εκπαίδευσης, με την παρούσα έρευνα έγινε προσπάθεια να δοθούν απαντήσεις στα εξής ερωτήματα:

1. Σε τι βαθμό το δείγμα γνωρίζει τι και ποια είναι τα προσωπικά δεδομένα; Με ποιους τρόπους αυτά μπορούν να παραβιαστούν ή να υποκλαπούν;
2. Σε τι βαθμό το δείγμα θεωρεί ότι τα προσωπικά του δεδομένα είναι ασφαλή στο διαδίκτυο;
3. Σε τι βαθμό το δείγμα γνωρίζει για την παραβίαση των πνευματικών δικαιωμάτων ή και γενικότερα για παράνομες πράξεις στο διαδίκτυο; Που απευθύνεται σε περίπτωση παραβίασης;
4. Το φύλο και το έτος σπουδών των μελλοντικών εκπαιδευτικών σχετίζεται με τις παραπάνω γνώσεις;

Μέθοδος

Για τη λήψη ερευνητικών δεδομένων συντάχθηκε ερωτηματολόγιο, το οποίο κλήθηκαν να απαντήσουν ανώνυμα μελλοντικοί εκπαιδευτικοί πρωτοβάθμιας εκπαίδευσης (φοιτητές του Παιδαγωγικού Τμήματος Δημοτικής Εκπαίδευσης του Πανεπιστημίου Πατρών) από όλα τα έτη σπουδών. Το ερωτηματολόγιο συνίστατο από τρία μέρη.

Το πρώτο μέρος περιείχε τέσσερες (4) ερωτήσεις που αφορούσαν στο φύλο, το έτος σπουδών, την συχνότητα πλοήγησης στο διαδίκτυο και τους λόγους για τους οποίους χρησιμοποιούν το διαδίκτυο.

Στο δεύτερο μέρος υπήρχαν δώδεκα (12) ερωτήσεις για την ανίχνευση των γνώσεων των συμμετεχόντων για τα cookies, τα προσωπικά και ευαίσθητα προσωπικά δεδομένα, την ασφάλεια και παραβίαση των προσωπικών δεδομένων, τρόπους υποκλοπής προσωπικών δεδομένων, την πολιτική και όρους χρήσης δικτυακών τόπων, στοιχεία κατά την εγγραφή σε ένα δικτυακό τόπο, το Γενικό Κανονισμό Προστασίας Δεδομένων. Από τις ερωτήσεις αυτές οι 4 ήταν ανοικτού τύπου, οι 3 κλειστού τύπου πολλαπλών επιλογών και οι 6 κλειστού τύπου με απαντήσεις σε κλίμακα Likert (2 ερωτήσεις), με απαντήσεις σε κλίμακα τύπου Likert (2 ερωτήσεις) και διχοτομικές (Ναι - Όχι, 2 ερωτήσεις). Οι διχοτομικές ερωτήσεις ζητούσαν περαιτέρω πληροφορία στην περίπτωση της θετικής απάντησης (ανοικτού τύπου).

Στο τρίτο μέρος υπήρχαν τρεις (3) ερωτήσεις κλειστού τύπου για την ανίχνευση των γνώσεων των συμμετεχόντων για την παραβίαση των πνευματικών δικαιωμάτων στο διαδίκτυο, τις παράνομες ενέργειες στο διαδίκτυο και τους φορείς στους οποίους μπορούν να απευθυνθούν οι παθόντες, για καταγγελία και προστασία.

Ο απαιτούμενος χρόνος για τη συμπλήρωση του ερωτηματολογίου, κάτι που έγινε οικειοθελώς από το δείγμα, ήταν περίπου 15 λεπτά.

Η δειγματοληψία ήταν βολική (Cohen et al., 2007). Το ερωτηματολόγιο ελέγχθηκε ως προς την εγκυρότητα και την αξιοπιστία του (Rovinnelli & Hambleton, 1977; Παναγιωτακόπουλος & Σαρρής, 2016). Η σύνταξη των ερωτήσεων βασίστηκε στην ελληνική και διεθνή βιβλιογραφία. Μετά την αρχική του σύνταξη ελέγχθηκε και διορθώθηκε από δύο (2) ειδικούς

σε θέματα ΤΠΕ και ΤΠΕ στην εκπαίδευση. Τέλος, πριν την τελική διανομή, έγινε πιλοτική χρήση του σε 5 φοιτητές του Τμήματος από την οποία ελήφθησαν παρατηρήσεις και έγιναν οι τελικές διορθώσεις.

Μετά τη συλλογή και την κωδικοποίηση των δεδομένων ακολούθησε περιγραφική και επαγωγική στατιστική ανάλυση τους. Οι απαντήσεις των ανοικτού τύπου ερωτήσεων κατηγοριοποιήθηκαν και κωδικοποιήθηκαν με βάση το περιεχόμενό τους. Επίσης, όλες οι ερωτήσεις του 2^{ου} και 3^{ου} μέρους του ερωτηματολογίου κατηγοριοποιήθηκαν και κωδικοποιήθηκαν ως προς την ορθότητα και την πληρότητα των απαντήσεων. Οι ανοικτού τύπου ερωτήσεις κωδικοποιήθηκαν στην κλίμακα: 0-καμία απάντηση, 1-λανθασμένη απάντηση, 2-λανθασμένη απάντηση/συνηθισμένη παρανόηση, 3-ορθή απάντηση χωρίς αιτιολόγηση και 4-ορθή απάντηση με αιτιολόγηση. Οι κλειστού τύπου ερωτήσεις κωδικοποιήθηκαν στην κλίμακα: 0-λανθασμένη απάντηση, 1-μερικώς ορθή απάντηση και 2-ορθή απάντηση (μερικώς ορθή απάντηση θεωρείται η απάντηση όταν σε αυτή περιλαμβάνεται τουλάχιστον 1 σωστή επιλογή).

