



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

מדיניות אבטחת מידע למערכת אנטי וירוס (sep14), סריקת המחשב והתקנים נתיקים

טבלת מהדורות:

תאריך עדכון	מאשר	תיאור השינוי	מהדורה
24.6.18		כתיבת המסמך	
	מר אבנר שריקר-מנהל חטיבת אבטחת מידע וסייבר שע"מ	מר בני מזרחי- ראש גף אב"מ, שע"מ	1
	מר קובי קרוזדו- מנהל אגף א' ביטחון, חירום אבטחת מידע וסייבר, מס הכנסה ומסמ"ק	מר דרור בנימין- מנהל תחום אב"מ, מס הכנסה ומסמ"ק	2



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

תוכן העניינים

4.....	1. הקדמה
4.....	1.1. מה זה וירוס מחשב.....
5.....	1.2. הווירוס הישראלי הראשון.....
5.....	1.3. כיצד מתגוננים מהוירוסים (רוגלות).....
5.....	1.4. מאפייני תוכנות האנטי-וירוס.....
6.....	1.5. תכונות מערכת האנטיווירוס.....
7.....	2. כיצד אנו מבצעים סריקה של ההתקן הנייד או את המחשב.....
7.....	2.1. סריקת התקן נייד.....
13.....	3. סריקת המחשב כולו.....
17.....	4. חיבור טלפון סלולארי.....
18.....	5. נספח-1.....
19.....	6. נספח-1.....



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

**אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין**

אגף אבטחת מידע שע"מ

1. הקדמה.

לאחרונה מתקבלות התראות להימצאות וירוסים ורוגלות במחשבים של עובדי מס הכנסה ומיסוי מקרקעין במשרדים, אשר אותרו ע"י תוכנת האנטי וירוס שלא מצליחה להסירם, דבר העלול להוות סיכון ופגיעה במערכת שע"מ וכן בציוד ובמאגר המידע. לאור האמור אנו רואים לנכון ולהביא לידיעת העובדים את הדרכים להתגוננות מפני וירוסים (רוגלות) אלו וכיצד לסרוק את מחשבם האישי. באופן כללי רקע וסקירה בנושא וירוסים (רוגלות) והגנה מפניהם.

1.1. מה זה וירוס מחשב?

וירוס מחשב (באנגלית: Computer Viruses) (וע"פ האקדמיה ללשון עברית: רוגלה) הם מהצרות הגדולות ביותר של עולם המחשב, אך בניגוד לתקלות אחרות, שלרוב נגרמות באקראי בגלל רשלנות או בשל כשלי חומרה, הוא נעשה בזדון ומתוך כוונת מכוון, להסב נזק! פעילותו דומה לזו של וירוס ביולוגי. כשם שווירוס ביולוגי חודר לגרעין התא של אורגניזם חי ומורה לו לשכפל את ה-DNA הוויראלי, כך הוא משתמש בחלבוני התא לייצר וירוסים נוספים במקום לשכפל את התא עצמו, וירוס מחשב, הוא בעצם תוכנה לכל דבר ועניין, שחודרת למחשב באופן סמוי, משתמשת במשאבי המחשב להעתיק ולהפיץ את עצמה ולרוב פוגעת בפעולה התקינה של המחשב הנגוע.

וירוס המחשב הידוע הראשון נוצר ברשת ה-ARPAnet, כאשר סטודנט ערך ניסוי בהחדרת קוד בלתי נראה לרשת, והצליח מעל לתחזיותיו.

בשנת 1985 היו מוכרים 11 סוגי וירוסים שונים, ובשנת 2008 המספר הגיע למיליון וירוסים שונים. במוצע מתגלים בכל חודש בין 50 ל-100 וירוסים חדשים. ישנם וירוסים חלקם מתקדמים יותר וחלקם פחות. הווירוס עלול לגרום לנזק בלתי הפיך למחשב - להרוס את מערכת ההפעלה או למחוק קבצי מידע חשובים, בנוסף ליכולתיו להפיץ את עצמו ביעילות מרובה ולהסוות את עצמו בפני תוכנת האנטי-וירוס.

בשנת 2004 התגלה הווירוס הראשון לטלפון נייד. הווירוס, שכונה "קאביר", נוצר כדי להראות היתכנות של הדבקה. ב-2007 כבר היו ידועים כמה מאות של וירוסים לטלפונים ניידים. רובם של הווירוסים הניידים תוקפים טלפונים בעלי מערכת הפעלה מסוג סימביאן, שהייתה המערכת הנפוצה בטלפונים חכמים (עד שנת 2011) שתי דרכי הפצה העיקריות בטלפונים ניידים הם באמצעות תקשורת הבלוטותי ובאמצעות מסרי המולטימדיה המהירים MMS.

כיום ישנם מערכת אנדרואיד ומערכת ההפעלה של האייפון – iOS שגם הם סובלות ממתקפות וירוסים.



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

**אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין**

אגף אבטחת מידע שע"מ

הווירוס הישראלי הראשון באוקטובר 1987 הופיע וירוס 'ירושלים' באוניברסיטה העברית. זה היה הווירוס הראשון שתוכנן לפגוע בזיכרון המקומי. וירוס 'ירושלים' היה הרביעי בסדרת וירוסים שנוצרה כנראה ע"י אותו אדם. וירוס זה היה הווירוס הראשון שהדביק קבצים בעלי סיומות COM EXE. וירוס זה חולל שמות, לפני 24 שנה זיהו שני סטודנטים ישראלים במקרה את "וירוס ירושלים" ופיתחו בלילה אחד תוכנה שנלחמת בו. בהתחלה חילקו אותה בחינם, הקימו חברה ואחר כך מכרו אותה, שלימים הפכה להיות הבסיס הראשון לענקית האבטחה צ'ק פוינט.

