**Δομή Σχεδίου Μαθήματος 2**

**1. ΤΑΥΤΟΤΗΤΑ ΣΧΕΔΙΟΥ ΜΑΘΗΜΑΤΟΣ**

#### **Τίτλος Σχεδίου Μαθήματος: Διαδίκτυο: Ένας ολόκληρος κόσμος γεμάτος μυστικά**

***Δημιουργός/οί***

***Βαθμίδα – Τάξη: Στ’ Δημοτικού***

***Εμπλεκόμενες γνωστικές περιοχές και συμβατότητα με ΠΣ***

- ***Γνωστικό αντικείμενο*** Πληροφορική

***Θεματικό πεδίο***: Υπολογιστικά συστήματα, ψηφιακές συσκευές, Δίκτυα

***Θεματική ενότητα:*** Δίκτυα υπολογιστών και το διαδίκτυο

- ***Προσδοκώμενα μαθησιακά αποτελέσματα όπως αναφέρονται στο ΠΣ***

* Να περιγράφουν την έννοια του διαδικτύου των πραγμάτων (‘’*internet of things’’*) και τις μελλοντικές του εφαρμογές στην ανθρώπινη δραστηριότητα.
* Να αναγνωρίζουν τις αρνητικές επιπτώσεις και τους κινδύνους από τη χρήση του διαδικτύου.
* Να γνωρίζουν και να λαμβάνουν απλά μέτρα πρόληψης απέναντι στις αρνητικές πτυχές του ψηφιακού κόσμου.
* Να ερμηνεύουν την επίδραση του διαδικτύου των πραγμάτων (‘’*internet of things’’*) στην καθημερινή μας ζωή.
* Να γνωρίζουν τις έννοιες του pharming, phishing και hacking και να αναζητούν πληροφορίες σχετικά με αυτές, αναλύοντας τις προεκτάσεις τους και προτείνοντας μέσα πρόληψης.

- Σ***χέση με άλλες θεματικές ενότητες ή/και θεματικά πεδία του γνωστικού αντικειμένου ή/και άλλα γνωστικά αντικείμενα***

**Διαθεματική προσέγγιση με άλλα γνωστικά αντικείμενα**

**Κοινωνική και πολιτική αγωγή (Στ’ Δ): Κεφ. 1: «Η Οικουμενική Διακήρυξη των δικαιωμάτων του ανθρώπου» (Ενότητα 4η: Το άτομο και η διεθνής κοινότητα).** Μετά από δύο παγκόσμιους πολέμους, τα κράτη αποφάσισαν να προστατέψουν τα δικαιώματα του ανθρώπου, όπως το δικαίωμα **της ζωής, της αξιοπρέπειας, της ασφάλειας, της ελευθερίας, της μόρφωσης, της ίσης προστασίας από το νόμο**. Στις 10 Δεκεμβρίου του 1948 η Γενική Συνέλευση των Ηνωμένων Εθνών υιοθέτησε την **Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου**, με την οποία τα κράτη αναγνώρισαν τα ατομικά, πολιτιστικά, οικονομικά, πολιτικά και κοινωνικά δικαιώματα του ανθρώπου. Παράλληλα, διακήρυξαν ότι τα ανθρώπινα δικαιώματα αποτελούν διεθνή ευθύνη και όχι μόνο εσωτερική υπόθεση των κρατών.
Από το 1948 και εξής η Οικουμενική Διακήρυξη δεσμεύει όλα τα κράτη. Με αυτόν τον τρόπο διασφαλίζεται ότι τα δικαιώματα του ανθρώπου γίνονται σεβαστά από όλα τα κράτη και ισχύουν για όλους τους πολίτες, ανεξάρτητα από το φύλο, τη γλώσσα, την καταγωγή ή τη θρησκεία τους. To συγκεκριμένο κεφάλαιο συνδυάζεται με Τα δικαιώματα των παιδιών σε σχέση με το διαδίκτυο, όπως παρουσιάζονται στην ιστοσελίδα saferinternetgr.

