

Γραμματισμός σε Θέματα Ψηφιακής Ασφάλειας: Μια Ποιοτική Εμπειρική Μελέτη με Εκπαιδευτικούς Πρωτοβάθμιας Εκπαίδευσης

Γεώργιος Πανέτας, Ανθή Καρατράντου, Χρήστος Παναγιωτακόπουλος
georgios.panetas@upnet.gr, akarat@upatras.gr, cpanag@upatras.gr
Τμήμα Επιστημών της Εκπαίδευσης και Κοινωνικής Εργασίας, Πανεπιστήμιο Πατρών

Περίληψη

Οι ικανότητες στον τομέα της ψηφιακής ασφάλειας αποτελούν βασική συνιστώσα του ψηφιακού αλφαριθμητισμού για τον πολίτη του 21^{ου} αιώνα και αναδεικνύονται ως κρίσιμες για την εκπαιδευτική κοινότητα, η οποία οφείλει να δημιουργεί ένα ασφαλές ψηφιακό περιβάλλον για τους μαθητές και ταυτόχρονα να τους υποστηρίζει να καλλιεργήσουν τις ψηφιακές τους ικανότητες. Ο ψηφιακός γραμματισμός των εκπαιδευτικών, στον τομέα της ψηφιακής ασφάλειας διασφαλίζει όχι μόνο τη δική τους ασφάλεια αλλά και την ασφάλεια των μαθητών τους, ιδιαίτερα στο δημοτικό σχολείο. Σκοπός της παρούσας μελέτης ήταν η διερεύνηση των γνώσεων εκπαιδευτικών Πρωτοβάθμιας εκπαίδευσης σε θέματα ψηφιακής ασφάλειας. Στην έρευνα συμμετείχαν 20 εκπαιδευτικοί δημοτικών σχολείων. Εργαλείο της έρευνας αποτέλεσε ημιοδομημένη συνέντευξη με ερωτήσεις που αφορούσαν το επίπεδο βασικών γνώσεων στον τομέα της ψηφιακής ασφάλειας, την ενημέρωση των γονέων καθώς και τις ανάγκες υποστήριξης των εκπαιδευτικών σε θέματα ψηφιακής ασφάλειας. Τα αποτελέσματα έδειξαν ότι όλοι οι συμμετέχοντες γνωρίζουν σε ικανοποιητικό βαθμό για τους κινδύνους του διαδικτύου, θεωρούν σημαντική την ενημέρωση των γονέων για θέματα ψηφιακής ασφάλειας και ζητούν στοχευμένη επιμόρφωση σε θέματα διαχείρισης της ψηφιακής ασφάλειας στην εκπαιδευτική κοινότητα.

Λέξεις κλειδιά: εκπαιδευτικοί Πρωτοβάθμιας Εκπαίδευσης, ψηφιακές δεξιότητες, ψηφιακή ασφάλεια

Εισαγωγή

Η χρήση των ψηφιακών τεχνολογιών και του διαδικτύου σε όλους τους τομείς της ζωής μας συνοδεύεται από πληθώρα ευκαιριών, αλλά ενέχει επίσης πολλούς κινδύνους και προκλήσεις. Οι εκπαιδευτικοί διαδραματίζουν σημαντικό ρόλο στην ενδυνάμωση των μαθητών για το πώς να χρησιμοποιούν αυτές τις τεχνολογίες με ασφάλεια, ηθική και υπευθυνότητα. Τα ζητήματα που αφορούν τη χρήση των ψηφιακών τεχνολογιών από τους νέους βρίσκονται ψηλά στην ατζέντα της Ευρωπαϊκής Επιτροπής (ΕΚ), με θέματα όπως η *ψυχική υγεία*, ο *εκφοβισμός στον κυβερνοχώρο*, ο *εθισμός στη χρήση ψηφιακών εφαρμογών* και η *προστασία των νέων* να λαμβάνουν ιδιαίτερη προσοχή (Dede, 2009· Gallego-Arrufat et al., 2019· Gordillo et al., 2021).

Το Ευρωπαϊκό Πλαίσιο Ψηφιακών Ικανοτήτων για τους Πολίτες (DigComp) παρέχει μια κοινή γλώσσα για τον προσδιορισμό και την περιγραφή 5 βασικών τομέων ψηφιακών ικανοτήτων, με τη Ψηφιακή Ασφάλεια να είναι ένας από αυτούς (Carretero, et al., 2017). Η Ευρωπαϊκή Επιτροπή έχει επίσης αναπτύξει ένα κοινό πλαίσιο αναφοράς, το DigCompEdu (Digital Competence of Educators), το οποίο ορίζει και περιγράφει τις ψηφιακές ικανότητες που πρέπει να διαθέτει ένας εκπαιδευτικός προκειμένου να είναι σε θέση να αξιοποιήσει τις δυνατότητες της τεχνολογίας για να ενισχύσει, να καινοτομήσει και να αναπτύξει τον ψηφιακό γραμματισμό των μαθητών (Redecker & Punie, 2017), περιλαμβάνει έξι διαφορετικούς τομείς ικανοτήτων με συνολικά 22 ικανότητες, με θέματα ψηφιακής ασφάλειας να διατρέχουν οριζόντια τους τομείς και τις ικανότητες αυτές.

Η Ψηφιακή ασφάλεια των μαθητών αποτελεί μία από τις ερευνητικές προτεραιότητες της παιδαγωγικής των μέσων και της σχολικής πρακτικής (Gordillo, et al., 2021· Govender & Skea, 2019). Η σημασία της ψηφιακής ασφάλειας στο πλαίσιο της Πρωτοβάθμιας Εκπαίδευσης

αποκτά ιδιαίτερη σημασία όταν λαμβάνουμε υπόψη ότι οι εκπαιδευτικοί και οι γονείς είναι αυτοί που φέρουν την κύρια ευθύνη για τη διαμόρφωση συνηθειών ασφαλούς χρήσης των μέσων στους νεαρούς χρήστες. Οι εκπαιδευτικοί πρέπει να λαμβάνουν μέτρα για να διασφαλίζουν τη σωματική, ψυχολογική και κοινωνική ευημερία των μαθητών όταν χρησιμοποιούν ψηφιακές τεχνολογίες και να τους δίνουν την δυνατότητα να τις διαχειρίζονται και να τις χρησιμοποιούν με ασφάλεια και υπευθυνότητα (Reisoğlu & Çebi, 2020· Rocha et al., 2022· Sarva et al., 2022· Thuy Nguyen & Habók, 2024· Tomczyk, 2020).

