

ΣΧΕΔΙΑΣΜΟΣ ΜΙΚΡΟΔΙΔΑΣΚΑΛΙΑΣ:

Αναγνώριση και Αντιμετώπιση Ύποπτων Ηλεκτρονικών Μηνυμάτων (Phishing) στην Α' Γυμνασίου

A. ΤΑΥΤΟΤΗΤΑ ΜΙΚΡΟΔΙΔΑΣΚΑΛΙΑΣ

Το εκπαιδευτικό σενάριο εστιάζει στην κατανόηση και αντιμετώπιση των phishing emails, ως μια από τις πιο διαδεδομένες μορφές ψηφιακής απάτης. Οι μαθητές της Α' Γυμνασίου μαθαίνουν να εντοπίζουν ύποπτα χαρακτηριστικά σε μηνύματα ηλεκτρονικού ταχυδρομείου, να κατανοούν τους σχετικούς κινδύνους και να διαμορφώνουν πρακτικές ψηφιακής αυτοπροστασίας.

Η διδακτική προσέγγιση ακολουθεί το μοντέλο 5E και αξιοποιεί τεχνικές βιωματικής μάθησης. Οι μαθητές εμπλέκονται ενεργά μέσω ψηφιακών εργαλείων όπως εκπαιδευτικά παιχνίδια, συλλογικές πλατφόρμες, καθώς και μέσω της δημιουργίας ενός εκπαιδευτικού email, το οποίο λειτουργεί ως προϊόν κατανόησης και υπενθύμισης προς άλλους. Το σενάριο καλλιεργεί δεξιότητες ψηφιακής κριτικής σκέψης, υπεύθυνης διαδικτυακής συμπεριφοράς και επικοινωνίας σχετικά με την πληροφορική.

Συναίνεση για δημοσιοποίηση: ΝΑΙ

Γνωστικό Αντικείμενο - Ένταξη στο Πρόγραμμα Σπουδών

- **Μάθημα:** Πληροφορική
- **Βαθμίδα:** Γυμνάσιο
- **Τάξη:** Α' Γυμνασίου
- **Θεματική Ενότητα:** Κυβερνοασφάλεια

Το αντικείμενο της μικροδιδασκαλίας εντάσσεται στο μάθημα της Πληροφορικής της Α' Γυμνασίου, στο πλαίσιο της θεματικής ενότητας "Δίκτυα υπολογιστών και το Διαδίκτυο" και υποενότητα "Κυβερνοασφάλεια". Σύμφωνα με το νέο Πρόγραμμα Σπουδών του ΙΕΠ (2022), στόχος είναι η ανάπτυξη δεξιοτήτων αναγνώρισης ψηφιακών απειλών, υπεύθυνης χρήσης του διαδικτύου και προστασίας προσωπικών δεδομένων. Η δραστηριότητα επικεντρώνεται στην αναγνώριση στοιχείων phishing emails και στην καλλιέργεια κριτικής σκέψης σχετικά με την αξιολόγηση ψηφιακού περιεχομένου.

Σκοπός & Προσδοκώμενα Μαθησιακά Αποτελέσματα

Ο βασικός **σκοπός** της μικροδιδασκαλίας είναι:

- Οι μαθητές να καλλιεργήσουν κριτική σκέψη κατά την αξιολόγηση ηλεκτρονικών μηνυμάτων.
- Να αναγνωρίζουν τα χαρακτηριστικά ύποπτων emails (phishing) και

- Να υιοθετούν υπεύθυνες στάσεις για την προστασία των προσωπικών τους δεδομένων.
- Παράλληλα, μέσω της χρήσης ψηφιακών εργαλείων, ενισχύεται η υπολογιστική πρακτική της δημιουργίας και αλληλεπίδρασης με ψηφιακά αντικείμενα, σύμφωνα με τις κατευθύνσεις του νέου Προγράμματος Σπουδών Πληροφορικής.

