


תוכנות ריגול

כיצד תוכנות הריגול נכנסות למחשב שלנו ?

תוכנות הריגול נכנסות למחשב שלנו באחת מהצורות הבאות :


א. נפתח חלון של פרסומת "קופצת" על המסך, ולחצנו עליו.


במקרים מסויימים הפרסומת שנפתחת בחלון נראית כמו פרסומת לאתר קניות, אתר חיפוש או כל אתר אחר - אך יש לזכור - פרסומות "קופצות" יש לסגור מייד - אם באמצעות סמל ה-X בפינת החלון או על ידי צרוף המקשים ALT+F4 שסוגר את החלון גם במידה ואין לו X בפינה.

לעתים הפרסומת מסווה את עצמה להודעת שגיאה של Windows, ובתוך חלון הפרסומת יהיה סמל של  או של .

כמו הודעת שגיאה סטנדרטית של Windows.

אז איך יודעים אם זוהי באמת הודעת שגיאה של Windows או פרסומת מתוחכמת? **פשוט מאוד!**

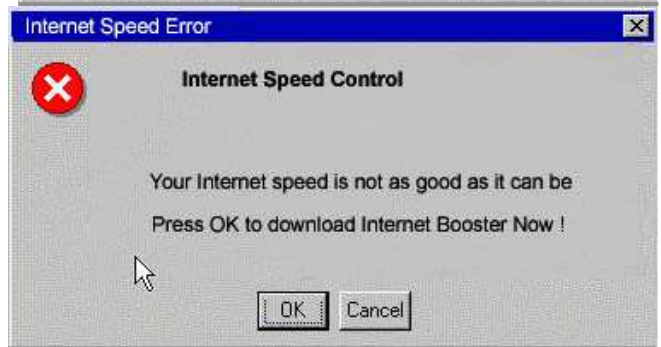
אם כאשר מציבים את סמן העכבר על הפרסומת (או החלון שחשוד שהוא פרסומת), סמן העכבר נראה בצורת כף יד  - זוהי פרסומת ולא הודעת שגיאה של Windows - ומומלץ לא ללחוץ עליה.

אם כאשר מציבים את סמן העכבר על הפרסומת (או החלון שחשוד שהוא פרסומת), סמן העכבר נראה בצורת חץ  (הסמל הרגיל של סמן העכבר) - זוהי הודעת שגיאה של Windows ולא פרסומת קופצת.

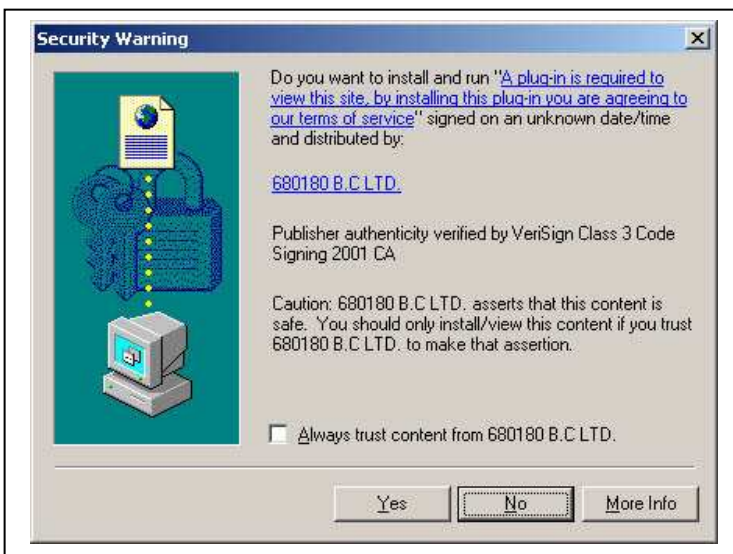
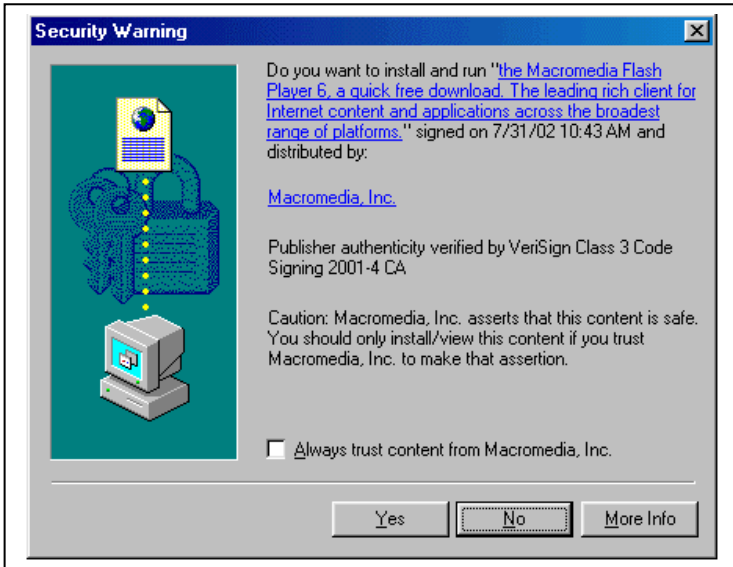
דוגמה :

