<u>תוכנית עבודה לפרויקט תוסף כרום לזיהוי אימיילים עם קישורים חשודים</u>

<u>(מיני פרויקט בנושאים מערכות הגנה לרשת)</u>

<u>מגישי הפרויקט-</u>

מתן פייג 207272956, לידור ברמי 315406207

מטרה כללית:
הפרויקט שלנו מיועד לפתח תוסף כרום שיבצע זיהוי של אימיילים עם קישורים חשודים או תוכן חשוד. התוסף יאפשר לנו לזהות אימיילים שמגיעים מדומיינים לא אמינים ולקשר אותם לפוטנציאל של מתקפות פישינג.

שלב 1: הגדרת מטרות ודרישות הפרויקט

בשלב זה נגדיר את מטרות הפרויקט ואת הדרישות הטכניות. נקבע מהם הפיצ'רים שצריך לכלול בתוסף שלנו ונוודא מהם הכלים והטכנולוגיות שנרצה להשתמש בהם, כמו לדוגמה שימוש ב API-של.Google Safe Browsing

הערכה לזמן 1-2 ימים

שלב 2: פיתוח מנגנון זיהוי של פתיחת אימייל

בשלב הזה נפתח את הפונקציות שיאפשרו לנו לזהות כאשר אימייל נפתח בדפדפן) בעיקר עבור GMAIL .(נבנה לוגיקה שתוודא שהאימייל נפתח ויתממשק עם ה DOM-של הדף.

הערכה לזמן 2-3 ימים

שלב 3: שליפת פרטי האימייל (נושא, שולח, גוף)

בשלב הזה נפתח פונקציות שיבצעו שליפה של פרטי האימייל, כמו הנושא, השולח, וגוף האימייל. נשתמש ב HTML ו JavaScript- על מנת לחלץ את המידע הנדרש בצורה מדויקת.

הערכה לזמן 2-3 ימים

שלב 4: זיהוי קישורים חשודים בגוף האימייל

בשלב הזה ניישם את המנגנון שיסרוק את גוף האימייל לאיתור קישורים חשודים. כל קישור ייבדק אם הוא מגיע מדומיינים לא אמינים, עם שימוש ב API-של Google Safe Browsing ו/או רשימה מקומית של דומיינים חשודים.

הערכה לזמן 3-4 ימים

שלב 5: זיהוי דומיינים חשודים של השולח

בשלב הזה נפתח את הפונקציות שיבדקו אם דומיין השולח הוא דומיין לא אמין (כמו דומיינים המיוחסים לפישינג). נוודא אם הדומיין נמצא ברשימת דומיינים חשודים או נבדוק אותו חיצונית באמצעות API.

הערכה לזמן 3-4 ימים

שלב 6: אינטגרציה עם Google Safe Browsing API

בשלב הזה נטמיע את החיבור עם Google Safe Browsing API שיאפשר לנו לבדוק אם קישורים הם חשודים מבחינת אבטחה. נשתמש ב fetch-על מנת לשלוח בקשות ולבדוק את הקישורים.

הערכה לזמן 2-3 ימים

שלב 7: חישוב ציון חשד(Suspicion Score)

כאן נבנה מנגנון לחישוב ציון חשד עבור האימייל בהתבסס על קריטריונים כמו קישורים חשודים, תוכן פישינג, ודומיין השולח. הציון יציין את רמת הסיכון של האימייל.

הערכה לזמן 3-4 ימים

שלב 8: פיתוח ממשק המשתמש (UI)

מטרה:

לפתח ממשק משתמש ידידותי ואינטואיטיבי שיציג למשתמש:

ציון רמת החשד באימייל (לדוגמה: "נמוך", "בינוני", "גבוה").

מידע נוסף כגון קישורים ודומיינים חשודים או דפוסים בעייתיים באימייל.

אפשרויות פעולה כגון דיווח על האימייל או התעלמות.

משימות:

עיצוב ותצוגה:

יצירת חלון קופץ שמציג את המידע הרלוונטי בצורה מסודרת וברורה.

שימוש בצבעים (כגון ירוק, כתום, אדום) לתצוגת רמת החשד.

שילוב דינמי:

התאמת התוכן למידע שמתקבל מפונקציות הניתוח (למשל, סיבות לחשד).

שיפור חוויית המשתמש:

הוספת כפתורים לפעולות: דיווח או סגירת ההודעה.

יצירת עיצוב פשוט ונגיש לכל משתמש.

הערכה לזמן

2-3 ימים.

שלב 9: ביצוע טסטים ובדיקות סופיות

בשלב הזה נבצע בדיקות פונקציונליות וטעינה, על מנת לוודא שהתוסף פועל בצורה נכונה גם תחת עומס. נתקן בעיות שהתגלו במהלך הבדיקות.

הערכה לזמן 2-3 ימים

שלב 10: סיכום והגשה

בשלב האחרון, נכין את הדוח הסופי, אשר יסביר את המנגנונים שפיתחנו ואת תהליך העבודה, ונגיש את הקוד והמדריך למרצה.

הערכה לזמן 1-2 ימים

סך הכל זמן משוער:

כשלושה שבועות (20-24 ימים).