כיצד מתגוננים מהווירוסים (רוגלות) ?

על מנת להתגונן מהווירוסים המזיקים המציאו את תכנת האנטי וירוס, אנטי-וירוס היא תוכנה שנועדה לאתר וירוסי מחשב ולהגן על המחשב מפני פעילותם.

מאפייני תוכנות האנטי-וירוס:

שומר בזמן אמת, מבצע סריקות בכל זמן פעילות המחשב, בודק ללא הרף דפוסים ועקבות של פעילות ויראלית, בזיכרון, בפעולות העיבוד ובגזרת ההפעלה. סורק דואר אלקטרוני, בודק בזמן קבלת דואר אלקטרוני או שליחתו שהדואר האלקטרוני אינו נגוע בוירוס. סורק כללי לבקשת המשתמש או על פי תזמון, סורק את הכוננים ומדיות האחסון של המחשב במטרה לזהות דפוסים ועקבות של וירוסים. מרבית תוכנות האנטי-וירוס מותקנות מקומית על המחשב ומתעדכנות משרתים מרכזיים כדי לחדש את מאגר הווירוסים המוכר להן. מלבד האנטי וירוס שאמור להגן על המחשב, ישנו את הפן האנושי שאמור להימנע מלהתקין תוכנות לא מוכרות או לא להשתמש בהתקנים ניידים לא מאושרים ע"י המשרד. כאשר מקבלים התקן נייד או כל קובץ המותקן על תקליטור או דיסק קבצים שמתקבלים ממשרדי רואה-חשבון ו/או עורכי דין או כל מייצג אחר, בטרם הפעלת הקבצים או ההתקנים הניידים יש לבצע סריקה ע"י תוכנת האנטי וירוס המותקנת במחשבכם. תוכנת האנטי וירוס המותקנת במערכות שע"מ ובמשרדי המשתמשים הינה אחת מהתוכנות הטובות בעולם בתחום ההגנה מווירוסים ורוגלות, תכנת Symantec Endpoint Protection תכונות מערכת האנטי וירוס: תוכנת האנטי וירוס תוכננה ותוכנתה לבצע מספר פעולות נוספות הפועלות ברקע, העובד ו/או המשתמש לא יודע / מרגיש את פעולתם.



שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	מס' הנוהל
תחילת תוקף:	מהדורה מס': 1

**אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין**

אגף אבטחת מידע שע"מ

קובץ החתימות מתעדכן מידי באופן אוטומטית (מתבצעת פעולת עדכון לגבי רוגלות או וירוסים חדשים שמתגלים מדי יום).

מתבצעת סריקה באופן אוטומטי של תחנות העבודה ללא התקנים נתיקים אחת לשבוע. מחלקת אבטחת מידע של שע"מ בשיתוף עם אגף הביטחון ואבטחת מידע של מס הכנסה ומיסוי מקרקעין מבצעים נעילה של כניסות USB להתקנים ניידים .

לצורך נעילה של התקנים אלו מתבקש שיתוף פעולה עם משרדי מס הכנסה ומיסוי מקרקעין.. על כל משרד לשלוח רשימת עובדים המורשים (להלן נספח 1) להשתמש בהתקנים ניידים באופן קבוע, הרשימה תהיה מאושרת ע"י מנהל המשרד ובשיתוף נאמן אבטחת מידע משרדי .

ניהול פתיחה וסגירה של ההתקן יתבצע למול אגף הביטחון ואבטחת מידע של מס הכנסה ומיסוי מקרקעין, שלאחר בדיקה תועבר אל הצוות המטפל בשע"מ .

כאשר מדובר באישור לתקופה קצרה יש לציין את משך התקופה לה נדרשת פתיחת ההתקן

למורשים להשתמש בהתקנים הניידים, ישנה אפשרות לסריקת ההתקנים הניידים באמצעות תוכנת האנטי וירוס המותקנת בתחנת הקצה .

חשוב לדעת:

במידה והמשתמש לא הצליח להפעיל את ה- CONSOLE של תוכנת האנטי וירוס ו/או לא מותקנת אצלו התכנה כמפורט מטה – יש לפתוח קריאה בדלפק הסיוע.

במידה והמשתמש לא מצליח להסיר/למחוק קובץ נגוע יש לפנות מיידית לדלפק הסיוע

השימוש בהתקנים ניידים מתבצע באופן של הרשאת התקן אל מול תחנה קצה (לא כל התקן ייפתח בתחנה), לכל התקן נוסף, נדרש אישור חדש.

בשלב מאוחר יותר ההתקנים יוצפנו, כך שההתקן המוצפן יזוהה בתחנה של העובד בלבד.

פתיחה ונעילת התקנים תהיה בהתאם לבקשת המנהל או מי מטעמו שתופנה למחלקת אבטחת מידע של מס הכנסה ומיסוי מקרקעין אל מול הצוות המטפל בשע"מ.



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:



אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

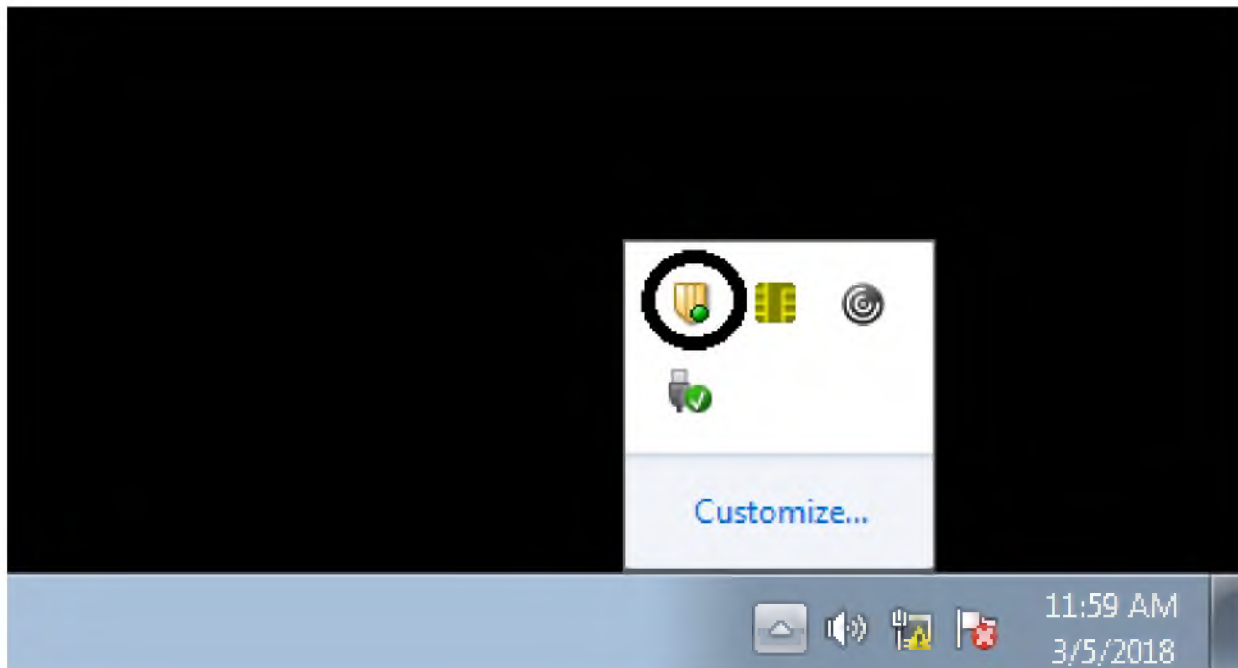
אגף אבטחת מידע שע"מ

1. כיצד אנו מבצעים סריקה של ההתקן הנייד או את המחשב?
עם חיבור ההתקן נייד, או העלאת קובץ יש לסרוק את ההתקן ו/או את הקובץ באופן הבא:

סריקת התקן נייד:

שלב א'

תכנת האנטי וירוס מותקנת במחשב ומופיעה בסרגל ההתחלה מצד שמאל (מסומנת בעיגול שחור)





מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

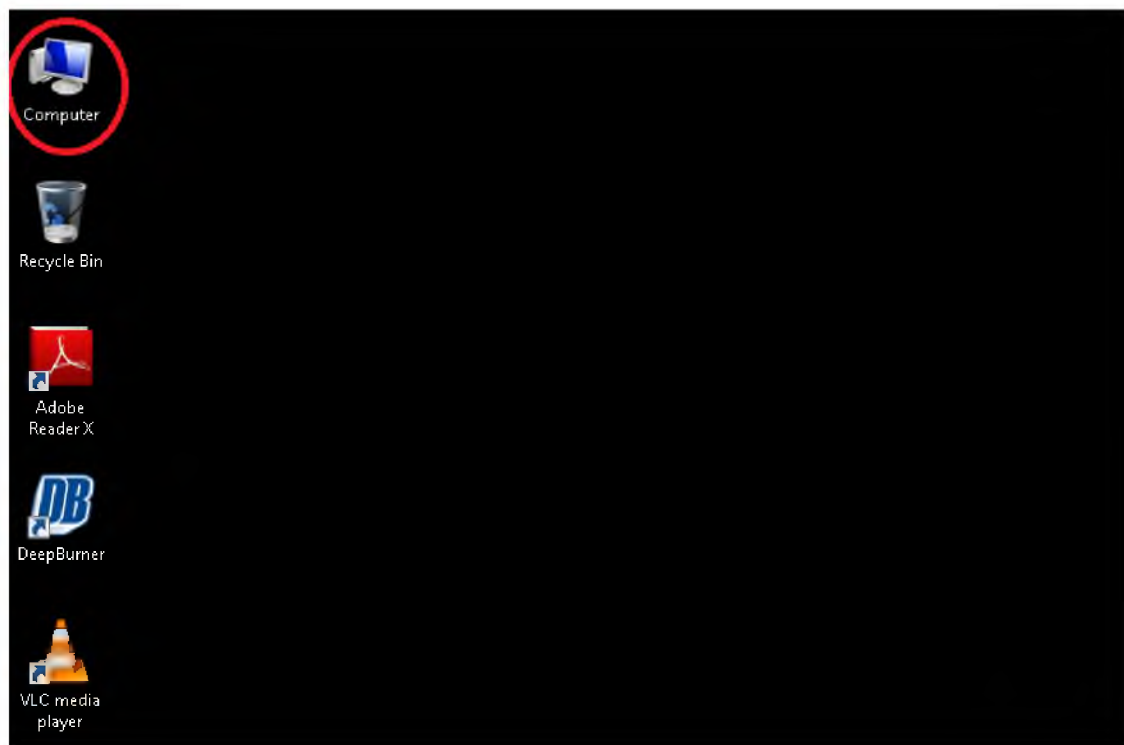


אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

שלב ב'

עם חיבור ההתקן הנייד, או העלאת קובץ יש לסרוק את ההתקן ו/או את הקובץ יש לעבור למחשב שלי המופיע על שולחן העבודה המופיע בתחנה הקצה (מסומן בעיגול אדום)