Χρησιμοποιήθηκαν ο στατιστικός έλεγχος καλής προσαρμογής χ^2 (Chi square goodness-of-fit test) και ο έλεγχος ανεξαρτησίας χ^2 (Chi square test of independence) για την ανίχνευση στατιστικά σημαντικών διαφορών στις απαντήσεις του δείγματος και ανάμεσα στις υποομάδες του δείγματος. Κατά την ανάλυση των αποτελεσμάτων χρησιμοποιήθηκε ως βάση το επίπεδο σημαντικότητας $\alpha=0,05$.

Ευρήματα, ανάλυση και συζήτηση

Από τα 201 ερωτηματολόγια που διανεμήθηκαν, τα 180 απαντήθηκαν από φοιτήτριες (γυναίκες) και τα 21 από φοιτητές (άνδρες). Στην έρευνα συμμετείχαν 46 φοιτητές από το 1^ο έτος σπουδών, 45 από το 2^ο έτος, 47 από το 3^ο έτος και 63 από το 4^ο ή μεγαλύτερο έτος σπουδών. Το 79,1% του δείγματος δήλωσε πως χρησιμοποιεί το διαδίκτυο περισσότερες από μια φορές την ημέρα για διάφορα θέματα, ενώ ένα πολύ μικρό ποσοστό (0,5%) μια φορά την εβδομάδα.

Εκ των 201 συμμετεχόντων, 190 (94,5%) δήλωσαν πως χρησιμοποιούν το διαδίκτυο για ψυχαγωγία, 162 (80,6%) για ενημέρωση, 153 (76,1%) για την αναζήτηση πηγών και συγγραφή εργασιών, 31 (15,4%) για επαγγελματική χρήση και 4 (2%) για άλλη χρήση.

Στην ερώτηση 5: «Τι πιστεύετε πως είναι τα cookies;», η κατηγοριοποίηση των απαντήσεων έδωσε τα ακόλουθα: 68 (33,8%) εκ των ερωτηθέντων απάντησαν λανθασμένα, 62 (30,8%) έδωσαν απαντήσεις και πάλι λανθασμένες συνδεδεμένες όμως με συνηθισμένη παρανόηση (π.χ. τα Cookies παρακολουθούν τις κινήσεις των χρηστών), 58 (28,9%) δεν έδωσαν καμία απάντηση, ενώ μόνο 13 (6,5%) έδωσαν ορθή απάντηση, ότι τα Cookies είναι μικρά αρχεία που αποθηκεύονται στον υπολογιστή κατά την επίσκεψη ενός δικτυακού τόπου ώστε σε επόμενη επίσκεψη στον ίδιο δικτυακό τόπο οι πληροφορίες να είναι, κατά το δυνατό, προσωποποιημένες (Πίνακας 1). Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=37,8$; $df=3$; $p<0,001$).

Πίνακας 1. Η ταξινόμηση των απαντήσεων στην ερώτηση για τα Cookies

Απαντήσεις	Συχνότητα	Ποσοστό %
Ορθή απάντηση με αιτιολόγηση	13	6,5
Λανθασμένη απάντηση	68	33,8
Λανθασμένη απάντηση/ συνηθισμένη παρανόηση	62	30,8
Καμία απάντηση	58	28,9

Περαιτέρω ανάλυση των απαντήσεων έδειξε ότι 98 (48,9%) εκ των ερωτηθέντων θεωρούν ότι τα cookies συνδέονται με δεδομένα (ασφάλεια δεδομένων, έλεγχος δεδομένων, συλλογή

δεδομένων, πρόσβαση στα δεδομένα, αποθήκευση ιστοσελίδων μέσω των δεδομένων και διαφημίσεις που προκύπτουν ύστερα από την αποθήκευση των δεδομένων), 53 (26,5%) εξ αυτών θεωρούν ότι συνδέονται με διάφορες λειτουργίες (όπως με ιούς, με καλύτερη πλοήγηση και με διευκόλυνση της πλοήγησης, με επιβράδυνση της λειτουργίας του υπολογιστή ή με κάποιο λογισμικό). Χαρακτηριστικές απαντήσεις: «... με την εμφάνισή τους μπορεί να κολλήσει ο υπολογιστής κάποιον ιό που θα είναι επιβλαβής και θα επιφέρει πολλά προβλήματα...», «...να επιβαρυνθεί/να καλυτερεύσει η πλοήγηση...», «...είναι μικρά αρχεία που αποθηκεύονται κατά τη διάρκεια μιας πλοήγησης στον υπολογιστή με σκοπό όταν επισκεφθεί ξανά τις ίδιες ιστοσελίδες κάποιος να του εμφανίσει σχετικά με αυτές πράγματα», «...είναι κάποιο λογισμικό παρόμοιο με αυτά που διαθέτει ο υπολογιστής...». Επίσης, 29 (14,6%) συνέδεσαν τις απαντήσεις τους με μηνύματα, με ρυθμίσεις του υπολογιστή και με όρους χρήσης και πολιτικής της επίσκεψης σε ιστοσελίδες, ενώ 49 από αυτούς (24,4%) φαίνεται να μη γνωρίζουν καθόλου τι είναι τα cookies. Τέλος, όπως αναφέρθηκε και πιο πάνω, 58 εξ αυτών (28,9%) δεν απάντησαν στην ερώτηση.

