

ΣΧΕΔΙΟ ΜΑΘΗΜΑΤΟΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΕΣ ΕΝΗΛΙΚΩΝ/ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Όνομα Ενότητας: Επικοινωνία και Συνεργασία	
Υπο-Ενότητα 4 Τίτλος: Ψηφιακή Πολιτότητα	
Σχέδιο Μαθήματος 35 – Κώδικας Δεοντολογίας στο Διαδίκτυο	
Διάρκεια: 90 λεπτά	
Στόχος	Ο κύριος στόχος αυτού του σχεδίου μαθήματος είναι η παροχή όλων των απαραίτητων πληροφοριών σχετικά με τα ψηφιακά δικαιώματα και τις υποχρεώσεις, την ψηφιακή ασφάλεια και ιδιωτικότητα και την ψηφιακή υγεία και ευεξία.
Ομάδα-στόχος	Ενήλικες (τρίτης ηλικίας)
Εγκατάσταση/ Εξοπλισμός	• Τάξη • Πρόσβαση στο Διαδίκτυο • Προτζέκτορας • Λευκός Πίνακας (Πίνακας Μαρκαδόρου)
Εργαλεία/ Υλικά	• Συνοδευτικό υλικό 1 • Συνοδευτικό υλικό 2 • Συνοδευτικό υλικό 3
Βασικές εργασίες	1. Εργασία 1: Εισαγωγή στον κώδικα δεοντολογίας στο διαδίκτυο 1.1 Ξεκινήστε την εργασία με το βίντεο: https://www.youtube.com/watch?v=FWMk_Zv7nB8&ab_channel=AngelRivera (3 λεπτά) 1.2 Ερωτήσεις για το βίντεο (15 λεπτά) • Τι είναι ο "κώδικας δεοντολογίας στο διαδίκτυο" • Γιατί ο κώδικας δεοντολογίας στο διαδίκτυο είναι σημαντικός; 2. Εργασία 2: Βασικοί κανόνες δεοντολογίας στο διαδίκτυο - Τι πρέπει να κάνετε στο Διαδίκτυο! 2.1 Οι εκπαιδευτές θα πρέπει, να εξηγήσουν στους μαθητές ορισμένους βασικούς κανόνες δεοντολογίας και συμβουλές, για το τι πρέπει να κάνουν στο διαδίκτυο (βλ. Συνοδευτικό υλικό 1) (20 λεπτά)

	3. Εργασία 3: Τι <u>ΔΕΝ</u> πρέπει να δημοσιεύετε στο διαδίκτυο; Βασικές συμβουλές! 3.1 Ξεκινήστε την εργασία με το βίντεο: https://www.youtube.com/watch?v=iup8_fLhCiQ&ab_channel=Vickpoint (3 λεπτά) 3.2 Οι εκπαιδευτές θα πρέπει, να εξηγήσουν στους μαθητές ορισμένους βασικούς κανόνες συμπεριφοράς και συμβουλές, για το τι ΔΕΝ πρέπει να δημοσιεύουν στο διαδίκτυο (βλ. Συνοδευτικό υλικό 2) (20 λεπτά) 4. Εργασία 4: Συμβουλές αυτοπροστασίας ! 4.1 Οι εκπαιδευτές θα πρέπει, να δώσουν στους μαθητές μερικές συμβουλές, για το τι πρέπει να προσέχουν και τι πρέπει να αποφεύγουν, όταν και πριν δημοσιεύσουν κάτι στο Διαδίκτυο (βλ. Συνοδευτικό υλικό 3) (20 λεπτά) 5. Εργασία 5: Σύνοψη (10 λεπτά)
--	--

ΣΥΝΟΔΕΥΤΙΚΟ ΥΛΙΚΟ 1: Βασικοί κανόνες και συμβουλές του Κώδικα Δεοντολογίας στο Διαδίκτυο

1. Κάντε τους πραγματικούς ανθρώπους προτεραιότητά σας: Όταν είστε με ανθρώπους στην πραγματική ζωή, ασχοληθείτε μαζί τους και όχι με τις ηλεκτρονικές συσκευές σας!

2. Θυμηθείτε το κοινό σας – Να γνωρίζετε πού βρίσκεστε: Οι κανόνες συμπεριφοράς διαφέρουν, ανάλογα με το τι κάνετε στο διαδίκτυο!