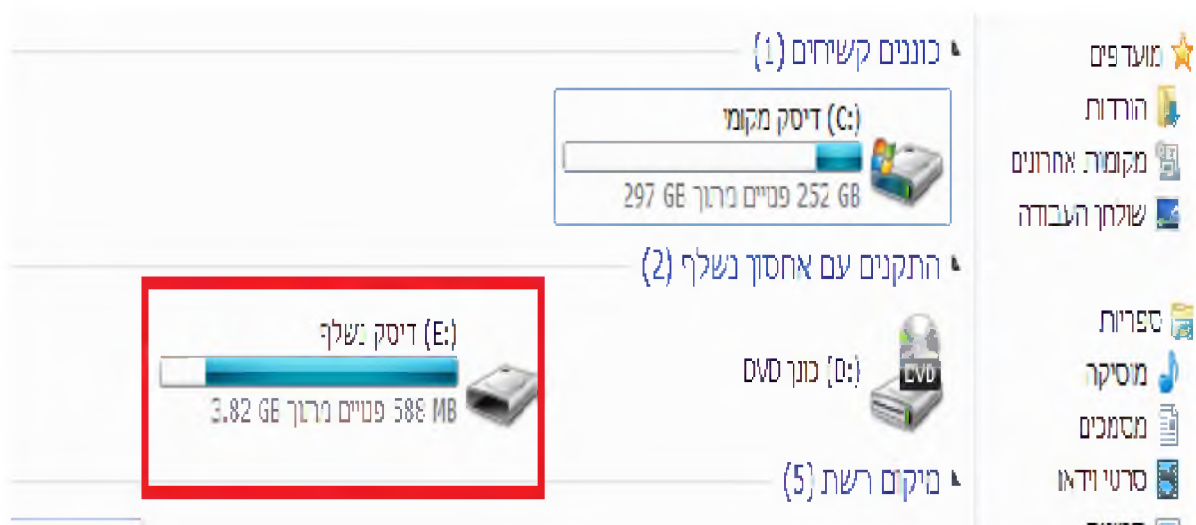
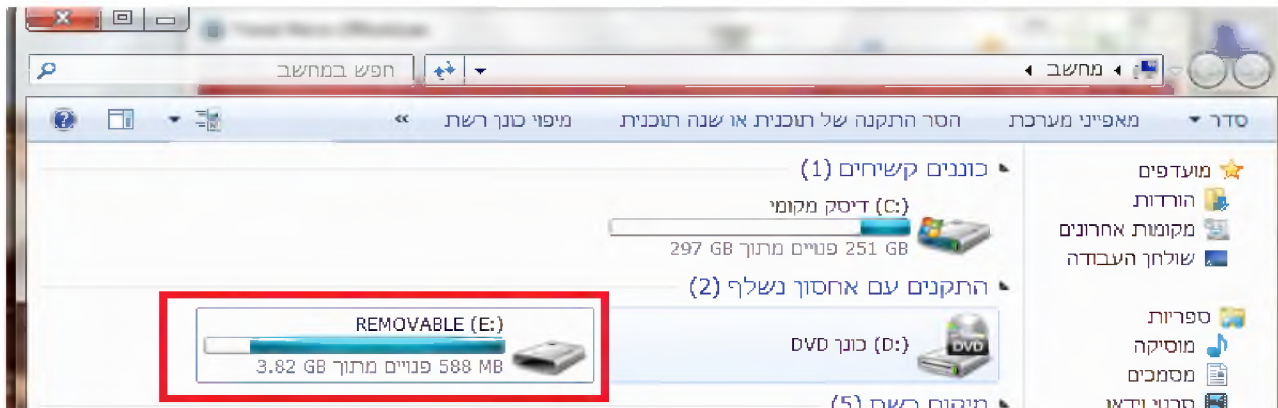
שם הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
מס' הנוהל	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

שלב ג'

לאחר כניסה למחשב שלי שבתחנת הקצה יש להגיע לקובץ בדרך כלל יופיע ככונן (E:) REMOVABLE או בשם (E:) דיסק נשלף (מסומן במלבן אדום)





מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

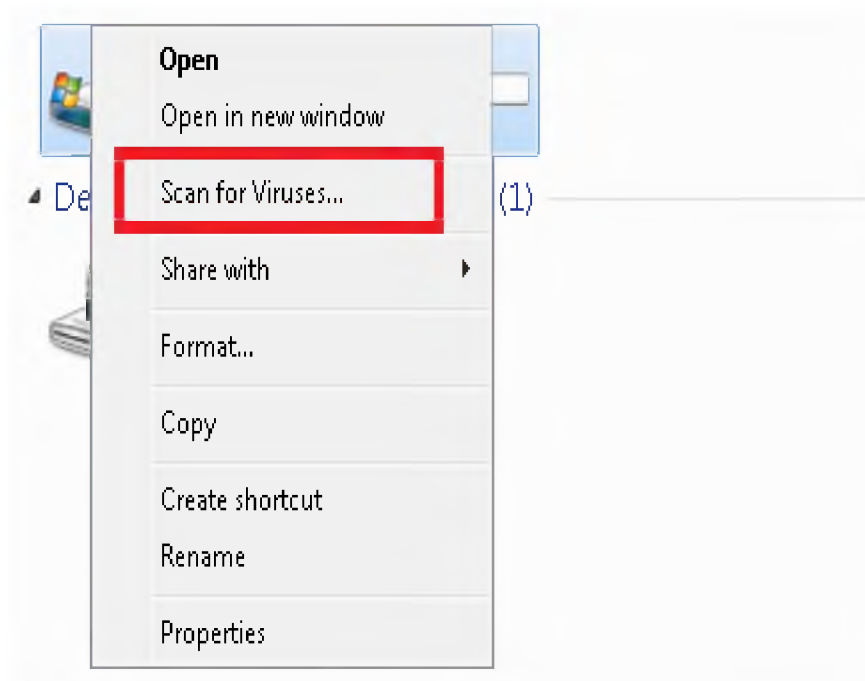


אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

שלב ד'

ניגשים לכונן E: ולוחצים על הקליק הימני בעכבר יפתח מסך ובו תופיע האפשרות Scan for viruses (מסומן במלבן אדום).





