Εισαγωγική Επιμόρφωση για την εκπαιδευτική αξιοποίηση Τ.Π.Ε.

Επιμόρφωση Β1 επιπέδου ΤΠΕ

Συστάδα: Πληροφορικής

ΕΠΙΜΟΡΦΩΤΙΚΟ ΥΛΙΚΟ

Συνεδρία 11 -

Ψηφιακή Πολιτειότητα - Ασφαλής χρήση διαδικτύου

ΕΠΙΜΟΡΦΩΤΙΚΟ ΥΛΙΚΟ

Έκδοση 1η

Μάρτιος 2024

Πράξη:	ΕΠΙΜΟΡΦΩΣΗ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΓΙΑ ΤΗΝ ΑΞΙΟΠΟΙΗΣΗ ΚΑΙ ΕΦΑΡΜΟΓΗ ΤΩΝ ΨΗΦΙΑΚΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΣΤΗ ΔΙΔΑΚΤΙΚΗ ΠΡΑΞΗ (ΕΠΙΜΟΡΦΩΣΗ Β' ΕΠΙΠΕΔΟΥ ΤΠΕ)/ Β' Κύκλος
Φορείς Υλοποίησης:	Δικαιούχος φορέας: ΙΤΥΕ "ΔΙΟΦΑΝΤΟΣ" ινστιτουτο τεχνολογιας υπολογιστων & εκδοσεων
	Συμπράττων φορέας: ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΙΕΠ ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ


ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας και Θρησκευμάτων
Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού,
Εκπαίδευση και Διά Βίου Μάθηση
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ
2014-2020

ΠΕΡΙΕΧΟΜΕΝΑ

1 Προοίμιο

Το παρόν επιμορφωτικό υλικό δημιουργήθηκε για να καλύψει τις ανάγκες της «Εισαγωγικής Επιμόρφωσης για Εκπαιδευτική Αξιοποίηση των Τ.Π.Ε.» (Επιμόρφωση Β1 επιπέδου ΤΠΕ) που υλοποιείται σε Κέντρα Στήριξης Επιμόρφωσης (Κ.Σ.Ε.) σε όλη την Ελλάδα, για εκπαιδευτικούς όλων των κλάδων και ειδικοτήτων, στο πλαίσιο της Πράξης «Επιμόρφωση Εκπαιδευτικών για την Αξιοποίηση και Εφαρμογή των Ψηφιακών Τεχνολογιών στην Διδακτική Πράξη (Επιμόρφωση Β' επιπέδου Τ.Π.Ε.)/Β' κύκλος», http://e-pimorfosi.cti.gr, του Επιχειρησιακού Προγράμματος «Ανάπτυξη Ανθρώπινου Δυναμικού – Εκπαίδευση και Δια Βίου Μάθηση». Το έργο αυτό συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο, ΕΣΠΑ 2014-2020) και το Ελληνικό Δημόσιο.

Η επιμόρφωση Β1 επιπέδου Τ.Π.Ε. και το αντίστοιχο επιμορφωτικό υλικό σχεδιάστηκε και υλοποιήθηκε αρχικά, το διάστημα 2017 – 2019, για 4 «συστάδες» κλάδων εκπαιδευτικών ως εξής: Β1.1: «Θεωρητικές επιστήμες και Καλλιτεχνικά», Β1.2 «Φυσικές Επιστήμες, Τεχνολογία, Φυσική Αγωγή και Υγεία», Β1.3 «Μαθηματικά, Πληροφορική και Οικονομία – Διοίκηση» και Β1.4: «Πρωτοβάθμια Εκπαίδευση».

Το διάστημα 2021 -2022, στο πλαίσιο της παραπάνω πράξης, η επιμόρφωση Β1 επιπέδου Τ.Π.Ε. επικαιροποιήθηκε, εμπλουτίστηκε και υλοποιείται αναμορφωμένη πλέον σε 13 «συστάδες» ομοειδών ή σχετικών κλάδων εκπαιδευτικών ως εξής: Β1.1 «Φιλολογικά», Β1.2 «Φυσικές Επιστήμες», Β1.3 «Μαθηματικά», Β1.4 «Πληροφορική», Β1.5 «Πρωτοβάθμια Εκπαίδευση - Δάσκαλοι», Β1.6 «Πρωτοβάθμια Εκπαίδευση - Νηπιαγωγοί», Β1.7 «Ξένες Γλώσσες», Β1.8 «Καλές Τέχνες», Β1.9 «Φυσική Αγωγή και Υγεία», Β1.10 «Εκπαιδευτικοί Μηχανικοί», Β1.11 «Οικονομία, Διοίκηση και Κοινωνικές Επιστήμες», Β1.12 «Επαγγέλματα Γης» και Β1.13 «Ειδική Αγωγή».

Το επιμορφωτικό υλικό Β1 επιπέδου Τ.Π.Ε διατίθεται και αξιοποιείται στο πλαίσιο της επιμόρφωσης με τη μορφή «μαθήματος»/ e-course (ένα ανά συστάδα), μέσω της πλατφόρμας ηλεκτρονικής μάθησης του έργου, η οποία βασίζεται στο ελεύθερο λογισμικό/ λογισμικό ανοικτού κώδικα moodle. Περιλαμβάνει υλικό μελέτης-αναφοράς και εκπαιδευτικές δραστηριότητες, ενώ εν γένει συνοδεύεται από υποστηρικτικό και άλλο πρόσθετο υλικό (οδηγίες προς τους Επιμορφωτές και προς τους επιμορφούμενους, αρχεία παρουσιάσεων κ.ά.).

Συντάχθηκε υπό την επίβλεψη και στο πλαίσιο των αρμοδιοτήτων του ειδικού Επιστημονικού Συμβουλίου[1] του Ι.Τ.Υ.Ε. – «Διόφαντος», το οποίο έχει συσταθεί με την υπ' αριθ. Π568/28.07.2011 Απόφαση, και στην παρούσα Πράξη λειτουργεί ως εξειδικευμένο επιστημονικό συμβουλευτικό όργανο του Ι.Τ.Υ.Ε. - «Διόφαντος», δικαιούχου φορέα υλοποίησης της Πράξης.

Συμπληρωματικά και για την κάλυψη των απαιτήσεων των «νέο»-εισερχόμενων στην επιμόρφωση κλάδων / ειδικοτήτων εκπαιδευτικών (βλ. παραπάνω, συστάδες Β1.7 έως Β1.13), στο πλαίσιο της παρούσας Πράξης λειτουργεί ευρύτερη Επιστημονική Επιτροπή, η οποία

[1] Το Επιστημονικό Συμβούλιο του Ι.Τ.Υ.Ε.-«Διόφαντος» για την επιμόρφωση, αποτελείται από τους Καθηγητές: i) Χαράλαμπο Ζαγούρα, Πανεπιστήμιο Πατρών, ο οποίος έχει την ευθύνη συντονισμού των εργασιών του Συμβουλίου, ii) Βασίλειο Δαγδιλέλη, Πανεπιστήμιο Μακεδονίας, iii) Βασίλειο Κόμη, Πανεπιστήμιο Πατρών, iv) Δημήτριο Κουτσογιάννη, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, v) Πολυχρόνη Κυνηγό, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών και vi) Δημήτριο Ψύλλο, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

αποτελείται από τους παρακάτω Καθηγητές, επιστημονικούς συνεργάτες του δικαιούχου (Ι.Τ.Υ.Ε. – «Διόφαντος»), καθώς και του συμπράττοντα φορέα υλοποίησης της Πράξης (Ι.Ε.Π.):

- Χαράλαμπο Ζαγούρα, Πανεπιστήμιο Πατρών, ο οποίος έχει την ευθύνη συντονισμού των εργασιών της Επιτροπής
- Παναγιώτη Αντωνίου, Δημοκρίτειο Πανεπιστήμιο Θράκης, ως Επιστημονικά Υπεύθυνο για τη Συστάδα «Φυσική Αγωγή και Υγεία»
- Βασίλειο Δαγδιλέλη, Πανεπιστήμιο Μακεδονίας, ως Επιστημονικά Υπεύθυνο για τη συστάδα «Πληροφορική»
- Χαράλαμπο Καραγιαννίδη, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, ως Επιστημονικά Υπεύθυνο για τη συστάδα «Ειδική Αγωγή»
- Βασίλειο Κόμη, Πανεπιστήμιο Πατρών, ως Επιστημονικά Υπεύθυνο για τις συστάδες «Πρωτοβάθμια Εκπαίδευση – Δάσκαλοι» και «Πρωτοβάθμια Εκπαίδευση – Νηπιαγωγοί»
- Δημήτριο Κουτσογιάννη, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, ως Επιστημονικά Υπεύθυνο για τη συστάδα «Φιλολογικά»
- Πολυχρόνη Κυνηγό, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, ως Επιστημονικά Υπεύθυνο για τη συστάδα «Μαθηματικά»
- Βασιλική Μητσικοπούλου, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, ως Επιστημονικά Υπεύθυνη για τη συστάδα «Ξένες Γλώσσες»
- Σπύρο Παπαδόπουλο, Πανεπιστήμιο Θεσσαλίας, ως Επιστημονικά Υπεύθυνο για τη συστάδα «Καλές Τέχνες»
- Κυπαρισσία Παπανικολάου, Ανωτάτη Σχολή Παιδαγωγικής και Τεχνολογικής Εκπαίδευσης ως Επιστημονικά Υπεύθυνη για τη συστάδα «Εκπαιδευτικοί Μηχανικοί»
- Παναγιώτη Σιμιτζή, Γεωπονικό Πανεπιστήμιο Αθηνών ως Επιστημονικά Υπεύθυνο για τη συστάδα «Επαγγέλματα Γης»
- Ιωάννη Τσίρμπα, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, ως Επιστημονικά Υπεύθυνο για τη συστάδα «Οικονομία, Διοίκηση και Κοινωνικές Επιστήμες»
- Δημήτριο Ψύλλο, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Επιστημονικά Υπεύθυνο για τη συστάδα «Φυσικές Επιστήμες»

Ειδικότερα, στη δημιουργία **του ενιαίου μέρους του επιμορφωτικού υλικού Β1 επιπέδου ΤΠΕ**, το οποίο αποτέλεσε τη βάση για τον περαιτέρω εμπλουτισμό και εξειδίκευσή του ανά συστάδα, συνέβαλαν, με την επίβλεψη και τον συντονισμό μελών της Επιστημονικής Επιτροπής, οι:

- Μαρία Ακριτίδου, Εκπαιδευτικός ΠΕ02, Δρ Νεοελληνικής Φιλολογίας
- Σταυρούλα Αντωνοπούλου, Εκπαιδευτικός ΠΕ02, Δρ Γλωσσολογίας
- Χαράλαμπος Αποστόλου, Δρ., MSc, MEd, Συντονιστής Εκπαιδευτικού Έργου - ΠΕ04, Περιφέρεια Δ. Μακεδονίας
- Γεώργιος Βουνάτσος, ΜΑ Εκπαιδευτικός Μηχανολόγος Μηχανικός
- Αγορίτσα Γόγουλου, Δρ. Εκπαιδευτικής Τεχνολογίας, Εργαστηριακό Διδακτικό Προσωπικό, Τμήμα Πληροφορικής & Τηλεπικοινωνιών, ΕΚΠΑ
- Βασίλειος Δαγδιλέλης, Καθηγητής, Πανεπιστήμιο Μακεδονίας
- Δημήτρης Διαμαντίδης, Εκπαιδευτικός ΠΕ03 Μαθηματικών
- Φιλήμονας Διαμαντίδης, Εκπαιδευτικός Μηχανολόγος Μηχανικός
- Χαράλαμπος Καραγιαννίδης, Καθηγητής, Πανεπιστήμιο Θεσσαλίας
- Αγγελική Καραματσούκη, Εκπαιδευτικός ΠΕ86-Πληροφορικής και ΠΕ87.02-Νοσηλευτικής
- Βασίλειος Κόμης, Καθηγητής, Πανεπιστήμιο Πατρών

- Εμμανουήλ Κουσλόγλου, MSc Φυσικός ΠΕ04.01, Υποψήφιος Διδάκτορας Τμήμα Φυσικής ΑΠΘ
- Φίλιππος Κουτσάκας, Εκπαιδευτικός ΠΕ86-Πληροφορικής
- Δημήτριος Κουτσογιάννης, Καθηγητής, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
- Πολυχρόνης Κυνηγός, Καθηγητής, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών
- Ιωάννης Λεύκος, Δρ., Ε.ΔΙ.Π., Τμήμα Εκπαιδευτικής & Κοινωνικής Πολιτικής, ΠΑΜΑΚ
- Ευστρατία Λιακοπούλου, Συντονίστρια Εκπαιδευτικού Έργου Πληροφορικής
- Χρήστος Μάλλιαρης, Εκπαιδευτικός ΠΕ03 Μαθηματικών
- Αναστάσιος Μάτος, Εκπαιδευτικός ΠΕ02, Συντονιστής εκπαίδευσης, Δρ Ψηφιακών Τεχνολογιών στην Εκπαίδευση
- Αναστασία Μισιρλή, Δρ., ΕΔΙΠ, ΤΕΕΑΠΗ, Πανεπιστήμιο Πατρών
- Αναστάσιος Μολοχίδης, Επίκουρος Καθηγητής, Τμήμα Φυσικής, ΑΠΘ
- Δέσποινα Παπαδοπούλου, Δρ. Χημικός, MSc, Υπεύθυνη Εργαστηριακού Κέντρου Φυσικών Επιστημών (ΕΚΦΕ) Ν. Καβάλας
- Κυπαρισσία Παπανικολάου, Καθηγήτρια, Ανωτάτη Σχολή Παιδαγωγικής και Τεχνολογικής Εκπαίδευσης
- Γεώργιος Σκουντζής, Εκπαιδευτικός Πρωτοβάθμιας εκπαίδευσης
- Αγγελική Τζαβάρα, Δρ., ΕΔΙΠ, ΤΕΕΑΠΗ, Πανεπιστήμιο Πατρών
- Γιάννης Τζωρτζάκης, MSc Εκπαιδευτικός Πολιτικός Μηχανικός, Συντονιστής Εκπαιδευτικού Έργου Περιφερειακής Διεύθυνσης Εκπαίδευσης Πελοποννήσου
- Ανδρομάχη Φιλιππίδη, Δρ., Εκπαιδευτικός Πρωτοβάθμιας εκπαίδευσης
- Γεώργιος Χοροζίδης, Υποψήφιος Διδάκτορας, Παιδαγωγικό Τμήμα Ειδικής Αγωγής, Πανεπιστήμιο Θεσσαλίας
- Δημήτριος Ψύλλος, Καθηγητής, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Ο εμπλουτισμός και η εξειδίκευση του επιμορφωτικού υλικού για τη Συστάδα Β1.4 Πληροφορικής έγινε από συγγραφική ομάδα με την επιστημονική ευθύνη του αντίστοιχου μέλους της Επιστημονικής Επιτροπής και συμμετέχοντες τους:

- Αλεξούδα Γεωργία, Πληροφορικό
- Λεύκο Ιωάννη, μέλος Ε.ΔΙ.Π. Πανεπιστημίου Μακεδονίας
- Μαλλιαράκη Χρήστο, Πληροφορικό
- Μαυροχαλυβίδη Γεώργιο, Πληροφορικό
- Ξινόγαλος Στυλιανός, μέλος ΔΕΠ Πανεπιστημίου Μακεδονίας
- Παπαδάκη Σταμάτη, Πληροφορικό

Στο παρόν επιμορφωτικό υλικό, με τρόπο έμμεσο ή άμεσο έχει ενσωματωθεί ένα μέρος από παλιότερο υλικό. Στην αρχική του μορφή το Γενικό Μέρος του Επιμορφωτικού υλικού δημιουργήθηκε από συγγραφική ομάδα, με επικεφαλής τον Βασίλη Δαγδιλέλη, Καθηγητή του Πανεπιστημίου Μακεδονίας και συμμετέχοντες τους:

- Καψάλη Αχιλλέα, πρώην Καθηγητή στο Πανεπιστήμιο Μακεδονίας.
- Παπαδόπουλο Ιωάννη, Επίκουρο Καθηγητή στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.
- Φαχαντίδη Νικόλαο, Αναπληρωτή Καθηγητή στο Πανεπιστήμιο Μακεδονίας.
- Ταμπούρη Ευθύμιο, Καθηγητή στο Πανεπιστήμιο Μακεδονίας

Στην παρούσα έκδοση του Επιμορφωτικού Υλικού Γενικού Μέρους έχουν συμβάλει τα μέλη του Επιστημονικού Συμβουλίου Βασίλειος Δαγδιλέλης, Βασίλειος Κόμης, Δημήτριος Κουτσογιάννης, Πολυχρόνης Κυνηγός, Δημήτριος Ψύλλος, καθώς και οι εξής:

- Σταυρούλα Αντωνοπούλου, υποψήφια διδάκτωρ Εφαρμοσμένης Γλωσσολογίας, ΑΠΘ
- Μαριάνθη Γριζιώτη, εκπαιδευτικός ΠΕ86 (ΠΕ19/20),
- Ελισάβετ Καλογερία, εκπαιδευτικός ΠΕ03,
- Ελένη Κουστριάβα, Καθηγήτρια στο Πανεπιστήμιο Μακεδονίας,
- Χρήστος Μάλλιαρης, εκπαιδευτικός ΠΕ03,
- Μάριος Ξένος, εκπαιδευτικός ΠΕ86 (ΠΕ19/20),
- Γεώργιος Πανσεληνάς, εκπαιδευτικός ΠΕ86 (ΠΕ19/20),
- Γεώργιος Σκουντζής, εκπαιδευτικός ΠΕ70,
- Μάριος Σπάθης, εκπαιδευτικός ΠΕ03,
- Αθανάσιος Ταραμόπουλος, εκπαιδευτικός ΠΕ04

Κατά τη δημιουργία του υλικού αυτού, χρησιμοποιήθηκαν πόροι από το αντίστοιχο εκπαιδευτικό και επιμορφωτικό υλικό της εκπαίδευσης των επιμορφωτών Β' επιπέδου Τ.Π.Ε. στα ΠΑ.Κ.Ε. και εκπαιδευτικών στα Κέντρα Στήριξης της Επιμόρφωσης (Κ.Σ.Ε.) που αναπτύχθηκε στο πλαίσιο προηγούμενων σχετικών έργων επιμόρφωσης Β' επιπέδου ΤΠΕ*. Επομένως, στη δημιουργία του υλικού αυτού συνέβαλαν έμμεσα και όσοι είχαν συνεργαστεί στη δημιουργία του υλικού για την εκπαίδευση των επιμορφωτών στα ΠΑ.Κ.Ε. και την επιμόρφωση των εκπαιδευτικών στα Κ.Σ.Ε. στο πλαίσιο των έργων αυτών και οι οποίοι αναφέρονται αναλυτικά στα αντίστοιχα κείμενα επιμορφωτικού υλικού που δημοσιεύονται στους αντίστοιχους κόμβους ενημέρωσης*.