3. Να δείχνετε σεβασμό: Μην ξεχνάτε ότι όταν είστε στο διαδίκτυο, αλληλεπιδράτε με πραγματικούς ανθρώπους, ακόμη και αν βλέπετε μόνο ένα όνομα χρήστη ή μια εικόνα. Ως εκ τούτου, πρέπει να είστε ευγενικοί και να έχετε σεβασμό! Μην ενεργείτε, όπως δε θα ενεργούσατε και στον πραγματικό κόσμο.

4. Να είστε ηθικοί: Ακολουθήστε τους νόμους και τους κανόνες (γραπτούς ή άγραφους), όπως θα κάνατε στον πραγματικό κόσμο. Να θυμάστε ότι υπάρχουν ηθικές συνέπειες σε όλες τις πράξεις μας!

5. Διατηρείστε μια καλή εικόνα του εαυτού σας στο διαδίκτυο - Μοιραστείτε με διακριτικότητα: Να είστε προσεκτικοί με το περιεχόμενο που μοιράζεστε. Είναι καλύτερο, να μην μοιράζεστε κάτι ντροπιαστικό, παράνομο ή ακατάλληλο! Σκεφτείτε δύο φορές, πριν δημοσιεύσετε κάτι στο διαδίκτυο!

6. Σεβαστείτε το χρόνο των άλλων ανθρώπων: Όταν δημοσιεύετε κάτι στο διαδίκτυο, κάνετε ένα σχόλιο ή στέλνετε ένα μήνυμα/ email, χρειάζεται χρόνος για να διαβαστεί από τους άλλους! Θα πρέπει να διασφαλίσετε, ότι ο χρόνος που δαπανείται μέχρι την ανάγνωση της ανάρτησής σας, δεν είναι χαμένος χρόνος!

7. Σεβασμός της ιδιωτικής ζωής των άλλων ανθρώπων: Θα πρέπει να είστε πολύ προσεκτικοί, όταν χειρίζεστε πληροφορίες, στις οποίες έχετε προνομιακή πρόσβαση και αφορούν άλλους! Πρέπει να διασφαλίσετε, ότι δεν μοιράζεστε προσωπικές πληροφορίες άλλων και δεν χρησιμοποιείτε ποτέ τους λογαριασμούς ή τις συσκευές τους χωρίς άδεια!

8. Έλεγχος γεγονότων πριν από την αναδημοσίευση: Το διαδίκτυο είναι γεμάτο με πληροφορίες που προέρχονται από κάθε είδους πηγές. Θα πρέπει να είστε προσεκτικοί κατά την παροχή ή την κοινή χρήση πληροφοριών. Θα πρέπει να ελέγξετε όλα όσα διαβάσατε, ειδικά πριν το δημοσιεύσετε ξανά!



9. Απαντήστε άμεσα στους άλλους: Εάν σας απευθυνθεί κάποιος στο διαδίκτυο, περιμένει προφανώς να επικοινωνήσετε μαζί του ή να του απαντήσετε. Συνιστάται να το κάνετε!

10. Ενημέρωση διαδικτυακών πληροφοριών: Μην αφήνετε ανακριβείς ή λανθασμένες πληροφορίες στο διαδίκτυο, εάν μπορείτε να τις διορθώσετε!

11. Μοιραστείτε τις γνώσεις σας: Μία από τις βασικές αρχές των διαδικτυακών κοινοτήτων είναι η κοινοποίηση! Εάν έχετε γνώσεις ή εμπειρία σχετικά με ένα συγκεκριμένο θέμα να είστε ευγενικοί και να το μοιραστείτε με τους άλλους!

12. Διατηρήστε τη διαφωνία υγιή: Δεν είναι κακό να διαφωνείτε με κάποιον στο διαδίκτυο! Απλά να θυμάστε, ότι όταν έχετε μια διαφωνία, είναι σημαντικό να παραμείνετε ευγενικοί και να ξέρετε πότε να σταματήσετε!

13. Μην φωνάζετε, παρακαλώ: Υπάρχει χρόνος και χώρος για τα πάντα - ΑΛΛΑ ΣΤΙΣ ΠΕΡΙΣΣΟΤΕΡΕΣ ΠΕΡΙΠΤΩΣΕΙΣ Η ΠΛΗΚΤΡΟΛΟΓΗΣΗ ΜΕ ΟΛΑ ΤΑ ΓΡΑΜΜΑΤΑ ΚΕΦΑΛΑΙΑ ΕΙΝΑΙ ΑΚΑΤΑΛΛΗΛΗ. Οι περισσότεροι αναγνώστες τείνουν να την αντιλαμβάνονται, ως φωνές! Γι' αυτό, σας παρακαλώ, μην το κάνετε!

