קוד מקרו – השער לנוזקות

ברק גונן

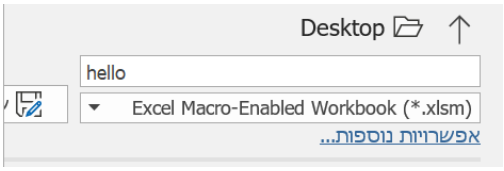
מהו קוד מקרו ובשביל מה הוא טוב?

במסמכי office של מייקרוסופט, כגון excel, word, powerpoint, יש אפשרות להוסיף קוד שיבצע אוטומטית פעולות מסויימות. קוד זה נועד לאפשר גמישות עבודה ולבצע משימות באופן אוטומטי. לדוגמה, נניח שברשותנו קובץ אקסל עם טאבים רבים, וכעת אנחנו רוצים להוסיף לכל אחד מהטאבים עמודה חדשה בשם כלשהו. באמצעות מקרו של אקסל ניתן לבצע את העבודה באופן אוטומטי. עוד על אוטומציה ושימושים טובים לקוד מקרו ניתן למצוא בסרטון הקצר הבא-

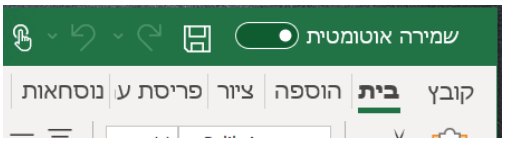
https://www.youtube.com/watch?v=ufpxojT0iAk

כיצד כותבים קוד מקרו?

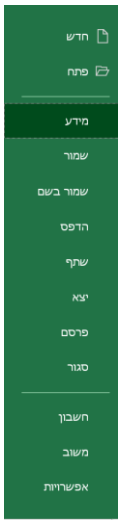
פיתחו קובץ אקסל חדש. שימרו אותו תחת שם כלשהו, לדוגמה "hello", והקפידו שהפורמט יהיה xlsm- היחיד שמאפשר הרצת קוד מקרו.



כעת הקליקו על הטאב "קובץ"

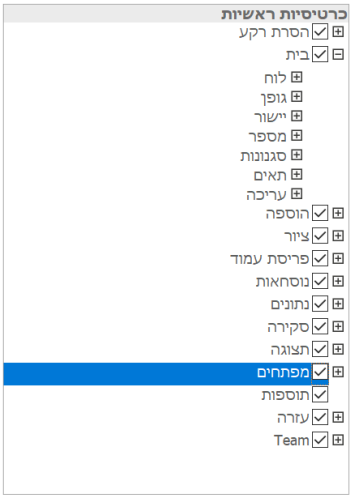


מהאפשרויות בתפריט, בחרו "אפשרויות"

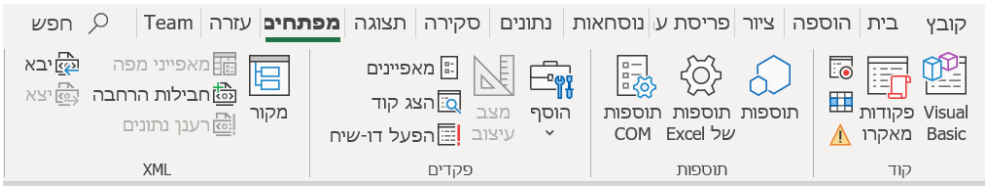


כעת בחרו "התאמה אישית של רצועת הכלים"

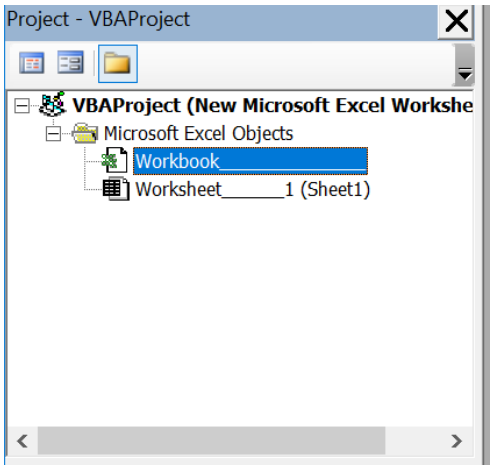
וסמנו את הלחצן של "מפתחים"



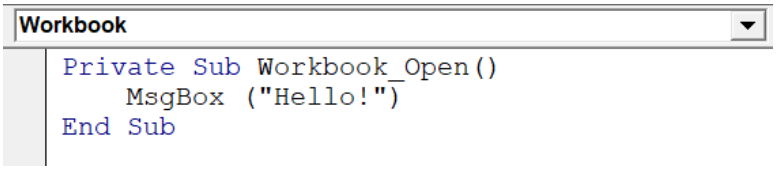
כעת מופיע לכם טאב "מפתחים" בתפריט העליון. תתחדשו! בואו נקליק עליו.