Σκοπός της παρούσας έρευνας είναι να διερευνήσει το βαθμό γνώσεων εν ενεργεία εκπαιδευτικών σχολείων Πρωτοβάθμιας Εκπαίδευσης σε ζητήματα ψηφιακής ασφάλειας καθώς και να ανιχνεύσει ανάγκες υποστήριξης τους. Τα ερευνητικά ερωτήματα της παρούσας εργασίας έχουν ως ακολούθως:

- Τι γνωρίζουν οι εκπαιδευτικοί Πρωτοβάθμιας Εκπαίδευσης για τους κινδύνους του Διαδικτύου;
- Σε βαθμό ενημερώνουν τους γονείς για θέματα ψηφιακής ασφάλειας;
- Ποιες είναι οι ανάγκες υποστήριξης των εκπαιδευτικών Πρωτοβάθμιας Εκπαίδευσης σε θέματα ψηφιακής ασφάλειας;

Θεωρητικό πλαίσιο

Στην ψηφιακή εποχή σήμερα, ένα από τα σημαντικότερα μαθήματα που ένας εκπαιδευτικός μπορεί να προσφέρει στους μαθητές του είναι η σημασία της κυβερνοασφάλειας. Δεν είναι μόνο ζωτικής σημασίας για τον εκπαιδευτικό να είναι ψηφιακά ασφαλείς, αλλά έχει επίσης την ευθύνη και την ευκαιρία να καθοδηγήσει τους μαθητές του να περιηγηθούν στον διαδικτυακό κόσμο με ασφάλεια και υπευθυνότητα. Θεωρείται ότι οι ψηφιακοί ιθαγενείς (*άτομα που δεν γνωρίζουν τον κόσμο χωρίς ηλεκτρονικά μέσα*) διαθέτουν γνώσεις και δεξιότητες που τους δίνουν τη δυνατότητα να χρησιμοποιούν τα εργαλεία ΤΠΕ αβίαστα. Ωστόσο, οι ηλεκτρονικές απειλές που σχετίζονται με την ασφάλεια και αναδύονται επειδή οι νέοι στερούνται βασικών ψηφιακών δεξιοτήτων, αναγκάζουν τους ενήλικες να αναπτύξουν και να εφαρμόσουν προληπτικά μέτρα (Tomczyk, 2020). Οι έφηβοι ψηφιακοί ιθαγενείς θα πρέπει να αναπτύξουν τις ικανότητές τους στην ασφαλή χρήση των ηλεκτρονικών μέσων. Αυτό, είναι εφικτό μόνο μέσω της συνεργασίας κατάλληλα προετοιμασμένων εκπαιδευτικών (Karatrantou & Stamatelos, 2025· Thuy et al., 2024). Η διαμόρφωση στάσεων που αυξάνουν το επίπεδο ψηφιακής ασφάλειας υποστηρίζει το γενικό επίπεδο του ψηφιακού γραμματισμού, που απαιτεί μια ολιστική προσέγγιση. Πρέπει να λαμβάνει υπόψη όλους τους σημαντικούς άλλους στη διαδικασία κοινωνικοποίησης των μέσων: *εκπαιδευτικούς, γονείς* (Rocha Estrada et al., 2022) και *φορείς που παρέχουν υποστήριξη σε κρίσιμες καταστάσεις*, όπως εγκλήματα στο διαδίκτυο (π.χ. μακροχρόνιος διαδικτυακός εκφοβισμός, πειρατεία, σεξουαλική κακοποίηση, εθισμοί). Οι εκπαιδευτικοί έχουν πολλές γνώσεις σχετικά με μεθόδους για την ενίσχυση της *κριτικής σκέψης*, της *δημιουργικότητας*, της *επικοινωνίας* και των *δεξιοτήτων συνεργασίας* των μαθητών, χαρακτηριστικά που ενσωματώνουν τους νέους στη σύγχρονη κοινωνία, και μπορούν να τους βοηθήσουν να χρησιμοποιούν με ασφάλεια τα μέσα μαζικής ενημέρωσης και να συμμετέχουν στον πολιτισμό που διαμεσολαβείται από τα μέσα κοινωνικής δικτύωσης (Tomczyk, 2020). Όμως, το επίπεδο γνώσεων και δεξιοτήτων των εκπαιδευτικών στην ψηφιακή ασφάλεια εξακολουθεί να απαιτεί εκπαίδευση και κατάρτιση.

Εκτός από τα πλαίσια DigComp και DigCompEdu, η Ευρωπαϊκή Επιτροπή έχει προωθήσει διάφορες πρωτοβουλίες για την προώθηση της ανάπτυξης της ψηφιακής ικανότητας στον τομέα της εκπαίδευσης. Η ευαισθητοποίηση και πρόσβαση σε πόρους για την διαδικτυακή ασφάλεια σε όλη την σχολική κοινότητα (στελέχη, εκπαιδευτικοί, γονείς, μαθητές) είναι

υψίστης σημασίας και αποτελεί προτεραιότητα του δικτύου των Κέντρων Ασφαλούς Διαδικτύου στην Ευρώπη. Σε διεθνές επίπεδο, μια από τις πιο σχετικές πρωτοβουλίες είναι το πρόγραμμα σπουδών για τον γραμματισμό στα μέσα και την πληροφόρηση για τους εκπαιδευτικούς που αναπτύχθηκε από την UNESCO (2018), το οποίο ορίζει ένα πλαίσιο ικανοτήτων που συμπληρώνει το πλαίσιο ικανοτήτων ΤΠΕ για τους εκπαιδευτικούς που αναπτύχθηκε από τον ίδιο οργανισμό.