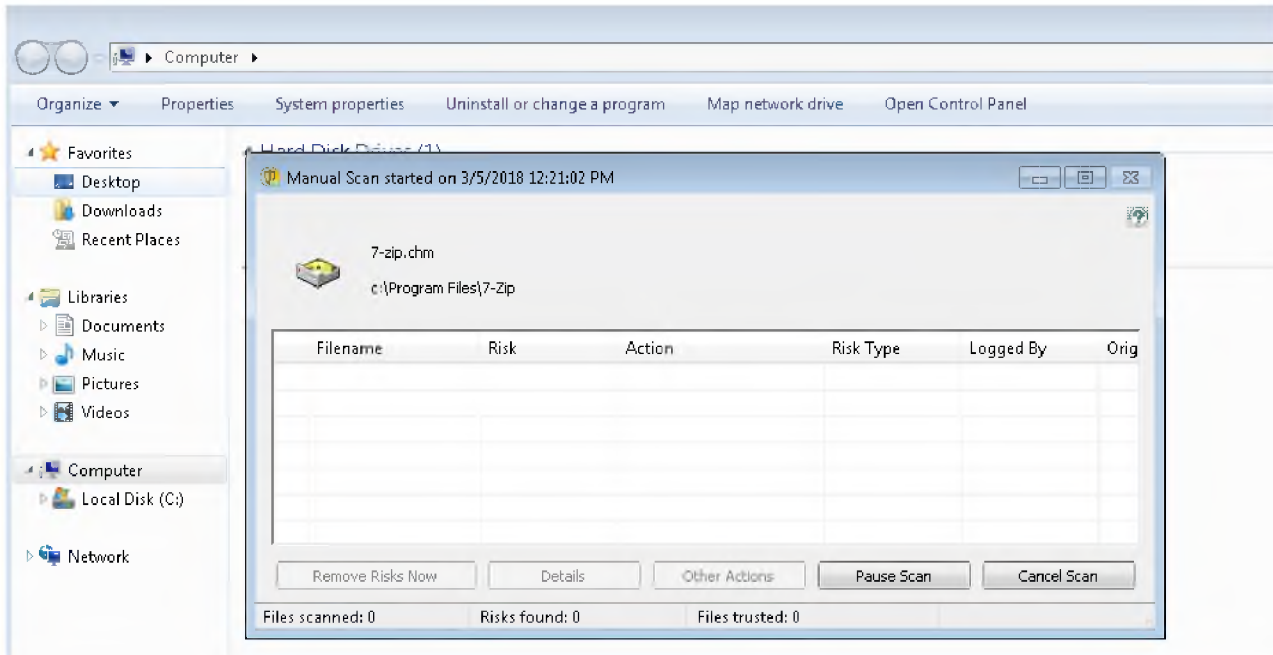
מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

שלב ה'

מקליקים על האפשרות המתוארת בשלב ד' ומתחילה הסריקה של ההתקן הנייד (כמופיע בתמונה)





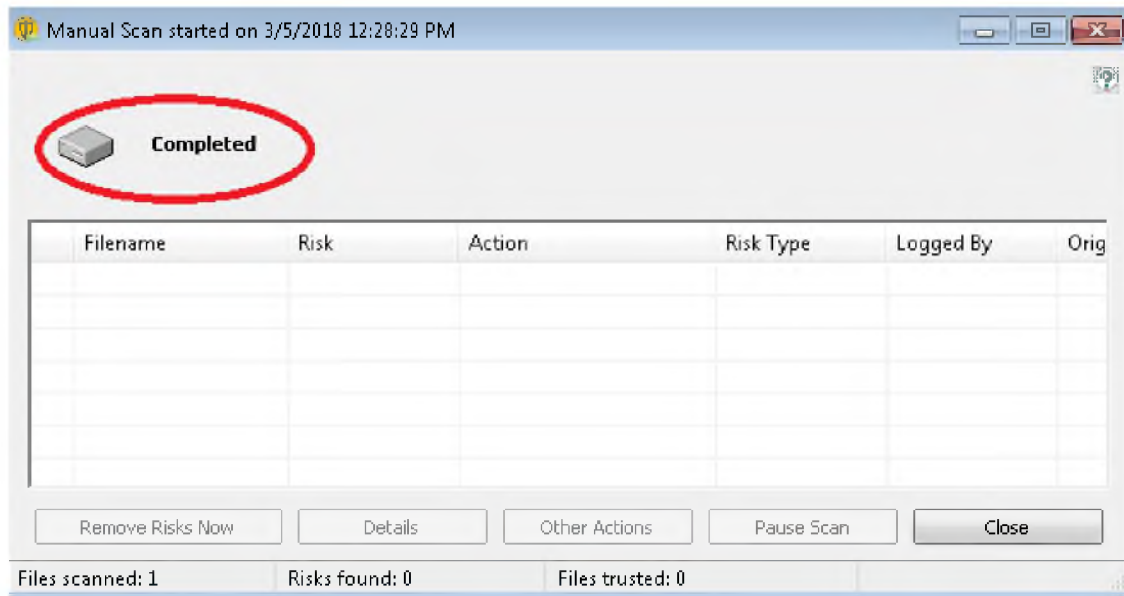
שם הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
מס' הנוהל	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

שלב ו'

עם תום הסריקה ע"י האנטי וירוס אמור להופיע המסך שמודיע שהסריקה הסתיימה כמופיע ומסומן באליפסה אדומה (הסריקה בוצעה בהצלחה ולא נמצאו וירוסים במידה והמערכת תמצא וירוסים, יוצג בטבלה שם הקובץ, שם הווירוס, הפעולה שבוצעה וכו').



שלב ז'

חשוב!