Το επιμορφωτικό υλικό Β1 επιπέδου Τ.Π.Ε., αποτελεί ιδιοκτησία του ΥΠΑΙΘΑ και καλύπτεται από την ισχύουσα νομοθεσία για την προστασία των πνευματικών δικαιωμάτων των δημιουργών.

* Πράξη: «Επιμόρφωση Εκπαιδευτικών στη χρήση και αξιοποίηση των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) στην εκπαιδευτική διδακτική διαδικασία", ΕΠΕΑΕΚ ΙΙ, Γ' ΚΠΣ, http://b-epipedo.cti.gr

Πράξεις: «Επιμόρφωση Εκπαιδευτικών για την αξιοποίηση και εφαρμογή των Τ.Π.Ε. στη Διδακτική πράξη», Επιχειρησιακό Πρόγραμμα «Εκπαίδευση και Δια Βίου Μάθηση», ΕΣΠΑ 2007-2013, http://b-epipedo2.cti.gr

2 Σκοπός

Σκοπός της παρούσας ενότητας είναι οι επιμορφούμενοι να γνωρίσουν τη βασική προβληματική της Ψηφιακής Πολιτειότητας και της ασφαλούς χρήσης του Διαδικτύου. Αυτός ο σκοπό εμπορεί να διατυπωθεί αναλυτικότερα ως εξής:

(1) να αποκτήσουν μερικές βασικές γνώσεις γύρω από τις νέες μορφές *ψηφιακής πολιτειότητας*

(2) να αποκτήσουν λειτουργικού χαρακτήρα γνώσεις για τη φύση και το είδος των κινδύνων που συνδέονται με τη χρήση των ΤΠΕ, γενικότερα των ψηφιακών πόρων και κυρίως του Διαδικτύου

(3) να αποκτήσουν γνώσεις διδακτικής οι οποίες θα τους επιτρέψουν να διδάξουν τα σχετικά θέματα στους μαθητές τους (ψηφιακής πολιτειότητας και διαχείρισης της πληροφορίας)

3 Στόχοι

Οι ειδικότεροι στόχοι του μαθήματος είναι οι επιμορφούμενοι:

1. να είναι σε θέση να προσδιορίσουν ποιοι θεωρούνται γενικά κίνδυνοι που συνδέονται με τη χρήση και διαχείριση ψηφιακών πόρων και ιδιαίτερα του Διαδικτύου.
2. να είναι σε θέση να προσδιορίσουν ποιοι από τους κινδύνους είναι ιδιαίτερα συνδεδεμένοι με τις μικρές ηλικίες, το σχολείο, την εκπαίδευση.
3. να αποκτήσουν γνώσεις και δεξιότητες για την αντιμετώπιση των κινδύνων και τη διδασκαλία των σχετικών θεμάτων είτε με τρόπο άμεσο (οργανώνοντας μαθήματα επί τούτου), είτε έμμεσα (στα πλαίσια δραστηριοτήτων άλλων γνωστικών αντικειμένων)
4. να αποκτήσουν γνώσεις και δεξιότητες σχετικές με την e-πολιτειότητα, το σύνολο των ψηφιακών πρακτικών που συνδέονται με την ιδιότητα του πολίτη
5. να αποκτήσουν γνώσεις σχετικά με τη διαχείριση ψηφιακών πληροφοριών (θέματα στρατηγικών αναζήτησης πληροφοριών, αναφοράς πηγών πληροφοριών, ελέγχου της ποιότητας των πληροφοριών, καλών πρακτικών επικοινωνίας και διάχυσης/μεταβίβασης πληροφοριών)
6. να αποκτήσουν βασικές γνώσεις που θα τους επιτρέψουν να είναι διαρκώς ενήμεροι στις νεότερες εξελίξεις για τα θέματα κινδύνων στο Διαδίκτυο, ψηφιακής πολιτειότητας και διαχείρισης των ψηφιακών πληροφοριών

4 Κίνδυνοι στο Διαδίκτυο και ασφαλής πλοήγηση

4.1 Ορισμοί των «κινδύνων στο Διαδίκτυο»

Η καθολική επικράτηση του Διαδικτύου και γενικότερα των ψηφιακών τεχνολογιών συνδέεται με μια σειρά αρνητικών χαρακτηριστικών που ονομάζονται, με ένα γενικό τρόπο, «κίνδυνοι στο Διαδίκτυο».

Ο όρος δεν είναι απολύτως ακριβής, καθώς ο όρος «κίνδυνοι» αντιστοιχεί σε χαρακτηριστικά που μπορεί να έχουν αρνητικό χαρακτήρα, αλλά δεν αποτελούν ακριβώς κινδύνους. Για παράδειγμα,

πολλά ανεπιθύμητα μηνύματα (τα λεγόμενα spam), μπορεί να έχουν ανεπιθύμητες συνέπειες (κατανάλωση χρόνου για τη διαγραφή τους ή υπερπλήρωση του ηλεκτρονικού γραμματοκιβωτίου με άχρηστα μηνύματα), αλλά δεν αποτελούν ακριβώς «κινδύνους».

Προκαταρκτικά, θα πρέπει πάντως να επισημανθούν δυο στοιχεία:

<1> **η έννοια του κινδύνου** (συνδεδεμένη και με την έννοια της «απειλής» αλλά και της αντίθετης εννοίας της «ασφάλειας» και της «προφύλαξης», όπως και με την έννοια της «απαγόρευσης» για την προστασία των ευάλωτων ατόμων) είναι σε μεγάλο βαθμό μια κοινωνική κατασκευή και δεν είναι «σταθερή» στο χρόνο και στο χώρο, σε κάθε κουλτούρα. Ο κίνδυνος είναι μια συνάρτηση πολλών παραγόντων όπως ο χρόνος, ο τόπος, η ηλικία (τόσο αυτού που κρίνει, όσο και αυτού που βρίσκεται «εν κινδύνω»), ακόμη και παραγόντων κοινωνικών και ιδεολογικών. Υπάρχουν άφθονα παραδείγματα, από τετριμμένα ως λιγότερο προφανή, που υποστηρίζουν τη θεωρητική αυτή θέση, που είναι μάλλον γενικά αποδεκτή. Για παράδειγμα στο Μεσαίωνα, η υπερβολική ενασχόληση με τα βιβλία (η ανάγνωση δηλαδή) και μάλιστα η σιωπηλή ανάγνωση δε θεωρήθηκε αρχικά ως θετικό στοιχείο της ανθρώπινης προσωπικότητας, καθώς ως τότε η ανάγνωση ήταν μεγαλόφωνη και «... *γινόταν με συγκεκριμένους κανόνες σε προκαθορισμένο τόπο και χρόνο*» (Χ. Μπάνου, 2010). Ακόμη, αναγνώσματα που σήμερα θεωρούνται ως κατάλληλα για τα νεαρά άτομα και τα παιδιά (για παράδειγμα ο δημοφιλής «Μικρός Ήρως»), πριν από 50 ή 60 χρόνια είχαν θεωρηθεί ως επικίνδυνα αναγνώσματα για τη νεολαία. Σχετικά είναι και τα (Γ. Μπαλιάς 2009) και (F. Ewald, 1986). Οι εκπαιδευτικοί θα πρέπει, με ένα γενικό τρόπο, να έχουν μια κριτική στάση απέναντι σε ό,τι συλλήβδην χαρακτηρίζεται ως «επικίνδυνο».

<2> **θα πρέπει επίσης να αναγνωρίσουμε ότι πολύ συχνά η νεολαία, και ιδιαίτερα οι έφηβοι, «περνούν τα όρια»,** έλκονται από τον κίνδυνο και αγνοούν τις απαγορεύσεις, ίσως γιατί αυτή η συμπεριφορά αποτελεί συστατικό στοιχείο της διαδικασίας διαμόρφωσης της προσωπικότητάς τους, της ταυτότητάς τους. Αυτό ίσως σημαίνει πως όποια μέτρα και αν λάβουν το σχολείο και οι γονείς, όσες παραινέσεις και να κάνουν, οι έφηβοι στον ιδιωτικό τους χώρο και χρόνο θα επισκεφτούν ιστοχώρους που θεωρούνται ακατάλληλοι ή επικίνδυνοι και θα δοκιμάσουν να κάνουν ενέργειες που δεν εγκρίνουν οι ενήλικοι. Αυτό δε σημαίνει βέβαια πως δεν πρέπει να ληφθούν μέτρα για την προστασία τους – το αντίθετο μάλιστα.

Η έννοια του κινδύνου, όπως αναφέρουμε λίγο παραπάνω, δεν είναι απολύτως προσδιορισμένη με ένα καθολικά αποδεκτό τρόπο. Ορισμένα παραδείγματα ορισμών (τα οποία παρατίθενται ενδεικτικά) είναι τα ακόλουθα:

Ο (M. J. Volkmann in Α. Καμάρης 2014, σ. 16) αναφέρει:

Οι Διαδικτυακοί κίνδυνοι μπορούν να οριστούν ως κάθε τι που μπορεί να προκαλέσει βλάβη σε ένα χρήστη του Διαδικτύου. Η βλάβη αυτή μπορεί να είναι διαφόρων μορφών όπως φυσική, συναισθηματική, ψυχολογική, οικονομική, κοινωνική ή αναφερόμενη στην υπόληψη του χρήστη.

Η (J. M. Warner-Blankenship 2011, in Α. Καμάρης 2014, σ. 16) υποστηρίζει ότι:

Οι Διαδικτυακοί κίνδυνοι είναι κίνδυνοι που σχετίζονται με το να είναι κάποιος χρήστης του Διαδικτύου. Οι κίνδυνοι αυτοί μπορεί επίσης να αφορούν στην πρόσβαση σε ανεπιθύμητες πληροφορίες. Υπάρχει μεγάλη ποικιλία Διαδικτυακών κινδύνων από θέματα ασφάλειας έως διάφορα είδη θυματοποίησης.

Τέλος, στη Wikipedia.org για την παρεμφερή έννοια της «Απειλής στον Ιστό» (Web threat) το σχετικό άρθρο αναφέρει (in Α. Καμάρης 2014, σ. 17):

Απειλή στον Ιστό είναι κάθε απειλή που χρησιμοποιεί το Παγκόσμιο Ιστό για να διευκολύνει το έγκλημα στο Διαδίκτυο.

Συνοψίζοντας, το γενικότερο πνεύμα μελέτης του φαινομένου κινείται γύρω από την ευρύτερη διαπίστωση πως κίνδυνο αποτελεί καθετί που απειλεί τη ζωή, την ασφάλεια ή την ακεραιότητα ενός προσώπου ή ενός πράγματος και αντίστοιχα ασφάλεια είναι η κατάσταση που χαρακτηρίζεται από την απουσία κινδύνου (Α. Καμάρης 2014).

4.2 Κατηγορίες κινδύνων, ενοχλητικών, ανεπιθύμητων στοιχείων στο Διαδίκτυο και τους ψηφιακούς πόρους

Με ένα γενικό τρόπο, θα πρέπει να υπενθυμίσουμε πως ταυτόχρονα με τις νέες δυνατότητες, τα σύγχρονα κινητά μέσα πρόσβασης στο Διαδίκτυο (smart phones, tablets κ.τ.ό.) αυξάνουν και την πιθανότητα να βρεθεί κάποιος χρήστης εκτεθειμένος σε όλα αυτά τα αρνητικά στοιχεία που περιγράφονται παρακάτω. Ιδιαίτερα η αύξηση της χρήσης (για παράδειγμα οι online συναλλαγές) των ψηφιακών μέσων, απαιτεί και μεγαλύτερη προσοχή από τη μεριά των χρηστών. Μια σχετικά πλήρης καταγραφή των διαφόρων κατηγοριών των στοιχείων αυτών περιλαμβάνεται στο (Α. Καμάρης 2014, κείμενο το οποίο αποτελεί βασική πηγή για την παρούσα ενότητα) και περιλαμβάνει τα εξής (μαζί με την αντίστοιχη Αγγλική ορολογία):

1. Ακατάλληλο – προσβλητικό περιεχόμενο ιστοχώρων (Offensive content)
2. Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages)
3. Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation). Διαμόρφωση ταυτότητας. Έκθεση στα κοινωνικά δίκτυα
4. Ηλεκτρονική αποπλάνηση χρηστών (Online grooming)
5. Βίαια παιχνίδια (Violent games)
6. Διαδικτυακός εθισμός ή εξάρτηση των χρηστών (Internet addiction)
7. Διαδικτυακός εκφοβισμός (Cyber bullying)
8. Παρώθηση σε επιβλαβείς συμπεριφορές
9. Ηλεκτρονικός τζόγος (Online gambling)
10. Κακόβουλο λογισμικό που μολύνει Ηλεκτρονικούς Υπολογιστές (Malware)

Δες σχετικό βίντεο: https://www.youtube.com/watch?v=9XS6RhDJzxk

11. Παιδική πορνογραφία (Child pornography)
12. Παραβίαση της ιδιωτικότητας των χρηστών (Internet privacy) και επιπτώσεις ακόμη και στην κινητή τηλεφωνία
13. Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation). Ψευδή νέα και ο πολλαπλασιασμός τους. Αστικοί μύθοι. Ψηφιακές φάρσες.
14. Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Phishing»
15. Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Pharming»

16. Φυσικές παθήσεις που προκαλούνται από παρατεταμένη χρήση του Η/Υ

Από τις παραπάνω κατηγορίες αναπτύσσονται ορισμένες (1,2,3,7,13) ενώ για τις υπόλοιπες παρατίθενται βιβλιογραφικές αναφορές.

4.2.1 Ακατάλληλο, προσβλητικό και επιβλαβές περιεχόμενο ιστοχώρων (Offensive content)

Το περιεχόμενο ενός ιστοχώρου (λεκτικό, οπτικό ή ακουστικό) θεωρείται ακατάλληλο ή προσβλητικό όταν παραβιάζει τα κοινωνικά, θρησκευτικά ή πολιτισμικά πρότυπα ή τις προσωπικές και οικογενειακές αξίες του ατόμου. Είναι προφανές ότι όλες αυτές οι διατυπώσεις πρέπει να λαμβάνονται υπόψη μέσα στη σχετικότητά τους, αφού τα πολιτισμικά, κοινωνικά ή θρησκευτικά πρότυπα δεν έχουν καθολικό χαρακτήρα. Έτσι, η ακαταλληλότητα του περιεχομένου ενός ψηφιακού πόρου και ο βαθμός επικινδυνότητας του σχετίζεται με τα ατομικά χαρακτηριστικά του χρήστη. Είναι εξίσου προφανές ότι τα άτομα που δεν έχουν ακόμη τα κατάλληλα γνωστικά και ψυχικά εφόδια που θα τους επέτρεπαν να εξετάσουν κριτικά το αντίστοιχο περιεχόμενο, ενδεχομένως είναι πιο ευάλωτα. Έτσι, για παράδειγμα, έφηβοι, παιδιά , άτομα γενικά νεαρής ηλικίας μπορεί να ενοχληθούν, να ταραχτούν ή να παρωθηθούν σε παραβατικές ή ανάρμοστες συμπεριφορές από κείμενα, εικόνες και γενικά πόρους των οποίων το «μήνυμα» δεν είναι πάντοτε σε θέση να αντιμετωπίσουν, να κατανοήσουν και να εξετάσουν κριτικά. Φυσικά, το ίδιο περιεχόμενο μπορεί να θεωρείται κατάλληλο για ενήλικα άτομα.