נקליק על Visual Basic ונעבור למסך חדש:



יש לפנינו שתי אפשרויות בחירה. באמצעות Workbook אנחנו יכולים ליצור פקודות מקרו שיתאימו לקובץ האקסל כולו. באמצעות Sheet1 נוכל ליצור פקודות מקרו שיפעלו רק על דף האקסל בשם זה. נבחר באפשרות הראשונה באמצעות הקלקה כפולה ונועבר למסך תכנות המקרו. קוד המקרו נכתב בשפת Visual Basic. לימוד שפה זו הוא מעבר למטרות שלנו כרגע, אך נתנסה בטעימה קטנה. כיתבו בתוכו את הקוד הבא:

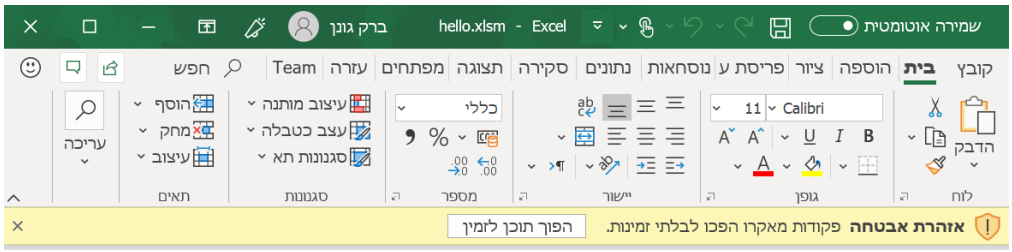


אל תשכחו לשמור את מה שכתבתם באמצעות אייקון הדיסקט, או באמצעות צירוף המקשים Ctrl+S.

הקוד שכתבנו כולל פונקציה בשם Workboo_Open. זוהי פונקציה שנקראת אוטומטית ברגע שקובץ האקסל נפתח. בתוכה קיימת פקודה - כדי לגלות מה היא עושה לחצו על מקש ה-F5, שמשמעותו במרבית עורכי הקוד היא "הרץ את הקוד". ניתן גם להריץ את הקוד מהתפריט העליון, היכן שכתוב Run.

סוגיות אבטחה

סיגרו את קובץ האקסל. כעת הריצו אותו שוב. שימו לב להודעה שמופיעה בראש הקובץ:



אקסל מודיע למשתמש כי הקובץ כולל פקודות מקרו, שעלולות להיות בעיית אבטחה. מדוע יש בעיית אבטחה? מכיוון שכפי שראינו, פקודות המקרו נכתבו כך שהן ירוצו מיד עם טעינת הקובץ, ללא שליטה של המשתמש.

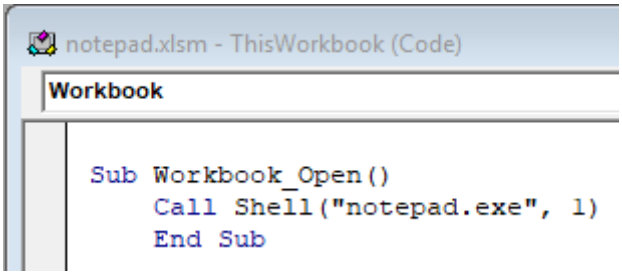
הקוד שכתבנו הוא אמנם תמים, אך אותה השיטה עלולה לשמש גם גורם זדוני. הגורם הזדוני עלול לדוגמה לשלוח לנו מייל לעבודה ובו הודעה בסגנון "פתח את הקובץ המצורף כדי לצפות בנתוני השכר החדשים שלך". הגורם הזדוני יודע שאקסל יהפוך את פקודות המקרו ללא זמינות, ולכן הוא גם יצרף למייל הנחיה כגון "עקב בעיית תאימות יש להקליק על אישור ברגע שהקובץ עולה". קורבן לא מיומן עלול ליפול בפח, ללחוץ על הכפתור ולשגר את קוד המקרו- בלי להיות מודע לכך בכלל.

היפכו את התוכן לזמין, וצפו במקרו שלכם בפעולה!

קריאה לקוד "זדוני"

פתיחת תיבת טקסט באמצעות קוד מקרו היא אמנם חמודה, אבל לא שימושית יותר מדי. כדי להבין מה קוד זדוני עלול לעשות, נצטרך להמחיש איך קוד מקרו זדוני עלול לגרום להרצה של תוכנה, שעלולה להיות זדונית. במקרה שלנו, התוכנה אותה קוד המקרו יריץ אינה באמת זדונית, אלא רק כתבן notepad, אך קוד מקרו זדוני מבצע באופן עקרוני תהליך דומה מאד. על כן, סביר שהדברים הבאים ייחסמו על ידי אנטיוירוס.