Στην ερώτηση 6: «Όταν κάνετε πλοήγηση σε μία ιστοσελίδα, αποδέχεστε τα cookies ή όχι και γιατί;», οι απαντήσεις έχουν ως εξής: 123 (61,2%) εκ των ερωτηθέντων απάντησαν ότι τα αποδέχονται με διάφορες αιτιολογίες (π.χ. «παρέχουν προστασία...», «σελίδες που εμπιστεύομαι...», «σελίδες που με ενδιαφέρουν...», «για να εμφανιστεί όλο το περιεχόμενο της σελίδας...», κ.ά.). Από τους παραπάνω, οι 37 (18,4%) δεν αιτιολόγησαν γιατί αποδέχονται τα cookies. Σε αντίθεση, 78 (38,8%) δεν αποδέχονται τα cookies με διάφορες αιτιολογίες (π.χ. επειδή «...δεν γνωρίζω τι κάνουν...», «...με την αλοδοχή τους έχουν πρόσβαση στα προσωπικά δεδομένα των χρηστών με σκοπό την υποκλοπή τους...», «...μπορεί να είναι κάποιος ιός...», κ.ά.).

Στην ερώτηση 7: «Ποιο/ποια από τα: ονοματεπώνυμο, αριθμός τηλεφώνου, μορφωτικά χαρακτηριστικά, κατοικίδιο ζώο, κωδικοί, email, φωτογραφίες, ρούχα, ηλικία, θεωρείτε πως είναι προσωπικά δεδομένα;», η κατηγοριοποίηση των απαντήσεων έδωσε τα εξής: 187 (93%) απάντησαν μερικώς ορθά (δηλ. στις απαντήσεις τους είχαν 1 τουλάχιστον σωστή επιλογή), 9 (4,5%) εκ των ερωτηθέντων απάντησαν λανθασμένα ενώ μόνο 5 (2,5%) απάντησαν ορθά. Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=322,5$; $df=2$; $p<0,001$). Αναλυτικά, οι απαντήσεις φαίνονται στον επόμενο πίνακα (Πίνακας 2).

Πίνακας 2. Οι απαντήσεις στην ερώτηση περί προσωπικών δεδομένων

Απαντήσεις	Συχνότητα	Ποσοστό (%)
Αριθμός τηλεφώνου	192	95,5
Κωδικοί πρόσβασης σε ιστοσελίδες/πлатφόρμες/κοινωνικά δίκτυα	186	92,5
Φωτογραφίες	169	84,1
Ηλεκτρονική διεύθυνση - e-mail	151	75,1
Ονοματεπώνυμο	146	72,6
Ηλικία	103	51,2
Μορφωτικά χαρακτηριστικά	53	26,4
Κατοικίδιο ζώο	13	6,5
Ρούχα	13	6,5

Κάτι που πρέπει να σημειωθεί, είναι η εσφαλμένη θεώρηση 13 (6,5%) συμμετεχόντων για το κατοικίδιο ζώο και 13 (6,5%) για τα ρούχα, τα οποία (λανθασμένα) συμπεριέλαβαν μεταξύ των προσωπικών δεδομένων.

Στην ερώτηση 8: «Ποιο/α από τα: υγεία, αθλητική ομάδα, συμμετοχή σε ενώσεις, καφετέρια που συχνάζω, μέσα μαζικής μεταφοράς που χρησιμοποιώ, σεξουαλικές συνήθειες και προτιμήσεις, συνδικαλιστική δράση, θεωρείτε ότι είναι ενδίαστοιτα προσωπικά δεδομένα;», οι απαντήσεις έχουν ως ακολούθως: 173 (86,1%) από τους συμμετέχοντες υπέδειξαν τις σεξουαλικές συνήθειες και

προτιμήσεις, 143 (71,1%) την *υγεία* και 74 (36,8%) τη *συνδικαλιστική δράση*. Ουσιαστικά, 113 (56,2%) απάντησαν ορθά, 76 (37,8%) εκ των ερωτηθέντων απάντησαν μερικώς ορθά ενώ 12 (6%) εξ αυτών απάντησαν καθολικά λανθασμένα (Πίνακας 3). Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=77,9$; $df=2$; $p<0,001$).

Πίνακας 3. Η ταξινόμηση των απαντήσεων στην ερώτηση για τα ευαίσθητα προσωπικά δεδομένα

Απαντήσεις	Συχνότητα	Ποσοστό %
Ορθή απάντηση	113	56,2
Μερικώς ορθή απάντηση	76	37,8
Λανθασμένη απάντηση	12	6,0

Στην ερώτηση 9: «Όταν κάνετε πλοήγηση, θεωρείτε ότι τα προσωπικά σας δεδομένα είναι ασφαλή;», η κατηγοριοποίηση των απαντήσεων έδωσε τα εξής: 83 (41,3%) εκ των ερωτηθέντων απάντησαν *μπορεί να είναι ασφαλή αλλά μπορεί και όχι* ενώ 104 (51,7%) θεωρούν ότι τα δεδομένα τους *δεν είναι ασφαλή ή δεν είναι καθόλου ασφαλή*. Μόνον 14 ερωτηθέντες (7,0%) θεωρούν ότι κατά τη διάρκεια μιας πλοήγησης τα δεδομένα *διατηρούνται ασφαλή ή απολύτως ασφαλή* (Πίνακας 4). Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2= 122,5$; $df=4$; $p<0,001$).