Παρά τις διάφορες προσπάθειες που έχουν καταβληθεί μέχρι σήμερα για την εκπαίδευση στην ψηφιακή ικανότητα, υπάρχουν ισχυρές ενδείξεις, όχι μόνο ότι οι μαθητές έχουν σήμερα ανεπαρκή ψηφιακή ικανότητα, αλλά και ότι υπάρχει ένα ανησυχητικό χάσμα μεταξύ της ψηφιακής ικανότητας που θα έπρεπε να έχουν οι εκπαιδευτικοί για να αναπτύξουν με επιτυχία την ψηφιακή ικανότητα των μαθητών τους και αυτής που έχουν σήμερα (Karatrantou & Papalouka, 2025· Tomczyk, 2020). Συνεπώς, υπάρχει σαφής και επείγουσα ανάγκη προώθησης επιμορφωτικών δράσεων για την ανάπτυξη της ψηφιακής ικανότητας των εκπαιδευτικών (Tomczyk, et al., 2023).

Ο τομέας της ψηφιακής ασφάλειας καλύπτει ικανότητες που σχετίζονται με την προστασία των συσκευών και του ψηφιακού περιεχομένου, την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής σε ψηφιακά περιβάλλοντα, την κατανόηση των κινδύνων και των απειλών σε ψηφιακά περιβάλλοντα, την κατάλληλη χρήση και ανταλλαγή προσωπικών δεδομένων, την πρόληψη από κινδύνους για την υγεία και απειλές για τη σωματική και ψυχολογική ευεξία κατά τη χρήση ψηφιακών τεχνολογιών και την κατανόηση των περιβαλλοντικών επιπτώσεων των ψηφιακών τεχνολογιών και της χρήσης τους. Διάφορες μελέτες που έχουν διεξαχθεί τα τελευταία χρόνια έχουν επισημάνει τη γενική έλλειψη κατάρτισης των εκπαιδευτικών στον τομέα αυτό και, ειδικότερα, την έλλειψη κατάρτισης σχετικά με την ψηφιακή ταυτότητα, την ιδιωτικότητα και την προστασία και χρήση των προσωπικών δεδομένων (Tomczyk, 2021).

Για την ελληνική πραγματικότητα, σε έρευνα των Πανέτα κ.ά. (2025), η πλειοψηφία των συμμετεχόντων εκπαιδευτικών στην έρευνα απάντησε ορθά στις ερωτήσεις γνώσεων σχετικά με τους κινδύνους του διαδικτύου, τη χρήση μέσων κοινωνικής δικτύωσης από τους μαθητές και τους βασικούς κανόνες προστασίας χρηστών στο διαδίκτυο. Ως παράγοντες που επηρεάζουν τις βασικές γνώσεις και δεξιότητες των εκπαιδευτικών σε θέματα ασφάλειας του Διαδικτύου καταγράφονται ο βαθμός χρήσης Η/Υ, το χρονικό διάστημα χρήσης ΤΠΕ στη διδασκαλία τους, η κατοχή επιμόρφωσης σε θέματα ΤΠΕ και η κατοχή επιμόρφωσης σε θέματα ψηφιακής ασφάλειας.

Μεθοδολογία

Στην εργασία αυτή αξιοποιήθηκε ποιοτική ερευνητική μεθοδολογία με στοχευμένη ημιδομημένη συνέντευξη ως ερευνητικό εργαλείο. Οι ερωτήσεις της συνέντευξης βασίστηκαν στο ερωτηματολόγιο των Tomczyk et al. (2023). Ο οδηγός συνέντευξης περιλάμβανε 20 ερωτήσεις: 14 ερωτήσεις αφορούν γνώσεις των εκπαιδευτικών για τους κινδύνους του Διαδικτύου, 2 ερωτήσεις αφορούν την ενημέρωση των γονέων για θέματα ψηφιακής ασφάλειας και 4 ερωτήσεις αφορούν ανάγκες υποστήριξης των εκπαιδευτικών σε θέματα ψηφιακής ασφάλειας.

Για τον έλεγχο της εγκυρότητας και αξιοπιστίας του ερωτηματολογίου πραγματοποιήθηκε μετάφραση/προσαρμογή των ερωτήσεων στα ελληνικά με βάση τη διαδικασία Back-translation. Ενώ ομάδα ειδικών ερευνητών σε ζητήματα ψηφιακού γραμματισμού και ψηφιακής ασφάλειας έλεγξαν την εγκυρότητα περιεχομένου (content validity) του εργαλείου, Τέλος, μέσω πιλοτικής έρευνας διασφαλίστηκε η φαινομενική εγκυρότητα (face validity).

Η δειγματοληψία ήταν συνδυασμός σκόπιμης και δειγματοληψίας χιονοστιβάδας. Για την ανάλυση των δεδομένων αξιοποιήθηκε η μεθοδολογία της ανάλυσης περιεχομένου με μονάδα ανάλυσης το θέμα (θεματική ανάλυση) ανά ερώτηση. Για την έλεγχο της αξιοπιστίας της

ανάλυσης περιεχομένου αξιοποιήθηκε ο έλεγχος αναπαραγωγιμότητας κωδικών με τη συμμετοχή επιπλέον 2 κωδικογράφων και διενεργήθηκε πιλοτική ανάλυση περιεχομένου μιας συνέντευξης και από τους τρεις κωδικογράφους (Krippendorff, 2004). Η αξιοπιστία των κωδικών ήταν υψηλή, όπως φάνηκε από το δείκτη της ποσοστιαίας συμφωνίας μεταξύ των κωδικογράφων (0,92).

Ευρήματα και συζήτηση

Κατά τη διάρκεια της έρευνας, πραγματοποιήθηκαν συνολικά είκοσι (20) συνεντεύξεις, σε εκπαιδευτικούς Πρωτοβάθμιας Εκπαίδευσης στην περιφέρεια Δυτικής Ελλάδας. Πρόκειται για δεκατρείς (13) γυναίκες και επτά (7) άνδρες, είχαν από 1 έως 36 χρόνια υπηρεσίας και οι ηλικίες τους κυμαίνονταν από 26 έως 62 ετών, ήταν κατάλληλα καταρτισμένοι, καθώς κατείχαν επιμορφώσεις στις ΤΠΕ και μεταπτυχιακούς τίτλους σπουδών. Ορισμένοι από αυτούς είχαν επιμορφωθεί σε θέματα ψηφιακής ασφάλειας και υπηρετούσαν σε ποικίλες γεωγραφικά σχολικές μονάδες (αστική, ημιαστική, ορεινή-αγροτική).