Πώς χρησιμοποιούμε μια οικιακή συσκευή; Πώς δίνουμε πληροφορίες και οδηγίες για να χρησιμοποιήσουμε το διαδίκτυο;

***-Χρονική διάρκεια:*** Το διδακτικό σενάριο προβλέπεται να διαρκέσει 1 διδακτική ώρα (1 μάθημα).

**2. *ΣΚΕΠΤΙΚΟ ΣΧΕΔΙΟΥ ΜΑΘΗΜΑΤΟΣ*– ΕΠΙΣΤΗΜΟΝΙΚΟ/ΓΝΩΣΤΙΚΟ ΠΕΡΙΕΧΟΜΕΝΟ**

* Οι μαθητές θα γνωρίσουν την έννοια του ***διαδικτύου των πραγμάτων*** (internet of things) και την επιρροή του στην ανθρώπινη δραστηριότητα («έξυπνα» σπίτια, wearable συσκευές για παρακολούθηση της φυσικής κατάστασης των χρηστών).
* Θα κατανοήσουν τις έννοιες pharming, phishing και hacking, ενώ θα προτείνουν μέσα πρόληψης και προστασίας.
* Θα κατανοήσουν το γεγονός ότι ως χρήστες του διαδικτύου έχουν δικαιώματα και υποχρεώσεις.

Μια κοινή παρανόηση των μαθητών είναι η αντίληψη ότι γνωρίζουν «σε βάθος» το διαδίκτυο, επειδή κάποιοι, και ίσως οι περισσότεροι, χρησιμοποιούν κατά κόρον μέσα κοινωνικής δικτύωσης, είτε διαθέτουν συσκευές υψηλής ποιότητας αλλά και τιμής. Είναι σημαντικό να αναφερθεί ότι ελάχιστοι μαθητές γνωρίζουν την έννοια του ***διαδικτύου των πραγμάτων*** (internet of things) με τον συγκεκριμένο όρο, παρά το γεγονός ότι διαθέτουν πλήθος συσκευών που ανήκουν σε αυτό .

**3. ΠΡΟΑΠΑΙΤΟΥΜΕΝΕΣ ΓΝΩΣΕΙΣ ΚΑΙ ΕΠΙΘΥΜΗΤΕΣ ΔΕΞΙΟΤΗΤΕΣ**

Οι μαθητές/τριες είναι σημαντικό να έχουν έρθει σε επαφή με συσκευές που αποτελούν το ***διαδικτύο των πραγμάτων*** (internet of things), ακόμα κι αν δε γνωρίζουν τον όρο αυτό. Είναι απαραίτητο να έχουν πλοηγηθεί σε ιστοσελίδες και μέσα κοινωνικής δικτύωσης.

**4. ΣΚΟΠΟΣ ΣΧΕΔΙΟΥ ΜΑΘΗΜΑΤΟΣ - ΠΡΟΣΔΟΚΩΜΕΝΑ ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ**

**Διδακτικός σκοπός**: Οι μαθητές αναμένεται να αναγνωρίζουν τους πιθανούς κινδύνους του Διαδικτύου, όπως pharming, phishing και hacking. Η πιο διαδεδομένη μέθοδος κλοπής ταυτότητας (identity theft) είναι το “phishing”. Η τεχνική του “**pharming**” αποτελεί μέθοδο εξαπάτησης μέσω του διαδικτύου η οποία ουσιαστικά περιλαμβάνει και το “phishing”. Εκτός, από την αναγνώριση των πιθανών κινδύνων, οι μαθητές θα γνωρίσουν τρόπους πρόληψης και αντιμετώπισης. Παράλληλα, θα γνωρίσουν τον κόσμο του ***διαδικτύου των πραγμάτων*** (internet of things) και τους τρόπους που επηρεάζει τη ζωή τους.