Το ακατάλληλο-προσβλητικό υλικό μπορεί να περιλαμβάνει ρατσιστικά, βίαια ή σεξουαλικώς προκλητικά στοιχεία, υλικό που προστατεύεται από πνευματικά δικαιώματα, απαγορευμένο ή παράνομο υλικό, να προάγει την ξενοφοβία, τη βία, τα ναρκωτικά, τα τυχερά παιχνίδια (τζόγο), επικίνδυνες ή εγκληματικές δραστηριότητες, ακραίες φυλετικές απόψεις, προώθηση της φασιστικής ιδεολογίας και άλλες μη ασφαλή στοιχεία, όπως λόγου χάρη διατροφικές διαταραχές ή πορνογραφικό υλικό.

Οι ακόλουθες εικόνες είναι από μια σειρά παρόμοιων εικόνων την εποχή που ήταν πολύ ανεπτυγμένο το κίνημα της «νευρικής ανορεξίας» (anorexia nervosa):

Είναι προφανές ότι εικόνες όπως αυτές όχι μόνο μπορούν να σοκάρουν, αλλά και κατά κάποιο τρόπο, να «ενισχύσουν» την απήχηση της ιδέας σε νεαρά άτομα τα οποία, μπορεί να εμφανίσουν διατροφικές διαταραχές για λόγους ψυχολογικούς.

Θα πρέπει να σημειωθεί ότι, με ένα γενικό τρόπο, το μήνυμα ενός ιστοχώρου μπορεί να είναι έμμεσο και για το λόγο αυτό πολύ πιο δύσκολα ανιχνεύσιμο. Για παράδειγμα, ορισμένες ιστοσελίδες μπορούν έμμεσα να προβάλλουν ως μεγάλη αξία τη σωματική ρώμη και η ανίχνευση και ταυτοποίηση αυτού του μηνύματος να είναι πιο δύσκολη από άτομα που δεν είναι εξοικειωμένα με μια κριτική εξέταση ενός κειμένου. Γενικά τα γραφικά στοιχεία, μπορούν να εμπεριέχουν έμμεσα εκφρασμένα μηνύματα ακόμη σε πολύ «δευτερεύοντα» χαρακτηριστικά τους όπως τα μεγέθη και η θέση των εικόνων, οι χρησιμοποιούμενες γραμματοσειρές κ.ά.

4.2.2 Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages)

Ένα από τα πλέον διαδεδομένα φαινόμενα στον κυβερνοχώρο είναι τα ανεπιθύμητα (spam messages) και τα ασπρόσκλητα γενικότερα μηνύματα (unsolicited messages) που οι χρήστες δέχονται στο ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα. Τα μηνύματα αυτά σχετίζονται συχνά με διαφημίσεις προϊόντων ή υπηρεσιών, την προώθηση τυχερών παιχνιδιών (καλυμμένων ενίοτε ως κερδών σε μια κλήρωση στην οποία ο χρήστης ποτέ δε συμμετείχε), με πορνογραφικό υλικό κ.ά. Μερικές φορές, με πρόσχημα μια ιστορία στην οποία (υποτίθεται ότι) υπάρχουν αδιάθετα κάποια σημαντικά χρηματικά ποσά, ο χρήστης καλείται να συμμετάσχει προσφέροντας υπηρεσίες για τις οποίες (υποτίθεται πάντα ότι) θα αμειφθεί πλουσιοπάροχα. Η πιο γνωστή κατηγορία εξεπάτησης αυτού του είδους είναι η «απάτη της Νιγηρίας» (Nigeria scam). Τα μηνύματα αυτά πολλές φορές αποστέλλονται μαζικά σε μεγάλους αριθμούς (bulk mails) και μεταφράζονται από γλώσσα σε γλώσσα με αυτόματους μεταφραστές. Στις περιπτώσεις αυτές, οι ίδιες οι μεταφράσεις παράγουν κείμενα ακατανόητα ή με χονδροειδή γλωσσικά ή επικοινωνιακά λάθη, καθιστώντας πολύ εύκολη τη διαπίστωση ότι πρόκειται για ψευδή μηνύματα.

Για παράδειγμα το ακόλουθο (αληθινό) μήνυμα εστάλη, υποτίθεται από μια Τράπεζα:

Αγαπητε πελατη,
Εχετε λαβει ενα νεο κοινοποιηση
Καντε κλικ εδω για να διαβασετε.

Είναι προφανές ότι πρόκειται για μήνυμα που αποσκοπεί στην εξαπάτηση του χρήστη. Εξάλλου ο υπερδεσμός (στο κλικ) οδηγεί σε έναν άσχετο με οιαδήποτε Τράπεζα και πιθανότατα επικίνδυνο ιστοχώρο (για να το διαπιστώσει, αρκεί να «περάσει» κανείς με το ποντίκι πάνω από τον υπερδεσμό χωρίς να κάνει «κλικ»).

Μια ενδιαφέρουσα προσέγγιση στο φαινόμενο του spam, είναι η οικολογική: η παραγωγή και διάδοση των ανεπιθύμητων μηνυμάτων, όπως αναφέρουν οι σχετικές έρευνες, προκαλεί τόση μόλυνση, όση, για παράδειγμα, η κυκλοφορία εκατοντάδων χιλιάδων αυτοκινήτων.

4.2.3 Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation)

Παρατηρείται κυρίως σε νεαρά άτομα, αλλά όχι αποκλειστικά. Οι χρήστες ασχολούνται σταδιακά ολοένα και περισσότερο με διαδικτυακά και γενικότερα ψηφιακά παιχνίδια, με την άμεση online συνομιλία (chat rooms), με σελίδες κοινωνικής δικτύωσης κ.ά. και αποξενώνονται από το φυσικό

και κοινωνικό τους περίγυρο. Ο χρόνος που αφιερώνουν στις εναχολήσεις αυτές γίνεται τελικά τόσο μεγάλος, που αποκλείει άλλου είδους δραστηριότητες ατομικές ή ομαδικές, σε ακραίες περιπτώσεις ακόμη και την ατομική φροντίδα του εαυτού και τη στοιχειώδη υγιεινή. Οι σχέσεις με τους άλλους ανθρώπους του περίγυρου, ους φίλους, του γονείς γίνονται προβληματικές και σπάνιες. Δημιουργείται έτσι μια συναισθηματική και κοινωνική αποξένωση των χρηστών από τον περίγυρό τους (εκτός των άλλων). Είναι σα μια «δεύτερη», παράλληλη, εικονική ή online ζωή στην οποία ζούν οι εθισμένοι χρήστες και η οποία προοδευτικά διογκώνεται και γίνεται πιο σημαντική από την πραγματική ζωή. Το φαινόμενο είναι τόσο σημαντικό και διαδεδομένο, ώστε έχει αναγνωριστεί ως ένα είδος πάθησης που χρειάζεται θεραπεία, ακόμη και σε εξειδικευμένα θεραπευτικά κέντρα.

4.2.4 Διαδικτυακός εκφοβισμός (Cyber bullying)

Ο Διαδικτυακός Εκφοβισμός ορίζεται από τους P.K. Smith, J. Madhavi, M. Carvalho, M. Fisher, S. Russell και N. Tippett ως «μια επιθετική, σκόπιμη και επαναλαμβανόμενη πράξη η οποία πραγματοποιείται από ένα άτομο ή μια ομάδα ατόμων, μέσω της χρήσης ηλεκτρονικών μορφών επικοινωνίας, εναντίον ενός ατόμου που δεν μπορεί εύκολα να υπερασπιστεί τον εαυτό του».

Η ολοένα αυξανόμενη χρήση των ηλεκτρονικών συσκευών και του Διαδικτύου καθιστά τον Διαδικτυακό Εκφοβισμό ως τη μορφή εκφοβισμού με το μεγαλύτερο ρυθμό αύξησης (Cart, 2010).

Πραγματοποιείται συνήθως μέσα από το ηλεκτρονικό ταχυδρομείο, τα δωμάτια συζητήσεων, τους ιστότοπους κοινωνικής δικτύωσης (social networking sites), τις ιστοσελίδες (web sites), τα ιστολόγια (blogs), τα Διαδικτυακά παιχνίδια και τα κινητά τηλέφωνα. Οι μορφές που μπορεί να έχει είναι:

- Η διακωμώδηση ή/και εξευτελισμός του θύματος
- Η αποστολή προσβλητικών και άσεμνων μηνυμάτων μέσω Διαδικτυακών εφαρμογών
- Το άσεμνο περιεχόμενο κατά τη διάρκεια συνομιλιών
- Ο εξευτελισμός ενός νεαρού ατόμου με τη δημιουργία ενός προφίλ ή ιστολογίου το οποίο περιλαμβάνει σκόπιμα λανθασμένα στοιχεία ή εξευτελιστικό περιεχόμενο
- Η αποστολή απειλητικών μηνυμάτων
- Η δημοσιοποίηση προσωπικών βίντεο ή φωτογραφιών χωρίς τη συγκατάθεση του ατόμου

Η ιδιαιτερότητα του Διαδικτυακού Εκφοβισμού έγκειται στο γεγονός πως επεμβαίνει στον προσωπικό χώρο του θύματος, ενώ είναι δύσκολος ο περιορισμός του εξαιτίας της αδυναμίας ελέγχου του αριθμού και του περιεχομένου των μηνυμάτων που μπορεί να λάβει ένας χρήστης του Διαδικτύου.

Ο κυβερνοεκφοβισμός (cyberbullying) είναι η συνέχεια του εκφοβισμού με ψηφιακά μέσα. Σύμφωνα με τον ιστοχώρο digitrust (δες παρακάτω), *αυτοί που ασκούν εκφοβισμό χρησιμοποιούν τις νέες τεχνολογίες για να απειλήσουν, να εκφοβίσουν, να παρενοχλήσουν, να δυσφημήσουν και να αποκλείσουν νέους, και, σε μερικές περιπτώσεις, να τους υποδυθούν ή να υποκλέψουν την ταυτότητά τους. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:*

- Εκφοβισμός με γραπτό μήνυμα: το παιδί ίσως λάβει δυσάρεστα, προσβλητικά ή απειλητικά μηνύματα.

- Παρενόχληση/κλήσεις-φάρσα: κάποιος ίσως καλεί επίμονα το παιδί στο κινητό του και του λέει δυσάρεστα και προσβλητικά πράγματα.
- Δημοσίευση και διαμοιρασμός εικόνων χωρίς τη συγκατάθεση του παιδιού: φωτογραφίες, βίντεο ή οπτικό υλικό τραβηγμένο με webcam, όπου εμφανίζεται το παιδί, θα μπορούσαν να κυκλοφορήσουν μέσω email ή μηνυμάτων, να αναρτηθούν στο διαδίκτυο ή να μπουν σε δημόσιο ιστότοπο με το όνομα του παιδιού σε ετικέτα.
- «Happy slapping»: κάποιος θα μπορούσε με το κινητό του να φωτογραφίσει ή να βιντεοσκοπήσει το παιδί καθώς το κακοποιεί λεκτικά ή σωματικά.
- Εκφοβισμός μέσω email ή άμεσων μηνυμάτων: το παιδί θα μπορούσε να λάβει δυσάρεστα, προσβλητικά ή ενοχλητικά email ή άμεσα μηνύματα από κάποιον που γνωρίζει ή από έναν άγνωστο.
- Εκφοβισμός σε chatroom: ένας άλλος χρήστης του chatroom θα μπορούσε να πει αγενή πράγματα στο, ή για το, παιδί σας.
- Εκφοβισμός μέσω κοινωνικού δικτύου: κάποιος θα μπορούσε να αναρτήσει δυσάρεστα ή προσβλητικά μηνύματα για το παιδί σας σ' έναν ιστότοπο σαν το Facebook, ή να φτιάξει ένα πλαστό προφίλ του παιδιού.
- Εκφοβισμός στη διάρκεια ενός διαδραστικού παιχνιδιού: αν το παιδί παίζει παιχνίδια για πολλούς παίκτες, κάποιος συμπαίκτης του ίσως προσπαθήσει να το αποκλείσει ή να το αγνοήσει. Οι έρευνες δείχνουν πως αυτού του είδους ο διαδικτυακός εξοστρακισμός έχει αντίκτυπο στην αυτοεκτίμηση.

4.2.5 Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation)

Το Διαδίκτυο αφενός μεν παρέχει αναρίθμητους πόρους και ευκαιρίες μάθησης, αφετέρου δε, σε αντίθεση με τα παραδοσιακά έντυπα μέσα, δεν διαθέτει τις απαραίτητες δικλείδες ασφαλείας για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται, με αποτέλεσμα σε κάποιες περιπτώσεις με τη δημοσίευση αναληθών, τροποποιημένων ή ελλιπών πληροφοριών μπορεί ο χρήστης να οδηγηθεί σε λανθασμένα, ανακριβή και αναξιόπιστα συμπεράσματα.

Χαρακτηριστικό παράδειγμα της παραπληροφόρησης είναι οι αστικοί μύθοι (urban legends) οι οποίοι λόγω του Διαδικτύου διαδίδονται με μεγαλύτερη ευκολία, σε περισσότερο πληθυσμό. Ο Connie Chesner, εκπαιδευτής στο Πανεπιστήμιο Wake Forest των Η.Π.Α. αναφέρει πως νέα χαρακτηριστικά, όπως η κακόβουλη πρόθεση, ο εμπλουτισμός με τεχνολογία υψηλότερης ποιότητας και με γνωρίσματα που παρέχουν φαινομενική αυθεντικότητα, κάνουν τους σημερινούς Διαδικτυακούς αστικούς μύθους πιο αληθοφανείς και ενδεχομένως πιο επιβλαβείς.

Κατά συνέπεια, κρίνεται αναγκαία η ανάπτυξη κριτικής σκέψης από το χρήστη του Διαδικτύου, προκειμένου κρίνει την ακρίβεια των πληροφοριών αυτών και ξεχωρίσει τη μη έγκυρη πληροφορία. Όπως είναι φυσικό ο κίνδυνος της παραπληροφόρησης είναι ιδιαίτερα αυξημένος με απρόβλεπτα αποτελέσματα σε νεαρά άτομα τα οποία λόγω ηλικίας δεν έχουν οξυμένη την κριτική τους σκέψη και ικανότητα.

4.3 Τρόποι αντιμετώπισης των επικίνδυνων ή αρνητικών στοιχείων του Διαδικτύου

Με ένα γενικό τρόπο, οι μέθοδοι για την αντιμετώπιση αυτών των αρνητικών στοιχείων χωρίζονται σε δυο κατηγορίες: μεθόδους με τεχνικό χαρακτήρα και μεθόδους ενημερωτικού και παιδαγωγικού χαρακτήρα.

4.3.1 Μέθοδοι τεχνικού χαρακτήρα

Στις μεθόδους τεχνικού χαρακτήρα περιλαμβάνονται μια πλειάδα από συστήματα που έχουν αναπτυχθεί για την άμεση προστασία των χρηστών (κυρίως ευάλωτων χρηστών, όπως για παράδειγμα τα παιδιά), αλλά και συστήματα συμβουλών, εκπαίδευσης, σήμανσης ιστοχώρων και περιεχομένου με σκοπό οι χρήστες να αναγνωρίζουν το επικίνδυνο ή αμφίβολο περιεχόμενο και να αντιδρούν κατάλληλα (Α. Καμάρης 2014, σελ. 32).

Ως τέτοιες μεθόδους μπορούμε να αναφέρουμε τα διάφορα είδη φίλτρων που υφίστανται. Τα φίλτρα αυτού του είδους μπορούν να είναι (σύμφωνα με τον ιστοχώρο SaferIntenet, http://www.saferinternet.gr/index.php?objId=Category36&childobjId=Category113&parentobjId=Page2) πολλών ειδών και επιτελούν πολλές λειτουργίες, όπως *να προειδοποιήσουν για προβληματικές ιστοσελίδες, να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη στο Διαδίκτυο, να μπλοκάρουν ύποπτους ιστοχώρους, να επιτρέπουν την πρόσβαση συγκεκριμένες ώρες και ημέρες, ακόμα και να κλείσουν τελείως τον υπολογιστή*.

Φίλτρα αυτού του είδους είναι (Ibid):

Οι λεγόμενες «**περιφραγμένες τοποθεσίες**» (walled gardens) ή «λευκές λίστες» (white lists) είναι λίστες από ιστοσελίδες κατάλληλες για ανηλίκους. Οι «**μαύρες λίστες**» λειτουργούν με αντίστοιχο τρόπο – για παράδειγμα απαγορεύουν την αποστολή e-mails από δευθύνσεις που έχουν παρατηρηθεί να στέλνουν συχνά spam σε άλλες διευθύνσεις.

Οι **λίστες ψηφιακών πόρων με ακατάλληλο περιεχόμενο** συνιστούν άλλο ένα είδος τέτοιου φίλτρου. Οι χρήστες δεν έχουν πρόσβαση σε ιστοχώρους που περιλαμβάνονται σε αυτές τις λίστες. Συχνά οι λίστες δεν περιλαμβάνουν συγκεκριμένους ιστοχώρους, αλλά λέξεις ή όρους «απαγορευμένους» και αποκλείουν την πρόσβαση σε ιστοσελίδες που περιέχουν (στο κείμενο ή τον τίτλο τους) τις λέξεις αυτές ή τους αντίστοιχους όρους. Εκτός του ότι οι λίστες αυτές χρειάζοναι συχνά επικαιροποίηση, πολλές φορές αποκλείουν την πρόσβαση σε ιστοχώρους που δε θα έπρεπε να εξαιρούνται: ένα παράδειγμα αποτελεί η ιστορία ιστοσελίδων ενός αστεροσκοπείου στη Μ. Βρετανία που διδάσκει την αναγνώριση αστερισμών στον ουρανό με παρατήρηση δια «γυμνού οφθαλμού» (naked-eye) που είναι μη-προσβάσιμος καθώς η λέξη «γυμνός» θεωρείται «απαγορευμένη». Τα φίλτρα «γονεϊκού ελέγχου» (parental control) πολύ συχνά στηρίζονται σε λίστες αυτού του είδους. Χρησιμοποιούν όμως παράλληλα και άλλου είδους ελέγχους, όπως χρόνου έναρξης της πλοήγησης και γενικότερα πρόσβασης, διάρκειας χρήσης, καταγραφής δραστηριοτήτων του χρήστη (παιδιού) κ.ά.

