



BLOOMING
Inclusion and Diversity in STEAM

Μάθημα: Ασφαλίζοντας το Μέλλον – Κατανόηση της Ασφάλειας Δικτύων και της Κρυπτογραφίας

Στόχος:

Οι μαθητές θα μάθουν τα βασικά της ασφάλειας δικτύων, συμπεριλαμβανομένων των κοινών απειλών, της σημασίας της κρυπτογράφησης και των μεθόδων προστασίας των δεδομένων κατά τη μετάδοση. Το μάθημα θα εισαγάγει βασικές έννοιες όπως η κρυπτογραφία, η ασφάλεια ανθεκτική στην κβαντική απειλή και η ανίχνευση επιθέσεων σε πραγματικό χρόνο.

Υλικά:

- Προβολέας για διαφάνειες σχετικά με την ασφάλεια δικτύων
- Φυλλάδια για κοινές επιθέσεις δικτύων (π.χ., man-in-the-middle, denial of service, phishing)
- Υπολογιστές ή λάπτοπ για προσομοίωση της ασφάλειας δικτύων
- Εργαλεία λογισμικού για ασφάλεια δικτύων (π.χ., Wireshark, βασικά εργαλεία κρυπτογράφησης)
- Πρόσβαση στο Διαδίκτυο για έρευνα σε τρωτά σημεία δικτύων και μεθόδους άμυνας



Co-funded by
the European Union

Erasmus+
Enriching lives, opening minds.



BLOOMING
Inclusion and Diversity in STEAM

Βασικές Πληροφορίες:

Η ασφάλεια δικτύων αφορά πρακτικές και τεχνολογίες που έχουν σχεδιαστεί για να προστατεύουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων κατά τη μετάδοσή τους μέσω δικτύων. Καθώς οι κυβερνοεπιθέσεις γίνονται όλο και πιο εξελιγμένες, είναι απαραίτητη η εφαρμογή ισχυρών μέτρων ασφαλείας, όπως η κρυπτογράφηση, τα firewalls και η ανίχνευση επιθέσεων σε πραγματικό χρόνο. Αναδυόμενες απειλές, όπως η κβαντική υπολογιστική, δημιουργούν νέες προκλήσεις στις παραδοσιακές κρυπτογραφικές μεθόδους.

Δραστηριότητες Μαθήματος

1. Εισαγωγή στην Ασφάλεια Δικτύων (15 λεπτά):

- Ξεκινήστε με μια επισκόπηση της σημασίας της ασφάλειας δικτύων στη σημερινή ψηφιακή εποχή.
- Εξηγήστε πώς τα δίκτυα είναι ευάλωτα σε διάφορες μορφές επιθέσεων, όπως επιθέσεις man-in-the-middle (MITM), denial of service (DoS), και phishing.
- Εισάγετε βασικούς όρους, όπως κρυπτογράφηση, firewalls, και πρωτόκολλα δικτύων.
- Συζητήστε την αναδυόμενη πρόκληση της κβαντικής υπολογιστικής και πώς απειλεί τα παραδοσιακά συστήματα κρυπτογράφησης.

2. Κοινές Επιθέσεις Δικτύων και Άμυνα (20 λεπτά):

- Χωρίστε την τάξη σε μικρές ομάδες και αναθέστε σε κάθε ομάδα μια κοινή επίθεση δικτύου (π.χ., MITM, DoS, phishing ή SQL injection).
- Ζητήστε από κάθε ομάδα να ερευνήσει και να παρουσιάσει:



Co-funded by
the European Union

Erasmus+
Enriching lives, opening minds.