Γνώσεις σε θέματα ψηφιακής ασφάλειας

Σημαντικό είναι να τονιστεί πως οι απαντήσεις όλων των συμμετεχόντων στις γνωστικού τύπου ερωτήσεις ήταν ορθές. Αναλυτικότερα, κωδικοποιημένες οι απαντήσεις των εκπαιδευτικών φαίνονται παρακάτω:

Διαδικτυακός εκφοβισμός

- Συμπεριφορά θύτη προς το θύμα απειλητική (15#20), επιθετική (13#20), προσβλητική (2#20), υβριστική (2#20).
- Υπαρξη διάρκειας προκειμένου μια κατάσταση να χαρακτηριστεί ως περιστατικό διαδικτυακού εκφοβισμού (2#20).
- Η εκδήλωση της συμπεριφοράς συμβαίνει μέσα από την αποστολή μηνυμάτων (4#20), την απειλή για δημοσίευση βίντεο (2#20) φωτογραφιών των θυμάτων (2#20).
- Σύνδεση περιστατικών σχολικού εκφοβισμού και διαδικτυακού εκφοβισμού (4#20).

Βλάβες διαδικτυακού εκφοβισμού

- Προκαλεί βλάβες στο θύμα (20#20): ψυχολογικές (20#20), κοινωνικές (8#20), ακαδημαϊκές (5#20), σωματικές (4#20), ηθικές (2#20) και υλικές (1#20).
- Δυσκολία αναγνώρισης - εντοπισμού περιστατικών διαδικτυακού εκφοβισμού (2#20).

Συχνότητα διαδικτυακού εκφοβισμού

- Πολύ συχνό φαινόμενο (18#20).
- Αύξηση των περιστατικών διαδικτυακού εκφοβισμού τα τελευταία χρόνια (7#20), λόγω της ραγδαίας αύξησης της χρήσης κοινωνικών δικτύων (5#20), της χρήσης του διαδικτύου (2#20) και της χρήσης ψηφιακών συσκευών (2#20) από την παιδική ηλικία.
- Ποσοστό του διαδικτυακού εκφοβισμού στα παιδιά ως μεσαίου (10#20), χαμηλού (8#20) και υψηλού (2#20) επιπέδου.
- Αύξηση του διαδικτυακού εκφοβισμού όσο αυξάνεται η ηλικία των παιδιών (2#20).
- Υπαρξη αρκετών περιστατικών διαδικτυακού εκφοβισμού που δεν γνωστοποιούνται από τα θύματα σε κάποιον (4#20).

Πρόληψη διαδικτυακού εκφοβισμού

- Ανάγκη παρέμβασης των γονέων για την αποφυγή περιστατικών διαδικτυακού

εκφοβισμού (20#20), όπως: εποπτεία των παιδιών τους κατά τη διάρκεια της πλοήγησης (8#20), ενημέρωσή τους για το διαδικτυακό εκφοβισμό (7#20), ενημέρωση των παιδιών για τους κινδύνους του διαδικτύου (7#20), υποστήριξη των παιδιών τους (7#20), περιορισμός του χρόνου παραμονής στο διαδίκτυο και στα μέσα κοινωνικής δικτύωσης (4#20), εποπτεία των κινήσεων των παιδιών (4#20), ενημέρωση των γονέων για την αντιμετώπιση των περιστατικών διαδικτυακού εκφοβισμού (4#20), απαγόρευση κατοχής λογαριασμών σε μέσα κοινωνικής δικτύωσης στα παιδιά τους (3#20), ενημέρωση των παιδιών για την κατάλληλη χρήση του διαδικτύου (3#20) και εγκατάσταση λογισμικών γονικού ελέγχου (2#20).

- Ανάγκη ενεργειών από τις σχολικές μονάδες για την αποφυγή περιστατικών διαδικτυακού εκφοβισμού (14#20), όπως: διοργάνωση ενημερωτικών δράσεων για το διαδικτυακό εκφοβισμό και την καλή χρήση των ψηφιακών μέσων για τους μαθητές (9#20), για τους γονείς (3#20) και για τους εκπαιδευτικούς (3#20), υποστήριξη των μαθητών για την κοινοποίηση περιστατικών διαδικτυακού εκφοβισμού (1#20) και αντιμετώπισή τους με συνεργασία γονέων και σχολικής μονάδας (1#20).
- Ανάγκη ενεργειών από τους εκπαιδευτικούς (10#20), όπως: επιμόρφωση των εκπαιδευτικών για την αντιμετώπιση των περιστατικών διαδικτυακού εκφοβισμού και κινδύνων του διαδικτύου (6#20), ενημέρωση των μαθητών για τους κινδύνους του διαδικτύου (5#20), καλλιέργεια σχέσεων συνεργασίας με τους γονείς των μαθητών (2#20) και ανάγκη επικοινωνίας με τους μαθητές για την αντιμετώπιση των περιστατικών διαδικτυακού εκφοβισμού (2#20).
- Ανάγκη ενεργειών από τους ίδιους τους μαθητές (9#10), όπως: να είναι σε θέση να ενημερώσουν άμεσα το περιβάλλον τους όταν δεχτούν διαδικτυακό εκφοβισμό (8#20), να αποκλείουν λογαριασμούς από τους οποίους δέχονται κακόβουλα μηνύματα (2#20) και να αγνοούν κακόβουλα μηνύματα που δέχονται (1#20).
- Ανάγκη ενεργειών από την Πολιτεία για την αποφυγή περιστατικών διαδικτυακού εκφοβισμού (4#10), όπως: αλλαγές στο Αναλυτικό Πρόγραμμα (1#20), ενημέρωση των γονέων (1#20), των εκπαιδευτικών (1#20) και γενικότερα του συνόλου των πολιτών για τον διαδικτυακό εκφοβισμό (1#20).

Cyberstalking

- 12 εκπαιδευτικοί δεν γνωρίζουν τον όρο cyberstalking
- 8 εκπαιδευτικοί αναφέρουν ορθά τη σημασία του όρου cyberstalking και επισημαίνουν ως βασικό χαρακτηριστικό του θύτη την εμμονή του με την παρακολούθηση των διαδικτυακών ιχνών του θύματος.
- 7 από τους συμμετέχοντες τονίζουν την ύπαρξη νομικών συνεπειών για το χρήστη-θύτη.