Σε ορισμένες περιπτώσεις, με συγκατάθεση των ιδιοκτητών των σχετικών ιστοχώρων, οι πάροιχοι πρόσβασης στο Διαδίκτυο **επισημαίνουν με κατάλληλες ψηφιακές ετικέτες** του ιστοχώρους που έχουν εν δυνάμει επιβλαβές περιεχόμενο. Η Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου ICRA (Internet Content Rating Association, https://www.fosi.org/icra/) δημιουργεί εικέτες αυτού του είδους που μπορούν να χρησιμοποιηθούν από φίλτρα διαφόρων ειδών. Σχετικό με αυτά είναι το ευρωπαϊκό σύστημα PEGI (http://www.pegi.info/gr/), ένα σύστημα **ηλικιακής διαβάθμισης**. Σύμφωνα με την ιστοσελίδα του ίδιου του συστήματος PEGI, *οι ηλικιακές*

διαβαθμίσεις είναι συστήματα που χρησιμοποιούνται για να εξασφαλίσουν ότι όλα τα προϊόντα ψυχαγωγικού περιεχομένου, όπως κινηματογραφικές ταινίες, βίντεο, DVD και παιχνίδια υπολογιστή, φέρουν σαφή επισήμανση βάσει ηλικίας σύμφωνα με το περιεχόμενό τους. Οι ηλικιακές διαβαθμίσεις προσφέρουν καθοδήγηση στους καταναλωτές (ιδίως τους γονείς), βοηθώντας τους να αποφασίσουν αν θα αγοράσουν ή όχι ένα συγκεκριμένο προϊόν.

Έλεγχος εισερχομένων μηνυμάτων για ανεπιθύμητα μηνύματα (spam). Η πλειοψηφία των παρόχων υπηρεσιών ηλεκτρονικής αλληλογραφίας ελέγχει τα εισερχόμενα μηνύματα κάθε χρήστη και χαρακτηρίζει ως ανεπιθύμητα όσα κρίνει ως τέτοια (μερικές φορές μάλιστα τα απορρίπει αυτομάτως). Ο έλεγχος χρησιμοποιεί ένα συνδυασμό διαφόρων μεθόδων όπως αυτές που περιγράφονται παραπάνω και πολύ προηγμένες τεχνικές για να εκτιμήσει την καταλληλότητα των εισερχομένων μηνυμάτων. Ωστόσο πολλές φορές ούτε αυτά τα μέτρα αρκούν και ορισμένα e-mails χαρακτηρίζονται ως spam ενώ δεν είναι, ενώ αντίθετα μερικά spam καταλήγουν στο χρήστη χωρίς χαρακτηρισμό. Για παράδειγμα οι έλεγχοι λέξεων μπορεί να αποφανθούν ότι οι ειδικοί χαρακτήρες @, /, |, \ και τα γράμματα R και G δε μπορούν φυσικά να παραγάγουν κείμενο, αλλά ένας χρήστης θα αναγνωρίσει στο συνδυασμό \/ | @ G R @ πιθανότατα ένα γνωστό φάρμακο. Έτσι το σχετικό e-mail θα «περάσει» σχετικό έλεγχο, αλλά ο παραλήπτης θα διαβάσει μια διαφήμιση για το φάρμακο.

Τέλος, στην κατηγορία αυτή περιλαμβάνονται το λ**ογισμικό καταπολέμησης των ιών** (antivirus και antispyware), όσο και το «**τείχος προστασίας**» (Firewall). Η γενική ονομασία «ιοί» καλύπτει στην πραγματικότητα μια πλειάδα κατηγοριών λογισμικών όπως (Α. Καμάρης 2014) Ιοί αρχείων (File Viruses), οι Δούρειοι ίπποι (Trojan Horses), τα Σκουλήκια (Worms), Καταγραφείς πληκτρολόγησης (Keyloggers), το Λογισμικό Spyware – Adware (ο κατάλογος δεν είναι εξαντλητικός).Το «**Τείχος προστασίας**» (Firewall) είναι ειδικό λογισμικό σχεδιασμένο ώστε να αποτρέπει ή να διακόπτει τη μη εξουσιοδοτημένη πρόσβαση από τον «έξω» κόσμο του δικτύου ή Διαδικτύου στον ή στους προστατευόμενους Η/Υ και αντίστροφα την ανεξέλεγκτη ροή πληροφορίας προς τον «έξω» κόσμο.

4.3.2 Μέθοδοι που βασίζονται στην ενημέρωση και τη διαπαιδαγώγηση

Με τον όρο διαπαιδαγώγηση δεν αναφερόμαστε αποκλειστικά στην παιδική ηλικία, αλλά γενικότερα στους χρήστες. Κατά κανόνα, οι πάροχοι περιεχομένου ή υπηρεσιών που αποτελούν δημοφιλείς «στόχους», φροντίζουν να δίνουν συμβουλές για καλές πρακτικές ασφαλείας στους χρήστες που κάνουν χρήση των ψηφιακών πόρων και υπηρεσιών τους. Για παράδειγμα, οι Τράπεζες συστηματικά συμβουλεύουν τους online πελάτες τους, όπως παρακάτω (αυθεντικό μήνυμα):

Για την προστασία σας από προσπάθειες υποκλοπής στοιχείων Κωδικού Χρήστη (User ID) , Μυστικού Κωδικού (Password) και Ηλεκτρονικού Κλειδάριθμου (i-code) μέσω της αποστολής παραπλανητικών μηνυμάτων (phishing emails), σας ενημερώνουμε ότι:

Η Τράπεζα XXXXX δεν θα σας ζητήσει ποτέ και με κανένα τρόπο (τηλεφωνικώς, μέσω e-mail ή οποιοδήποτε άλλο μέσο επικοινωνίας) τους **κωδικούς** σας User ID, Password ή το i-code.

Μην απαντάτε σε e-mail που σας ζητούν **προσωπικά σας στοιχεία.** Διαγράψτε τα αμέσως. Σε περίπτωση που έχετε ήδη απαντήσει σε τέτοιου είδους μήνυμα και έχετε συμπληρώσει στοιχεία σας, **επικοινωνήστε άμεσα** με το Κέντρο Τηλεφωνικής Εξυπηρέτησης της Τράπεζας στα

τηλέφωνα: **888888** (απο Ελλάδα) ή **888888888** (από εξωτερικό) και μη χρησιμοποιήσετε το Internet Banking της Τράπεζας πριν έλθετε σε επικοινωνία με τα παραπάνω τηλέφωνα.

Μην παρασύρεστε από συνδέσμους (links) που πιστεύετε ότι θα σας οδηγήσουν σε site της XXXXX Τράπεζας. Πάντα πληκτρολογείτε τη διεύθυνση της ιστοσελίδας μόνοι σας **(www.xxx.gr)** και **όχι** μέσω σύνδεσης (link) που πιθανόν σας σταλεί μέσω e-mail ή δημοσιεύεται σε ιστοσελίδες άλλων εταιρειών, μηχανών αναζήτησης κλπ.

Προστατεύστε τον υπολογιστή σας με προγράμματα **antivirus και antispyware** και φροντίστε για την συχνή ενημέρωσή τους με τις τελευταίες εκδόσεις.

Σε τι όμως συνίσταται αυτή η προσέγγιση, της διαπαιδαγώγησης, όταν αναφερόμαστε σε παιδιά ή εφήβους;

Κατά κάποιο τρόπο, η φωτογραφία παραπάνω συμπυκνώνει το νόημα της διαπαιδαγώγησης.

Η θάλασσα μπορεί να είναι, ή μάλλον είναι, ένας πολύ επικίνδυνος τόπος: άνθρωποι χάνονται, εξαφανίζονται, πνίγονται. Τρομακτικά βάθη ανεξερεύνητα και επικίνδυνα ζώα. Πολλοί φοβούνται τη θάλασσα.

Όμως η μητέρα της φωτογραφίας (τελικά και όλοι οι γονείς) δεν απαγορεύει την επαφή με τη θάλασσα. Αντίθετα εξοικειώνει τα παιδιά με τη θάλασσα (όπως υπονοείται στην παραπάνω φωτογραφία), την απολαμβάνει μαζί τους, τους μαθαίνει τους κανόνες για την ασφαλή «χρήση» της θάλασσας: πως κολυμπάει κανείς με ασφάλεια, πώς αντιμετωπίζει ένα πρόβλημα στη θάλασσα. Πιθανότατα θα παίξει μαζί τους στη θάλασσα, και σταδιακά τα παιδιά θα αυτονομηθούν και θα κολυμπούν μόνα τους, αλλά με ασφάλεια. Θα είναι ευχαρίστηση και για αυτήν και για τα παιδιά να έχουν στιγμές που χαίρονται τη θάλασσα μόνοι τους, αλλά και στιγμές που τη χαίρονται όλοι μαζί.

Με μια αναλογία, θα λέγαμε ότι για την ασφαλή χρήση των ψηφιακών πόρων και την ασφαλή πλοήγηση στο Διαδίκτυο, η κατακλείδα είναι να μάθει κανείς στο παιδί του (ή στο μαθητή του) κανόνες της ασφαλούς χρήσης και να το εξοικειώσει με το Διαδίκτυο μοιραζόμενος μαζί του πόρους (κείμενα, φωτογραφίες, βίντεο, ιστοχώρους, τεχνικές, ειδήσεις,...) και δραστηριότητες (πλοήγηση, παιχνίδια κ.ά.) που είναι θετικοί, ευχάριστοι, σύμφωνοι με την κουλτούρα και τις αξίες τους. Η ιδέα είναι τελικά ότι η διαπαιδαγώγηση είναι, κατά κάποιο τρόπο, το πιο ισχυρό όπλο απέναντι στα επιβλαβή ή επικίνδυνα στοιχεία του Διαδικτύου.

Η εξέλιξη των επιβλαβών ή επικίνδυνων ψηφιακών πόρων έχει μια δυναμική απρόβλεπτη και είναι δύσκολο να αντιμετωπιστούν με τεχνικά και μόνο μέσα. Αντίθετα, ο συνδυασμός προφύλαξης με τεχνικά μέσα (όπως, για παράδειγμα, τα antivirus λογισμικά) και με τη σωστή διαπαιδαγώγηση, φαίνεται να είναι ο βέλτιστος.

Αυτός είναι και ο στόχος πολλών προγραμμάτων και ψηφιακών πόρων που έχουν αναπτυχθεί για την ασφαλή χρήση των ψηφιακών πόρων και του Διαδικτύου ιδιαίτερα.

Για παράδειγμα, το project educaunet (πρόγραμμα της Ευρωπαϊκής Ένωσης, από το 2002 (ίσως και άλλα προγράμματα πριν από αυτό) είχε ως σκοπό του την παραγωγή ποικίλων μέσων και δραστηριοτήτων που θα βοηθούσαν τους νεαρούς μαθητές να υιοθετήσουν καλές πρακτικές.

Πολλές φορές τα νεαρά άτομα και ιδιαίτερα τα παιδιά έχουν εσφαλμένες ιδέες ως προς το τι συνιστά κίνδυνο στο Διαδίκτυο.

Το παιχνίδι «**δενείσαισυ**» είναι ακριβώς ένα παιχνίδι ρόλων που αποσκοπεί στην ευαισθητοποίηση των νεαρών μαθητών (πρωτοβάθμιας Εκπαίδευσης) όσον αφορά τις διαπροσωπικές επικοινωνίες μέσω Διαδικτύου. Το παιχνίδι αυτό περιγράφεται λεπτομερώς στις Δραστηριότητες.

Οι εκπαιδευτικοί εξάλλου, μπορούν να συζητούν τα σχετικά θέματα όχι μόνο στη διάρκεια δραστηριοτήτων οργανωμένων ειδικά για την ασφαλή πλοήγηση, αλλά εκμεταλλευόμενοι κάθε είδους δραστηριότητα στην οποία εμπλέκονται ψηφιακοί πόροι και το Διαδίκτυο.

Στην επόμενη ενότητα περιγράφονται μια σειρά πηγών (ψηφιακών και μη-ψηφιακών) οι οποίες είναι προορισμένες να υποστηρίξουν και τις τρείς ομάδες εμπλεκομένων προσώπων, δηλαδή τους μαθητές, τους εκπαιδευτικούς και τους γονείς. Περιέχουν πολλές δραστηριότητες, οδηγίες και γενικά υλικό το οποίο είναι χρήσιμο για την αντιμετώπιση των προβλημάτων που συνδέονται με την ασφαλή χρήση γενικά των ψηφιακών πόρων. Το υλικό αυτό είναι μάλλον προσανατολισμένο προς την ενημέρωση γονέων και εκπαιδευτικών και τη διαπαιδαγώγηση των μαθητών, παρά προς τις τεχνικές λύσεις.

4.4 Ψηφιακοί και μη-ψηφιακοί πόροι υποστήριξης ατόμων για την ασφαλή πλοήγηση

Ιστοχώροι και πύλες με πληροφόρηση για απάτες, φάρσες, ψευδείς ειδήσεις και αστικούς μύθους: υπάρχουν αρκετοί ιστοχώροι που είναι αφιερωμένοι στην ανάλυση ψευδών ειδήσεων, αστικών μύθων κ.τ.ό.

Ο ιστοχώρος http://www.hoaxbusters.org/ (ο οποίος έχει αναγγείλει ότι σταματάει τη λειτουργία του) περιλαμβάνει μια μακρά λίστα από ψευδείς ειδήσεις, και οι ιστοχώροι http://hoaxes.org/ και

http://www.snopes.com/ περιλαμβάνουν πολλά σχετικά στοιχεία. Μια σειρά άλλων τέτοιων ιστοχώρων μπορεί εύκολα να εντοπιστεί στο Διαδίκτυο με μια απλή αναζήτηση.

Στην Ελλάδα, ένας ιστοχώρος για τις ψευδείς ειδήσεις είναι οι http://ellinikahoaxes.gr.

Πόσο αξιόπιστες ή «ουδέτερες» (από πολιτική ή κοινωνική άποψη) είναι οι σχετικές πηγές; Δηλαδή πόσο αντικειμενικοί είναι αυτοί οι ιστοχώροι που ελέγχουν τις ψευδείς ειδήσεις; Αυτή η εκτίμηση, τελικά, εναπόκειται στην κρίση του κάθε χρήστη. Πάντως, ο χρήστης που επιθυμεί να ελέγξει την ακρίβεια μιας είδησης, ίσως καλό θα ήταν να ελέγχει με διασταύρωση από δυο ή περισσότερες τέτοιες πηγές για να διαπιστώσει αν είναι αληθινή ή ψεύτικη (hoax).

Ιστοχώροι και πύλες για την ψηφιακή ασφάλεια: υπάρχουν πολλοί ιστοχώροι αφιερωμένοι στην ψηφιακή ασφάλεια (κυρίως των παιδιών).

Ο ιστοχώρος http://www.saferinternet.gr/ είναι ένας γνωστός ιστοχώρος που περιλαμβάνει παιχνίδια, συμβουλές (για παιδιά, εκπαιδευτικούς και γονείς), οργάνωση δραστηριοτήτων, οργάνωση σεμιναρίων, εγχειρίδια online, πληροφορίες και τα τελευταία σχετικά νέα για την ασφαλή πλοήγηση στο Διαδίκτυο. Αποτελεί τον εθνικό κόμβο ενός Ευρωπαϊκού Δικτύου για την ασφαλή πλοήγηση (Δίκτυο Insafe, https://www.betterinternetforkids.eu/) και συνεργάζεται με άλλους οργανισμούς (δημόσιους φορείς, ΜΚΟ κ.λπ.) για τη διάδοση των καλών πρακτικών που σχετίζονται με την ασφαλή πλοήγηση και συναφή θέματα. Ας σημειωθεί ότι καμπάνιες για την ασφαλή πλοήγηση διοργανώνονται και σε Ευρωπαϊκό επίπεδο, καθώς το πρόβλημα της ασφαλούς πλοήγησης στο Διαδίκτυο είναι ένα παγκόσμιο πρόβλημα. Ο κόμβος safeineternet και η Μ.Κ.Ο. που τον διαχειρίζεται συνεργάζονται με την γραμμή καταγγελιών safeline (http://www.safeline.gr/) , έναν ιστοχώρο και μια τηλεφωνική γραμμή (**help-line 210 6007686)** που έχουν ως σκοπό την παροχή βοήθειας, υποστήριξης και συμβουλών για θέματα που σχετίζονται με την ασφαλή χρήση του Διαδικτύου, του κινητού τηλεφώνου και των ηλεκτρονικών παιχνιδιών. Η safeline συνεργάζεται με το Διεθνή Σύνδεσμο Ανοικτών Γραμμών Διαδικτύου «INHOPE», ένα ενεργό και συνεργατικό δίκτυο πενήντα ενός Γραμμών Καταγγελιών σε σαράντα πέντε Χώρες παγκοσμίως για την αντιμετώπιση του παράνομου Διαδικτυακού περιεχομένου και της παιδικής σεξουαλικής κακοποίησης μέσω Διαδικτύου (Α. Καμάρης, 2014). Ανάλογες υπηρεσίες προσφέει και το Πανελλήνιο Σχολικό Δίκτυο.