רק לאחר קבלת ההודעה (שלב ו') יש להפעיל את ההתקן הנייד או את הקובץ.

סריקת המחשב כולו:

לסריקת המחשב כולו יש לבצע את השלבים הבאים כאשר בשלב ג נבחר הפעם את כונן Local Disk C:

שלב א'

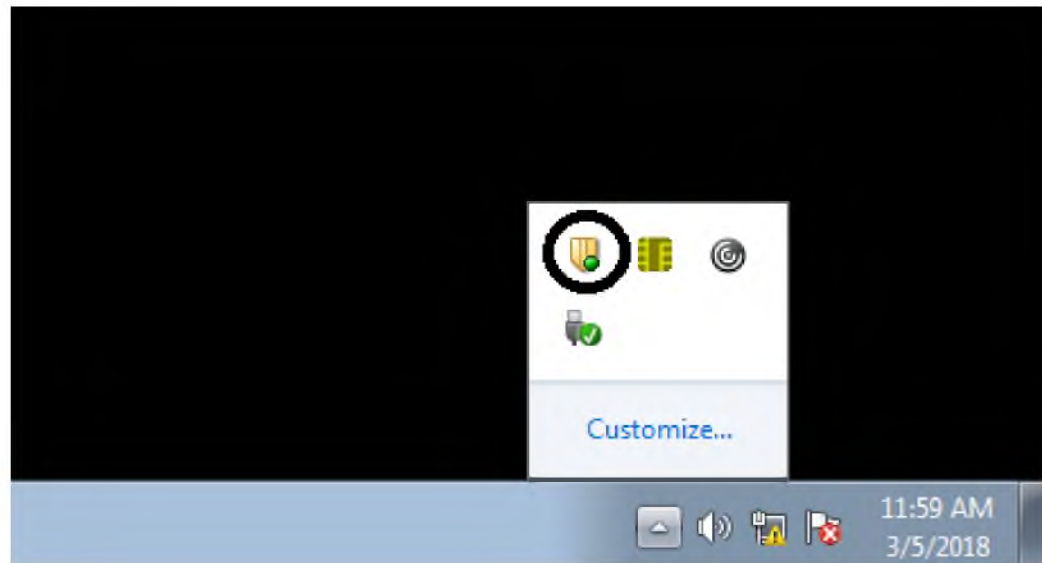
תכנת האנטי וירוס מותקנת במחשב ומופיעה בסרגל ההתחלה מצד שמאל (מסומנת בעיגול שחור)



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

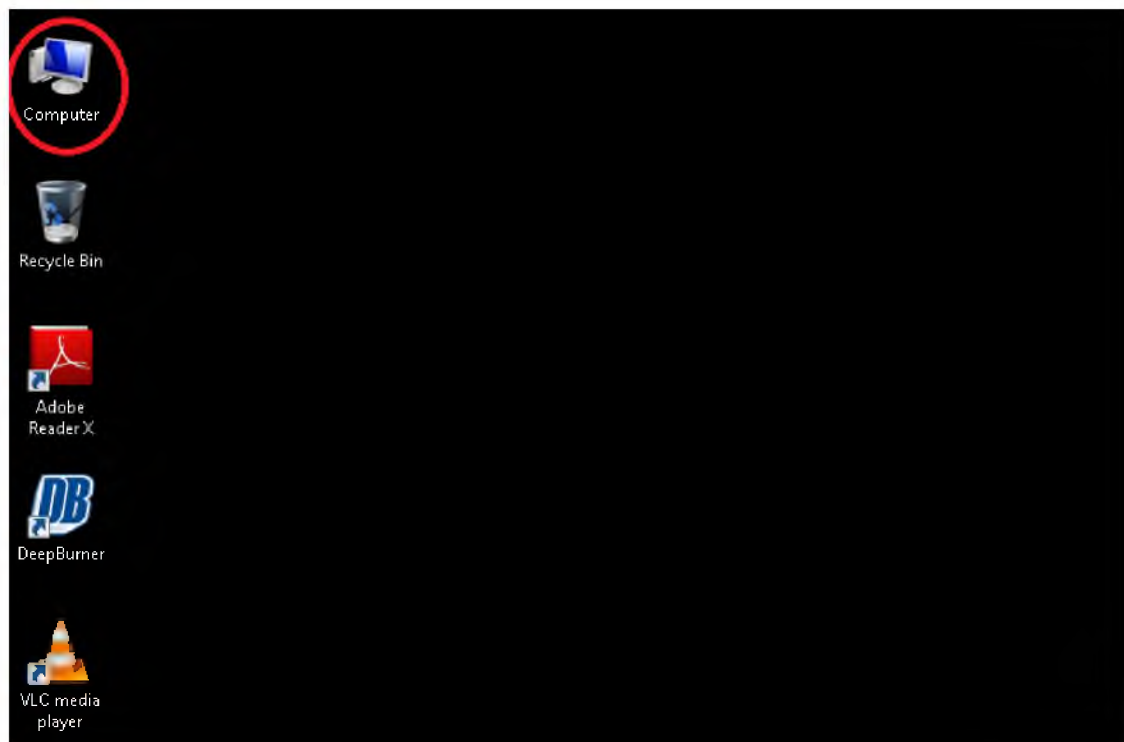
אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ



שלב ב'

אחת לכמה זמן יש צורך לבצע סריקה יזומה לדיסק המקומי של המחשב, לצורך כך יש לעבור למחשב שלי המופיע על שולחן העבודה המופיע בתחנה הקצה (מסומן בעיגול אדום)