ΠΜΑ

Στο τέλος της δραστηριότητας, οι μαθητές θα είναι σε θέση να:

- Εντοπίζουν χαρακτηριστικά που κάνουν ένα email ύποπτο.
- Αναλύουν το περιεχόμενο ενός email για ενδείξεις phishing
- Εξηγούν τους κινδύνους που προκύπτουν από την αλληλεπίδραση με phishing μηνύματα.
- Προτείνουν τρόπους προστασίας προσωπικών δεδομένων στο διαδίκτυο.
- Αξιολογούν την αξιοπιστία ενός μηνύματος και επιλέγουν υπεύθυνη στάση.
- Συνθέτουν ένα εκπαιδευτικό παράδειγμα ύποπτου email για να ενημερώσουν άλλους.

Η μικροδιδασκαλία ενισχύει την υπολογιστική πρακτική της επικοινωνίας σχετικά με την Πληροφορική, καθώς οι μαθητές:

- δημιουργούν εκπαιδευτικό περιεχόμενο (ψεύτικο email προσομοίωσης),
- διατυπώνουν συμβουλές προστασίας για τρίτους,
- και συμμετέχουν σε συλλογική συζήτηση για θέματα ασφάλειας στο διαδίκτυο.

Μέσω αυτών των δραστηριοτήτων, αναπτύσσουν την ικανότητα να εκφράζονται με σαφήνεια και υπευθυνότητα γύρω από τεχνολογικά ζητήματα, κάτι που αποτελεί οριζόντια ικανότητα του ΠΣ Πληροφορικής Γυμνασίου.

Συνοπτική περιγραφή

Η μικροδιδασκαλία ακολουθεί το μοντέλο 5E και εστιάζει στην αναγνώριση ύποπτων emails και στην προστασία από απάτες τύπου phishing. Ξεκινά με την παρουσίαση ενός παραδείγματος ύποπτου email για ενεργοποίηση της σκέψης των μαθητών και ακολουθεί δραστηριότητα διερεύνησης μέσω εκπαιδευτικού παιχνιδιού.

Μετά την εμπειρική φάση, παρουσιάζεται θεωρία για το τι είναι phishing, πώς το αναγνωρίζουμε και ποιοι είναι οι κίνδυνοι. Στη συνέχεια, αναπτύσσονται πρακτικές προστασίας ενώ στο τέλος, οι μαθητές ανακεφαλαιώνουν όσα έμαθαν δημιουργώντας ένα υπενθυμιστικό email με σκοπό την ενημέρωση φίλων ή οικογένειας.

B. ΤΕΚΜΗΡΙΩΣΗ

Παιδαγωγική – Διδακτική προσέγγιση

Ο σχεδιασμός της μικροδιδασκαλίας βασίστηκε στην ανακαλυπτική μάθηση και στη βιωματική-ενεργητική προσέγγιση, σύμφωνα με τις αρχές του εποικοδομητισμού. Συγκεκριμένα οργανώθηκε σύμφωνα με το διδακτικό μοντέλο των 5E (Engage,

Explore, Explain, Elaborate, Evaluate), το οποίο ενθαρρύνει την ενεργητική συμμετοχή των μαθητών και προάγει τη βαθιά κατανόηση μέσω βιωματικής μάθησης.

Στη φάση Engage, οι μαθητές καλούνται να αναγνωρίσουν ύποπτα χαρακτηριστικά μέσα από ένα παράδειγμα ενός phishing email, ενεργοποιώντας τις πρότερες γνώσεις και εμπειρίες τους.

Στη φάση Explore, μέσω του εκπαιδευτικού παιχνιδιού, αναπτύσσουν την ικανότητά τους να εντοπίζουν κριτικά επικίνδυνα μηνύματα.

Στη φάση Explain, γίνεται θεωρητική παρουσίαση, στηριζόμενη σε παραδείγματα από τη δραστηριότητά τους, ώστε να θεμελιωθεί η νέα γνώση και τρόπος σκέψης με βάση την εμπειρία.