Το saferinternet διαθέτει ένα συνοπτικό οδηγό με οδηγίες για τους μαθητές, για ασφαλή χρήση των ψηφιακών μέσων στη διεύθυνση:
http://www.saferinternet.gr/index.php?action=download&objId=File382

Αντίστοιχες πρακτικές οδηγίες για τους γονείς μπορούν να ευρεθούν στο:
http://www.saferinternet.gr/index.php?action=download&objId=File483

Οι οδηγίες αυτές απευθύνονται σε γονείς και έχουν ένα γενικό χαρακτήρα όπως: *π*ροτιμήστε να τοποθετήσετε τον Η/Υ σας σε χώρους, όπως είναι το σαλόνι και όχι σε υπνοδωμάτια. Έτσι θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται. Κάντε την πλοήγηση στο Internet μία οικογενειακή δραστηριότητα. Χρησιμοποιείστε τον Η/Υ μαζί με τα παιδιά σας. Ενημερώστε τα παιδιά σας για τους κινδύνους που υπάρχουν όταν συνομιλούν με αγνώστους μέσω chatrooms κ.τ.ό

Παρομοίως η Πύλη Ψηφιακής Ασφάλειας για την Α' Γυμνασίου περιλαμβάνει πολλά στοιχεία για την ψηφιακή ασφάλεια, με προεξάρχοντα τις οδηγίες προς γονείς, εκπαιδευτικούς και μαθητές καθώς και ένα διαδικτυακό παιχνίδι (χρειάζεται όμως ο χρήστης να έχει λογαριασμό στο ΠΣΔ, Πανελλήνιο Σχολικό Δίκτυο για να συμμετάσχει). Ο ιστοχώρος παρέχει και ένα εγχειρίδιο της

Αρχές Διασφάλισης Απορρήτο Επικοινωνιών για την ασφαλή χρήση ψηφιακών υπηρεσιών επικοινωνίας: http://www.adae.gr/fileadmin/cybersecurity/index.html.

Σχετική είναι και η δράση της Ελληνικής Εταιρείας Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο (το Δεκέμβριο του 2016, η ιστοσελίδα της Εταιρείας δε λειτουργούσε και είχε παρουσία μόνο στο Facebook)

Η Μη-Κυβερνητική Οργάνωσης «Συνήγορος του Παιδιού» μέσω ενός κλειστού ηλεκτρονικού φόρουμ της Κοινότητας Εφήβων Συμβούλων του Συνηγόρου του Παιδιού, δημιούργησε τη Συνταγή Ασφαλούς Πλοήγησης στο Διαδίκτυο η οποία παρουσιάζεται στην εικόνα που ακολουθεί (Α. Καμάρης, 2014):

https://issuu.com/synigorostoypaidioy/docs/syntagi_prostasia_internet (η εικόνα μπορεί να μεγενθυθεί):

Δημόσιοι φορείς που υποστηρίζουν την ασφαλή πλοήγηση και χρήση ψηφιακών πόρων: υπάρχουν πολοί δημόσιοι φορείς που υποστηρίζουν την ασφαλή πλοήγηση στο Διαδίκτυο, όπως (ενδεικτικά):

- το Τμήμα Ασφαλούς Διαδικτύου της Μονάδας Εφηβικής Ηλικίας (Μ.Ε.Υ.), που λειτουργεί από τη Β' Παιδιατρική Κλινική του Πανεπιστημίου Παίδων «Π. & Α. Κυριακού» για εφήβους ηλικίας 11 έως 18 ετών και τις οικογένειες τους προσφέροντας υπηρεσίες, μεταξύ άλλων και οι δυσκολίες που αντιμετωπίζουν οι νέοι σχετικά με την ορθή χρήση του Διαδικτύου
- η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας. Σύμφωνα με τον (Α. Καμάρη, 2014), η υπηρεσία αυτή έχει ως αποστολή την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών που διαπράττονται με τη χρήση του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

4.4.1 Αντιμετώπιση του κυβερνοεκφοβισμού

Δεν είσαι μόνος, δεν είσαι ο μόνος

Παρατίθενται μερικές συμβουλές για τους γονείς και τους εκπαιδευτικούς και αφορούν τη σχέση των παιδιών με τον διαδικτυακό εκφοβισμό (σύμφωνα με οδηγίες από σχετικους ιστοχώρους):

- Μιλήστε στα παιδιά για το διαδικτυακό εκφοβισμό όπως θα το κάνατε για άλλα είδη εκφοβισμού, και προτρέψτε τα να έρθουν σε εσάς αν ποτέ οποιοσδήποτε τους προκαλέσει αναστάτωση στο διαδίκτυο, στο κινητό τους ή άλλες συσκευές. Ρωτήστε το παιδί πράγματα όπως:
- Αν έλαβε ποτέ κάποιο email ή γραπτό μήνυμα που το αναστάτωσε.
- Αν ανάρτησε κανείς στο διαδίκτυο μια φωτογραφία ή ένα βίντεο με το παιδί, χωρίς να του ζητήσει την άδεια.
- Αν συμμετείχε στον εκφοβισμό κάποιου άλλου στο διαδίκτυο ή μέσω του κινητού του.
- Αν το παιδί σας, σας πει ότι έχει πέσει θύμα διαδικτυακού εκφοβισμού, προσφέρετέ του και πρακτική και συναισθηματική υποστήριξη:
- Καθησυχάστε το, πως έπραξε ορθά λέγοντάς σας τι συμβαίνει.
- Εξηγήστε ότι δεν πρέπει να απαντά στον εκφοβισμό, καθώς αυτό θα μπορούσε να χειροτερέψει τα πράγματα.
- Καθίστε με το παιδί να καταγράψετε το περιστατικό εκφοβισμού και να συλλέξετε στοιχεία, π.χ. σώζοντας γραπτά μηνύματα ή εκτυπώνοντας email και στιγμιότυπα οθόνης από ιστοτόπους. Μην σβήσετε τίποτε.
- Εκμεταλλευθείτε στο μέγιστο τα ενσωματωμένα εργαλεία στις υπηρεσίες διαδικτύου ή κινητής τηλεφωνίας του παιδιού σας, ώστε να αποτρέψετε περαιτέρω εκφοβισμό. Για παράδειγμα, μπορείτε να αφαιρέσετε από τις λίστες των «φίλων» αυτόν που διέπραξε τον εκφοβισμό και να ρυθμίσετε το προφίλ κοινωνικής δικτύωσης του παιδιού σας ώστε να είναι «απόρρητο», αν δεν είναι ήδη.
- Επικοινωνήστε με τον πάροχο των υπηρεσιών διαδικτύου, κινητής τηλεφωνίας ή κοινωνικής δικτύωσης. Αν ό,τι συνέβη παραβαίνει τους Όρους Χρήσης ή τις Οδηγίες Κοινότητας του παρόχου, αυτός μπορεί να αναστείλει το λογαριασμό του ατόμου που διέπραξε τον εκφοβισμό, να καταργήσει περιεχόμενο ή να εγκαταστήσει νέο αριθμό κινητού, για παράδειγμα.
- Αν το παιδί σας πιστεύει πως αυτός που διέπραξε τον εκφοβισμό είναι συμμαθητής του, μιλήστε στο δάσκαλό του.
- Αν πιστεύετε ότι διεπράχθη έγκλημα ή αν ανησυχείτε ότι το παιδί σας διατρέχει άμεσο κίνδυνο, επικοινωνήστε με την αστυνομία και συγκεκριμένα με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Αν πιστεύετε ότι το παιδί σας θα μπορούσε να χρησιμοποιεί νέες τεχνολογίες για να εκφοβίσει κάποιον άλλον:

- Μιλήστε του σχετικά με το διαδικτυακό εκφοβισμό και εξηγήστε γιατί αυτό είναι απαράδεκτο και πρέπει να σταματήσει.
- Συζητήστε ανοιχτά με το παιδί σας. Ρωτήστε το γιατί το κάνει κι ακούστε τι έχει να σας πει.
- Αν δεν είχε συνειδητοποιήσει πως αυτό που έκανε ήταν εκφοβισμός, εξηγήστε του ότι ο εκφοβισμός δεν είναι απλώς σωματικός. Το να χρησιμοποιείς την τεχνολογία για να πειράζεις, να εξευτελίζεις και να διαβάλλεις, είναι επίσης εκφοβιστική συμπεριφορά.
- Μιλήστε στο δάσκαλό του σχετικά με το τι συμβαίνει και δείξτε του ότι είστε πρόθυμος να συνεργαστείτε με το σχολείο ώστε να εξασφαλίσετε πως δεν θα ξανασυμβεί.

- Καθησυχάστε το παιδί σας, πως ακόμη το αγαπάτε, αλλά ξεκαθαρίστε του ότι η συμπεριφορά του πρέπει να αλλάξει.
- Προτρέψτε το να μιλήσει σε εσάς ή σ' ένα δάσκαλο, για οποιονδήποτε εκφοβισμό στον οποίον είναι μάρτυρας, συμπεριλαμβανομένων των περιστατικών διαδικτυακού εκφοβισμού.

5 Πολιτειότητα και Ψηφιακή Πολιτειότητα (e-citizenship): μερικά στοιχεία

Με τον όρο *πολιτειότητα* (μερικές φορές ο χρησιμοποιούμενος όρος είναι *πολιτότητα*) νοείται γενικά το δικαίωμα, αλλά και η υποχρέωση του να είναι κανείς πολίτης, δηλαδή νοείται ο πολιτικός, κοινωνικός και νομικός δεσμός που συνδέει κάποιον ως πολίτη ενός κράτους με το κράτος αυτό και συνεπάγεται ορισμένα δικαιώματα και υποχρεώσεις.

Η ιδιότητά του ατόμου ως ενεργού, συνεπούς και υπεύθυνου υποκειμένου στα πλαίσια μιας σύγχρονης διευρυμένης, [...] κοινωνίας φωτίζει, επαναδομεί και αναδομεί το περιεχόμενο της πολιτειακής του οντότητας. Ο σημερινός άνθρωπος είναι ο (ενεργός) πολίτης *ενός υπερ-τοπικού, υπερεθνικού ενδεχομένως παγκόσμιου χώρου*, μιας μη-περιοριστικής μορφής Πολιτείας που διαχέεται και διαστέλλεται στο χωρο-χρόνο, αναπτύσσεται δυναμικά και πολυδιάστατα, δημιουργώντας νέες συνθήκες μέσα στις οποίες το υποκείμενο/πολίτης εξελίσσεται. Οφείλοντας, (ως πολίτης) εξ ορισμού να ανταποκριθεί ορθολογικά, με σεβασμό, σύνεση και υπευθυνότητα σε ένα εξόχως ανομοιογενές και ετερόκλητο, πλέον, πλέγμα σχέσεων, διασφαλίζει την αρμονική του 'συμβίωση' (ως κοινωνικού όντος) εντός και εκτός πραγματικών όρων και πλαισίων, με τον κυβερνοχώρο να συνιστά και να λειτουργεί ως μια παράλληλη διάσταση της σύγχρονης Πολιτείας - *ή, ακριβέστερα, ως μιας επέκτασης της σύγχρονης Πολιτείας*. Η νέα μορφή πολιτειότητας ακολουθεί κατά πόδας τις επιταγές (και ανάγκες) της ψηφιακής εποχής, διαμορφώνοντας ένα εξελιγμένο πλαίσιο εννοιολογήσεων εντός του οποίου καλείται ο σύγχρονος πολίτης, με την εκπαίδευση ως το πιο ενδεδειγμένο μέσο ενίσχυσης της ταυτότητάς του, να βρει το δρόμο του μέσα από τις πολύπλοκες και ενίοτε αποπροσανατολιστικές ατραπούς που ορίζει η τεχνολογική πρόοδος και εξέλιξη, αποφεύγοντας [...] και τα παραπλανητικά θέλγητρα ενός σύγχρονου (κι ενίοτε α-σύγχρονου) σύμπαντος λόγων (Μαρινάκη, 2015, περίληψη)

Η πολιτειότητα θα πρέπει να νοηθεί ως κάτι ευρύτερο από την εθνικότητα, την υπηκοότητα και την ιθαγένεια (οι οποίοι είναι συγγενικοί, αλλά εν πολλοίς είναι νομικοί όροι). Το βάρος στην πολιτειότητα δίνεται ακριβώς στο πολιτικό και κοινωνικό σκέλος του ορισμού: αυτό που ενδιαφέρει είναι κατά κύριο λόγο το πώς μπορεί κανείς να διεκδικήσει τα δικαιώματά του και να ανταποκριθεί στις υποχρεώσεις του ως πολίτη, ιδιαίτερα στην ψηφιακή εποχή και στο σύγχρονο ψηφιακό οικοσύστημα. Κεντρικό ερώτημα της ψηφιακής πολιτειότητας είναι το ακόλουθο: ποιος ακριβώς είναι ο ρόλος των ατόμων, αλλά και των διαφόρων συλλογικοτήτων (ενώσεων, συλλόγων, κοινοτήτων κ.λπ.) στη διαμόρφωση του δημόσιου βίου και των πόλεων ή ακόμη και των κρατών στην ψηφιακή εποχή;

Πρόκειται για μια έννοια ρευστή, δηλαδή μια έννοια που δεν έχει ίσως έναν ακριβή ορισμό και θα πρέπει να γίνει αντιληπτή μάλλον ως ένα σύνολο από δυνατότητες, από κοινωνικές πρακτικές που εξελίσσονται (και μάλιστα γρήγορα), από έννοιες που αναπτύσσονται, από γνώσεις και δεξιότητες που έχουν ένα ιδιαίτερο νόημα στον κυβερνοχώρο. Κατ' αρχάς η e-πολιτειότητα μπορεί να

περιλαμβάνει ένα σύνολο από συναλλαγές και επικοινωνίες μεταξύ κράτους και πολίτη: ο πολίτης μπορεί, για παράδειγμα, να επικοινωνεί με τις διάφορες δημόσιες υπηρεσίες για να πληροφορηθεί για διάφορα θέματα, να αιτηθεί και να παραλάβει διάφορα πιστοποιητικά, να ρυθμίσει τις φορολογικές ή ασφαλιστικές του υποχρεώσεις. Μπορεί ακόμη να λάβει μέρος σε δημόσιες online συζητήσεις και να εκφράσει η γνώμη του για ζητήματα στα οποία η πολιτεία θέλει να έχει τα σχόλια των πολιτών. Το σύνολο των δυνατοτήτων και δραστηριοτήτων αυτού του είδους είναι γενικά γνωστό ως *ηλεκτρονική διακυβέρνηση* (e-government). Με μια γενικότερη έννοια όμως, αυτό που ονομάζουμε ψηφιακή πολιτειότητα συνδέεται με τον ψηφιακό γραμματισμό, με τον ίδιο τρόπο που η πολιτειότητα συνδέεται με τον γραμματισμό: αναμένουμε από ένα συνειδητό και καλλιεργημένο άτομο να συμπεριφέρεται υπεύθυνα ως πολίτης και μάλιστα ως ενεργός πολίτης, δηλαδή να συμμετέχει ενεργά σε αυτό που ονομάζουμε *κοινά*. Στο πλαίσιο της ψηφιακής πολιτειότητας προσπαθούμε λοιπόν να μελετήσουμε την έννοια του πολίτη, και μάλιστα του ενεργού πολίτη, όπως διαμορφώνεται στη σύγχρονη εποχή της ψηφιακής τεχνολογίας.

Η ενότητα αυτή θα μελετηθεί και μέσα από συγκεκριμένα παραδείγματα (generic examples). Πριν από αυτό να αναφέρουμε ωστόσο και μια χρήση του όρου καθαρά τεχνική (αλλά συνδεόμενη άμεσα με το θέμα της πολιτειότητας, όπως προσδιορίστηκε παραπάνω). Με τον όρο e-citizenship νοείται και η e-απόκτηση μερικής πολιτειότητας, μια μάλλον ασυνήθιστη διαδικασία απόκτησης επίσημης κάρτας παραμονής ενός «πολίτη από απόσταση», μιας «μερικής υπηκοότητας».

Για παράδειγμα, το project e-σθονία[2] (από το e- και Εσθονία, https://e-estonia.com/) που ξεκίνησε η Εσθονία το 2014, σκοπεύει να εγγράψει μέχρι το 2025 περίπου 10 εκατομμύρια «πολίτες από απόσταση», πολίτες δηλαδή οι οποίοι θα αποκτήσουν ορισμένα πολιτικά δικαιώματα στην Εσθονία, κυρίως συνδεδεμένα με επιχειρηματικότητα και γενικά την ανάπτυξη οικονομικής φύσεως δραστηριοτήτων. Παρόλο που το εγχείρημα (το οποίο είναι σε εξέλιξη την ώρα που γράφονται οι γραμμές αυτές, Δεκέμβριο του 2021) έχει καθαρά οικονομικούς στόχους, δεν έλειψαν και σχολιασμοί για τη δημιουργία e-δημοκρατιών και ίσως e-κρατών. Στην ίδια γραμμή, δηλαδή στο πλαίσιο μιας κρατικής υπόστασης στα ψηφιακά μέσα, αξίζει να αναφερθεί το εγχείρημα Second House of Sweden (SHoS[3], πληροφορίες στο σχετικό blog) δηλαδή η δημιουργία μιας Σουηδικής πρεσβείας στο περιβάλλον εικονικής πραγματικότητας Second Life από το 2007 ως το 2012.