Πίνακας 4. Οι απαντήσεις στην ερώτηση για την ασφάλεια των δεδομένων στο διαδίκτυο

Απαντήσεις	Συχνότητα	Ποσοστό %
Δεν είναι καθόλου ασφαλή	35	17,4
Δεν είναι ασφαλή	69	34,3
Άλλοτε ναι άλλοτε όχι	83	41,3
Είναι ασφαλή	11	5,5
Είναι απολύτως ασφαλή	3	1,5

Στην ερώτηση 10: «Θεωρείτε ότι γίνεται υποκλοπή προσωπικών δεδομένων όταν συνδέεστε στο διαδίκτυο;», η κατηγοριοποίηση των απαντήσεων έδωσε τα εξής: 55 (27,4%) εξ αυτών απάντησαν καταφατικά, 101 (50,2%) απάντησαν ότι κατά τη διάρκεια μια πλοήγησης μπορεί να γίνει υποκλοπή/παραβίαση των δεδομένων αλλά κάτω από κάποιες προϋποθέσεις (π.χ. «...Δε σημαίνει ότι κάθε φορά που θα συνδέεται κανείς, θα τον παραβιάζουν παράλληλα εκτός κι αν υπάρχει κάποιος συγκεκριμένος λόγος ή έχει κάτι πολύτιμο...»). Δεν γνωρίζουν τι ακριβώς συμβαίνει 39 (19,4%), ενώ 6 (3%) φαίνονται να νιώθουν ασφαλείς στο διαδίκτυο, δηλώνοντας ότι *δεν μπορεί να γίνει παραβίαση των δεδομένων όταν συνδέονται στο διαδίκτυο*. Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2= 93,2$; $df= 3$; $p<0,001$).

Στην ερώτηση 11: «Ένας από τους χρησιμοποιούμενους τρόπους για την υποκλοπή των δεδομένων είναι το WebCam Hacking. Γνωρίζετε τι είναι; Αν ναι, γράψτε...», οι απαντήσεις έχουν ως εξής: 125 εκ των ερωτηθέντων (62,2%) δεν έδωσαν καμία απάντηση, μη γνωρίζοντας κάτι σχετικό, 70 (34,8%) απάντησαν αιτιολογώντας ορθά ότι πρόκειται για πρόσβαση στην κάμερα του ηλεκτρονικού υπολογιστή για υποκλοπή στοιχείων, λήψη βίντεο ή και φωτογραφιών με σκοπό την παραβίαση της ιδιωτικής ζωής και τον εκβιασμό, 6 ερωτηθέντες (3%) έδωσαν λάθος απάντηση θεωρώντας πως το WebCam Hacking είναι είδος κάμερας που χρησιμοποιείται διαδικτυακά ή έλεγχος προτιμήσεων κατά τη διάρκεια μιας βιντεοκλήσης ή λογισμικό παρακολούθησης σε εφαρμογές τύπου

Skype. Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=114,0$; $df=2$; $p<0,01$).

Στην ερώτηση 12: «*Το Phishing είναι μια μέθοδος για την υποκλοπή προσωπικών δεδομένων. Γνωρίζετε τι ακριβώς είναι; Αν ναι, γράψτε...*») οι απαντήσεις έχουν ως εξής: 195 (97%) συμμετέχοντες δεν γνώριζαν τι είναι και πώς λειτουργεί το Phishing. Μόνο 6 (3%) έγραψαν ότι πρόκειται για υποκλοπή δεδομένων μέσω διαφημίσεων, πλαστών ιστοσελίδων ή παρασιληθτικών e-mails. Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=177,7$; $df=1$; $p<0,001$). Από τις 6 ορθές απαντήσεις, μία μόνο ήταν πλήρως εμπεριστατωμένη (...*e-mails που στέλνονται και μπορεί να περιλαμβάνουν διάφορα links, τα οποία παρασύρουν τον χρήστη, εισβάλλουν στα προσωπικά δεδομένα του και τα χρησιμοποιούν για διάφορους σκοπούς με διάφορους τρόπους*).

Στην ερώτηση 13: «*Όταν κάνετε εγγραφή σε ένα κοινωνικό δίκτυο ή κάνετε πλοήγηση σε μία ιστοσελίδα, διαβάζετε την πολιτική και τους όρους χρήσης;*», οι απαντήσεις έχουν ως εξής: μόνο 14 εκ των ερωτηθέντων (7%) απάντησαν πως τα διαβάζουν κάθε φορά για να είναι ενημερωμένοι και να γνωρίζουν τι θα συμβεί σε περιπτώσεις κινδύνου, ενώ 36 (17,9%) τα διαβάζουν μερικές φορές. Επίσης, 79 (39,3%) ανέφεραν ότι δεν τα διαβάζουν ποτέ αλλά παρόλα αυτά κάνουν αποδοχή και 72 (35,8%) τα διαβάζουν σπάνια. Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=56$; $df=3$; $p<0,001$). Συνεπώς, όπως φαίνεται από τις απαντήσεις τους, το μεγαλύτερο ποσοστό (75,1%) των ερωτηθέντων δεν ασχολείται σχεδόν καθόλου με τους όρους και την πολιτική.