Στη φάση Elaborate, ενθαρρύνεται η κριτική σκέψη, στην ανάπτυξη στρατηγικών προστασίας στο διαδίκτυο και ενδυναμώνεται η υπεύθυνη στάση των μαθητών.

Στη φάση Evaluate, οι μαθητές συνθέτουν ένα ενημερωτικό μήνυμα (ύπο την μορφή ενός ψεύτικου phishing email) για να ευαισθητοποιήσουν άλλους, επιτυγχάνοντας την αυτοαξιολόγηση των γνώσεων τους.

Η επιλογή του μοντέλου 5E αιτιολογείται από την ανάγκη:

- Να ενεργοποιηθεί η πρότερη εμπειρία των μαθητών,
- Να ερευνηθούν νέα φαινόμενα μέσω βιωματικής δραστηριότητας,
- Να δομηθεί η νέα γνώση στηριγμένη στις ανακαλύψεις τους,
- Να εφαρμοστεί η γνώση σε νέο πλαίσιο,
- Να αξιολογηθεί η κατανόηση μέσω δημιουργικής παραγωγής (υπενθυμιστικό email).

Σύμφωνα με το Νέο Πρόγραμμα Σπουδών Πληροφορικής, αναδεικνύεται η ανάγκη ανάπτυξης δεξιοτήτων αναγνώρισης ψηφιακών απειλών, αξιολόγησης ψηφιακών πληροφοριών και υπεύθυνης ψηφιακής συμπεριφοράς, στόχοι που εξυπηρετούνται μέσω των δραστηριοτήτων της μικροδιδασκαλίας.

Ρόλος Εκπαιδευτικού

Ο εκπαιδευτικός λειτουργεί ως:

- Καθοδηγητής,
- Συντονιστής συζήτησης και φορέας πληροφορίας,
- Αξιολογητής κατά την παραγωγή του τελικού προϊόντος.

Ο εκπαιδευτικός δεν μεταδίδει άμεσα έτοιμη γνώση από την αρχή, αλλά δημιουργεί πλαίσια εμπειρίας μέσα από τα οποία οι μαθητές ανακαλύπτουν, οργανώνουν και εφαρμόζουν τη γνώση.

Ρόλος Μαθητών

Οι μαθητές:

- Συμμετέχουν ενεργά στην αναγνώριση και κατηγοριοποίηση στοιχείων,
- Δοκιμάζουν υποθέσεις και ελέγχουν κριτήρια κατά τη φάση της διερεύνησης,
- Οργανώνουν νέες γνώσεις μέσα από συζήτηση και ανάλυση,
- Εφαρμόζουν δημιουργικά όσα έμαθαν για να ευαισθητοποιήσουν άλλους

Υπολογιστικά/Διαδικτυακά Εκπαιδευτικά Περιβάλλοντα

Κατά τη διάρκεια της μικροδιδασκαλίας αξιοποιούνται ποικίλα ψηφιακά περιβάλλοντα που υποστηρίζουν τη βιωματική και ενεργητική μάθηση. Η κύρια διάδραση γίνεται μέσα από περιβάλλοντα βασισμένα σε HTML/JS, φιλοξενούμενα στο GitHub Pages, καθώς και από εργαλεία συμμετοχής και συνεργασίας όπως το Slido.

Συγκεκριμένα:

- Χρησιμοποιείται το διαδραστικό παιχνίδι Catch the Phish: https://icyaria.github.io/catch_the_phish/ για τη διερεύνηση και αναγνώριση ύποπτων emails.
- Οι μαθητές συμμετέχουν ενεργά σε συζήτηση μέσω Slido (ή παρόμοιου εργαλείου), όπου καταθέτουν συμβουλές προστασίας από ηλεκτρονικές απάτες.
- Χρησιμοποιείται προσαρμοσμένο περιβάλλον προσομοίωσης <https://icyaria.github.io/phishing-lab>, όπου οι μαθητές δημιουργούν εκπαιδευτικά phishing emails ώστε να κατανοήσουν πώς λειτουργεί μια απάτη. Το τελικό αρχείο αποθηκεύεται ως .html και υποβάλλεται μέσω Google Form ή άλλης υπηρεσίας αποστολής αρχείων.