14. Διαβάστε πρώτα, σκεφτείτε πριν ρωτήσετε: Εάν κολλήσετε με μια ερώτηση, είναι καλύτερο να αναζητήσετε μια απάντηση στο διαδίκτυο, πριν ρωτήσετε άλλους. Τις περισσότερες φορές δεν θα χρειαστεί να συμπεριληφθούν τρίτα μέρη.

15. Μείνετε στο θέμα: Όταν υπάρχει μια συζήτηση στο διαδίκτυο είναι εύκολο να απομακρυνθείτε από το αρχικό θέμα, ειδικά όταν υπάρχουν πολλοί άνθρωποι που συμμετέχουν σε αυτό! Η παραμονή στο θέμα εξασφαλίζει ότι οι περιττές πληροφορίες και τα σχόλια δεν εμποδίζουν τους άλλους, από το να βρουν τις χρήσιμες πληροφορίες.



ΣΥΝΟΔΕΥΤΙΚΟ ΥΛΙΚΟ 2: Τι ΔΕΝ πρέπει να δημοσιεύετε στο διαδίκτυο; Βασικές συμβουλές

1.

Η προσωπική σας τοποθεσία: Η κοινοποίηση της προσωπικής σας τοποθεσίας μπορεί να είναι επικίνδυνη. Η ενημέρωση των ανθρώπων σχετικά με το πού βρίσκεστε, μπορεί δυνητικά να είναι επιβλαβής για εσάς, καθώς επιτρέπει σε όσους θέλουν να σας ενοχλήσουν, να γνωρίζουν πού βρίσκεστε και σε πιθανούς κλέφτες να γνωρίζουν πού δε βρίσκεστε (π.χ. δε βρίσκεστε στο σπίτι σας, όταν είστε σε διακοπές).

2.

Η διεύθυνση κατοικίας ή ο προσωπικός σας αριθμός τηλεφώνου: Η διεύθυνση και οι αριθμοί τηλεφώνου είναι δύο σημεία δεδομένων, που μπορούν να χρησιμοποιήσουν οι διαδικτυακοί κλέφτες για να κλέψουν την ταυτότητά σας! Όπως δε θα φωνάζατε τη διεύθυνση ή τον αριθμό τηλεφώνου σας σε δημόσιο χώρο στον πραγματικό κόσμο, σας συμβουλεύουμε να κάνετε το ίδιο και στο διαδίκτυο!

3.

Η οικονομική σας κατάσταση - Τραπεζικά στοιχεία και στοιχεία κάρτας: Είναι σημαντικό να διατηρήσετε αυτές τις πληροφορίες ιδιωτικές! Η κοινοποίηση πληροφοριών οικονομικής κατάστασης μπορεί να κινήσει το ενδιαφέρον των διαδικτυακών κλεφτών ταυτότητας! Οι φωτογραφίες οποιωνδήποτε τραπεζικών στοιχείων και λεπτομερειών πιστωτικής κάρτας θα πρέπει να αποφεύγονται με κάθε κόστος!

4.

Πληροφορίες, φωτογραφίες και βίντεο άλλων χωρίς να ερωτηθούν: Αν θέλετε να μοιραστείτε περιεχόμενο που περιλαμβάνει άλλους, θα πρέπει πρώτα να πάρετε την άδειά τους. Θα πρέπει να έχουν την επιλογή για το, αν θέλουν το περιεχόμενο αυτό στο διαδίκτυο ή όχι!

5.

Περιεχόμενο "Ενηλίκων" – Ακατάλληλες προσωπικές εικόνες: Το Διαδίκτυο είναι ένας δημόσιος χώρος, ακόμα και όταν νομίζετε ότι μοιράζεστε κάτι ιδιωτικά. Έτσι, πριν δημοσιεύσετε μια selfie με το μαγιό σας, σκεφτείτε, αν είστε εντάξει με το να σας βλέπουν έτσι στο γραφείο ή παιδιά.

6.

Ψευδείς ή αναληθείς δηλώσεις: Η κοινοποίηση ψευδών ή αναληθών πληροφοριών είναι λάθος! Πόσο μάλλον όταν πρόκειται για ένα συγκεκριμένο άτομο!

7.