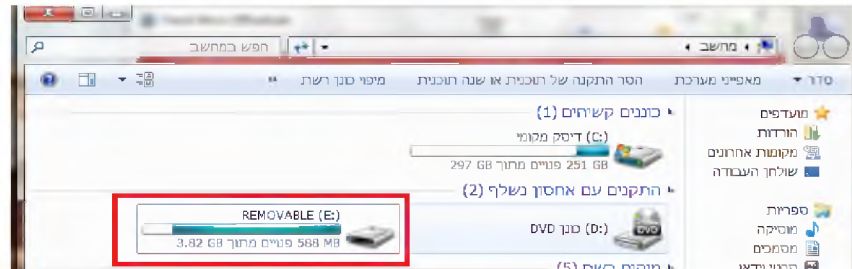
מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

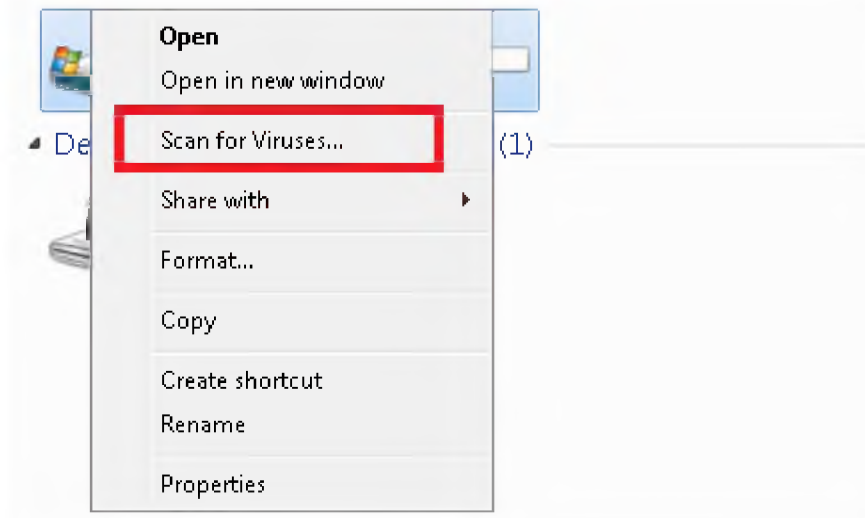
שלב ג'

לאחר כניסה למחשב שלי שבתחנת הקצה יש להגיע לכונן (C:) הרשום כדיסק מקומי



שלב ד'

נגישים לכונן c: ולוחצים על הקליק הימני בעכבר יפתח מסך ובו תופיע האפשרות Scan for viruses (מסומן במלבן אדום) .





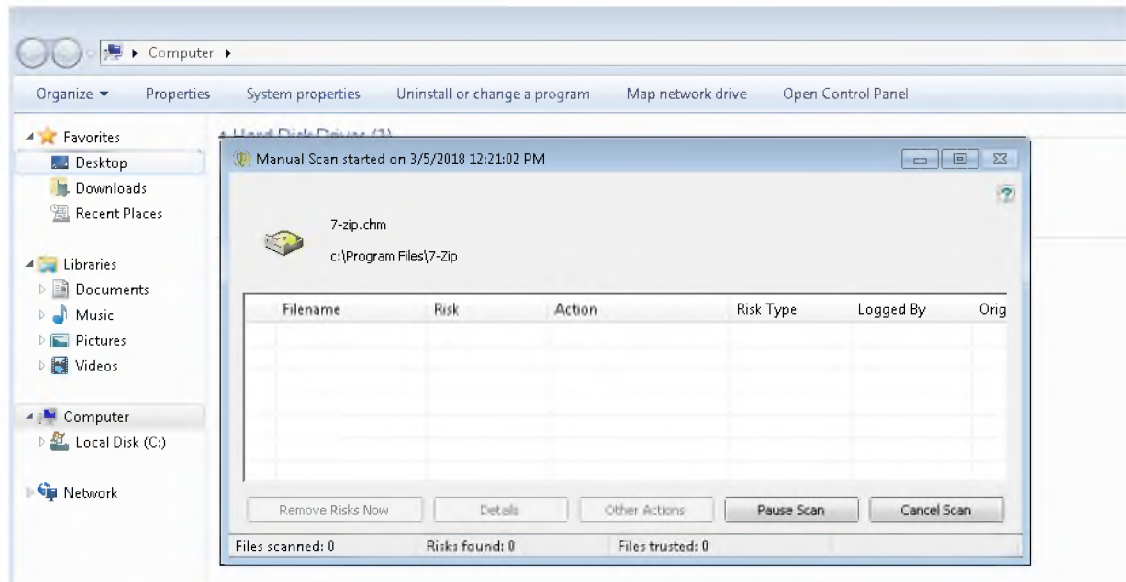
מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

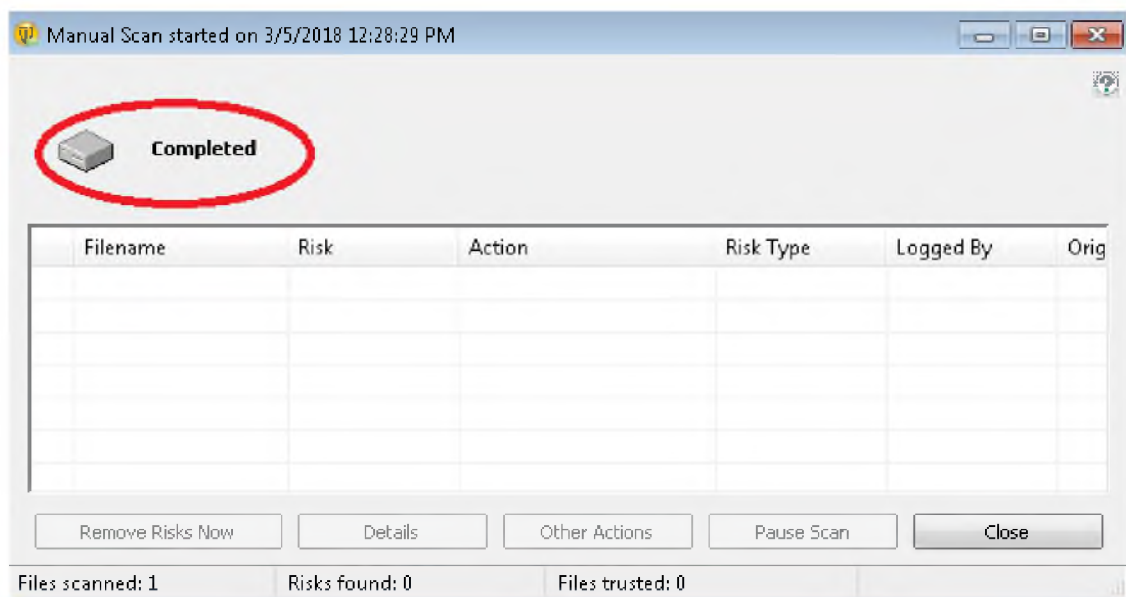
שלב ה'