Τα περιβάλλοντα αυτά είναι φιλικά προς τον χρήστη και δεν απαιτούν εξειδικευμένες τεχνικές γνώσεις από τους μαθητές. Συνδυάζουν θεωρία, παιχνίδι και δημιουργία, ενισχύοντας την κατανόηση μέσα από πρακτική εφαρμογή.

Αξιοποίηση της ΤΝ στον εκπαιδευτικό σχεδιασμό

Κατά τον εκπαιδευτικό σχεδιασμό της μικροδιδασκαλίας, αξιοποιήθηκε η παραγωγική τεχνητή νοημοσύνη (ChatGPT) για τη δημιουργία του εκπαιδευτικού παιχνιδιού προσομοίωσης ηλεκτρονικού ταχυδρομείου.

Συγκεκριμένα, το ChatGPT χρησιμοποιήθηκε για:

- την παραγωγή σεναρίων ύποπτων και ασφαλών emails,
- την υποστήριξη στη συγγραφή του κώδικα HTML και JavaScript που υλοποιεί την αλληλεπίδραση με τον μαθητή.

Prompt:

```
Θέλω να φτιάξω μια προσομοίωση ενός email server σε μορφή παιχνιδιού όπου θα εμφανίζονται μείλ και θα πρέπει ο χρήστης να επιλέξει πιο είναι phishing. Η 1η πιστα θα έχει 3 μείλ (2 ασφαλή και 1 ύποπτο και η 2η αλλά 3 όπου τα 2 θα είναι ύποπτα και το ένα ασφαλές). Θέλω μια βασική δομή με φιλικό υί για χρήση από παιδιά α γυμν σε js για τη δομή του παιχνιδιού και css για το front end
```

Η χρήση της τεχνητής νοημοσύνης συνέβαλε στην επιτάχυνση της δημιουργίας του παιχνιδιού και στη διαμόρφωση ενός εκπαιδευτικού περιβάλλοντος προσαρμοσμένου στις ανάγκες και το επίπεδο των μαθητών της Α' Γυμνασίου.

Γ. ΑΝΑΛΥΣΗ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

Πορεία μικροδιδασκαλίας

1. Engage (3')

- Παρουσιάζεται στους μαθητές ένα υποθετικό ύποπτο email μέσω προβολής, και τίθεται σύντομα η ερώτηση: "Θα εμπιστευόσασταν αυτό το email; Γιατί;" Οι μαθητές παρατηρούν και εκφράζουν άμεσα τις πρώτες σκέψεις / υποψίες τους. (Θα προβληθεί η πρώτη διαφάνεια της παρουσίασης που χρησιμοποιείται και παρακάτω: [ΜΕΝΟΥΜΕ ΑΣΦΑΛΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ - Phishing Emails](#))

Σύνδεση με ΠΜΑ: Οι μαθητές αρχίζουν να εντοπίζουν στοιχεία που κάνουν ένα email ύποπτο.

2. Explore (6')

- Link Παιχνιδιού: [Catch The Phish](#)
Οι μαθητές παίζουν το διαδραστικό παιχνίδι προσομοίωσης email server. Βλέπουν 6 email, εκ των οποίων 3 είναι ύποπτα και 3 ασφαλή. Επιλέγουν ποια θεωρούν ύποπτα και στο τέλος απαντάνε 3 ερωτήσεις που συνδέονται με αυτά που είδαν. Ο εκπαιδευτικός παρέχει οδηγίες χρήσης του παιχνιδιού, υποστηρίζει τεχνικά και παρατηρεί χωρίς να παρεμβαίνει.