הזינו את הקוד הבא לתוך המקרו שלכם:

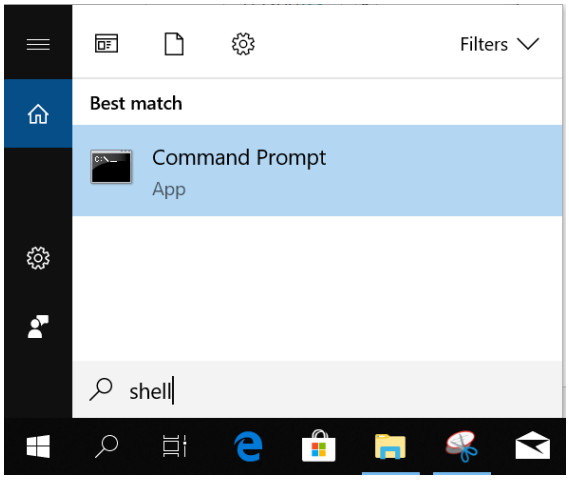


נסקור מה מבצע קוד זה. הפקודה Call מאפשרת לקרוא לפונקציות ספריה של windows. אחת מפונקציות הספריה נקראת Shell. במקרה שתזקקו לזה בעתיד, את התיעוד על הפונקציה הזו – וכל הפונקציות של windows – אפשר למצוא בקלות באתר של מייקרוסופט. האתר נקרא MSDN, קיצור של Microsoft Developers Network. חפשו בגוגל MSDN Shell ותגיעו לתיעוד של הפונקציה הנ"ל.

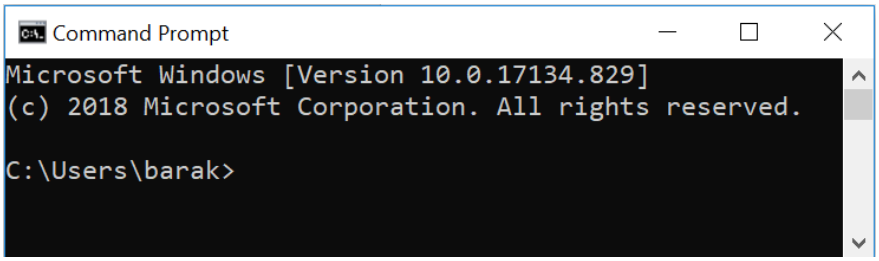
https://docs.microsoft.com/en-us/office/vba/language/reference/user-interface-help/shell-function

כאמור, אין צורך שתכנסו לשם, אך כדאי שתזכרו לעתיד 😊

אז מהו ה-shell? כדי לראות את זה, בואו ננסה בדיקה קטנה. במסך המחשב שלכם יש אייקון של זכוכית מגדלת- לחצו עליו וכיתבו shell.



כפי שאתם רואים, זוהי אפליקציה של command prompt, או בעברית- שורת הפקודה. אפליקציה זו מאפשרת לנו לנהל ולפקד על המחשב שלנו, כך שמי שמשיג גישה אליה יכול לעשות במחשב כרצונו. הפעילו את ממשק שורת הפקודה באמצעות קליק על האייקון שלו.



כעת, כאשר הפעלנו את ממשק הפקודה, נשתמש בו כדי להריץ את תוכנת notepad. כיתבו notepad.exe בממשק הפקודה ולחצו enter. הידד! הפעלתם את notepad באמצעות ממשק שורת הפקודה.

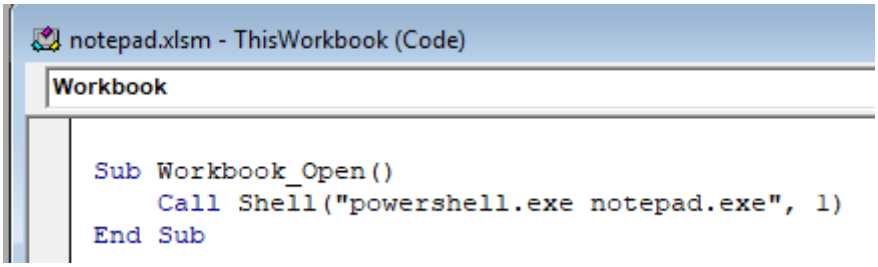
כעת אנחנו מבינים שהפקודה-

call shell (“notepad.exe”)

מבצעת באופן אוטומטי בדיוק את מה שעשינו כרגע באופן ידני- גורמת לפתיחת אפליקציה של notepad. הדבר האחרון שנותר לנו להבין הוא מהו ה-1 שורת הפקודה, וממנו קוראת לתוכנית שבסוף הפקודה?. כדי להבין מה הוא עושה, פשוט נשנה אותו ונלמד לבד. קיבעו את הערך שלו ל-3 והריצו את המקרו. לאחר מכן ל- 2 והריצו. מה ההבדל?

כעת נתקרב עוד שלב קטן לחיקוי הדרך שבה נוזקות עובדות.

העתיקו את הפקודה הבאה:



הוספנו לפקודה עוד חלק- powershell.exe. מה יתבצע כעת? הריצו ובידקו בעצמכם!

כפי שראיתם, הורצו שתי תוכנות. ראשונה עלתה תוכנית בעלת מסך כחול. שניה עלתה notepad. התוכנה עם המסך הכחול נקראת powershell, והיא זו שמריצה את Notepad. מהי תוכנת Powershell וכיצד היא פועלת? על כך נלמד בהמשך.