מקליקים על האפשרות המתוארת בשלב ד' ומתחילה הסריקה של ההתקן הנייד (כמופיע בתמונה)



שלב ו'

עם תום הסריקה ע"י האנטי וירוס אמור להופיע המסך שמודיע שהסריקה הסתיימה כמופיע ומסומן באליפסה אדומה (הסריקה בוצעה בהצלחה ולא נמצאו וירוסים במידה והמערכת תמצא וירוסים, יוצג בטבלה שם הקובץ, שם הווירוס, הפעולה שבוצעה וכו').





מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

**אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין**

אגף אבטחת מידע שע"מ

חיבור טלפון סלולארי :

מכשירי הטלפון החכמים אינם עוד מכשיר שנועד בעיקרו לשיחת טלפון אלא מדובר למעשה במחשבים ניידים לכל דבר וככאלו משמשים למעשה ככלי העבודה הנייד המשמעותי ביותר כיום והמקושר לכל מערכות המחשב האחרות בהם אנו עושים שימוש.

שני איומים מרכזיים איתם יש להתמודד כאשר אנו עוסקים בהגנה בהיבטי אבטחת המידע: איסוף מידע באמצעות המכשירים הן על ידי תוקף חיצוני והן על ידי עובדי הארגון עצמו וזאת בעיקר על ידי התחברות באמצעות המכשיר למערכות המחשב של הארגון ושאיבת מידע מתוך הרשתות ואף החדרה של פוגענים שונים (וירוסים, תולעים ועוד). כמו גם איסוף מידע על ידי צילום, המכשירים מצוידים במצלמות באיכות גבוהה מאוד וכן הקלטת שיחות או דיונים רגישים באמצעות המיקרופון והאפשרות להעביר קבצי תמונה וקול בזמן אמת באמצעות האינטרנט או הבלוטוס.

בנוסף, כל המכשירים מצוידים ברכיב ג'י פי אס מובנה המאפשר את איתורו המדויק של המכשיר וכתוצאה מכך את מיקומו של המשתמש על כל המשתמע מכך. ראוי להדגיש כי יכולות אלו של המכשירים ניתנות לשליטה מרחוק ולהפעלה גם מבלי שהמשתמש חש בכך, רק לאחרונה פורסמו מספר מקרים שבהם חוקרים פרטיים עשו שימוש ביכולות כאלו לאחר שרכשו תוכנות לפריצה שמחירן עומד על מאות בודדות! של דולרים, ברור כי יכולותיהם של ארגוני ביון גבוהות מכך.

איום מרכזי נוסף שיש לתת עליו את הדעת היא היכולת לשאוב את המידע שעשוי בחלקו להיות רגיש האגור במכשיר עצמו כמו מיילים, מסמכים, מצגות ומסרונים. ראוי כמובן לציין כי יכולותיו של המכשיר הופכות אותו לכלי תקיפה מרכזי בתחום לוחמת הסייבר. בכדי להתמודד בהצלחה מרבית מול האיומים אנו נדרשים למצוא פתרונות, בעיקרם טכנולוגיים, שימנעו את האפשרות לפרוץ את המכשירים ולשאוב את המידע שנאגר בתוכם אך חשוב לא פחות מכך שימנעו את אפשרות השימוש ביישומים השונים במיוחד באותם אזורים המוגדרים כרגישים, כפי שנקבעו על ידי הארגון, הן על ידי המשתמש עצמו והן על ידי תוקף המפעיל יישומים אלו מרחוק. פתרונות פורצי דרך מסוג זה קיימים כבר כיום בישראל ואף נעשה בהם שימוש בשע"מ ורשות המסים.

בעת חיבור טלפון חכם (Smartphone), הטלפון יזוהה ככונן נייד באופן זהה להתקן נייד אחר ויש לנהוג לפי אותם השלבים!



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

נספח 1:

רשימת העובדים המורשים להתקנים ניידים למשרד _____					
מס"ד	שם	ת.ג.	תפקיד	מס' ציוד מחשב	מס' טלפון

אישור נאמן אבטחת מידע

אישור מנהל המשרד



מס' הנוהל	שם הנוהל: מדיניות אבטחת מידע למערכת אנטי וירוס, סריקת המחשב והתקנים נתיקים	
	מהדורה מס': 1	תחילת תוקף:

אגף הביטחון ואבטחת מידע
מס הכנסה ומיסוי מקרקעין

אגף אבטחת מידע שע"מ

נספח 2 :

טופס בקשה להוספת התקן נוסף :

מספר ציוד מחשב	שם עובד	ת"ז	תפקיד	ההתקן	מס' טלפון	קבוע/זמני

אישור נאמן אבטחת מידע

אישור מנהל המשרד