Στην ερώτηση 14: «*Όταν κάνετε εγγραφή σε ένα κοινωνικό δίκτυο, τι στοιχεία δίνετε;*», οι απαντήσεις έχουν ως ακολούθως: 183 εξ αυτών (91%) απάντησαν ότι δίνουν το ονοματεπώνυμο και 165 (82,1%) το email τους, τα οποία είναι τα δύο βασικά στοιχεία που ζητούνται κατά την εγγραφή. Επίσης, 119 (59,2%) δίνουν την ηλικία τους, 41 (20,4%) τον αριθμό του κινητού τηλεφώνου τους, 27 (13,4%) την επαγγελματική τους κατάσταση, 15 (7,5%) τον τόπο της κατοικίας τους, 5 (2,5%) την οικογενειακή τους κατάσταση, 3 (1,5%) τα πολιτικά/θρησκευτικά ενδιαφέροντα και 1 (0,5%) τον τραπεζικό λογαριασμό.

Στην ερώτηση 15: «*Θεωρείτε πως από τη στιγμή που δίνετε τα στοιχεία σας γίνονται συγχρόνως ευάλωτα;*», η ανάλυση έδωσε τα ακόλουθα: 31 εκ των ερωτηθέντων (15,4%) συμφωνούν απολύτως, ενώ 89 (44,3%) συμφωνούν ότι τα στοιχεία που δίνουν σε μία ιστοσελίδα ή σε κάποιο κοινωνικό δίκτυο γίνονται ευάλωτα. Όμως, 69 ερωτηθέντες (34,3%) δεν φαίνεται ούτε να συμφωνεί, ούτε να διαφωνεί γιατί δε γνωρίζει τι συμβαίνει πραγματικά. Τέλος, 12 (6%) εκ των ερωτηθέντων απάντησαν ότι τα στοιχεία που δίνουν δεν νομίζουν ότι γίνονται ευάλωτα. Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=73,4$; $df=3$; $p<0,001$). Η ανάλυση των απαντήσεων στην ερώτηση 16: «*Από τι θεωρείτε ότι μας προστατεύει ο Γενικός Κανονισμός Προστασίας Δεδομένων;*», φαίνεται στον επόμενο πίνακα (Πίνακας 5).

Πίνακας 5. Οι απαντήσεις στην ερώτηση για τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)

Απαντήσεις	Συχνότητα	Ποσοστό (%)
Από τους hackers	5	2,5
Από διαρροή προσωπικών δεδομένων	38	18,9
Από υποκλοπή προσωπικών δεδομένων	94	46,8
Από τους ιούς	2	1,0
Από τίποτα	10	5,0
Δεν ξέρω	31	15,4
Καμία απάντηση	66	32,8

Παρατηρώντας τον παραπάνω πίνακα, αξίζει να σημειωθεί ότι πολλοί από τους ερωτηθέντες φαίνεται να μη γνωρίζουν κάτι για τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και το χώρο αναφοράς του.

Στην ερώτηση 17 «Ποια από τα παρακάτω θεωρείται ότι είναι παραβίαση πνευματικών δικαιωμάτων στο διαδίκτυο;» οι απαντήσεις φαίνονται στον επόμενο πίνακα (Πίνακας 6):

Πίνακας 6. Η ταξινόμηση των απαντήσεων στην ερώτηση για τα πνευματικά δικαιώματα

Απαντήσεις	Συχνότητα	Ποσοστό (%)
Διακίνηση κειμένων εργασιών	125	62,2
Ανάρτηση φωτογραφιών	122	60,7
Διακίνηση ταινιών	116	57,7
Διακίνηση αρχείων ήχου mp3	94	46,8
Διαμοίραση λογισμικού	85	42,3
Διακίνηση απόψεων για διάφορα θέματα	48	23,9

Από τα παραπάνω δεδομένα φαίνεται ότι λανθασμένα οι ερωτηθέντες θεώρησαν ότι η ανάρτηση φωτογραφιών (60,7%) και η διακίνηση απόψεων για διάφορα θέματα (23,9%) εμπλέκονται σε θέματα παραβίασης των πνευματικών δικαιωμάτων. Αντίθετα, τουλάχιστον η διακίνηση ταινιών θα περίμενε κανείς να απηχεί τις απόψεις όλων των ερωτηθέντων. Κατηγοριοποιώντας περαιτέρω τις απαντήσεις φάνηκε ότι ορθή απάντηση έδωσαν 66 (32,8%), μερικώς ορθή 92 (45,8%), ενώ εσφαλμένη 43 (21,4%). Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=17,9$; $df=2$; $p<0,001$)

Στην ερώτηση 18: «Τι θεωρείτε παράνομο στο διαδίκτυο από τα παρακάτω;», οι απαντήσεις φαίνονται στον επόμενο πίνακα (Πίνακας 7).

Πίνακας 7. Η ταξινόμηση των απαντήσεων στην ερώτηση για παράνομες πράξεις στο διαδίκτυο

Απαντήσεις	Συχνότητα	Ποσοστό (%)
Τρομοκρατία	190	94,5
Πορνογραφία	180	89,6
Ηλεκτρονικά casino	114	56,7
Αποστολή/λήψη αρχείων μουσικής	63	31,3
Ηλεκτρονικά παιχνίδια	18	9,0
Χρήση κοινωνικών δικτύων	9	4,5

Οι απαντήσεις των ερωτηθέντων φαίνεται ότι σε μεγάλο βαθμό δεν είναι ορθές αναφορικά με τα ηλεκτρονικά casino (56,7%), τα ηλεκτρονικά παιχνίδια (9,0%) και τη χρήση κοινωνικών δικτύων (4,5%). Κατηγοριοποιώντας περαιτέρω τις απαντήσεις φάνηκε ότι ορθή απάντηση έδωσαν 82 (40,8%) συμμετέχοντες, μερικώς ορθή 115 (57,2%), ενώ εσφαλμένη 4 (2,0%). Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=96,9$; $df=2$; $p<0,001$).