Σεξουαλικό ή πορνογραφικό υλικό στο διαδίκτυο

- Είναι πολύ πιθανό τα παιδιά να συναντήσουν πορνογραφικό υλικό στο διαδίκτυο (20#20): κατά την πλοήγησή τους στο διαδίκτυο (19#20), μέσα από τις παρέες τους με συνομηλίκους (16#20) και με μεγαλύτερα ηλικιακά παιδιά (6#20) και μέσα από την προτροπή ενηλίκων μελών της οικογένειάς τους (2#20), μέσα από την εμφάνιση σχετικών διαφημίσεων κατά την πλοήγησή τους στο διαδίκτυο (7#20), μέσα από τους λογαριασμούς τους στα κοινωνικά δίκτυα (5#20).
- Το Tik-tok ως το κοινωνικό δίκτυο ευνοεί τη συνάντηση των παιδιών με σεξουαλικό ή πορνογραφικό υλικό (2#20).
- Έλλειψη εποπτείας των παιδιών από τους γονείς τους κατά την διάρκεια της

πλοήγησης τους στο διαδίκτυο (6#20)

- Τα παιδιά αναζητούν σεξουαλικό ή πορνογραφικό υλικό στο διαδίκτυο για την κάλυψη της περιέργειάς τους αναφορικά με τη σεξουαλική τους ανάπτυξη (6#20).

Συνάντηση φίλων από το διαδίκτυο

- Τα παιδιά του Δημοτικού Σχολείου δεν συναντούν από κοντά φίλους που έχουν γνωρίσει στο διαδίκτυο (10#20), εξαιτίας: της μικρής ηλικίας τους (6#20), του φόβου τους για την αντίδραση των γονέων τους (5#20), του φόβου τους για το άγνωστο (3#20) και λόγω της απαγόρευσης από τους γονείς της συνάντησης με άγνωστα άτομα (3#20).
- Τα παιδιά επιζητούν μόνο την αύξηση του πλήθους των διαδικτυακών φίλων τους και όχι τη συνάντηση μαζί τους (1#20).
- Τα παιδιά του Δημοτικού σχολείου συναντούν από κοντά φίλους που έχουν γνωρίσει στο διαδίκτυο (10#20) εξαιτίας: της θέλησης τους για κάλυψη της ανάγκης τους για επικοινωνία (4#20), της περιέργειάς τους να γνωρίσουν άγνωστα άτομα (3#20), της έλλειψης ανεπτυγμένης κριτικής σκέψης (2#20), της παραμέλησης που αισθάνονται από την οικογένειά τους (1#20).

Sexting

- Οι 12 από τους συμμετέχοντες (ορίζουν ορθά τον όρο sexting, τονίζοντας πως πρόκειται για ανταλλαγή μηνυμάτων (12#20), βίντεο (12#20) και φωτογραφιών (11#20) σεξουαλικού περιεχομένου με σκοπό την σεξουαλική ικανοποίηση των χρηστών-ατόμων μέσα από το διαδίκτυο.
- οι 6 από τους συμμετέχοντες αναφέρουν ότι δεν γνωρίζουν τον όρο sexting.
- 2 από τους συμμετέχοντες (2#20) ορίζουν λανθασμένα τον όρο.

Ρητορική μίσους

- Οι 16 από τους συμμετέχοντες ορίζουν ορθά την "ρητορική μίσους", τονίζοντας ότι η ρητορική μίσους διώκεται ποινικά (11#20).
- Τα άτομα χρησιμοποιούν τους λογαριασμούς τους σε μέσα κοινωνικής δικτύωσης για να επιτεθούν σε άτομα-χρήστες ή ομάδες χρηστών και να ενθαρρύνουν τη βία απέναντι τους από άλλους χρήστες (11#20).
- Στόχος των επιθέσεων τους είναι χαρακτηριστικά των θυμάτων-χρηστών που σχετίζονται με την θρησκεία (6#20), τη φυλή (6#20), την πολιτική τοποθέτηση (5#20), το φύλο (4#20), την εθνικότητα (3#20), την ηλικία (1#20) ή την αναπηρία τους (1#20).
- Ανισορροπία δυνάμεων ανάμεσα στους θύτες και στα θύματα, σε μια αντιστοιχία ισχυρού και ανίσχυρου (4#20).

Ψευδείς ειδήσεις

- Σκοπός των ψευδών ειδήσεων είναι η παραπληροφόρηση των πολιτών (14#20).
- Δυσκολία αναγνώρισης των ψευδών ειδήσεων (12#20).
- Τρόποι αναγνώρισης των ψευδών ειδήσεων: η διασταύρωση των πληροφοριών μέσα από διάφορες πηγές (14#20), η αναγνώριση συγκεκριμένων χαρακτηριστικών στα γραφικά εικόνων ή βίντεο (3#20), η αξιοποίηση εφαρμογών τεχνητής νοημοσύνης (2#20) και η Ανάπτυξη της κριτικής γνώμης στους πολίτες (2#20).
- Υπαρξη πάρα πολλών ψευδών ειδήσεων που δέχονται οι πολίτες καθημερινά (10#20).
- Η χρήση της τεχνητής νοημοσύνης έχει οδηγήσει σε αύξηση του πλήθους των ψευδών ειδήσεων και της δυσκολίας αναγνώρισης τους (8#20).

Παιχνίδια αυτοκαταστροφής

- 19 από τους συμμετέχοντες γνωρίζουν το παιχνίδι "Γαλάζια Φάλαινα" και τον αρνητικό αντίκτυπο του για τα παιδιά: παιδιά που οδηγήθηκαν στην αυτοκτονία (16#20) και αυτοτραυματισμοί (5#20) στο πλαίσιο του παιχνιδιού.
- 6 εξ αυτών γνωρίζουν το παιχνίδι "Superman", το οποίο έχει οδηγήσει πολλά παιδιά στο τραυματισμό (6#20)
- 2 γνωρίζουν το παιχνίδι Pokemon Go, το οποίο έχει οδηγήσει σε πολλούς τραυματισμούς από αμέλεια
- 5 από τους συμμετέχοντες επισημαίνουν ότι δεν γνωρίζουν κάποιο παρόμοιο παιχνίδι τύπου Challenge.
- 2 από τους συμμετέχοντες επισημαίνουν ότι το μέσο κοινωνικής δικτύωσης Tik-tok ευνοεί τη διάδοση και τη προώθηση παιχνιδιών τύπου challenge.