Τα εγχειρήματα αυτά είναι για την ώρα μεμονωμένα, αλλά αυτό δεν έχει ιδιαίτερη σημασία για δυο λόγους: πρώτον γιατί δεν είναι δυνατόν να γίνουν ασφαλείς προβλέψεις και ενδεχομένως τα φαινόμενα αυτού του τύπου να πολλαπλασιαστούν και δεύτερον γιατί ακόμη και αυτά τα μεμονωμένα παραδείγματα λειτουργούν ως ερωτήματα για τις έννοιες της υπηκοότητας, του ανήκειν, του κράτους, του πολίτη. Άραγε οι έννοιες αυτές παραμένουν ίδιες και αναλλοίωτες μέσα στα σύγχρονα μηντιακά τοπία και την ψηφιακή τεχνολογία;

[2] http://eudo-citizenship.eu/commentaries/citizenship-blog/1462-welcome-to-e-stonia-e-residence-and-citizenship-in-an-electronic-republic

[3] https://secondhouseofsweden.wordpress.com/page/2/

5.1 Ψηφιακός πολίτης, e-πολιτειότητα και standards

Τα θέματα που σχετίζονται με την ψηφική πολιτειότητα και τους ψηφιακούς πολίτες, θεωρούνται πολύ σημαντικά. Έτσι πολλά κράτη αλλά και Η Ευρωπαϊκή Ένωση δημιούργησαν πλαίσια για τον προσδιορισμό των χαρακτηριστικών εκείνων που διακρίνουν τον ψηφιακό πολίτη (τα λεγόμενα standards του e-citizenship). Στα πλαίσια αυτά περιγράφονται τα επιθυμητά χαρακτηριστικά που πρέπει να καλλιεργηθούν στους σημερινούς μαθητές/σπουδαστές, αλλά και τα αντίστοιχα χαρακτηριστικά και καθήκοντα των εκπαιδευτικών, των στελεχών της εκπαίδευσης κ.λπ. Τα χαρακτηριστικά αυτά, εύκολα μπορούν να μετατραπούν σε μαθησιακούς στόχους, σε αναλυτικό πρόγραμμα, σε δραστηριότητες. Παραθέτουμε στη συνέχεια τα standards για την e-πολιτειότητα, όπως τα προσδιορίζει η Διεθνής Ένωση για τις Τεχνολογίες στην Εκπαίδευση (ISTE).

5.1.1 ΟΙ ΣΠΟΥΔΑΣΤΕΣ

Ψηφιακός Πολίτης, e-πολιτειότητα Οι μαθητές αναγνωρίζουν τα δικαιώματα, τις ευθύνες και τις ευκαιρίες που δημιουργούνται για την ίδια τη ζωή, τη μάθηση και την εργασία σε έναν διασυνδεδεμένο ψηφιακό κόσμο. Ενεργούν λοιπόν και μοντελοποιούν (αναπαριστούν) με τρόπους ασφαλείς, νόμιμους και ηθικούς. Κριτική στάση, δημιουργική, συνεργατική

Α. Οι μαθητές καλλιεργούν και διαχειρίζονται την ψηφιακή τους ταυτότητα και φήμη και έχουν επίγνωση της μονιμότητας των πράξεών τους στον ψηφιακό κόσμο. Με τον όρο «ψηφιακή ταυτότητα και φήμη» εδώ θα πρέπει να νοηθεί η παρουσία ενός ατόμου στο δημόσιο ψηφιακό χώρο όπως αυτή συγκροτείται από τις ενέργειες, διασυνδέσεις, επιλογές στόχων (tags), δημοσιευμένες φωτογραφίες, αναρτήσεις σε χώρους κοινωνικής δικτύωσης σχόλια και αναρτημένες επισκοπήσεις. Ο χρήστης, εν προκειμένω οι μαθητές, πρέπει να είναι σε εγρήγορση σχετικά με τη δημόσια εικόνα του και την πρόσληψη της εικόνας αυτής από την κοινότητα. Τα ψηφιακά ίχνη λοιπόν και γενικότερα τα ψηφιακά στοιχεία των μαθητών στον κυβερνοχώρο «τείνουν» να είναι διαρκή: η πλήρης, μόνιμη και ολοκληρωτική τους διαγραφή δεν είναι πάντοτε μια εύκολη υπόθεση – σε μερικές περιπτώσεις μπορεί να απαιτεί εξειδικευμένες τεχνικές γνώσεις που δε διαθέτει κατά κανόνα ο μέσος χρήστης και ούτε οι μαθητές φυσικά. Άρα, κατά κάποιο τρόπο, τα ίχνη των ψηφιακών αναρτήσεων, των σχολίων που κάνουν οι μαθητές, τελικά του συνόλου των ψηφιακών δεδομένων που σχετίζονται με ένα μαθητή και γενικότερα έναν πολίτη, είναι εκτεθειμένα σε κοινή θέα για μεγάλο χρονικό διάστημα – δυνητικά για πάντα. Ακόμη και όταν οι χρήστες (οι μαθητές εν προκειμένω) δίνουν τη συγκατάθεσή τους για διαχείριση των δεδομένων που σχετίζονται με αυτούς, για παράδειγμα κατά την εγγραφή τους σε μια ψηφιακή πλατφόρμα ή υπηρεσία, δεν είναι βέβαιο ότι μπορούν να αντιληφθούν τις επιπτώσεις (και μάλιστα τις μακροχρόνιες), των όρων τους οποίους αποδέχονται με την υπογραφή τους. Ακόμη πιο σύνθετο πρόβλημα είναι το σύνολο των πληροφοριών που μπορούν να εξαχθούν (data mining) συνδυάζοντας δεδομένα από διαφορετικές, φαινομενικά άσχετες πηγές – όπως η συμπεριφορά στα μέσα κοινωνικής δικτύωσης, δεδομένα από το κινητό τηλέφωνο ή την καταναλωτική συμπεριφορά, τα οποία πολλές φορές εκχωρούν οικειοθελώς οι ίδιοι οι χρήστες στις εταιρείες έναντι κάποιων εκπτωτικών κουπονιών ή άλλων δώρων – πραγματικών ή ακόμη και συμβολικών.

Β. Οι μαθητές έχουν μια θετική, ασφαλή, νομικά ορθή και ηθική συμπεριφορά όταν χρησιμοποιούν τεχνολογία, συμπεριλαμβανομένων των κοινωνικών αλληλεπιδράσεων στο διαδίκτυο ή όταν χρησιμοποιούν δικτυωμένες συσκευές – όπως είναι ψηφιακά συστήματα στο Διαδίκτυο, τα κινητά τηλέφωνα ή τα ομαδικά ψηφιακά παιχνίδια με διασυνδεδεμένους παίκτες (multi-player games). Με τον όρο «θετική συμπεριφορά» εννοείται μια συμπεριφορά στην οποία οι αλληλεπιδράσεις των

μαθητών αντικατοπτρίζουν τον τρόπο με τον οποίο οι ίδιοι μαθητές επιθυμούν να γίνονται αντιληπτοί από τους άλλους αλλά επίσης και υγιείς αλληλεπιδράσεις με την ίδια την τεχνολογία – για παράδειγμα ορθολογική διαχείριση του χρόνου για βιντεοπαιχνίδια ή γενικά στο Διαδίκτυο, θέματα εργονομίας (σωστή στάση σώματος και χεριών) και μια ισορροπημένη κατανομή του χρόνου στα ψηφιακά μέσα και του χρόνου της καθημερινής φυσικής άσκησης. Η «ασφαλής συμπεριφορά» σηματοδοτεί αλληλεπιδράσεις και ενέργειες που κρατούν το μαθητή μακριά από αρνητικά ενδεχόμενα – για παράδειγμα όταν ο μαθητής ή η μαθήτρια αλληλεπιδρά με άτομα των οποίων γνωρίζει την ταυτότητα, έχει πλήρη επίγνωση των πληροφοριών που δημοσιοποιεί και διακινεί στον κυβερνοχώρο και γενικά προστατεύει τον εαυτό του από (ψηφιακές) απάτες, από ποικίλες απόπειρες για «ψάρεμα» προσωπικών δεδομένων (phising) και ακατάλληλες πρακτικές αγορών online (e-κλοπές). «Νομικά ορθή» συμπεριφορά θα μπορούσε να χαρακτηριστεί μια συμπεριφορά που λαμβάνει υπόψή της τις νομικές συνέπειες μιας ενέργειας, για παράδειγμα σεβόμενοι το γράμμα και την ουσία της πνευματικής ιδιοκτησίας, με την αποφυγή παράνομης διείσδυσης και μεταβολής προστατευμένων δεδομένων (hacking) και αποφυγής επίσης της χρήσης της ταυτότητας ενός άλλου ατόμου. Μια συμπεριφορά μπορεί να χαρακτηριστεί ως «ηθική» όταν είναι σύμφωνη με τον ηθικό κώδικα του χρήστη, για παράδειγμα μη-συμμετέχοντας σε ενέργειες κυβερνοεκφοβισμού (cyber-bullying), «τρολαρίσματος» ή εξαπάτησης (και μάλιστα παίρνοντας θέση εναντίον τους). Ακόμη, ως ηθική συμπεριφορά χαρακτηρίζεται η αποφυγή κάθε μορφή «αντιγραφής» και οικειοποίησης ψηφιακών πόρων και ο σεβασμός της ψηφιακής ταυτότητας άλλων χρηστών.

Γ. Οι μαθητές επιδεικνύουν κατανόηση και σεβασμό για τα δικαιώματα και τις υποχρεώσεις χρήσης και διαμοίρασης της πνευματικής ιδιοκτησίας. Αντιλαμβάνονται και συμμορφώνονται με τους κανόνες που ρυθμίζουν τα πνευματικά δικαιώματα και τη δίκαιη χρήση πόρων, κάνουν ορθή παραπομπή σε πόρους που χρησιμοποιούν, απόκτηση ή παροχή άδειας χρήσης περιεχομένου, αποφεύγουν και αποθαρρύνουν τη λογοκλοπή λογοκλοπής, κατανοούν και χρησιμοποιούν τα creative commons.

Δ. Οι μαθητές διαχειρίζονται τα προσωπικά τους δεδομένα για να διατηρήσουν το ψηφιακό απόρρητο και την ασφάλεια και γνωρίζουν την τεχνολογία συλλογής δεδομένων που χρησιμοποιείται για την παρακολούθηση της πλοήγησής τους και γενικότερα των ενεργειών τους στο διαδίκτυο.

5.1.2 Θέσεις του Συμβουλίου της Ευρώπης

Σε μια ανάλογη προβληματική, το Συμβούλιο της Ευρώπης εξέδωσε οδηγίες για την Ψηφιακή Πολιτειότητα, τις οποίες κατατάσσει σε 10 θεματικές ενότητες.

ΘΕΜΑΤΙΚΗ 1: Πρόσβαση και ολοκλήρωση

Αυτή η θεματική εστιάζει στην πρόσβαση στο ψηφιακό περιβάλλον και περιλαμβάνει μια ολόκληρη σειρά δεξιοτήτων που σχετίζονται όχι μόνο με την επίλυση (των προβλημάτων) των διαφορετικών μορφών ψηφιακού χάσματος αλλά και με τις απαραίτητες δεξιότητες για τη συμμετοχή των μελλοντικών πολιτών σε ψηφιακούς χώρους ανοιχτούς σε όλες τις μειονότητες και γενικότερα στις διαφορετικές απόψεις.

ΘΕΜΑΤΙΚΗ 2: Μάθηση και δημιουργικότητα

Αυτή η θεματική αφορά όχι μόνο την επιθυμία για μάθηση αλλά και τη στάση που υιοθετούμε για τη μάθηση μέσω ψηφιακών περιβαλλόντων, σε όλη τη διάρκεια της ζωής, για να αναπτύξουμε

διαφορετικές μορφές δημιουργικότητας χρησιμοποιώντας διαφορετικά εργαλεία μέσα σε πολλαπλά και ποικίλα πλαίσια. Η θεματική καλύπτει τις δεξιότητες προσωπικής ανάπτυξης και επαγγελματικές δεξιότητες που επιτρέπουν να προετοιμαστούν οι αυριανοί πολίτες για τις προκλήσεις που θα παρουσιαστούν από εταιρείες έντασης τεχνολογίας και να τις αντιμετωπίσουν με μια αίσθηση αυτοαποτελεσματικότητας και με καινοτόμους μάλιστα τρόπους.

ΘΕΜΑΤΙΚΗ 3: Ευχέρεια στα ΜΜΕ και την Πληροφοριακή Παιδεία

Αυτή η θεματική αφορά την ικανότητα ερμηνείας, κατανόησης πάντοτε με μια κριτική ματιά, και έκφρασης της δημιουργικότητάς μας δια των ψηφιακών μέσων. Η ικανότητα διαχείρισης των μέσων ενημέρωσης και των πληροφοριών είναι μια ικανότητα που θα έπρεπε να αναπτύσσονται μέσω της εκπαίδευσης και της συνεχούς ανταλλαγής με τους πραγματικότητα που μας περιβάλλει: είναι απαραίτητο να μην αρκούμαστε στην απλή χρήση του ενός ή του άλλου μέσου ή απλά να «ενημέρωσης» για κάποιο θέμα. Ένας ψηφιακός πολίτης πρέπει να διατηρεί συνεχώς κριτική προσέγγιση αν θέλει να είναι σε θέση να συμμετέχει πλήρως και γνήσια στη ζωή της κοινότητάς του.

ΘΕΜΑΤΙΚΗ 4: Ηθική και ενσυναίσθηση

Αυτή η θεματική σχετίζεται με την ηθική της διαδικτυακής συμπεριφοράς και τις αλληλεπιδράσεις με άλλους στο Διαδίκτυο και βασίζεται κυρίως με την ικανότητα αποδοχής και κατανόησης των συναισθημάτων και των απόψεων των άλλων. Η ενσυναίσθηση είναι απαραίτητη για μια θετική διαδικτυακή εμπειρία και αξιοποίηση των ευκαιριών που προσφέρει ο ψηφιακός κόσμος.

ΘΕΜΑΤΙΚΗ 5: Υγεία και ευεξία

Οι ψηφιακοί πολίτες βρίσκονται στους ενδιάμεσους χώρους ανάμεσα στους εικονικούς και τους πραγματικούς χώρους: γι' αυτό η απόκτηση των βασικών ψηφιακών δεξιοτήτων δεν επαρκεί. Τα άτομα καλούνται επίσης να αναπτύξουν στάσεις, δεξιότητες, αξίες και γνώσεις που τους οδηγούν να γίνουν πιο ευαίσθητα σε θέματα υγείας και ευεξίας (ευ ζειν). Η Υγεία και το ευ ζειν σε έναν κόσμο πλούσιο σε ψηφιακές τεχνολογίες περιλαμβάνουν την επίγνωση των θεμάτων και των δυνατοτήτων που μπορούν να επηρεάσουν ιδιαίτερα τη σφαίρα της ευεξίας, κυρίως, αλλά όχι μόνο, σε θέματα όπως ο εθισμός στο διαδίκτυο, όπως η εργονομία, η θέση αλλά και η υπερβολική χρήση ψηφιακών και φορητών συσκευών.

ΘΕΜΑΤΙΚΗ 6: Διαδικτυακή παρουσία και επικοινωνία

Αυτός ο τομέας αφορά την ανάπτυξη, στους ψηφιακούς πολίτες, προσωπικών και διαπροσωπικών δεξιοτήτων που θα τους βοηθήσουν να διαμορφώσουν και να διατηρήσουν μια παρουσία και μια online ταυτότητα καθώς και διαδικτυακές συναλλαγές που να είναι θετικές, συνεπείς και να αντικατοπτρίζουν με πιστότητα αυτό που είναι (ο χρήστης). Η θεματική καλύπτει αρκετές δεξιότητες, συμπεριλαμβανομένης της επικοινωνίας και της ανταλλαγής διαδικτυακά μέσω εικονικών κοινωνικών χώρων και τη διαχείριση του προσωπικών δεδομένων καθώς και των ιχνών (του χρήστη).

ΘΕΜΑΤΙΚΗ 7: Ενεργή συμμετοχή

Η ενεργή συμμετοχή στο Διαδίκτυο αφορά τις δεξιότητες που οι πολίτες πρέπει να διαθέτουν για να έχουν πλήρη επίγνωση των περιβαλλόντων στα οποία εξελίσσονται προκειμένου να λάβουν σωστές αποφάσεις και να συμμετέχουν ενεργά και θετικά στους δημοκρατικούς πολιτισμούς στους οποίους ζουν.