Στην ερώτηση 19: «Αν συμβεί κάτι που εσείς θεωρείτε ότι είναι παράνομο στο διαδίκτυο, που πιστεύετε ότι πρέπει να απευθυνθείτε;», η ανάλυση έδωσε τα ακόλουθα: 184 (91,5%) απάντησαν (ορθά) στη Δίωξη Ηλεκτρονικού Εγκλήματος, 69 (34,3%) απάντησαν (ορθά) στη Safeline (ανοιχτή

ελληνική γραμμή για τις παράνομες ηλεκτρονικές ενέργειες), 42 (20,9) απάντησαν (λανθασμένα) στο Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης, 5 (2,5%) δήλωσαν ότι δεν αποτελεί δική τους υποχρέωση και 9 (4,5%) δήλωσαν ότι δεν γνωρίζουν πού να απευθυνθούν. Κατηγοριοποιώντας περαιτέρω τις απαντήσεις φάνηκε ότι απολύτως ορθή απάντηση έδωσαν 145 (72,1%) εκ των συμμετεχόντων, μερικώς ορθή 45 (22,4%), ενώ απολύτως εσφαλμένη 11 (5,5%). Οι παρατηρούμενες διαφορές στις απαντήσεις σύμφωνα με τον έλεγχο καλής προσαρμογής χ^2 είναι στατιστικά σημαντικές ($\chi^2=144,8$; $df=2$; $p<0,001$).

Ο έλεγχος ανεξαρτησίας χ^2 (Chi square test of independence) χρησιμοποιήθηκε για την ανίχνευση στατιστικά σημαντικών διαφορών στις απαντήσεις των ερωτηθέντων ανάλογα με το φύλο και το έτος φοίτησής τους. Από τις αναλύσεις σε όλες τις ερωτήσεις προέκυψε ότι:

- Το φύλο δεν φαίνεται να επιδρά στις απαντήσεις των συμμετεχόντων αφού δεν ανιχνεύθηκαν στατιστικά σημαντικές διαφορές στις απαντήσεις όλων των ερωτήσεων ανάμεσα σε φοιτητές και φοιτήτριες ($p>0,05$).
- Το έτος φοίτησης φάνηκε να επιδρά μόνο στην αναγνώριση των ευαίσθητων προσωπικών δεδομένων ($\chi^2=16,41$; $df=8$; $p<0,05$) και στις γνώσεις σχετικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) ($\chi^2=22,23$; $df=8$; $p<0,05$). Και στα δύο αυτά ζητήματα τόσο οι φοιτητές του Α' έτους όσο και οι φοιτητές του Γ' έτους φαίνεται να έχουν περισσότερες γνώσεις από τους υπολοίπους που συμμετείχαν στην έρευνα. Αυτό μπορεί να δικαιολογηθεί από την παρακολούθηση ενός υποχρεωτικού μαθήματος που εστιάζει στη λειτουργία και στη χρήση του διαδικτύου και ενός επιλογής αντίστοιχα, το οποίο εστιάζει στις επιδράσεις από τη χρήση του διαδικτύου.

Συμπεράσματα

Στην εργασία αυτή έγινε προσπάθεια να διερευνηθεί η γνώση μελλοντικών εκπαιδευτικών Πρωτοβάθμιας Εκπαίδευσης για θέματα σχετικά με την ασφάλεια και την παραβίαση των προσωπικών δεδομένων στο διαδίκτυο. Η έρευνα εστίασε σε απαντήσεις που αφορούν στις γνώσεις τους σχετικά με τα προσωπικά δεδομένα, στους τρόπους παραβίασης των προσωπικών δεδομένων, στην ασφάλεια των προσωπικών δεδομένων καθώς και να ανιχνεύσει την σχέση που μπορεί οι γνώσεις αυτές να έχουν με το φύλο και το έτος σπουδών τους.

Από την ανάλυση των δεδομένων που συλλέχθηκαν, προέκυψαν απαντήσεις στα ερευνητικά ερωτήματα, οι οποίες παρατίθενται συνοπτικά πιο κάτω.

Σε σχέση με το πρώτο ερευνητικό ερώτημα («Σε τι βαθμό το δείγμα γνωρίζει τι και ποια είναι τα προσωπικά δεδομένα; Με ποιους τρόπους αυτά παραβιάζονται ή υποκλέπτονται;») τα αποτελέσματα έδειξαν ότι:

- Ένα πολύ μικρό ποσοστό (2,5%) μπορεί να αναγνωρίσει τα προσωπικά δεδομένα ενώ η μεγάλη πλειοψηφία (93,0%) αναγνώρισε μερικά μόνο από αυτά. Ένα μεγάλο ποσοστό των ερωτηθέντων (56,2%) αναγνώρισε ορθά τα ευαίσθητα προσωπικά δεδομένα και ένα μικρότερο (37,8%) μερικά από αυτά. Ένας μικρός αριθμός εκ των ερωτηθέντων και στις δύο περιπτώσεις, έδωσε εντελώς λανθασμένες απαντήσεις.
- Ένα πολύ μεγάλο ποσοστό (62,2%) δεν γνωρίζει καθόλου ή γνωρίζει λανθασμένα (3%) τι είναι ακριβώς το *WebCam Hacking*. Εξαιρετικά μεγάλο μέρος του δείγματος (97%) δεν γνωρίζει τι είναι η μέθοδος υποκλοπής δεδομένων *Phishing* και πολύ μεγάλο μέρος (75,1%) των ερωτηθέντων δεν ασχολείται σχεδόν καθόλου με τους όρους και την πολιτική όταν εγγράφεται σε έναν ιστοχώρο. Μάλιστα, κατά την εγγραφή τους σε κοινωνικά δίκτυα ένα μικρό ποσοστό δίνει (χωρίς όπως φαίνεται να προβληματίζεται) κάποια προσωπικά δεδομένα αλλά και κάποια ευαίσθητα προσωπικά δεδομένα. Μόνο

το 7% του δείγματος φαίνεται να διαβάζει την πολιτική και τους όρους χρήσης όταν κάνει εγγραφή σε ένα κοινωνικό δίκτυο ή πλοηγείται σε μία ιστοσελίδα.

Αναφορικά με το δεύτερο ερευνητικό ερώτημα («Σε τι βαθμό το δείγμα θεωρεί ότι τα προσωπικά του δεδομένα είναι ασφαλή στο διαδίκτυο;») τα αποτελέσματα έδειξαν ότι:

- Ένα μεγάλο ποσοστό (51,7%) εκ των ερωτηθέντων θεωρεί ότι τα προσωπικά δεδομένα του δεν είναι ασφαλή κατά την πλοήγησή του στο διαδίκτυο, ενώ μόνο το 7% θεωρεί το αντίθετο. Το 59,7% των ερωτηθέντων θεωρεί ότι τα δεδομένα που καταθέτει κατά την εγγραφή του σε έναν ιστοχώρο είναι ευάλωτα, ενώ ένα πολύ μικρό ποσοστό (6%) θεωρεί πως αυτά τα στοιχεία είναι ασφαλή.
- Είναι χαρακτηριστικό, ότι μόνο ένα μικρό ποσοστό του δείγματος (6,5%) γνωρίζει ορθά τι ακριβώς είναι και τι ακριβώς κάνουν τα Cookies.

Σε σχέση με το τρίτο ερευνητικό ερώτημα («Σε τι βαθμό το δείγμα γνωρίζει για την παραβίαση των πνευματικών δικαιωμάτων ή και γενικότερα για παράνομες πράξεις στο διαδίκτυο; Που απευθύνεται σε περίπτωση παραβίασης;»), τα αποτελέσματα έδειξαν ότι:

- Περισσότεροι από τους μισούς εκ των ερωτηθέντων (55,2%) έδειξαν να γνωρίζουν από τι μας προστατεύει ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), αλλά ένα μεγάλο επίσης ποσοστό δεν γνωρίζει ακριβώς και πλήρως τις ενέργειες που παραβιάζουν την πνευματική ιδιοκτησία στο διαδίκτυο. Πιο συγκεκριμένα, μόνο το 32,8% αναγνωρίζει πλήρως τις παραβιάσεις της, ενώ 45,8% μερικώς και 21,4% αγνοεί παντελώς το θέμα αυτό.
- Πλήρη επίγνωση για το ποια πράξη θεωρείται παράνομη στο διαδίκτυο φάνηκε να έχει η πλειοψηφία του δείγματος (72,1%).
- Ένα μεγάλο ποσοστό εκ των συμμετεχόντων στην έρευνα (72,1%) αναγνώρισε ορθά όλους τους φορείς στους οποίους μπορούν να απευθυνθεί για να καταγγείλει παράνομες ενέργειες στο διαδίκτυο, ενώ ένα μικρό μόνο ποσοστό (5,5%) δεν αναγνώρισε ορθά κανένα φορέα.

Αναφορικά με το τέταρτο ερευνητικό ερώτημα («Το φύλο και το έτος σπουδών των μελλοντικών εκπαιδευτικών σχετίζεται με τις παραπάνω γνώσεις;») τα αποτελέσματα έδειξαν ότι:

- Το φύλο δεν φαίνεται να επιδρά στις απαντήσεις των συμμετεχόντων αφού δεν ανιχνεύθηκαν στατιστικά σημαντικές διαφορές στις απαντήσεις μεταξύ ανδρών και γυναικών.
- Το έτος φοίτησης φάνηκε να επιδρά μόνο στην αναγνώριση των ευαίσθητων προσωπικών δεδομένων και στις γνώσεις σχετικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Οι φοιτητές του Α' και του Γ' έτους φαίνεται να έχουν περισσότερες γνώσεις πάνω στα δύο αυτά θέματα, γεγονός που μάλλον ερμηνεύεται από την παρακολούθηση σχετικών μαθημάτων (ενός υποχρεωτικού το οποίο εστιάζει στη λειτουργία και στις εξυπηρετήσεις του διαδικτύου και ενός επιλογής, το οποίο εστιάζει στις επιδράσεις από τη χρήση του διαδικτύου, αντίστοιχα).