**Γνωστικοί Στόχοι**

Οι μαθητές πρέπει να είναι σε θέση:

* να κατανοούν τα φαινόμενα όπως pharming, phishing και hacking, ώστε να τα αναγνωρίζουν και να γνωρίζουν πιθανές οικονομικές και κοινωνικές επιπτώσεις τους..
* να περιγράφουν το **διαδίκτυο των πραγμάτων (internet of things)**, τις εφαρμογές και τις επιπτώσεις του στη ζωή των χρηστών.
* να αναγνωρίζουν τις αρνητικές επιπτώσεις και τους πιθανούς κινδύνους από τη χρήση του διαδικτύου και να λαμβάνουν μέτρα πρόληψης.

**Παιδαγωγικοί στόχοι**

* να αναπτύσσουν στρατηγικές απόκρισης στους πιθανούς κινδύνους του διαδικτύου, συμπεριλαμβανομένου και του εντοπισμού τους.
* να εξερευνούν και να αναπτύσσουν τρόπους για να κάνουν το διαδίκτυο πιο ασφαλές και χωρίς αποκλεισμούς, αναπτύσσοντας την κριτική τους ικανότητα.
* να μπορούν να πειραματίζονται και να αναλαμβάνουν πρωτοβουλίες
* να καλλιεργούν κοινωνικές δεξιότητες, να μπορούν να εργάζονται σε ομάδες και να συνεργάζονται.
* να προτείνουν λύσεις σε πιθανά προβλήματα
* να λειτουργούν συμπεριληπτικά απέναντι σε συμμαθητές τους που δυσκολεύονται με κάποια διαδικασία.

 **Στόχοι Τεχνογραμματισμού**

* να γνωρίζουν τα χαρακτηριστικά και τις μεθόδους που χρησιμοποιούνται στο pharming, το phishing και το hacking.
* να αναπτύσσουν σε ομάδες απλές τεχνικές εντοπισμού των φαινομένων αυτών.
* να χρησιμοποιούν συσκευές στο πλαίσιο του διαδικτύου των πραγμάτων.

**5. ΟΡΓΑΝΩΣΗ ΤΗΣ ΔΙΔΑΣΚΑΛΙΑΣ ΚΑΙ ΑΠΑΙΤΟΥΜΕΝΗ ΥΛΙΚΟΤΕΧΝΙΚΗ ΥΠΟΔΟΜΗ**

**Οργάνωση τάξης**

* Οι μαθητές χωρίζονται σε ομάδες των τριών-τεσσάρων μελών και η κάθε ομάδα κάθεται μπροστά σε έναν υπολογιστή (φορητό ή σταθερό). Οι δραστηριότητες είναι ομαδικές και επιδιώκεται/θεωρείται απαραίτητη η συνεργασία και η συνεχής αλληλεπίδραση ανάμεσα στα μέλη.
* Σε κάθε υπολογιστή πρέπει να υπάρχει πρόσβαση στο διαδίκτυο.

 **Υλικοτεχνική Υποδομή**

* Το διδακτικό σενάριο υλοποιείται στο εργαστήριο Πληροφορικής ή σε σχολική τάξη που διαθέτει φορητούς υπολογιστές ή tablets.
* Απαιτείται διαδραστικός πίνακας ή βιντεοπροβολέας και ένας υπολογιστής (εκπαιδευτικού) για την εισαγωγή των μαθητών στη δραστηριότητα καθώς και η ύπαρξη τοπικού δικτύου με διαμοιραζόμενο δίσκο.
* 3 συσκευές συνδεδεμένες σε Wifi τηλεχειριζόμενη πρίζα- διακόπτη (“έξυπνη πρίζα’’). Προτείνεται καφετιέρα στιγμιαίου καφέ, επιτραπέζιο φωτιστικό, ηχείο
* να υπάρχει εγκατεστημένη σε έναν υπολογιστή η εφαρμογή eWeLink, όπου θα έχει δημιουργηθεί λογαριασμός από τον εκπαιδευτικό και θα γίνεται ο χειρισμός των συσκευών μέσω Wifi.

**6. ΔΙΔΑΚΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ**

 **Ερωτήσεις-κλειδιά για τη διδασκαλία**

* Pharming
* Phishing
* Hacking
* Διαδίκτυο, πιθανοί κίνδυνοι και μέτρα πρόληψης
* Διαδίκτυο των Πραγμάτων (‘’internet of things’’)

**Υποκείμενη θεωρία μάθησης**

Το θεωρητικό πλαίσιο που βασίζεται το παρόν σενάριο στηρίζεται στη θεωρία του εποικοδομισμού και του κοινωνικοπολιτιστικού εποικοδομητισμού.

**Μέθοδοι διδασκαλίας**

Εφαρμόζεται η ομαδοσυνεργατική, η βιωματική- επικοινωνιακή μέθοδος διδασκαλίας αφού οι μαθητές δουλεύουν σε ομάδες των 3-4 μελών σε κάθε υπολογιστή και επικοινωνούν μεταξύ τους αλλά και με τον εκπαιδευτικό σε όλη τη διάρκεια της διαδικασίας. Ακόμη, αξιοποιείται η χρήση πηγών- έρευνα αλλά και η μάθηση μέσα από την ολοκλήρωση ενός κοινού έργου (Project-Based Learning). Ο ρόλος του εκπαιδευτικού είναι να βοηθά (scaffolding) και να καθοδηγεί τους μαθητές, διορθωτικά κι όχι παρεμβατικά.

**7. ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΔΙΔΑΚΤΙΚΗΣ ΠΟΡΕΙΑΣ** (ενδεικτικά: περιγραφή δραστηριοτήτων, σταδίων/φάσεων, ενεργειών εκπαιδευτικού και μαθητών)

**1η φάση**

**Διάρκεια: 10 λεπτά**

* Οι μαθητές χωρίζονται σε ομάδες των τριών-τεσσάρων μελών και η κάθε ομάδα κάθεται μπροστά σε έναν υπολογιστή (φορητό ή σταθερό) και παρακολουθούν τμήμα βίντεο (4 λεπτών περίπου) από την ταινία μικρού μήκους του ErtFlix, The internet of everything (Το διαδίκτυο όλων των πραγμάτων, από 1.37’- 5.35’), [ΕΔΩ](https://www.youtube.com/watch?v=n8zXu0CsBt0)
* Ο/Η εκπαιδευτικός έχει τοποθετήσει σε διαφορετικά σημεία της τάξης τρεις συσκευές συνδεδεμένες σε Wifi τηλεχειριζόμενη πρίζα- διακόπτη (“έξυπνη πρίζα’’). Προτείνεται καφετιέρα στιγμιαίου καφέ, επιτραπέζιο φωτιστικό, ηχείο. Τις οποίες χειρίζεται από την εφαρμογή **eWeLink**, όπου θα έχει δημιουργηθεί λογαριασμός από τον εκπαιδευτικό και θα γίνεται ο χειρισμός των συσκευών μέσω Wifi. Ο εκπαιδευτικός προτρέπει και μαθητές να δοκιμάσουν, ενώ παράλληλα προκαλεί συζήτηση για άλλες πιθανές συσκευές που μπορεί να δυνδέονται στο **Διαδίκτυο των Πραγμάτων** (‘’internet of things’’). Αναφέρεται ο όρος του «έξυπνου» σπιτιού, όπου ο έλεγχος των συσκευών γίνεται είτε τοπικά με διακόπτες ή μέσα από smartphone ή με τους βοηθούς φωνητικών εντολών ( ok Google, amazon Alexa, Hey Siri) τα θετικά και τα αρνητικά του.

