אנשים עם פתרונות
www.eset.co.il

מדיניות טיפול בוירוסים במחשב בודד

לא לדלג על שום שלב בדרך!

1) במידה והמחשב הוא חלק מרשת, **יש לנתק אותו תחילה מכל חיבורי הרשת שלו.**
2) יש לבטל **System Restore.**
(My Computer > Properties > Advanced > system restore > Turn Off System Restore.
לאחר ניקוי הוירוסים יש להחזיר את ה System Restore)
3) מחיקת **Temporary Internet files**.
C:\Documents and Settings\user\Local Settings\Temporary Internet Files
4) מחיקת תכנים של תיקיות **Temp**.
c:\windows\temp
C:\Documents and Settings\user\Local Settings\Temp
בויסטה - c:\Users\user\AppData\Local\Temp
5) וידוא כי האנטי וירוס **מותקן** ו**פעיל**. במידה ומותקנת גרסה 3, יש לשדרג לגרסה 4 העדכנית ביותר.
6) וידוא כי האנטי וירוס **מעודכן**.
7) וידוא כי ההגדרות הבאות קיימות :
   א. Real Time Protection **Enable**
   ב. Advanced Heuristic **Enable** (בתוך ב Real Time Protection)
   ג. Potentially Unwanted Applications **Enable**
   ד. Anti-Stealth Technology **Enable**
8) **ביצוע עדכוני מיקרוסופט** Windows קריטיים.
9) סריקה יזומה **במצב בטוח** (Safe Mode).
במידה ולא מצליחים להתקין אנטי וירוס, ניתן להשתמש בשירות סריקה מקוון של ESET
(http://www.comsecure.co.il/maineos.aspx)
במידה והבעיה לא נפתרה, המשך לסעיפים הבאים:
10) **הרצת ESET Sysinspector** בפעם הראשונה והוצאת לוג (File > save as)
(http://www.eset.co.il/home/doc.aspx?mCatID=9930).
11) **שליחת לוג לתמיכה כדי לאפשר טיפול בתהליכים חשודים** שנמצאו בלוג של ה- Sysinspector .
12) **הרצת ESET Sysrescue CD** (http://www.eset.co.il/home/doc.aspx?mCatID=9930)
13) **הרצת ESET Sysinspector** בפעם השנייה והוצאת לוג סריקה.
14) **השוואה בין שני הלוגים** - הראשון והשני – באמצעות ה-Sysinspector.
15) **בדיקה ידנית** אחר מזיקים ותהליכים זדוניים שעלולים להימצא בנתיבים הבאים:
   א) *c:\windows\system32* יש לסנן לפי תאריך שינוי אחרון ולחפש אחר קבצי exe ו dll חשודים (הרצת חיפוש בגוגל)
   ב) *HKLM > software > Microsoft > Winnt > windows \ Winlogon > notify*
   ג) *HKLM > software > Microsoft > windows > current version > run*
   ד) *HKCU > software > Microsoft > Winnt > windows \ Winlogon > notify*
   ה) *HKCU > software > Microsoft > windows > current version > run*
16) במידה והמחשב נגוע בצורה הרסנית, יש לשקול בחיוב רב את פרמוט המחשב.

תמיד לשירותכם,
צוות תמיכה טכנית קומסקיור בע"מ
support@eset.co.il | www.eset.co.il/support