Απειλές: Όπως δεν είναι καλό, να απειλείς ανθρώπους στην πραγματική ζωή ανεξάρτητα από τη θέση τους, το ίδιο ισχύει και στο διαδίκτυο!

8.

Εικόνες παιδιών: Είναι δύσκολο, αν όχι αδύνατο, να έχετε τον έλεγχο στις πληροφορίες άπαξ και αναρτηθούν στο διαδίκτυο! Οι εικόνες των παιδιών πρέπει να αποφεύγονται στο διαδίκτυο, καθώς κανείς δεν ξέρει, πώς θα τις χρησιμοποιήσουν οι άλλοι. Μπορούν να αποτελέσουν πηγή διαδικτυακού εκφοβισμού ή ακόμα και επίθεσης από επικίνδυνους ανθρώπους!

ΣΥΝΟΔΕΥΤΙΚΟ ΥΛΙΚΟ 3: Συμβουλές αυτοπροστασίας!

- 1. Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης.** Μάθετε τι είναι ένας ισχυρός κωδικός πρόσβασης και πώς να τον δημιουργήσετε! Να θυμάστε, ότι συνιστάται να χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για διαφορετικές υπηρεσίες.
- 2. Ψάξτε για κρυπτογράφηση.** Προσπαθήστε, να χρησιμοποιείτε υπηρεσίες που προσφέρουν κρυπτογράφηση (μάθετε πώς)! Να θυμάστε, ότι το e-mail δεν είναι κρυπτογραφημένο, οπότε μην μοιράζεστε ποτέ προσωπικές πληροφορίες μέσω αυτού!
- 3. Εγκαταστήστε λογισμικό προστασίας από ιούς.** Μάθετε για την προστασία από ιούς και τη σημασία της εδώ.
- 4. Να είστε προσεκτικοί με τα μηνύματα ηλεκτρονικού ταχυδρομείου / συνδέσμους και συνημμένα.** Μην εμπιστεύεστε μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία και συνημμένα από αγνώστους! Μάθετε περισσότερα εδώ!
- 5. Βεβαιωθείτε ότι οι συσκευές σας είναι ενημερωμένες.** Βεβαιωθείτε ότι οι συσκευές σας και οι υπηρεσίες που χρησιμοποιείτε είναι ενημερωμένες! Οι ενημερώσεις συχνά περιλαμβάνουν κρίσιμες ενημερώσεις κώδικα για τυχόν κενά ασφαλείας, που ενδέχεται να έχουν εντοπιστεί στα προγράμματα ή τις συσκευές σας. Μάθετε περισσότερα εδώ!
- 6. Χρησιμοποιήστε έλεγχο ταυτότητας δύο παραγόντων όταν είναι διαθέσιμος.** Ο έλεγχος ταυτότητας δύο παραγόντων απαιτεί, να επαληθεύσετε την ταυτότητά σας αφού συνδεθείτε ακόμα και αν δώσετε το όνομα χρήστη και τον κωδικό πρόσβασής σας. Σε ορισμένες περιπτώσεις, θα σας ζητηθεί να επαληθεύσετε την ταυτότητά σας, εισάγοντας έναν κωδικό που αποστέλλεται μέσω μηνύματος στο τηλέφωνό σας ή μέσω ηλεκτρονικού ταχυδρομείου.
- 7. Αποφύγετε τη χρήση μη ασφαλούς δημόσιου Wi-Fi.** Θα πρέπει να αποφεύγετε να συνδέεστε στο διαδίκτυο, χρησιμοποιώντας μη ασφαλές δημόσιο Wi-Fi στις συσκευές σας. Η χρήση του μπορεί να σας κάνει ευάλωτους σε επιθετικές πρακτικές. Αυτός ο σύνδεσμος εξηγεί γιατί!
- 8. Να προσέχετε από πού συνδέεστε - αποφύγετε τη χρήση δημόσιων υπολογιστών.** Οι δημόσιοι υπολογιστές δεν είναι τόσο ασφαλείς όσο ο προσωπικός υπολογιστής, οπότε πρέπει να είστε προσεκτικοί! Ακολουθήστε τις συμβουλές για να διατηρήσετε τον εαυτό σας ασφαλή!
- 9. Τέλος, όπως έχουμε ήδη αναφέρει, ΝΑ ΠΡΟΣΕΧΕΤΕ ΤΙ ΔΗΜΟΣΙΕΥΕΤΕ ΣΤΟ ΔΙΑΔΙΚΤΥΟ!**