סייבר ריינג'רס – תכנית לימודים (כיתות ד'-ו')

סקירה כללית

תכנית "סייבר ריינג'רס" מציעה מסלול לימודים מקיף בתחומי הסייבר, אבטחת מידע, חקירה דיגיטלית ובינה מלאכותית, המותאם במיוחד לתלמידי כיתות ד'-ו'. התכנית בנויה משילוב של הרצאות תיאורטיות, מעבדות מעשיות ופרויקטים יישומיים.

פרטי הקורס

היקף התכנית

38 שיעורי חובה + 10 שיעורי העשרה (בחירה)

מתודולוגיית הוראה

למידה חווייתית מבוססת מעבדות, תרגולים אינטראקטיביים וכלים מקצועיים

טכנולוגיות ופלטפורמות

ChatGPT, DALL·E, VirusTotal, ML for Kids ועוד כלים מתקדמים מהתעשייה

מטרות הלימודים

התכנית מיועדת לא רק להקנות ידע טכני על פעולת האינטרנט והטכנולוגיה, אלא גם לפתח מיומנויות חיוניות במאה ה-21:

- **חשיבה ביקורתית** - ניתוח מידע דיגיטלי והערכת מקורות
- **אוריינות טכנולוגית** - הבנה מעמיקה של מערכות וכלים דיגיטליים
- **אתיקה דיגיטלית** - התנהלות אחראית ובטוחה במרחב המקוון
- **יכולות חקר** - פיתוח כישורי למידה עצמאית וחקירה דיגיטלית

כל יחידת לימוד משלבת היבטים תיאורטיים עם התנסות מעשית, תוך עידוד עבודת צוות, יצירתיות ופתרון בעיות.

חלק א' – יסודות הסייבר, AI ואתיקה (שיעורים 1-10)

בחלק זה התלמידים יפתחו הבנה בסיסית בעולם הסייבר, בינה מלאכותית ואתיקה דיגיטלית דרך התנסויות מעשיות.

שיעור 1: היכרות עם סייבר ו-AI

- **פעילות כיתתית:** דיון בכיתה על מה זה סייבר ומה זה בינה מלאכותית
- **מעבדה מעשית:** שיחה עם ChatGPT – "מה זה האקר?"

שיעור 2: מבנה האינטרנט וחיפוש חכם

- **פעילות כיתתית:** סרטון ותרשים זרימה של האינטרנט
- **מעבדה מעשית:** תרגול חיפוש מתקדם + ניסוח שאילתות עם ChatGPT

שיעור 3: IP, דומיינים וגלישה מסווית

- **פעילות כיתתית:** סימולציה של חיבור לרשת דרך VPN
- **מעבדה מעשית:** זיהוי IP וניתוח מיקום בעזרת iplocation.net

שיעור 4: מה אתרים יודעים עלינו?

- **פעילות כיתתית:** בדיקת האתר whoer.net
- **מעבדה מעשית:** השוואה בין שני דפדפנים + ניתוח התוצאה

שיעור 5: פרטיות, אתיקה ו-Deepfake

- **פעילות כיתתית:** צפייה בקטע וידאו מזויף וניתוח מוסרי
- **מעבדה מעשית:** זיהוי זיופים עם AI (Hive או Microsoft Designer)

שיעור 6: בריונות ושיימינג דיגיטלי

- **פעילות כיתתית:** משחק תפקידים – פוגע, נפגע, צופה
- **מעבדה מעשית:** בדיקת שיח בטוח עם עוזר AI

שיעור 7: משתמשים פיקטיביים

- **פעילות כיתתית:** דיון – איך מזהים פרופיל מזויף
- **מעבדה מעשית:** יצירת תמונת פרופיל עם Generated Photos + ניתוח

שיעור 8: יצירת זהות מזויפת ובדיקת הסיכון

- **פעילות כיתתית:** תכנון זהות מזויפת כחלק מתרגיל מוסרי
- **מעבדה מעשית:** ניתוח עמוד פיקטיבי עם AI

שיעור 9: מודיעין פתוח (OSINT)

- **פעילות כיתתית:** הסבר על מקורות מידע ציבוריים
- **מעבדה מעשית:** תרגיל איתור מייל, דומיין ו-IP עם כלי חקירה

שיעור 10: פרויקט חקירה דיגיטלית

- **פעילות כיתתית:** עבודה בקבוצות – "חקור את החשוד"
- **מעבדה מעשית:** שילוב של כלים מהשיעורים הקודמים על תיק פיקטיבי

חלק ב' – מיצוי מידע וניתוח חזותי (11–20)

תכנית הלימודים מתמקדת בכלים מתקדמים לאיסוף מידע, ניתוח תמונות ומיפוי גיאוגרפי, יחד עם פיתוח מיומנויות בהכנת דוחות מודיעין.