Επιλογή διαφημίσεων στα κοινωνικά δίκτυα

Οι 19 εκπαιδευτικοί επισημαίνουν ότι γνωρίζουν τους τρόπους με τους οποίους επιλέγονται οι διαφημίσεις που τους εμφανίζονται στα κοινωνικά δίκτυα: μηχανές αναζήτησης (18#20), φύλο (13#20), γεωγραφική τοποθεσία (12#20), ηλικία (10#20), ενδιαφέροντα και τις προτιμήσεις που έχουν δηλώσει στους λογαριασμούς τους στα μέσα κοινωνικής δικτύωσης (7#20), cookies που έχουν αποδεχτεί ως χρήστες (6#20), ακουστικά δεδομένα που καταγράφουν οι ψηφιακές συσκευές τους (5#20).

Ψηφιακή αποτοξίνωση

- Αρκετοί από τους συμμετέχοντες (17#20) ορίζουν ορθά τον όρο ψηφιακή αποτοξίνωση και υποστηρίζουν ότι η ψηφιακή αποτοξίνωση μπορεί να επιτευχθεί με μείωση της χρήσης του διαδικτύου (16#20) και τον περιορισμό της χρήσης ψηφιακών συσκευών (13#20).
- Η ψηφιακή αποτοξίνωση είναι μια διαδικασία που μπορεί να επιτευχθεί σταδιακά (15#20).
- Η ψηφιακή αποτοξίνωση να επιτευχθεί μέσα από τη προσφορά βοήθειας στα άτομα-εξαρτημένους από ειδικούς ψυχολόγους (6#20), από την προσφορά κατάλληλης ιατρικής βοήθειας (6#20) και μέσα από την υποστήριξη της οικογένειας των ατόμων (5#20).
- Η ενασχόληση με τον αθλητισμό βοηθάει στην αποτοξίνωση των εξαρτημένων χρηστών (4#20).

Κατοχή λογαριασμού σε κοινωνικό δίκτυο από μαθητές

Οι περισσότεροι εκπαιδευτικοί γνωρίζουν ότι οι μαθητές τους έχουν λογαριασμούς σε μέσα κοινωνικής δικτύωσης (17#20), ενώ μερικοί εξ αυτών (6#20) υποστηρίζουν ότι οι μαθητές τους δεν έχουν λογαριασμό στο Facebook, επειδή το θεωρούν μέσο κοινωνικής δικτύωσης παλαιότερης γενιάς.

Ενημέρωση εκπαιδευτικών και γονέων

- Οι γονείς πρέπει να εποπτεύουν τα παιδιά τους κατά τη πλοήγησή τους στο διαδίκτυο (14#20), να εγκαταστήσουν προγράμματα γονικού ελέγχου στις ψηφιακές συσκευές σύνδεσης των παιδιών τους στο διαδίκτυο (13#20), να θεσπίσουν χρονικούς περιορισμούς στα παιδιά τους κατά τη χρήση του διαδικτύου (9#20), να ενημερώσουν τα παιδιά τους για την ύπαρξη ψηφιακών κινδύνων (5#20), να απαγορεύουν την δημιουργία λογαριασμών σε μέσα κοινωνικής δικτύωσης στα παιδιά τους μέχρι αυτά να είναι άνω των 13 χρονών (3#20), να ελέγχουν το ιστορικό περιήγησης των παιδιών τους στο διαδίκτυο (2#20), να είναι σε θέση οι ίδιοι οι γονείς να θεσπίσουν και να

τηρήσουν όρια και κανόνες χρήσης του διαδικτύου για τον ίδιο τον εαυτό τους (1#20), να ενημερώνονται για τον αρνητικό αντίκτυπο που έχει για τα παιδιά τους η χρήση των ψηφιακών συσκευών και του διαδικτύου (1#20), να γνωρίζουν την ύπαρξη ή μη λογαριασμών των παιδιών τους σε 'μέσα κοινωνικής δικτύωσης και να έχουν διαθέσιμους για χρήση τους κωδικούς των λογαριασμών τους στα κοινωνικά δίκτυα (1#20), να εγκαταστήσουν τη συσκευή από όπου τα παιδιά τους εισέρχονται στο διαδίκτυο σε κοινόχρηστο χώρο του σπιτιού (1#20) και να μην επιτρέπουν στα παιδιά τους να έχουν τις δικές τους προσωπικές ψηφιακές συσκευές (1#20).

- 12 εκπαιδευτικοί δεν έχουν ενημερώσει τους γονείς των μαθητών τους για ζητήματα ψηφιακής ασφάλειας που επιφυλάσσουν κινδύνους για τους μαθητές τους κατά την πλοήγηση στο διαδίκτυο.
- 4 εκπαιδευτικοί δεν θεωρούν σημαντική την ενημέρωση των γονέων, παρά μόνο σε περιπτώσεις μαθητών αυξημένου κινδύνου που χρήζουν ιδιαίτερης προσοχής και χειρισμού και έχοντας ως έναυσμα κάποιο συγκεκριμένο περιστατικό.
- 8 εκπαιδευτικοί ενημερώνουν τους γονείς των μαθητών τους για ζητήματα ψηφιακής ασφάλειας που επιφυλάσσουν κινδύνους για τους μαθητές τους στο διαδίκτυο.