**הודעת שגיאה עם סמן של קישור (כף יד) - זוהי פרסומת - לא ללחוץ!
אין לדעת איזו תוכנה תתקין את עצמה או לאיזה אתר הפרסומת תכניס אותנו ברגע שנלחץ עליה.**

**הודעת שגיאה של מערכת ההפעלה עם סמן בצורת חץ - זוהי הודעת שגיאה אמיתית.
(כמובן בהודעת שגיאה אמיתית של Windows ההודעה תציג מידע אמיתי, ולא כמו בדוגמה הנ"ל - שבה ההודעה מציעה להוריד תוכנה שתאיץ עבורי את מהירות האינטרנט.)**



ב. נכנסנו לאתר כלשהו, ובעת הכניסה נפתח חלון של התקנת תוכנה, ואישרנו את התקנת התוכנה



אתרי אינטרנט רבים מנצלים את חוסר הידע של משתמשי אינטרנט רבים על מנת להתקין במחשביהם תוכנות לא רצויות. התקנה זו נוצרת כאשר האתר מבקש להתקין במחשב שלנו רכיב שחוסר על מנת להציג את האתר כראוי. הדף שנפתח על המסך נראה בצורה הבאה :

לדוגמה : בדף זה מוצגת בקשה להתקנת תוכנה (Plug-In) אשר דרושה לשם הצגת האתר כראוי. במקרה זה, זו תוכנת "ריגול" ולא תוכנה אמיתית שדרושה לפעולה תקינה של האתר.

אז כיצד יודעים אילו תוכנות ניתן להתקין ואילו אסור להתקין ?

שם החברה שמפיצה את התוכנה מוצג בצבע כחול במרכז החלון - במקרה זה :

LTD.B.C.680180

רוב התוכנות שמתקינות את עצמן בצורה זו מזדהות על ידי שם הגיוני, כגון: Flash Player 7 או Microsoft Windows Update וכדומה. רשימה מלאה של התוכנות שמתקינות את עצמן בצורה זו היא ארוכה מכדי לפרט כאן, אך אמליץ שבכל מקרה שנפתח חלון מעין זה אשר לא הוסבר עליו לפני כן באתר (למעט התוכנות שהזכרתי לעיל), מומלץ לענות על השאלה בחלון זה ב- NO.

ניתן גם לדעת מעט פרטים לגבי מהימנות חלון ההורדה הנ"ל על פי החברה שביצעה את החתימה האלקטרונית של התוכנה. לדוגמה, בחלון זה, רשום שהתוכנה היא Verified - חתומה, בידי חברת VeriSign, שהיא אחת החברות הגדולות בעולם לביצוע חתימות אלקטרוניות לתוכנות. למרות זאת, חלון זה הוא של תוכנת ריגול למדהרין ! לכן הכלל פשוט - **לא מכירים - לא מורידים.**

להלן דוגמה לחלון הורדה של תוכנה מהימנה :

כאמור, חלון ההורדה הנ"ל הוא של תוכנה מהימנה ולא של תוכנת ריגול. איך אני יודע ? כיוון שחלון זה נפתח על המסך **ביודעין**, לאחר שנאמר באתר החברה שעל מנת להתקין את התוכנה (במקרה זה, ההתקנה היא של נגן פלאש 6, שהיא תוכנה שזקוקים לה כיום על מנת לצפות באתרי אינטרנט אינטראקטיביים)