Τα προηγούμενα ευρήματα δείχνουν ασφαλώς ότι οι συμμετέχοντες στην έρευνα, ως υποψήφιοι εκπαιδευτικοί, χρειάζονται περισσότερη κατάρτιση σε θέματα που αφορούν τη χρήση του διαδικτύου. Ωστόσο, λόγω του τρόπου δειγματοληψίας, η οποία χαρακτηρίζεται ως βολική, τα αποτελέσματα είναι ενδεικτικά και δεν επιδέχονται γενίκευσης. Όμως, δείχνουν την κατάσταση για το συγκεκριμένο δείγμα κατά τη συγκεκριμένη συγκυρία και μπορούν να αποτελέσουν βάση για περαιτέρω μελέτη παρομοίων θεμάτων, σχετικών με γνώσεις και συμπεριφορές μελλοντικών εκπαιδευτικών ή εν ενεργεία εκπαιδευτικών που αφορούν την διαπαιδαγώγηση για την ασφάλεια των νέων στο διαδίκτυο.

Όπως φαίνεται μέσα από τις έρευνες σε διεθνές επίπεδο, ο ρόλος του σχολείου (εκτός από αυτόν της οικογένειας) είναι πάρα πολύ σημαντικός στη διαμόρφωση των αυριανών

ψηφιακών πολιτών και μέσα σε αυτόν, ο ρόλος των εκπαιδευτικών μπορεί να είναι καθοριστικός για την παροχή βοήθειας, υποστήριξης και ενημέρωσης σε παιδιά, εφήβους και γονείς για τους κινδύνους του δικτύου (Ασφάλεια στο διαδίκτυο, χ.η.).

Αναφορές

- Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education* (6th Edition). London: Routledge.
- Dunkels, E., Frånberg, G. M., & Hällgren, C. (2011). Young people and online risk. In E. Dunkels, G. Franberg, & C. Hallgren (eds), *Youth culture and net culture: online social practices* (pp. 1-16). Hershey, Pennsylvania (USA): IGI Global.
- Kurose J. F., & Ross K.W. (2004). *Δικτύωση Υπολογιστών* (μτφρ. Α. Μανιτοάρης, Π. Φουλήρας). Αθήνα: Εκδόσεις Μ. Γκιούρδας.
- LCAH Editorial (2018). Growing up in a digital world: benefits and risks. *The Lancet Child & Adolescent Health*, 2(2), 79.
- Livingstone, S., Kalmus, V., & Talves, K. (2013). Girls' and boys' experiences of online risk and safety. In C. Carter, L. Steiner, & L. McLaughlin (eds), *The Routledge Companion to Media and Gender* (pp. 190-200). London: Routledge.
- Mason, M. (2017). *The use of the internet and social media by young people*. U.K.: Youth Justice Board.
- Mateiu, M. (2017). *Spy game: the dangers of webcam hacking and how to avoid them*. AVG Technologies. Retrieved February 26, 2019, from <https://www.avg.com/en/signal/how-hackers-can-hijack-your-webcam-to-spy-on-you>
- Ramos-Soler, I., López-Sánchez, C., & Torrecillas-Lacave, T. (2018). Online risk perception in young people and its effects on digital behavior. *Comunicar. Media Education Research Journal*, 56(XXVI), 71-79.
- Rovinelli, R. J., & Hambleton, R. K. (1977). On the use of content specialists in the assessment of criterion-referenced test item validity. *Dutch Journal of Educational Research*, 2, 49-60.
- Saferinternet (n.d.). *Συχνές Ερωτήσεις. Ποιες ενέργειες είναι παράνομες στο διαδίκτυο;* Ανακτήθηκε στις 15 Απριλίου 2019 από <http://www.saferinternet.gr/index.php?parentobjId=Page72>
- Schulz, M., & Hennis - Plasschaert, J. A. (2016). Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. *Επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης*. Ανακτήθηκε στις 15 Απριλίου 2019 από <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679>
- Weiser, E. (2004). Gender Differences in Internet Use Patterns and Internet Application Preferences: A Two - Sample Comparison. *Cyber Psychology & Behavior*, 3(2), 167-178.
- Zilka, G. C. (2017). Awareness of eSafety and potential online dangers among children and teenagers. *Journal of Information Technology Education: Research*, 16, 319-338.
- Žumárová, M., Cerna, M., & Maněna, V. (2010). Young Generation and their Internet Communication. In *Proceedings of International Conference on Applied Computer Science* (pp. 313-316). Malta: Institute for Environment, Engineering and Applied Mathematics.
- Ασφάλεια στο διαδίκτυο (χ.η.). *Δράσεις για την ασφάλεια του Διαδικτύου*. Ανακτήθηκε στις 20 Απριλίου 2019 από <https://internetsafety.pi.ac.cy/parents-actions>
- Παναγιωτακόπουλος, Χ. (2013). *Οι Τεχνολογίες της Πληροφορίας και των Επικοινωνιών. Μία Συνολική Θεώρηση*. Αθήνα: Εκδόσεις ΙΩΝ.
- Παναγιωτακόπουλος, Χ. (2018). *Η ηθική στο διαδίκτυο και το ηλεκτρονικό έγκλημα*. Αθήνα: Εκδόσεις Παπαζήση.
- Παναγιωτακόπουλος, Χ., & Σαρρής, Μ. (2016). *Η συγγραφή μιας επιστημονικής εργασίας με τη χρήση των ΤΠΕ*. Αθήνα: Εκδόσεις ΙΩΝ.
- Τσιγκρης, Π. (2014). *Συμπεριφορές εξάρτησης στο διαδίκτυο. Πρόληψη μέσω προαγωγής και ανάπτυξης αλγοριθμικής σκέψης με τη χρήση ηλεκτρονικού υπολογιστή από την παιδική ηλικία (Διπλωματική Εργασία)*. ΕΚΠΑ, Αθήνα.