Ανάγκες υποστήριξης εκπαιδευτικών

- Ανάγκη επιμόρφωσης για ένταξη θεμάτων ψηφιακής ασφάλειας στη διδασκαλία (20#20).
- Ανάγκη συνεχούς επιμόρφωσης για την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία, λόγω της ραγδαίας εξέλιξης και εξάπλωσης της τεχνολογίας (6#20).
- Οι ευκαιρίες επιμόρφωσης που τους δίνονται δεν είναι οι κατάλληλες (6#20)
- Οι επιμορφώσεις που τους παρέχονται δεν είναι συγκεκριμένες, κατάλληλα συντονισμένες (3#20) και σχεδιασμένες (3#20).
- Έλλειψη πλήθους σχετικών επιμορφώσεων (2#20), για την ανάγκη λήψης πρωτοβουλιών από το Υπουργείο Παιδείας για την οργάνωση και τη διεξαγωγή σχετικών επιμορφωτικών προγραμμάτων (2#20).
- Έλλειψη συχνότητας διεξαγωγής σχετικών επιμορφώσεων (1#20).
- Δεν παρέχονται σχετικές ευκαιρίες επιμόρφωσης (8#20).
- Παρέχονται σχετικές ευκαιρίες επιμόρφωσης (6#20) από ιδιωτικούς φορείς (5#20), δημόσιους φορείς (5#20), Πανεπιστήμια (2#20) και από συμβούλους (1#20).
- Δυσκολία συμμετοχής των εκπαιδευτικών στις επιμορφώσεις λόγω του περιορισμένου χρόνου που μπορούν να διαθέσουν εκτός ωραρίου εργασίας (6#20), τη δημιουργία ομάδων επιμορφούμενων με διαφορετικό γνωστικό υπόβαθρο (1#20) και την αδυναμία συμμετοχής λόγω της υποστήριξης της οικογένειάς τους (1#20).
- Αναγκαία για την επιμόρφωση των εκπαιδευτικών: η διεξαγωγή των επιμορφώσεων εντός του εργασιακού ωραρίου των εκπαιδευτικών (3#20), η αυτονομία των εκπαιδευτικών στην αναζήτηση προγραμμάτων επιμόρφωσης (2#20), η θέσπιση κινήτρων για την επιμόρφωση των εκπαιδευτικών σε θέματα ένταξης της ψηφιακής ασφάλειας στη διδασκαλία τους (1#20), η παροχή δωρεάν επιμορφωτικών προγραμμάτων για τους εκπαιδευτικούς (1#20), η διεξαγωγή επιμορφώσεων μικρής χρονικής διάρκειας (1#20) και οι ενέλικτες επιμορφώσεις (1#20).
- Η προάσπιση της ψηφιακής ασφάλειας των μαθητών τους (2#20) αποτελεί το σημαντικότερο κίνητρο προκειμένου να επιμορφωθούν ως εκπαιδευτικοί.
- 11 εκπαιδευτικοί (11#20) υποστηρίζουν ότι δεν τους παρακινεί κανείς από τα σημαντικά γι' αυτούς άτομα στον εργασιακό τους χώρο για την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία τους.
- Τους παρακινεί κάποιο από τα σημαντικά γι' αυτούς πρόσωπο του εργασιακού τους χώρου για την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία τους: οι

συνάδελφοι-εκπαιδευτικοί (8#20), ο διευθυντής της σχολικής μονάδας (8#20).

- Οι υπεύθυνοι χάραξης και υλοποίησης της εκπαιδευτικής πολιτικής δεν υποστηρίζουν ουσιαστικά την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία (14#20).
- Οι υπεύθυνοι για τη χάραξη και την υλοποίηση της εκπαιδευτικής πολιτικής υποστηρίζουν την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία μέσα από: αλλαγές στο Αναλυτικό Πρόγραμμα (4#20), μέσα από την παροχή σχετικών επιμορφώσεων (3#20), την αποστολή σχετικών εγκυκλίων για την προτροπή διοργάνωσης δράσεων ενημέρωσης των μαθητών για την ψηφιακή ασφάλεια (2#20), την παροχή κατάλληλης υλικοτεχνικής υποδομής, όπως οι διαδραστικοί πίνακες (1#20) και μέσα από την ύπαρξη κειμένων για τη ψηφιακή ασφάλεια στα σχολικά εγχειρίδια (1#20).

Συμπεράσματα

Οι εκπαιδευτικοί Πρωτοβάθμιας Εκπαίδευσης φαίνεται να έχουν γνώσεις που αφορούν τους κινδύνους του Διαδικτύου και συγκεκριμένα τον Διαδικτυακό Εκφοβισμό, τις βλάβες που προκαλεί, τη συχνότητα του, την πρόληψη του, το Cyberstalking, σεξουαλικό ή πορνογραφικό υλικό στο διαδίκτυο, συνάντηση φίλων από το διαδίκτυο, το sexting, τη ρητορική μίσους, τις ψευδείς ειδήσεις, τα παιχνίδια αυτοκαταστροφής, τη ψηφιακή ατοτοξίνωση. Οι περισσότεροι εκπαιδευτικοί γνωρίζουν ότι οι μαθητές τους κατέχουν λογαριασμό σε μέσο κοινωνικής δικτύωσης.

Οι εκπαιδευτικοί θεωρούν πως οι γονείς πρέπει να γνωρίζουν για τους κινδύνους του διαδικτύου και την διαχείρισή τους, να γνωρίζουν αν τα παιδιά τους διαθέτουν λογαριασμό σε μέσο κοινωνικής δικτύωσης, να έχουν διαθέσιμους για χρήση τους κωδικούς των λογαριασμών τους στα κοινωνικά δίκτυα και να μην επιτρέπουν στα παιδιά τους να έχουν τις δικές τους προσωπικές ψηφιακές συσκευές. Όμως, οι μισοί περίπου εκπαιδευτικοί δεν έχουν ενημερώσει τους γονείς των μαθητών τους για ζητήματα ψηφιακής ασφάλειας που επιφυλάσσουν κινδύνους για τους μαθητές τους κατά την πλοήγηση στο διαδίκτυο.