ΘΕΜΑΤΙΚΗ 8: Δικαιώματα και υποχρεώσεις

Όπως κάθε πολίτης μιας κοινωνίας, οι ψηφιακοί πολίτες του διαδικτυακού κόσμου έχουν ορισμένα δικαιώματα και υποχρεώσεις. Μπορούν να ασκήσουν, μεταξύ άλλων, τα δικαιώματά τους στον σεβασμό της ζωής, την ιδιωτικότητα, ασφάλεια, πρόσβαση και ένταξη, καθώς και την ελευθερία έκφρασης. Αλλά αυτά τα δικαιώματα συνοδεύονται από μια σειρά ευθυνών, όπως η ηθική και η ενσυναίσθηση, καθώς και άλλες που στοχεύουν στη διασφάλιση ενός ψηφιακού περιβάλλοντος χωρίς κινδύνους και υπεύθυνο για όλον τον κόσμο.

ΘΕΜΑΤΙΚΗ 9: Απόρρητο και ασφάλεια

Αυτός ο τομέας καλύπτει δύο διαφορετικές έννοιες: η ιδιωτικότητα αφορά ουσιαστικά την προσωπική προστασία του χρήστη, τις δικές τους πληροφορίες στο Διαδίκτυο και τις πληροφορίες άλλων ατόμων, ενώ η ασφάλεια συνδέεται στενά με την επίγνωση του χρήστη για τις ενέργειες και τις συμπεριφορές στο Διαδίκτυο. Αυτός ο τομέας αφορά διάφορες δεξιότητες όπως η καλή διαχείριση των προσωπικών πληροφοριών που δημοσιεύονται στο Διαδίκτυο καθώς και πληροφοριών άλλων ατόμων ή αυτό που σχετίζονται με την διαδικτυακή ασφάλεια (χρήση φίλτρων πλοήγησης, κωδικούς πρόσβασης, λογισμικό προστασίας από ιούς και τείχος προστασίας, κ.λπ.) για την αποφυγή επικίνδυνων ή δυσάρεστων καταστάσεων.

ΘΕΜΑΤΙΚΗ 10: Ευαισθητοποίηση του καταναλωτή

Ο Ιστός, με όλες του τις διαστάσεις, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης ή άλλων εικονικών, κοινωνικών χώρων, είναι ένα περιβάλλον μέσα στο οποίο, συχνά, ο ψηφιακός πολίτης είναι και καταναλωτής. Κατανοήστε τις επιπτώσεις της δικής σας επιχειρηματικής πραγματικότητας μέσα σε πολυάριθμους διαδικτυακούς χώρους είναι μια από τις δεξιότητες που τα άτομα θα πρέπει να αποκτήσουν εάν θέλουν να μπορέσουν να διατηρήσουν τη δική τους αυτονομία ως ψηφιακοί πολίτες.

Είναι φανερό (και αναμενόμενο) ότι τα Standards του ISTE για τους σπουδαστές και οι οδηγίες του Συμβουλίου της Ευρώπης συγκλίνουν σε πολλά σημεία. Το βήμα που απομένι να γίνει είναι η αξιοποίησή τους στην εκπαιδευτική τους πρακτική, η δημιουργία διδακτικών δραστηριοτήτων και η υιοθέτηση ανάλογων στάσεων και πρακτικών από τους εκπαιδευτικούς που να είναι βασισμένες πάνω στις οδηγίες αυτές.

5.2 Η post-truth, τα fake-news και η παραπλάνηση των πολιτών.

Επιστρέφοντας στη μελέτη της ψηφιακή πολιτειότητα όπως προσδιορίστηκε παραπάνω, προτείνεται ένα θέμα για μελέτη: η έννοια του post-truth (μετα-αλήθεια) και των fake-news (ψευδείς ειδήσεις και ψευδοειδήσεις)

Post-truth κατά λέξη σημαίνει «μετα-αλήθεια». Ο όρος αυτός επελέγη ως *λέξη του 2016*[4] από τα Oxford Dictionaries ενώ η αντίστοιχη λεξη «Postfaktisch» (post-factual) επελέγη από την Εταιρεία

[4] https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016

για τη Γερμανική Γλώσσα[5]. Πρόκειται για επίθετα που χαρακτηρίζουν φαινόμενα τα οποία σχετίζονται με ή προσδιορίζουν περιστάσεις στις οποίες τα αντικειμενικά γεγονότα έχουν μικρότερη απήχηση στο σχηματισμό της κοινής γνώμης από όση έχουν τα συναισθήματα και τα προσωπικά «πιστεύω».

Ο όρος φαίνεται ότι υπάρχει εδώ και πολύ καιρό (ίσως και είκοσι ή παραπάνω χρόνια), αλλά έχει καταστεί ιδιαίτερα σημαντικός με την έλευση και την επικράτηση του Διαδικτύου. Σήμερα τα πλαστά νέα και «μετα-αλήθειες» αποτελούν πια μια συνηθισμένη πρακτική. Ο πρώην Αμερικανός Πρόεδρος Μπ. Obama, λίγο πριν την αποχώρησή του δήλωσε «στο νέο οικοσύστημα των μέσων ενημέρωσης τα πάντα είναι αλήθεια και τίποτα δεν είναι αλήθεια».

Τα τελευταία χρόνια, δυο γεγονότα με μεγάλη πολιτική σημασία, οι προηγούμενες Αμερικανικές εκλογές και πριν λίγα χρόνια το Brexit σημαδεύτηκαν από μια ασταμάτητη ροή ψευδών ειδήσεων και ψευδο-ειδήσεων, μερικές από τις οποίες είναι εξώφθαλμα λανθασμένες, αλλά παρόλα αυτά, υπάρχει πάντοτε ένα κοινό που τις πιστεύει. Παρόμοια φαινόμενα είδαμε και στον καιρό της πανδημίας.

Για τον τρόπο με τον οποίο δημιουργούνται αυτές οι ειδήσεις υπάρχει μεγάλη σχετική πληροφόρηση στο Διαδίκτυο. Αναφέρεται ένα χαρακτηριστικό κείμενο το οποίο εξετάζει το φαινόμενο από πολλές πλευρές: https://insidestory.gr/article/post-truth?token=C50B57L6F7

Βέβαια, σε ένα πλαίσιο κριτικής προσέγγισης των νέων που κυκλοφούν στο Διαδίκτυο, αυτά που αναφέρονται στο άρθρο πρέπει επίσης να επαληθευτούν. Για παράδειγμα, ένα σχετικό πρόσφατο άρθρο στους NY Times, αναφέρει ότι έρευνα που διεξήχθη πρόσφατα δείχνει ότι τελικά τα κοινωνικά δίκτυα ίσως δε συμβάλλουν ιδιαίτερα στη δημιουργία κλίματος πόλωσης στην πολιτική ζωή[6].

Στο ίδιο πλαίσιο, η ιδέα της οργανωμένης και συστηματικής δημιουργίας ακόμη και ψεύτικων λογαριασμών[7], είναι μια πρακτική που εφαρμόζεται σε μεγάλες κλίμακες. Η ίδια η Ευρωπαϊκή Επιτροπή εξέδωσε σχετικές οδηγίες για την καταπολέμηση των φαινομένων αυτών[8] Έτσι και αλλιώς τα μεγάλα κοινωνικά δίκτυα όπως το facebook και το twitter πολλές φορές έχουν αναγγείλει δημόσια την πρόσθεσή τους να καταπολεμήσουν τα fake-news. Γενικότερα πάντως οργανώνονται αρκετές δράσεις για τον περιορισμό και τον έλεγχο των ψευδών ειδήσεων, όπως στο: https://opengov.ellak.gr/2017/04/17/share-the-facts-mia-efarmogi-enantia-stis-psevdis-idisis/

5.3 Ποια είναι η πρακτική σημασία της e-πολιτειότητας για την Εκπαίδευση;

Από την πλευρά των εκπαιδευτικών, το ερώτημα είναι βέβαια το ακόλουθο: ποια είναι η σημασία και οι πρακτικές επιπτώσεις όλων αυτών των προσεγγίσεων για την Εκπαίδευση; Σίγουρα τα

[5] https://www.facebook.com/Gesellschaft-f%C3%BCr-deutsche-Sprache-186994827990942/

[6] https://www.nytimes.com/2017/04/13/us/political-polarization-internet.html?emc=edit_tnt_20170417&nlid=42819549&tntemail0=y&_r=0

[7] http://www.bbc.com/news/technology-31710738

[8] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52019JC0012&from=IT

μεγάλα πολιικά γεγονότα επηρεάζουν τις ζωές όλων μας, αλλά η πολιτική, με τη στενή έννοια, μένει μάλλον έξω από τους σχολικούς τοίχους.

Το βασικό συμπέρασμα όμως που συνάγεται από όλες τις παραπάνω περιπτώσεις είναι ότι οι μαθητές πρέπει να αποκτήσουν μια κριτκή στάση απέναντι στις πηγές που χρησιμοποιούν από το Διαδίκτυο, τόσο για τις σχολικές εργασίες τους, όσο και σε άλλες περιπτώσεις. Για παράδειγμα, θέματα που σχετίζονται με την οικολογία, συχνά αποτελούν αντικείμενα παραπληροφόρησης ή post-truth στόχους. Στο άρθρο που προτείνεται παραπάνω για τις post-truth, αναφέρεται ότι «*μια ερμηνεία της κλιματικής αλλαγής από έναν νομπελίστα φυσικό δείχνει ακριβώς ίδια στη ροή των ειδήσεων του Facebook, με την άποψη ενός αρνητή της που μισθοδοτείται από τους αδελφούς Κοχ» (μεγιστάνες του πετρελαίου)».* Είναι λοιπόν σχεδόν βέβαιο ότι οι μαθητές, είτε στο πλαίσιο εργασιών για το σχολείο, είτε σε άλλη περίσταση, θα έρθουν αντιμέτωποι με ειδήσεις, πληροφορίες, συζητήσεις, των οποίων το περιεχόμενο δε θα είναι αυταπόδεικτά ορθό. Οι μαθητές, σε κάθε περίπτωση θα πρέπει να επιζητούν τον έλεγχο και τη διασταύρωση για την επαλήθευση ή διάψευση των σχετικών πληροφοριών.

Όπως είναι φανερό, η έλξη που μπορούν να ασκήσουν ψεύτικες ή διαστρεβλωμένες ειδήσεις και πληροφορίες μπορεί να είναι μεγάλη, κυρίως όταν είναι σε συμφωνία με τις ιδέες του εκάστοτε χρήστη ή τα κοινωνικά στερεότυπα. Οι ευάλωτοι νεαροί μαθητές μπορούν δυσκολότερα να διακρίνουν το ψέμμα, τη διαστρέβλωση, την υπερβολή στην πληροφόρηση (είτε πρόκειται για πληροφόρηση ακαδημαϊκού χαρακτήρα, είτε για πληροφόρηση ειδησεογραφικού χαρακτήρα).

Οι εκπαιδευτικοί, με συστηματικό τρόπο, εκμεταλλευόμενοι κάθε ευκαιρία, θα πρέπει να διδάξουν στους μαθητές, έμμεσα ή άμεσα, την αξία της κριτικής στάσης απέναντι σε πληροφορίες και ειδήσεις που δεν επιβεβαιώνονται από πολλαπλές ανεξάρτητες πηγές. Από την άλλη πλευρά, θα πρέπει εξίσου επίμονα, να αναδεικνύουν τις θετικές πλευρές τοτυ ψηφιακού οικοσυστήματος στο οποίο καλούνται να ζήσουν οι μαθητές.

6 Πολιτειότητα, e-Πολιτειότητα και Τεχνητή Νοημοσύνη

Η εκπαίδευση στην ψηφιακή πολιτειότητα δίνει έμφαση στην εφαρμογή της Τεχνητής Νοημοσύνης (Artificial Intelligence) σε εκπαιδευτικά πλαίσια. Τα τελευταία χρόνια η Τεχνητή Νοημοσύνη (ΤΝ) εμφανίζεται να επιδρά σημαντικά σε πολλούς τομείς της καθημερινής ζωής και ιδιαίτερα στην εκπαίδευση, δημιουργώντας ευκαιρίες αλλά και πολυάριθμες απειλές οι οποίες καθιστούν αναγκαία τη συνεκτίμηση των αρχών των ανθρωπίνων δικαιωμάτων κατά την πρώιμη φάση σχεδιασμού της εφαρμογής της. Σε αυτή τη γραμμή και σύμφωνα με σχετική σύσταση από την Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης (Recommendation, 2019): «*Οι εκπαιδευτικοί πρέπει να έχουν επίγνωση των δυνατών και αδύνατων σημείων της τεχνητής νοημοσύνης στη μάθηση, ώστε να ενδυναμωθούν -και όχι να εξουδετερωθούν- από την τεχνολογία στις δικές τους πρακτικές εκπαίδευσης στην ψηφιακή πολιτειότητα .... Οι εξελίξεις στον τομέα της ΤΝ μπορούν να επηρεάσουν βαθιά τις αλληλεπιδράσεις μεταξύ εκπαιδευτικών και εκπαιδευομένων και μεταξύ των πολιτών γενικότερα, οι οποίες μπορεί να υπονομεύσουν τον ίδιο τον πυρήνα της εκπαίδευσης, δηλαδή την καλλιέργεια της ελεύθερης βούλησης και της ανεξάρτητης και κριτικής σκέψης μέσω ευκαιριών μάθησης ... Αν και φαίνεται πρόωρη η ευρύτερη χρήση της ΤΝ σε μαθησιακά περιβάλλοντα, οι επαγγελματίες στο χώρο της εκπαίδευσης και προσωπικό των σχολείων θα πρέπει να ενημερωθούν για την ΤΝ και τις ηθικές προκλήσεις που θέτει για τα σχολεία*».

Η ΤΝ υπηρετεί ωστόσο την εκπαίδευση για περισσότερα από σαράντα χρόνια (Benedict du Boulay, 2023; Watters, 2021). Ως αποτέλεσμα έχουν αναπτυχθεί διάφορα εργαλεία/περιβάλλοντα που παρέχουν εξατομικευμένη υποστήριξη, συστάσεις και συμβουλές σε εκπαιδευτικούς ή εκπαιδευόμενους όπως τα προσαρμοστικά περιβάλλοντα μάθησης, ευφυή συστήματα διδασκαλίας, ευφυή διαδραστικά περιβάλλοντα μάθησης ή εξατομικευμένα συστήματα μάθησης (Holmes et al., 2022). Στα τέλη του 20ού αιώνα, η μεγαλύτερη πρόοδος που σημειώθηκε στην ΤΝ αφορούσε τη συμβολική ΤΝ (symbolic AI) ή ΤΝ που βασίζεται σε κανόνες (rule-based AI), αλλά η πρόοδος ανακόπηκε από πολλαπλά εμπόδια, οδηγώντας σε ύφεση στην ανάπτυξή της. Στις αρχές του 21ου αιώνα, χάρη στους πολύ ταχύτερους επεξεργαστές και τη διαθεσιμότητα τεράστιων όγκων δεδομένων (που προέρχονται κυρίως από το διαδίκτυο), η Μηχανική Μάθηση (Machine Learning) έγινε κυρίαρχη και οδήγησε στα περισσότερα από τα σημαντικά επιτεύγματα της ΤΝ τα τελευταία χρόνια όπως η αυτόματη μετάφραση μεταξύ γλωσσών και το ChatGPT. Αυτή είναι εμπνευσμένη από τον τρόπο με τον οποίο είναι δομημένος ο ανθρώπινος εγκέφαλος (οι νευρώνες του) και η οποία εξάγει συμπεράσματα από συνήθως μεγάλες ποσότητες δεδομένων. Η περιοχή της παραγωγικής ΤΝ (Generative AI) αξιοποιεί τεχνικές από τον τομέα της μηχανικής μάθησης και αναπτύσσεται ραγδαία. Ωστόσο αυτά τα συστήματα ΤΝ μπορεί να είναι ιδιαίτερα ευαίσθητα και μια μικρή αλλαγή για παράδειγμα σε μια οδική πινακίδα μπορεί να εμποδίσει ένα σύστημα αναγνώρισης εικόνας που βασίζεται σε ΤΝ να την αναγνωρίσει. Μπορούν επίσης να είναι μεροληπτικά, επειδή τα δεδομένα στα οποία εκπαιδεύονται είναι μεροληπτικά (Access Now, 2018). Ενώ οι επιδόσεις των γλωσσικών μοντέλων τεχνητής νοημοσύνης, όπως το ChatGPT-3, χαρακτηρίζονται ως εντυπωσιακές, συχνά γράφουν ανακρίβειες.

Η διαφημιστική εκστρατεία γύρω από την ΤΝ μπορεί ωστόσο να οδηγήσει σε μη ρεαλιστικές προσδοκίες, περιττά εμπόδια και εστίαση στην ΤΝ ως πανάκεια και όχι ως εργαλείο που μπορεί να υποστηρίξει θετικές επιπτώσεις (Berryhill et al. 2019: 27). Ιδιαίτερα, η ενσωμάτωση της ΤΝ στην εκπαίδευση όχι μόνο πρέπει να ενδυναμώσει τους μαθητές/φοιτητές με ικανότητες που σχετίζονται με την αποτελεσματική ενασχόληση με την ΤΝ, αλλά και να αντιμετωπίσει ηθικά ζητήματα που προκύπτουν κατά την αξιοποίηση και ανάπτυξή της.

