משרד החינוך
מינהל חדשנות
וטכנולוגיה

יוצרים אפליקציה

זיהוי הודעות דיוג (פישינג)

יחידת לימוד בשילוב אוריינות דיגיטלית ובינה מלאכותית

סרטון חשיפה - פעילות יוצרים אפליקציה: דיוג (פישינג)

ברוכים הבאים לאתגר הסייבר החדש שלנו!

בפעילות הקרובה ניכנס לנעליים של מומחי אבטחת מידע ונלמד כיצד להתגונן מאחת הסכנות הנפוצות ביותר ברשת: דיוג (פישינג).

תחילה, נחקור את הנושא לעומק בעזרת הבינה המלאכותית של NotebookLM ונבין כיצד פועלות הונאות מסוג זה.

לאחר מכן, מתוך הידע שצברנו נשתמש ב- Vibe Coding כדי לפתח בעצמנו אפליקציה אינטראקטיבית שמזהה הודעות דיוג ומזהירה אותנו.

סרטון חשיפה לפעילות

מדריך לצוותי חינוך

שלב 1 - דיון כיתתי

צפו בסרטון הפתיחה לפעילות: **סרטון פתיחה**

דיון כיתתי

האם יצא לכם לקבל הודעה שנראתה לכם חשודה? ממי היא היתה?

↙ שלב 2 – יחידת החקירות

יחידת החקירות

נחקור מהו פישינג ומהם סימני האזהרה לזיהוי מתקפה.

פתחו את מקור המידע המצורף ל- NotebookLM והעתיקו את הקישור בשורת הכתובת של האתר.

מדריך ל- NotebookLM

כעת היכנסו ל- NotebookLM, העלו את מקורות המידע ובצעו חקר בעזרת NotebookLM.

נסו להבין את מנגנון הפישינג, נסחו שאלות וגלו:

- אילו סוגי מתקפות קיימים? (מעבר לסתם מייל, חפשו על התחזות למוסדות או חברים)
- מה קורה למי שלוחץ? (הבינו את הסיכון - מה ההאקרים מנסים להשיג?)
- מהם 10 סימני האזהרה המרכזיים שיעזרו לנו לזהות זיוף?

שלב 3 – סימנים מחשידים

1. **כתובת שולח חשודה:** שימוש בכתובת מייל פרטית כמו Gmail במקום כתובת רשמית, או חוסר התאמה בין שם השולח לכתובת המייל.
2. **תחושת דחיפות ולחץ:** הודעות המדרבנות אתכם לבצע פעולה מידית תחת לחץ כדי להטעות אתכם.
3. **היעדר פנייה אישית:** שימוש בפנייה כללית כמו "לקוח יקר" במקום בשמכם הפרטי, כפי שנהוג בארגונים רשמיים.
4. **נוסח חובבני:** הודעות הכוללות שגיאות כתיב, דקדוק או ניסוח לקוי שאינם אופייניים לגופים רשמיים.
5. **הבטחות מוגזמות:** הצעות לפרסים, זכיות או הבטחות בלתי סבירות הן בדרך כלל מזויפות.
6. **בקשת פרטים רגישים:** דרישה למסירת סיסמאות, קודים או פרטי אשראי ללא יוזמה מצידכם.
7. **קישורים מקוצרים:** שימוש בקישורים קצרים כמו bit.ly שנועדו להסתיר את כתובת היעד האמיתית והזדונית.
8. **אתרים מתחזים:** הפניה לאתר שכתובתו דומה מאוד לאתר המקורי, אך כוללת שינוי קטן בסדר האותיות או טעויות איות.
9. **כתובת אתר שגויה:** חוסר התאמה בין הקישור המוצג לכתובת האמיתית (ניתן לבדיקה על ידי ריחוף עם העכבר).
01. **קבצים מצורפים חשודים:** קבלת קובץ שלא ציפיתם לו, בדגש על קובצי הרצה סיומת EXE שעלולים להכיל קוד זדוני.

↙ שלב 4 - איך זה עובד?

Vibe Coding

כעת ניצור אפליקציה שתבדוק הודעות וקישורים ותיתן התראה במידה שההודעה לא בטוחה, את האפליקציה ניצור באמצעות **Vibe Coding**.

ווייב קודינג Vibe Coding היא גישה חדשנית שמאפשרת לכם לפתח אפליקציות ומשחקים מבלי לכתוב אפילו שורת קוד אחת.

בשיטה זו, אתם הופכים למעין "במאים" של התוכנה: במקום להתעסק בשפות תכנות מורכבות, אתם פשוט מסבירים לבינה המלאכותית בשפה יומיומית וטבעית מהו הרעיון שלכם (ה"ווייב").

ה- AI לוקח על עצמו את כל הביצוע הטכני וכותב את הקוד, בעוד שאתם ממשיכים לנהל מולו שיחה, בודקים את התוצאה ומבקשים שינויים ותיקונים עד שהחזון שלכם הופך למציאות בדיוק כפי שדמיינתם.

סרטון הדרכה

↙ שלב 4 - איך זה עובד?

תהליך יצירת אפליקציה ב-Vibe Coding

שלב 1: תיאור החזון מסבירים לבינה המלאכותית במילים פשוטות מה רוצים לבנות (למשל: אפליקציית רשימת מטלות).

שלב 2: ייצור הקוד על ידי ה-AI המחשב כותב את הקוד, בונה את המבנה ודואג שהכל יעבוד באופן אוטומטי.

שלב 3: שיפור תוך כדי שיחה בודקים את התוצאה ומבקשים מה- AI תיקונים או שינויים בשפה רגילה עד לתוצאה המושלמת.

↙ שלב 5 - יוצרים אפליקציה

יוצרים ב - Vibe Coding

ניצור אפליקציה באמצעות Vibe Coding שתזהה הודעות דיוג (פישינג):

1. חזרו אל NotebookLM בקשו ממנו (באמצעות הצ'אט) לעזור לכם לנסח את ארבעת החוקים המרכזיים לזיהוי הודעות דיוג (פישינג) כדי להכניס אותם לפרומפט שלכם ליצירת האפליקציה.
2. לאחר מכן לחצו כאן לפתיחת קובץ כתיבת הפרומפט וצרו עותק. השלימו את הפרומפט הכתוב במסמך המצורף במשימה.
3. העתיקו את הפרומפט והיכנסו ל **Gemini** בחרו בכלים את **canvas** והדביקו את הפרומפט בצ'אט ליצירת האפליקציה.

***חשוב מאוד לבדוק את האפליקציה ולהתנסות בה!**

סיימתם בהצלחה
את יחידת דיוג (פישינג)