BLOOMING

Inclusion and Diversity in STEAM

- Πώς λειτουργεί η επίθεση
 - Τι ζημιά μπορεί να προκαλέσει
 - Μεθόδους πρόληψης ή μετριασμού της επίθεσης (π.χ., χρήση κρυπτογράφησης, firewalls ή πολυπαραγοντική ταυτοποίηση).
 - Μετά από κάθε παρουσίαση, συζητήστε τη σημασία των πρωτοκόλλων ασφαλείας που μπορούν να ανιχνεύσουν και να αποτρέψουν τέτοιες επιθέσεις.
3. **Δραστηριότητα: Προσομοίωση Κυκλοφορίας Δικτύου και Ανίχνευση Επιθέσεων (30 λεπτά):**
- Στήστε ένα προσομοιωμένο δίκτυο χρησιμοποιώντας ένα εργαλείο ασφάλειας δικτύων, όπως το Wireshark.
 - Επιτρέψτε στους μαθητές να παρατηρήσουν φυσιολογική και κακόβουλη κυκλοφορία στο δίκτυο, κατανοώντας πώς εντοπίζονται επιθέσεις όπως MITM και DoS.
 - Οδηγήστε τους μαθητές να εντοπίσουν πιθανές αδυναμίες στο προσομοιωμένο δίκτυο και να προτείνουν πιθανές άμυνες, όπως ισχυρότερη κρυπτογράφηση ή τμηματοποίηση δικτύου.
 - Δείξτε πώς τα δεδομένα προστατεύονται κατά τη μετάδοση μέσω κρυπτογράφησης.
4. **Εξερεύνηση Κβαντικά Ανθεκτικής Κρυπτογραφίας (15 λεπτά):**
- Εισάγετε την έννοια της κβαντικής υπολογιστικής και γιατί αποτελεί απειλή για τις τρέχουσες μεθόδους κρυπτογράφησης.
 - Συζητήστε την κρυπτογραφία ανθεκτική στην κβαντική απειλή και πώς χρησιμοποιεί αλγορίθμους που σχεδιάζονται για να αντέχουν σε επιθέσεις κβαντικού επιπέδου.



Co-funded by
the European Union

Erasmus+
Enriching lives, opening minds.



BLOOMING

Inclusion and Diversity in STEAM

- Εξηγήστε πώς ερευνητές, όπως η Δρ. Anca Jurcut, αναπτύσσουν αυτούς τους αλγόριθμους για να διασφαλίσουν την ασφάλεια των μελλοντικών επικοινωνιών.

Οπτικοποίηση και Συζήτηση:

- Δημιουργήστε έναν οπτικό χάρτη διαφορετικών επιπέδων ασφάλειας δικτύου (firewalls, κρυπτογράφηση, συστήματα ανίχνευσης εισβολών, κ.λπ.) σε έναν πίνακα.
- Συζητήστε πώς αυτά τα επίπεδα συνεργάζονται για να δημιουργήσουν ένα ασφαλές δίκτυο.
- Ζητήστε από τους μαθητές να εξετάσουν πώς μπορεί να εξελιχθούν τα πρωτόκολλα ασφαλείας καθώς η τεχνολογία κβαντικής υπολογιστικής γίνεται πιο διαδεδομένη.

Αξιολόγηση:

Ζητήστε από τους μαθητές να γράψουν μια ανασκόπηση σχετικά με:

- Ποια επίθεση δικτύου βρήκαν πιο επικίνδυνη και γιατί.
- Πώς η κρυπτογράφηση προστατεύει τα δεδομένα κατά τη μετάδοση.
- Γιατί η κβαντική υπολογιστική αποτελεί πρόκληση για τις τρέχουσες μεθόδους κρυπτογράφησης και πώς η κρυπτογραφία ανθεκτική στην κβαντική απειλή βοηθά στην αντιμετώπιση αυτής της πρόκλησης.



Co-funded by
the European Union

Erasmus+
Enriching lives, opening minds.



BLOOMING

Inclusion and Diversity in STEAM

Αξιολογήστε τις ομαδικές παρουσιάσεις και τη συμμετοχή στη δραστηριότητα προσομοίωσης.



Co-funded by
the European Union

Erasmus+
Enriching lives, opening minds.