1 שיעור 11: חיפוש מתקדם בגוגל

פעילות כיתתית: בניית שאילתות מורכבות באמצעות אופרטורים מתקדמים

מעבדה מעשית: השוואה מובנית בין תוצאות חיפוש רגילות לעומת חיפושים מתקדמים

2 שיעור 12: ניתוח תמונות ברשת

פעילות כיתתית: הסבר על נתוני EXIF והמידע שניתן לחלץ מהם

מעבדה מעשית: ניתוח נתוני EXIF בתמונות וביצוע חיפוש הפוך לזיהוי מקור התמונה

3 שיעור 13: זיהוי מיקום לפי IP ותמונה

פעילות כיתתית: התנסות עם Google Earth וכלי IP Tracker לאיתור מיקומים

מעבדה מעשית: ניתוח תמונות המכילות רמזים גיאוגרפיים וזיהוי מיקומים מדויקים

4 שיעור 14: DNS ו־Whois

פעילות כיתתית: פירוק דומיין למרכיבים והבנת מבנה שמות מתחם

מעבדה מעשית: זיהוי וניתוח בעלי דומיינים באמצעות כלי Whois

5 שיעור 15: מיפוי גיאוגרפי עם AI

פעילות כיתתית: מציאת נקודות ציון וקואורדינטות ממפות דיגיטליות

מעבדה מעשית: שילוב כלי מיפוי (Waze, Google Earth) עם תמיכת ChatGPT לניתוח מתקדם

6 שיעור 16: תרגום שפות וחשיבה מידענית

פעילות כיתתית: שיטות לפענוח כתבות ומסמכים בשפות זרות

מעבדה מעשית: שימוש ב-DeepL/ChatGPT לתרגום והכנת סיכום מקצועי בעברית

7 שיעור 17: ניתוח פרופילים ברשתות

פעילות כיתתית: טכניקות להשוואה בין פרופילים אמיתיים ומזויפים

מעבדה מעשית: בניית דו"ח הערכת סיכונים בעזרת כלי בינה מלאכותית

8 שיעור 18: מיהם ההאקרים?

פעילות כיתתית: הכרת סוגי האקרים ומוטיבציות שונות לפעילות סייבר

מעבדה מעשית: שימוש ב-ChatGPT ליצירת פרופילים מפורטים של האקרים שונים

9 שיעור 19: דו"ח מודיעין בסיסי

פעילות כיתתית: לימוד שיטות לארגון ומיון מידע לפי קטגוריות מודיעיניות

מעבדה מעשית: הרכבת דו"ח מודיעין מובנה בהנחיית כלי AI

10 שיעור 20: פרויקט סיכום מודיעיני

פעילות כיתתית: ניתוח מקרה בוחן של אירוע ריגול סייבר אמיתי

מעבדה מעשית: הכנת תחקיר מקיף תוך שילוב כלים מגוונים שנלמדו בקורס

חלק ג' – קוד, תקיפות והגנה (21–30)

סילבוס לימודים מפורט לנושאי קוד, תקיפות והגנה בסייבר

1 שיעור 21: קוד מקור ודפדפנים

פעילות כיתה: פתיחת Developer Tools והסבר על תגובות

מעבדה מעשית: ניתוח אתר אמיתי

2 שיעור 22: Cookie Clicker וניתוח אינטראקטיבי

פעילות כיתה: הפעלת כלי קונסולה

מעבדה מעשית: שינוי ערכים במשחק עם קוד

3 שיעור 23: היסטוריה של וירוסים

פעילות כיתה: מצגת + דיון על מתקפה מפורסמת

מעבדה מעשית: השוואת וירוס בעבר ובהווה

4 שיעור 24: VirusTotal וחתימות

פעילות כיתה: הדבקה מדומה בקובץ מזויף

מעבדה מעשית: העלאת קובץ ל־VirusTotal וניתוח התוצאות

5 שיעור 25: מבוא ל־VBS

פעילות כיתה: כתיבת סקריפט עם הודעת שגיאה

מעבדה מעשית: ביצוע קוד בסיסי

6 שיעור 26: וירוס VBS בסיסי

פעילות כיתה: שיפור הסקריפט ליצירת וירוס מציק

מעבדה מעשית: בניית תסריט עם סיוע מ־AI

7 שיעור 27: וירוס מתקדם

פעילות כיתה: תכנון קוד מורכב

מעבדה מעשית: יצירת וירוס סיום אישי

8 שיעור 28: אנטי-וירוס ואמצעי זיהוי

פעילות כיתה: הכרות עם AV ומנגנוני זיהוי

מעבדה מעשית: ניסיון להסוות קוד מהאנטי וירוס

9 שיעור 29: סיסמאות ומנהלי סיסמאות

פעילות כיתה: תרגול יצירת סיסמה חזקה

מעבדה מעשית: עבודה עם KeePass/Bitwarden

10 שיעור 30: פריצת סיסמאות ואתגרים

פעילות כיתה: תרגיל פירוק סיסמה (שחזור/חיפוש)

מעבדה מעשית: ChatGPT כעוזר לפיצוח סיסמה מוצפנת

חלק ד' – הצפנה, רשתות ואתרים

מודול זה מכסה יסודות הצפנה, אבטחת רשתות ופיתוח אתרים בסיסי.