Έτσι με σκοπό την πιο συστηματική ανάλυση της σχέσης ΤΝ και Εκπαίδευσης, το 2021, το Συμβούλιο της Ευρώπης (ΣτΕ) - ένας διεθνής οργανισμός που ιδρύθηκε το 1949 για την προάσπιση των ανθρωπίνων δικαιωμάτων, της δημοκρατίας και του κράτους δικαίου στην Ευρώπη - συγκρότησε ομάδα εμπειρογνωμόνων για να διερευνήσει και να προτείνει ένα νομικό πλαίσιο για την εφαρμογή της ΤΝ στην εκπαίδευση και να αναπτύξει μια σειρά συστάσεων για τη διδασκαλία της ΤΝ (Γραμματισμός στην ΤΝ) για τα κράτη μέλη συμβάλλοντας στη διασφάλιση της εφαρμογής και της διδασκαλίας της ΤΝ στην εκπαίδευση για το κοινό καλό. Για περισσότερες πληροφορίες δείτε την αναφορά με τίτλο «ARTIFICIAL INTELLIGENCE AND EDUCATION. A critical view through the lens of human rights, democracy and the rule of law» (Holmes, Persson, Chounta, Wasson, and Dimitrova, 2022).

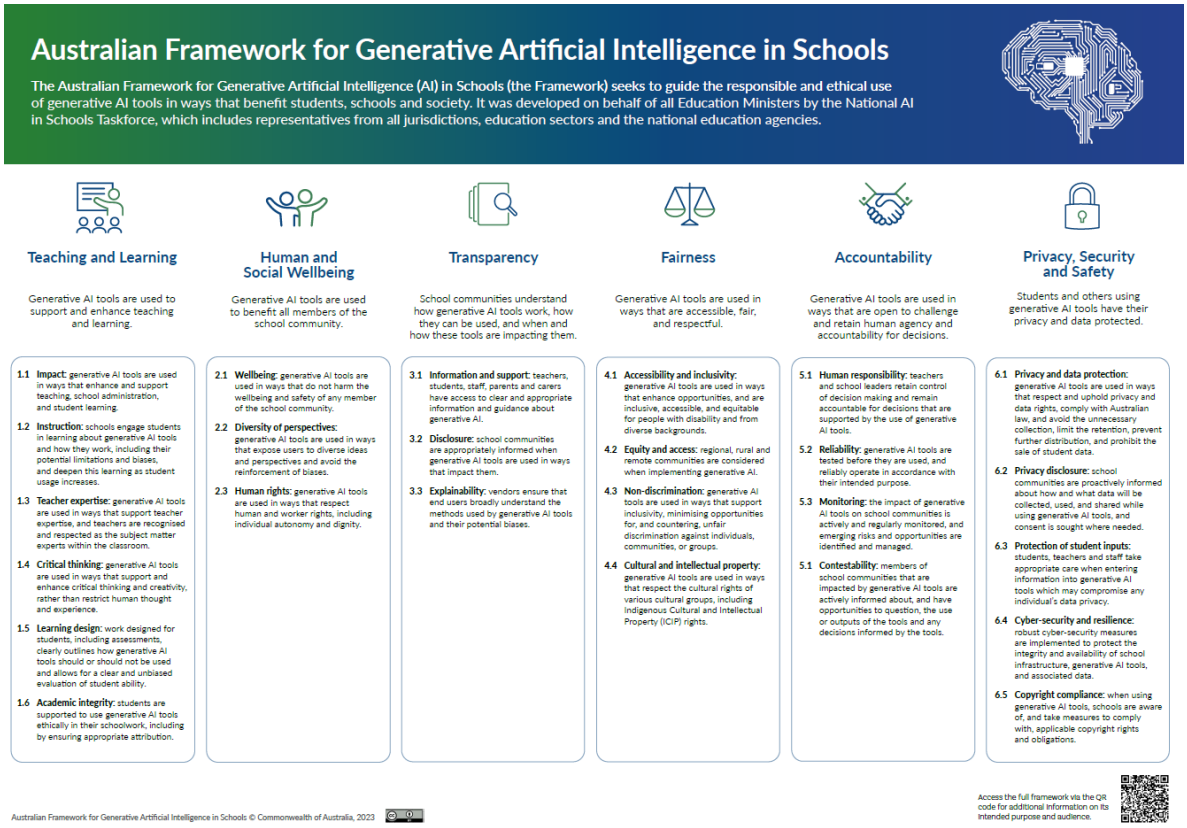
Ως θεμελιώδεις ικανότητες για την ανάπτυξη γραμματισμού στην Τεχνητή Νοημοσύνη (ΤΝ) θεωρούνται γνώσεις, δεξιότητες, στάσεις και αξίες στις ακόλουθες περιοχές (Ng κ.ά., 2021): γνώση και κατανόηση της ΤΝ, χρήση και εφαρμογή της ΤΝ, αξιολόγηση και δημιουργία ΤΝ, ηθική. Εδώ είναι σημαντικό να υπογραμμισθεί ότι σκοπός της εκπαίδευσης σε θέματα ΤΝ είναι να ενισχυθεί μεν η τεχνική επάρκεια στις τεχνολογίες και εφαρμογές ΤΝ αλλά και η κατανόηση για την ύπαρξη κοινωνικών επιπτώσεων και των ηθικών διαστάσεων που συνδέονται με τις τεχνολογίες ΤΝ.

Πιο συγκεκριμένα, τέσσερις σημαντικές διαστάσεις του γραμματισμού στην ΤΝ αποτελούν (Ng et al., 2021):

1. *γνώση και κατανόηση της ΤΝ*: οι μαθητές, εκτός από τελικοί χρήστες, θα πρέπει να κατανοούν τις βασικές τεχνικές και έννοιες που κρύβονται πίσω από τις εφαρμογές ΤΝ. Αυτές συνδέονται με δεξιότητες, όσο και με την αυτοπεποίθηση και την ετοιμότητά τους για μάθηση ΤΝ. Με το σκοπό αυτό προτείνονται αναλυτικά προγράμματα και δραστηριότητες για την πρωτοβάθμια και δευτεροβάθμια εκπαίδευση (Lin et al. (2021, Τσιωτάκης, 2023). Επίσης σημαντική είναι και η ανάπτυξη της επίγνωσης των μαθητών ώστε να αναγνωρίζουν τις εφαρμογές που αξιοποιούν ΤΝ και να κατανοούν τη λειτουργία τους (Wang et al., 2023).
2. *χρήση και εφαρμογή της ΤΝ*: οι μαθητές θα πρέπει να εφαρμόζουν και να χρησιμοποιούν αποτελεσματικά την ΤΝ σε διάφορες εργασίες στην καθημερινή ζωή.
3. *αξιολόγηση και δημιουργία ΤΝ*: ικανότητες που επιτρέπουν στα άτομα να αξιολογούν κριτικά τις τεχνολογίες ΤΝ, να επικοινωνούν και να συνεργάζονται αποτελεσματικά με εφαρμογές ΤΝ. Ιδιαίτερα η αξιολόγηση εμπλέκει δεξιότητες ανάλυσης, επιλογής και κριτικής αποτίμησης εφαρμογών ΤΝ και των αποτελεσμάτων τους.
4. *ηθική*: ενίσχυση επίγνωσης των ευθυνών και των κινδύνων που συνδέονται με την ΤΝ (Wang et al., 2023). Έχει διαπιστωθεί ότι τα συστήματα τεχνητής νοημοσύνης αναπαράγουν προκαταλήψεις (Ntoutsi et al., 2020) και τα συστήματα μηχανικής μάθησης απαιτούν εκπαίδευση σε μεγάλα σύνολα δεδομένων, γεγονός που οδηγεί σε ζητήματα δεοντολογίας και πνευματικών δικαιωμάτων. Η ενσωμάτωση επομένως της ΤΝ στην εκπαίδευση χρειάζεται να αντιμετωπίσει ζητήματα όπως η προκαταλήψεις, η δικαιοσύνη και τα πνευματικά δικαιώματα.

Η ενσωμάτωση της ΤΝ στην εκπαίδευση αποτελεί μια αναγκαία αλλαγή που αφορά τόσο την ανάπτυξη ικανοτήτων στους μαθητές και εκπαιδευτικούς, όσο και τη βελτίωση της εκπαιδευτικής διαδικασίας και την αντιμετώπιση εκπαιδευτικών ανισοτήτων. Ωστόσο αυτό χρειάζεται να συμβεί με τρόπο που να διασφαλίζεται ότι η ΤΝ χρησιμοποιείται υπεύθυνα και με ασφάλεια προστατεύοντας τα δικαιώματα των μαθητών και της εκπαιδευτικής κοινότητας. Σε αυτή την κατεύθυνση, η UNESCO ανέπτυξε έναν Οδηγό για το GenAI στην εκπαίδευση με σκοπό «να υποστηρίξει τις χώρες να υλοποιήσουν άμεσες δράσεις, να σχεδιάσουν μακροπρόθεσμες πολιτικές και να αναπτύξουν ανθρώπινες ικανότητες για να εξασφαλίσουν ένα ανθρωποκεντρικό όραμα αυτών των νέων τεχνολογιών.» (Holmes and Fengchun, 2023).

Κάποιες χώρες επίσης έχουν προχωρήσει στην κατάρτιση εθνικών σχεδίων για την ΤΝ στην Εκπαίδευση που θέτουν σαφείς κατευθυντήριες γραμμές για την ενσωμάτωση της ΤΝ στα εκπαιδευτικά προγράμματα (δείτε Εικόνα 1: The Australian Framework for Generative AI in Schools).



Εικόνα 1: The Australian Framework for Generative AI in Schools. Διαθέσιμο εδώ https://www.education.gov.au/schooling/resources/australian-framework-generative-artificial-intelligence-ai-schools

7 ΒΙΒΛΙΟΓΡΑΦΙΑ

"**Spam e-mails produce the same amount of greenhouse gas as 3,1 million cars**", *Mail Online,* 15 April 2009; www.dailymail.co.uk/sciencetech/article-1170177/Spam-emails-produce-greenhouse-gas-3-1million-cars.html (τελευταία επίσκεψη το Δεκέμβριο 2023)

Αθανάσιος Καμάρης (2014) Κίνδυνοι και ασφάλεια στο Διαδίκτυο για τη νεολαία: Μία κριτική επισκόπηση, Πτυχιακή Εργασία, Αθήνα, Τμήμα Πληροφορικής

Commonwealth of Australia, Dealing with offensive content (Greek), *Cybersmart*, 2015; www.cybersmart.gov.au/Parents/Resources/Educate%20yourself/Dealing%20with%20offensive%20content%20Greek.aspx (τελευταία επίσκεψη το Νοέμβριο του 2020)

Cooper, G. (2023). Examining Science Education in ChatGPT: An Exploratory Study of Generative Artificial Intelligence. *J Sci Educ Technol* 32, 444–452. https://doi.org/10.1007/s10956-023-10039-y

Cotton, D.R.E., Cotton, P.A. & Shipway, J. R. (2023). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International*. DOI: 10.1080/14703297.2023.2190148

Fiona Fui-Hoon Nah, Ruilin Zheng, Jingyuan Cai, Keng Siau & Langtao Chen (2023) Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration, *Journal of Information Technology Case and Application Research*, 25:3, 277-304, https://doi.org/10.1080/15228053.2023.2233814

Floridi, L., Chiriatti, M. (2020). GPT-3: Its Nature, Scope, Limits, and Consequences. *Minds & Machines* 30, 681–694. https://doi.org/10.1007/s11023-020-09548-1

Francois Ewald (1986) L'Etat providence, Grasset, Paris

http://tech.in.gr/presentations/article/?aid=1231217957 (τελευταία επίσκεψη το Δεκέμβριο 2023)

http://www.addictionrecov.org/Addictions/index.aspx?AID=43 (τελευταία επίσκεψη το Δεκέμβριο 2023)

Internet Addiction Disorder,

Jennifer M. Warner-Blankenship (2011), What are "Internet dangers?', *Education Technology Center,* https://wiki.uiowa.edu/pages/viewpage.action?pageId=49483037 (τελευταία επίσκεψη το Δεκέμβριο 2023)

Kasneci, E., Seßler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdel, C., Pfeffer, J., Poquet, O., Sailer, M., Schmidt, A., Seidel, T. Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. Learning and Individual Differences, 103, 1–9. https://doi.org/10.1016/j.lindif.2023.102274

Matthew J. Volkmann (2010) Internet Dangers, *Education Technology Center,* https://wiki.uiowa.edu/display/edtech/Internet+Dangers (τελευταία επίσκεψη το Δεκέμβριο 2023)

Matzakos, N., Doukakis, S. & Moundridou, M. (2023). Learning Mathematics with Large Language Models: A Comparative Study with Computer Algebra Systems and Other Tools. *International Journal of Emerging Technologies in Learning (iJET), 18*(20), 51-71. Kassel, Germany: International Journal of Emerging Technology in Learning. Retrieved February 9, 2024 from https://www.learntechlib.org/p/223774/.

Nigerian scams: https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams (τελευταία επίσκεψη το Δεκέμβριο 2023)

S. Mansell (2016) "*WFU expert cautions new internet myths may be more harmful*", Wake Forest University, 6 Jun. 2003; www.wfu.edu/wfunews/2003/060603r.html (Τελευταία επίσκεψη το Νοέμβριο του 2020).

Spamming, Wikipedia: https://en.wikipedia.org/wiki/Spamming (τελευταία επίσκεψη το Δεκέμβριο 2023)

wikipedia https://en.wikipedia.org/wiki/Internet_addiction_disorder καθώς και https://el.wikipedia.org/wiki/Εθισμός_στο_Διαδίκτυο (τελευταία επίσκεψη το Δεκέμβριο 2023)

Ακατάλληλο ή παράνομο υλικό, *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου;* www.saferinternet.gr/index.php?childobjId=Category120&objId=Category38&parentobjId=Page2 (τελευταία επίσκεψη το Νοέμβριο του 2023)

Ακατάλληλο Περιεχόμενο, *Ελληνικό Κέντρο Ασφαλούς Διαδικτύου*; www.saferinternet.gr/index.php?objId=Category291&parentobjId=Page187 (τελευταία επίσκεψη το Νοέμβριο του 2023)

Ανεπιθύμητη Αλληλογραφία (Spam), *Κέντρο Δικτύων Ε.Μ.Π., 06 Οκτ. 2010;* www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104 (τελευταία επίσκεψη το Δεκέμβριο 2023)

Γιώργος Μπάλιας (2009) ΠΕΡΙΒΑΛΛΟΝΤΙΚΟΙ ΚΙΝΔΥΝΟΙ: ΔΙΑΠΛΟΚΗ ΕΠΙΣΤΗΜΗΣ, ΔΙΚΑΙΟΥ ΚΑΙ ΠΟΛΙΤΙΚΗΣ, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα, 2009

Ένας ιστοχώρος για την καταπολέμηση του spam: http://spam.abuse.net/overview/whatisspam.shtml, (τελευταία επίσκεψη το Δεκέμβριο 2023)

Καριοφύλλης Α., "Ανεπιθύμητα e-mails (spam)", W-Learn: *Πρόσβαση στη Γνώση*, 2005-2014; www.wlearn.gr/index.php/2010-07-29-17-58-43-v15-214/219--emails-spam (τελευταία επίσκεψη το Δεκέμβριο 2023)

Κίνδυνοι: Αποξένωση από τον πραγματικό κόσμο, *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_apoxenosi.html (τελευταία επίσκεψη το Δεκέμβριο 2023)

Κίνδυνοι: Εκφοβισμός (Cyberbulling) *Παιδαγωγικό Ινστιτούτο Κύπρου: Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_ekfobismos.html (Τελευταία επίσκεψη το Νοέμβριο του 2020).

Μαρινάκη Μ. (2015) «Ψηφιακή Πολιτειότητα και Εκπαίδευση. Η ιδιότητα του πολίτη σήμερα: εννοιολογήσεις και προβληματισμοί», Διεθνές Συνέδριο για την Ανοικτή & εξ Αποστάσεως Εκπαίδευση, Τόμος 8, http://dx.doi.org/10.12681/icodl.47

Παιδαγωγικό Ινστιτούτο Κύπρου: *Ασφάλεια στο Διαδίκτυο* (2010) www.pi.ac.cy/InternetSafety/kindinoi_anepithminimata.html (τελευταία επίσκεψη το Δεκέμβριο 2023)

Παιδαγωγικό Ινστιτούτο Κύπρου: *Ασφάλεια στο Διαδίκτυο,* 2010; www.pi.ac.cy/InternetSafety/kindinoi_akatalperiex.html (τελευταία επίσκεψη το Νοέμβριο του 2020)

Σε ποιον κόσμο ζεις; Ελληνικό Κέντρο Ασφαλούς Διαδικτύου; www.saferinternet.gr/ (τελευταία επίσκεψη το Δεκέμβριο 2023)

Τι είναι ένα λογισμικό καταπολέμησης των ιών http://ti-einai.gr/antivirus/ (τελευταία επίσκεψη το Δεκέμβριο 2023)

Τολούδης Α. (2012) "Τι συμβαίνει όταν τα avatar εισβάλλουν στη ζωή μας", *Τεχνολογικές Συναντήσεις,* 16 Οκτ. 2012.

Τσιωτάκης Π. (2023). Το ChatGPT για εκπαιδευτικούς και μαθητές. Εκδόσεις Σαββάλας.

Χριστίνα Μπάνου (2010) Ο θρίαμβος της ανάγνωσης, http://www.bookpress.gr/afieromata/aprilios/o-thriamvos-tis-anagnosis (τελευταία επίσκεψη το Δεκέμβριο 2023)