**2η φάση**

**Διάρκεια: 25 λεπτά**

* Έπειτα, ο/η εκπαιδευτικός προβάλλει μια σελίδα από το δωρεάν εκπαιδευτικό υλικό του Saferinternet.gr, με τίτλο «H φάρμα του Διαδικτύου» ( <https://www.saferinternet.gr/index.php?parentobjId=Page15&objId=Category359&childobjId=Text1740> ). Είναι παιδικό βιβλίο που απευθύνεται σε παιδιά Δημοτικού, με στόχο να τα μυήσει στους βασικούς κανόνες χρήσης του Διαδικτύου από μικρή ηλικία. Μέσα από πέντε χαρούμενες ιστορίες που διαδραματίζονται σε μια φάρμα ζώων, τα παιδιά έρχονται σε επαφή με τα εξής σημαντικά θέματα σε σχέση με την πλοήγηση στους διαδικτυακούς κόσμους. Με αυτόν τον τόπο ξεκινάει η συζήτηση για τους κινδύνους του διαδικτύου.
* Αναφέρονται οι έννοιες **Pharming, Phishing και Hacking** και επεξηγούνται σύντομα από τον εκπαιδευτικό (βλ. παράρτημα).

**3η φάση**

**Διάρκεια: 10 λεπτά**

* Ο/Η εκπαιδευτικός προβάλλει σύντομο βίντεο (1:20) σχετικό με το **Phishing,** [**ΕΔΩ**](https://saferinternet.gr/index.php?parentobjId=Page15&objId=Category17&childobjId=Text310)**.**
* Αναθέτει τη δημιουργία είτε ψηφιακής αφίσας, ανά ομάδα, για την προστασία από το **Phishing, μέσω** [**https://www.canva.com/**](https://www.canva.com/)**, είτε συννεφόλεξου, μέσω https://wordart.com/**

**8. ΠΙΘΑΝΕΣ ΕΠΕΚΤΑΣΕΙΣ - ΠΡΟΣΑΡΜΟΓΕΣ ΣΧΕΔΙΟΥ ΜΑΘΗΜΑΤΟΣ**

Το παρόν σχέδιο διδασκαλίας επιδέχεται αναπροσαρμογές, με τη μείωση ή τη διαφοροποίηση του ήδη διαμορφωμένου υλικού, ενώ παράλληλα αποτελεί ιδανική επιλογή σε ειδικές συνθήκες εξ αποστάσεως διδασκαλίας. Αυτό σχετίζεται με τη φύση των μέσων που χρησιμοποιούνται: Η/Υ, εργαλεία web 2.0, σύνδεση στο διαδίκτυο, ‘’έξυπνες’’ πρίζες τα οποία είναι προσβάσιμα από την πλειονότητα των μαθητών/-τριών. Σε περίπτωση που δεν υπάρχει η πρόσβαση από κάποιων μαθητή/-τρια προτείνεται η παροχή εξοπλισμού από το σχολείο ή η χρήση tablet ή ακόμα και κινητού τηλεφώνου (android).

**9. ΒΙΒΛΙΟΓΡΑΦΙΑ – ΔΙΚΤΥΟΓΡΑΦΙΑ**

<https://www.youtube.com/watch?v=n8zXu0CsBt0>

<https://saferinternet4kids.gr/hot-topics/phishing-2/>

<https://saferinternet.gr/index.php?parentobjId=Page15&objId=Category17&childobjId=Text310>