שיעור 31: עולם ההצפנה הקלאסית

- הרצאה: מבוא לשיטות הצפנה היסטוריות, עקרונות שחלוף והיפוך (את-בש)
- מעבדה: פענוח צפנים בסיוע כלי AI מתקדמים

שיעור 32: פונקציות גיבוב (Hash)

- הרצאה: עקרונות פונקציות גיבוב ושימושיהן באבטחת מידע
- מעבדה: התנסות מעשית עם אלגוריתמי MD5 ו-SHA

שיעור 33: הצפנה מעשית

- הרצאה: יישום הצפנה בסביבות עבודה מודרניות
- מעבדה: הצפנת מסמכים וניתוח שיטות זיהוי הצפנה

שיעור 34: חומות אש ואבטחה בסיסית

- הרצאה: תרגול אינטראקטיבי בעקרונות חומת אש
- מעבדה: הגדרת מדיניות ב-Windows Defender Firewall

שיעור 35: אסטרטגיות הגנה רב-שכבתיות

- הרצאה: סימולציית תקיפה והגנה - משחק תפקידים
- מעבדה: ניתוח תרחישי תקיפה ופיתוח אסטרטגיות הגנה בעזרת AI

שיעור 36: תשתיות רשת וכתובות IP

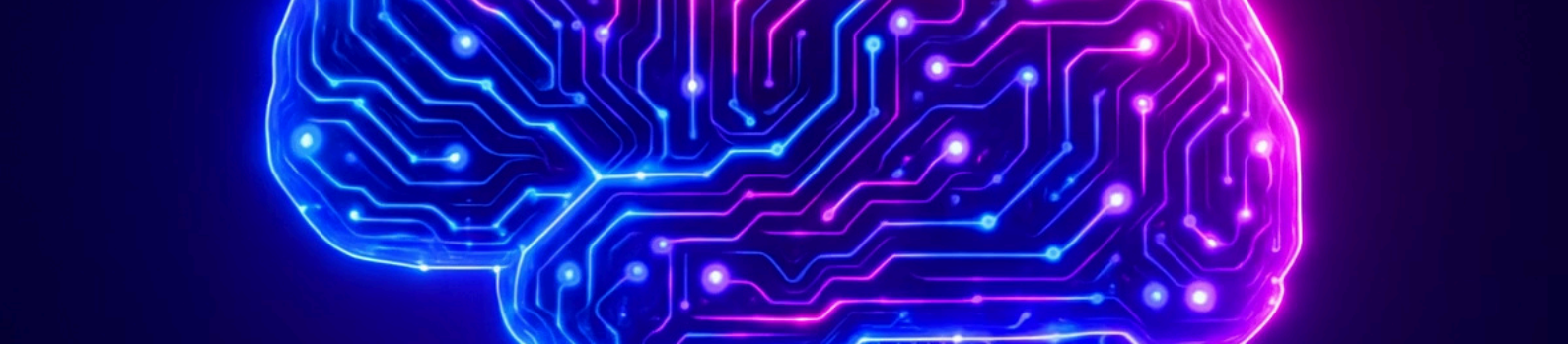
- הרצאה: תכנון וחלוקת רשתות IP מעשי
- מעבדה: עבודה עם סימולטור רשת מקצועי

שיעור 37: פיתוח אתרים ו-HTML בסיסי

- הרצאה: עקרונות מבנה אתר ותכנון דפי אינטרנט
- מעבדה: יצירת בלוג אישי בעזרת כלי AI לפיתוח קוד

שיעור 38: הערכה מסכמת

- הרצאה: תחרות ידע - Kahoot או חידון קבוצתי
- מעבדה: הגשת פרויקט סיכום והצגת תוצרים



שיעורי אקסטרה (בחירה)

מודולים נוספים שניתן לשלב בתוכנית הלימודים לפי צורך והתקדמות הכיתה:

למידת מכונה ובינה מלאכותית

פיתוח מיומנויות באינטגרציה וניתוח של טכנולוגיות AI

- בניית צ'אטבוט עם ML for Kids
- יצירת תמונה עם DALL·E וניתוח שימושים מזויפים
- זיהוי מייל מזויף עם ChatGPT
- סייבר במשחקים – איך AI מגיב

הגנה ותקיפה מעשית

התנסות בסימולציות מעשיות של תרחישי אבטחת מידע

- סימולציית פישינג + זיהוי עם AI
- תכנון מתקפה וירטואלית בקבוצה
- משחק תפקידים כחול / אדום – צוותי סייבר

פיתוח ומחקר סייבר

העמקת ידע טכני וניתוחי בתחומי פיתוח ומחקר

- קידוד מתקדם לאתר – CSS, JS
- ניתוח התנהגות משתמשים ברשת
- תרגול תחקור עם תיעוד ממוחשב

* כל שיעור אקסטרה כולל תרגול מעשי ופרויקט קצר להגשה