דוגמה למספר סוגי Plugins שניתן לסמוך עליהם: (שם התוכנה יופיע בטקסט הכחול שבחלון)

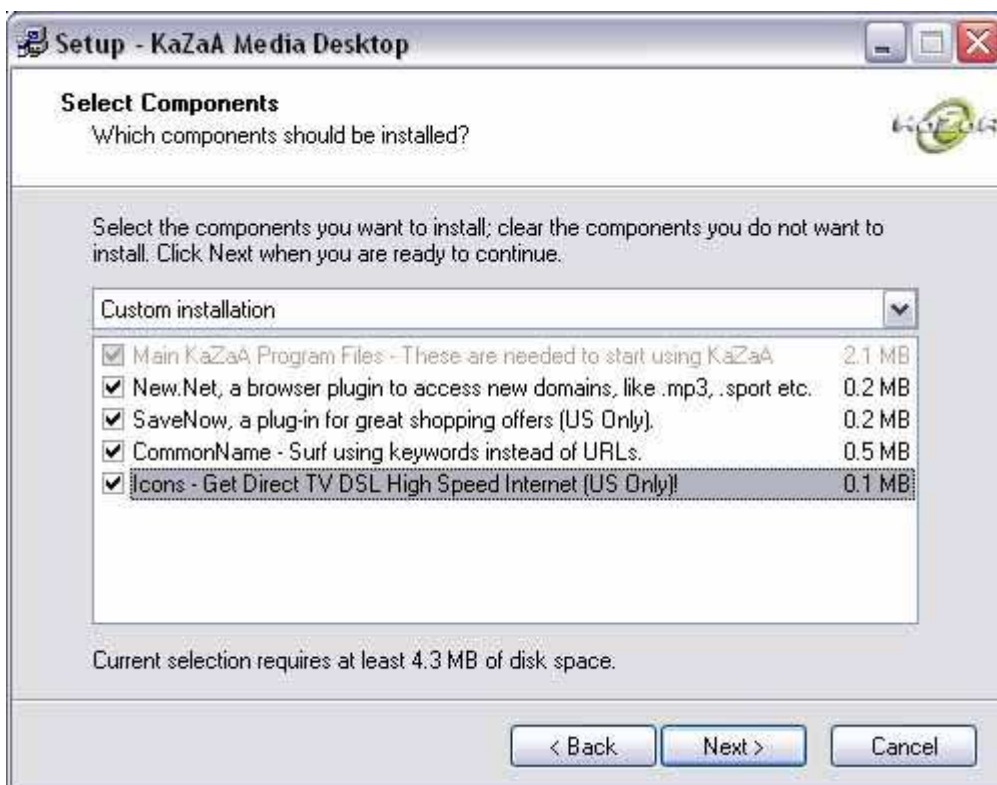
- Acrobat Reader (מציג קבצי PDF)
- Macromedia Flash (תוכנת עזר לצפייה באתרי פלאש)
- Shockwave (מולטימדיה תוסף)
- Media Player (תוסף מולטימדיה)
- Windows Update (חלונות תוכנת העדכון של)

ג. התקנה של תוכנת ריגול הנובעת מהתקנה של תוכנה אחרת

אחת הדרכים הנפוצות ביותר שבהן נכנסות תוכנות ריגול באין מפריע לתוך המחשב, הוא תוך כדי התקנה של תוכנה אחרת. בעת התקנה של תוכנות רבות, כגון Kazaa בגירסתה הרגילה ולא בגירסת Lite, יחד עם התוכנה מותקנות אצלנו במחשב תוכנות ריגול שאין בהן כל צורך. לדוגמה, תוכנת Domains New Net אשר מגיעה עם Kazaa בגירסתה המלאה, גורמת לפגיעה קשה בהגדרות הרשת וכן לביטול השיתוף של אינטרנט בין שני מחשבים, במידה וכזה שיתוף קיים.

הנה לדוגמה מוצג אחד מחלונות ההתקנה של תוכנת Kazaa Media Desktop. בחלון זה ניתן לראות עוד 4 תוכנות ריגול שמסומנות ב- ומתווספות להתקנה הסטנדרטית של התוכנה.