Σύνδεση με ΠΜΑ: Οι μαθητές αναλύουν το περιεχόμενο ηλεκτρονικών μηνυμάτων για ενδείξεις phishing

3. Explain (8')

- **Παρουσίαση:** [ΜΕΝΟΥΜΕ ΑΣΦΑΛΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ - Phishing Emails](#)
Γίνεται ανασκόπηση με οργανωμένη θεωρία:
 - Τι είναι phishing emails,
 - Πώς αναγνωρίζουμε χαρακτηριστικά ύποπτων μηνυμάτων,
 - Ποιοι είναι οι πιθανοί κίνδυνοι.Ταυτόχρονα γίνεται ενεργητική συζήτηση

Σύνδεση με ΠΜΑ: Οι μαθητές εξηγούν τους κινδύνους που προκύπτουν από τέτοια μηνύματα και αξιολογούν τη σοβαρότητα τέτοιων επιθέσεων μέσα από πραγματικά παραδείγματα.

4. Elaborate (7')

- **Δραστηριότητα:** [Sli.do](#)
Χρησιμοποιώντας εργαλείο συνεργατικής γραφής (Sli.do), οι μαθητές καταγράφουν τρόπους προστασίας από ύποπτα emails. Η τάξη συζητά και οργανώνει πρακτικές συμβουλές. Ο εκπαιδευτικός κατευθύνει την ανάρτηση ιδεών, διευκολύνει τη σύνθεση

των απόψεων και προωθεί τη συμμετοχικότητα ενώ οι μαθητές προτείνουν στρατηγικές προστασίας, αναρτούν ιδέες και σχολιάζουν απόψεις συμμαθητών.

Σύνδεση με ΠΜΑ: Οι μαθητές προτείνουν τρόπους προστασίας προσωπικών δεδομένων και συμμετέχουν στην επικοινωνία σχετικά με την πληροφορική, διατυπώνοντας συμβουλές για άλλους.

5. Evaluate (6')

- **Δραστηριότητα:** [Anti Phishing Lab](#)

Ο κάθε μαθητής δημιουργεί μέσω του παραπάνω εργαλείου την τελική του εργασία: ένα υποθετικό phishing email που υπενθυμίζει τις παγίδες που πρέπει να αποφεύγουμε. Το email κατεβαίνει τοπικά σε αρχείο .html και υποβάλλεται μέσω φόρμας Dropbox (ή Google Form).

Σύνδεση με ΠΜΑ: Οι μαθητές συνθέτουν ένα εκπαιδευτικό παράδειγμα ύποπτου email και επικοινωνούν υπεύθυνα την πληροφορία σε άλλους, με σκοπό την πρόληψη. Η φάση αυτή ενισχύει την οριζόντια ικανότητα της επικοινωνίας σχετικά με την Πληροφορική.

Φύλλο Εργασίας

Το Φύλλο Εργασίας είναι διαθέσιμο σε μορφή pdf εδώ: [Φύλλο Εργασίας.pdf](#)

Δ. Αξιολόγηση

Η αξιολόγηση των μαθητών πραγματοποιείται μέσω της τελικής δημιουργικής δραστηριότητας, όπου κάθε μαθητής καλείται να κατασκευάσει ένα υποθετικό phishing email χρησιμοποιώντας το ψηφιακό εργαλείο δημιουργίας email.

Το email που δημιουργούν αποθηκεύεται τοπικά ως αρχείο .html μέσω της επιλογής "Κατέβασε το Email σου" και υποβάλλεται μέσω φόρμας για αξιολόγηση από τον εκπαιδευτικό.

Κριτήρια Αξιολόγησης:

- Συμπερίληψη στοιχείων που χαρακτηρίζουν ένα ύποπτο email (ύποπτος αποστολέας, περίεργο θέμα, ύποπτο περιεχόμενο, παραπλανητικός σύνδεσμος).
- Ορθότητα και πληρότητα της δημιουργίας (όλα τα απαιτούμενα πεδία συμπληρωμένα).
- Κατανόηση του σκοπού του έργου (να ενημερώσει άλλους για την προσοχή σε επικίνδυνα emails).