Όλοι οι εκπαιδευτικοί σημειώνουν τη συνεχή ανάγκη επιμόρφωσης για την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία, εξαιτίας της ραγδαίας εξάπλωσης και εξέλιξης της τεχνολογίας στις μέρες μας. Κρίνουν όμως, πως οι ευκαιρίες επιμόρφωσης που τους δίνονται δεν είναι οι κατάλληλες, οι επιμορφώσεις που τους παρέχονται δεν είναι συγκεκριμένες, κατάλληλα συντονισμένες και αποτελεσματικά σχεδιασμένες. Καταγράφουν έλλειψη σχετικών επιμορφώσεων από το Υπουργείο Παιδείας ενώ οι παρεχόμενες δράσεις παρέχονται από ιδιωτικούς φορείς, δημόσιους φορείς, τα Πανεπιστήμια και τους σχολικούς συμβούλους. Οι μισοί εκπαιδευτικοί θεωρούν πως δεν τους παρακινεί κανείς από τα σημαντικά γι' αυτούς άτομα στον εργασιακό τους χώρο, όπως ο διευθυντής της σχολικής μονάδας και οι συνάδελφοι-εκπαιδευτικοί για την ένταξη ζητημάτων ψηφιακής ασφάλειας στη διδασκαλία τους και πως τα άτομα που είναι υπεύθυνα για τη χάραξη και την υλοποίηση της εκπαιδευτικής πολιτικής δεν υποστηρίζουν ουσιαστικά την ένταξη τέτοιων ζητημάτων στη διδασκαλία. Οι εκπαιδευτικοί κρίνουν ως σημαντικά αλλαγές στο Αναλυτικό Πρόγραμμα, όπως, η ένταξη νέων τεχνολογιών για τη διδασκαλία και η ένταξη του μαθήματος Εργαστήριο Δεξιοτήτων στο ωρολόγιο πρόγραμμα, την παροχή κατάλληλης υλικοτεχνικής υποδομής, και την ύπαρξη κειμένων για τη ψηφιακή ασφάλεια στα σχολικά εγχειρίδια.

Λόγω της φύσης της έρευνας αυτής, τα αποτελέσματά της δεν μπορούν να γενικευτούν. Περαιτέρω έρευνα, ποσοτική και ποιοτική, με μεγαλύτερο δείγμα εκπαιδευτικών, μελλοντικών εκπαιδευτικών, στελεχών της εκπαίδευσης αλλά και γονέων μπορεί να δώσει γενικεύσιμα συμπεράσματα και λεπτομερείς απαντήσεις στα ερευνητικά ερωτήματα.

Αναφορές

Carretero, S., Vuorikari, R., & Punie, Y. DigComp 2.1 (2017). *The digital competence framework for citizens*.

- with eight proficiency levels and examples of use. Publications Office of the European Union.
- Dede, C. (2009). Comparing frameworks for the 21st century skills. In J. A. Bellanca, & R. S. Brandt (Eds.), *21st century skills: Rethinking how students learn* (pp. 51-76). Solution Tree Press.
- European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan* (COM/2018/022 Final). European Commission.
- Gallego-Arrufat, M. J., Torres-Hernández, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar*, 27(61), 57-67. <https://doi.org/10.3916/C61-2019-05>
- Gordillo, A., Barra, E., López-Pernas, S., & Quemada, J. (2021). Development of teacher digital competence in the area of e-safety through educational video games. *Sustainability*, 13(15), 8485. <https://doi.org/10.3390/su13158485>
- Govender, I., & Skea, S. (2019). Teachers' understanding of e-safety: An exploratory case in KZN South Africa. *The Electronic Journal of Information Systems in Developing Countries*, 70, 1-17. <https://doi.org/10.1002/j.1681-4835.2015.tb00505.x>
- Karatrantou, A., & Papalouka, A. (2025) e-safety literacy of future primary school teachers. *Proceedings of the EDULEARN25* (pp. 10175-10184). IATED Digital Library.
- Karatrantou, A., & Stamatelos, J. M. (2025) What do pre-service teachers of primary education know about misinformation on the internet? *Proceedings of the EDULEARN25* (pp. 10166-10174). IATED Digital Library.
- Krippendorff, K. (2004). *Content analysis. An introduction to its methodology* (2nd Edition). SAGE.
- Redecker, C., & Punie, Y. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Publications Office of the European Union.
- Reisoğlu, İ., & Çebi, A. (2020). How can the digital competences of pre-service teachers be developed? Examining a case study through the lens of DigComp and DigCompEdu. *Computers & Education*, 156, 103940. <https://doi.org/10.1016/j.compedu.2020.103940>
- Rocha Estrada, F. J., George-Reyes, C. E., & Glasserman-Morales, L. D. (2022). Security as an emerging dimension of Digital Literacy for education: a systematic literature review. *Journal of e-Learning and Knowledge Society*, 18(2), 22-33. <https://doi.org/10.20368/1971-8829/1135440>
- Sarva, E., Purina-Bieza, K.E., & Daniela, L. (2022). Self-evaluation instrument for measuring educators' pedagogical digital competence. *Proceedings of the 2022 INTED Conference* (pp. 3568-3576). INTED <https://doi.org/10.21125/inted.2022.1002>
- Thuy Nguyen, L.A., & Habók, A. (2024). Tools for assessing teacher digital literacy: a review. *Journal of Computers in Education* 11(1), 305-346. <https://doi.org/10.1007/s40692-022-00257-5>
- Tomczyk, Ł. (2020). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, 25(1), 471-486. <https://doi.org/10.1007/s10639-019-09980-6>
- Tomczyk, Ł. (2021). Declared and real level of digital skills of future teaching staff. *Education Sciences*, 11, 619. <https://doi.org/10.3390/educsci11100619>
- Tomczyk, Ł., Fedeli, L., Włoch, A., Limone, P., Frania, M., Guarini, P., Szyszka, M., Mascia, M., L., & Falkowska, J. (2023). Digital competences of pre-service teachers in Italy and Poland. *Technology, Knowledge and Learning*, 28(2), 651-681. <https://doi.org/10.1007/s10758-022-09626-6>
- UNESCO. (2018). *UNESCO ICT Competency Framework for Teachers (Version 3)*. UNESCO.
- Πανέτας, Γ., Καρατράντου, Α., & Παναγιωτακόπουλος, Χρ. (2025). Ψηφιακή ασφάλεια και εκπαιδευτικοί πρωτοβάθμιας εκπαίδευσης δημοτικών σχολείων: Μελέτη περίπτωσης. Στο Α. Τζιμογιάννης, Γ. Κουτρομάνος, Π. Τσιωτάκης (Επιμ.). *Πρακτικά Περιλήψεων Εργασιών 5ου Πανελληνίου Συνεδρίου "Ηλεκτρονική Μάθηση και Ανοικτοί Εκπαιδευτικοί Πόροι"*. Τμήμα Εκπαιδευτικής και Κοινωνικής Πολιτικής, Πανεπιστήμιο Πελοποννήσου & ΠΤΔΕ ΕΚΠΑ.