<https://www.canva.com/>

<https://wordart.com/>

**10. ΠΑΡΑΡΤΗΜΑ**

|  |
| --- |
| * Σε ό,τι αφορά τις υπηρεσίες επικοινωνίας (e-mail, κοινωνικά δίκτυα κ.λπ.) καθώς και τις τραπεζικές υπηρεσίες μέσω διαδικτύου (web banking), τα συστήματα νεφελοειδούς αποθήκευσης (cloud – computing) κ.λπ., είναι πλέον διαδεδομένη η έννοια ενός προσωπικού χώρου (personal place) στο διαδίκτυο στον οποίο τα δεδομένα του κατόχου – χρήστη θα είναι ασφαλή, εμπιστευτικά, της διαθέσιμα και ακέραια.
* Στις υπηρεσίες αυτές απαιτούνται στοιχεία αυθεντικoποίησης (authorization/authedication) όπως όνομα χρήστη, κωδικός κ.λπ. προκειμένου ο χρήστης να έχει πρόσβαση. Τα στοιχεία αυτά αποτελούν ουσιαστικά την ταυτότητά του για την είσοδο στο συγκεκριμένο χώρο και είναι αυτά τα στοιχεία τα οποία οι hackers προσπαθούν να ανακαλύψουν προκειμένου να έχουν πρόσβαση στους προσωπικούς χώρους των χρηστών του διαδικτύου.
* Ο τρόπος είναι στους περισσότερους από εμάς γνωστός. Σχεδόν καθημερινά λαμβάνουμε e-mails τα οποία μας πληροφορούν ότι δήθεν έχουμε κάποιον λογαριασμό με «μπλοκαρισμένα» χρήματα σε κάποια μακρινή χώρα και προκειμένου να έλθουν στην κατοχή μας να αποστείλουμε σε κάποιον αυτά τα στοιχεία αυθεντικοποίησης λογαριασμού μας ή άλλα προσωπικά στοιχεία.
* **Η πιο διαδεδομένη μέθοδος κλοπής ταυτότητας (identity theft) είναι το “phishing”.**Ο δράστης εμφανίζεται ως ένα φαινομενικά έμπιστο **πρόσωπο**(με e-mail ή κάποιο άλλο στιγμιαίο μήνυμα) και προσπαθεί να παραπλανήσει το θύμα προκειμένου να αποσπάσει τα ως άνω στοιχεία. Ειδικότερα, ως “**phishing**” χαρακτηρίζεται η αποστολή ηλεκτρονικών μηνυμάτων (e-mails) που σκοπό έχουν να προκαλέσουν την κλοπή εμπιστευτικών στοιχείων που ανήκουν στον παραλήπτη του ηλεκτρονικού μηνύματος. Τα ηλεκτρονικά αυτά μηνύματα δίνουν την εντύπωση πως προέρχονται από κάποιο οικείο πρόσωπο και ζητούν από τον παραλήπτη με διάφορες δικαιολογίες και προφάσεις την αποκάλυψη ευαίσθητων δεδομένων, π.χ. τον αριθμό τραπεζικού λογαριασμού του, τον προσωπικό αριθμό αναγνώρισης (PIN).
* Pharming” είναι η εκμετάλλευση του τρωτού ενός DNS (Domain Name System) server software που επιτρέπει σε κάποιον να ανακατευθύνει τους επισκέπτες ενός website σε άλλο website.
* Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει κατά τέτοιο τρόπο, ώστε, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφθεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, ο συγκεκριμένος υπολογιστής τον “οδηγεί” μόνο σε πλαστές ιστοσελίδες, δηλαδή ο δράστης τροποποιεί το Domain Name Code με αποτέλεσμα οι χρήστες που αναζητούν μια ιστοσελίδα με αλλοιωμένη την αριθμητική της διεύθυνση (numerical address) να κατευθύνονται αυτόματα σε άλλη ιστοσελίδα.
* Η τεχνική του “**pharming**” αποτελεί μέθοδο εξαπάτησης μέσω του διαδικτύου η οποία ουσιαστικά περιλαμβάνει και “phising”, αφού ο δράστης στοχεύει στην απόκτηση των στοιχείων αυθεντικοποίησης του θύματος όχι με αποστολή από το ίδιο το θύμα αλλά παραπλανώντας το θύμα ότι ασφαλώς χρησιμοποιεί τα στοιχεία του στη σωστή ιστοσελίδα.
* Ωστόσο, η ψεύτικη ιστοσελίδα στην οποία έχει ανακατευθυνθεί το θύμα λειτουργεί προκειμένου να συλλέγει τα στοιχεία αυθεντικοποίησης για λογαριασμό των hackers.
 |