מיותר לציין, כי כברירת מחדל כל התוכנות מסומנות ב- ומותקנות עם התוכנה. אדם שמתקין את התוכנה רק על ידי לחיצה על NEXT יתקין בלא יודעין עוד מספר תוכנות ריגול יחד עם תוכנות סטנדרטיות שהוא מתקין במחשבו.



כל מי שטרי בעולם האינטרנט, וחושב שגלישה באתרי אינטרנט לא יכולה להזיק בשום דרך - טועה טעות מרה. גם אלו שרק גולשים ולא מורידים קבצים או משתמשים באינטרנט בצורה מקצועית חשופים למזיקים רבים. בחלק זה אסביר על תוכנות הריגול וכיצד להיפטר מהן.

אז מה זה תוכנת ריגול?

תוכנת ריגול היא תוכנת שמבצעת אחת או כמה מהאפשרויות הבאות:

- ✓ עוקבת אחר פעולות שמתבצעות בתוך המחשב ומעבירה אותן למחשב אחר או לאדם אחר באינטרנט.
 - ✓ גורמת לפתיחת מסכי פרסומת ללא כל צורך.
 - ✓ גורמת להאטה במהירות האינטרנט.
 - ✓ גורמת לפעילות מיותרת למחשב, מאמצת את מערכת ההפעלה ולא תורמת דבר למהירות העבודה.
 - ✓ שותלת קבצים בתוך הדיסק הקשיח, אשר נטענים בעת פתיחת המחשב ומשבשים את פעולתה התקינה של מערכת ההפעלה.
 - ✓ משבשת את הגדרות הרשת - למשל, מבטלת את שיתוף האינטרנט בין שני מחשבים או את החיגוי לאינטרנט.
 - ✓ מתקשרת אל מספר טלפון באמצעות המודם הרגיל וקו הטלפון - לעתים אל מספר טלפון בחו"ל, מבלי לבקש את אישור של המשתמש במחשב.
 - ✓ ישנם סוגים רבים של תוכנות ריגול, אך רובן ככולן גורמות לשיבושים בפעולתו התקינה של המחשב ושל הגלישה ברשת האינטרנט. לתוכנות רבות שאנו מורידים ומתקינים מרשת האינטרנט מתלוות תכונות של תוכנות ריגול. באופן כללי, ישנם 2 סוגים כלליים של תוכנות ריגול: **ADWARE - SPYWARE** : **SPYWARE** אלו תוכנות ריגול במלוא מובן המילה. הן עוקבות אחר פעילות המשתמש במחשב או מאיטות את העבודה במחשב, היות והן מתקינות לתוך המחשב תוכנות אשר עובדות "בסתר" ברקע של העבודה הרגילה. תוכנות אלו נכנסות לעתים בשל התקנה של תוכנות רגילות כגון Kazaa או אחרות, והן לא חושפות את עצמן בפני המשתמש.
 - ✓ אלו תוכנות שמזיקות פחות למחשב, אך לעתים הן יותר מציקות. תוכנות אלו גורמות לפתיחתם של חלונות פרסומת תוך כדי הגלישה, הצגה של פרסומות בתוך תוכנות ושינוי דף הבית של הדפדפן לדף הבית של החברה המפרסמת.
- לעתים תתקלו בשם **Malware** שמתייחס ל- **malicious software** - כלומר תוכנות בעלות כוונה זדונית - שהכוונה כאן גם לתוכנות ריגול, לזירוסים ול"סוסים טרויאניים" - שהן תוכנות שפורצות למחשב או הורסות אותו.

כללי ברזל - איך לא להידבק ומה לעשות אם נדבקנו

1. לא ללחוץ על פרסומות עם העכבר. יש לסגור אותן עם ה-**X** או אם אין, עם צרוף המקשים **Alt+F4** במקלדת.
2. לא לאשר התקנה של תוכנות לא מוכרות במחשב. הכלל פשוט **לא מכירים -- לא מאשרים**.
3. לא להתקין תוכנות ממקורות לא אמינים ולא מזוהים.
4. כאשר מתקינים כבר תוכנה - לשים לב לרכיבי התוכנה שאנו מתקינים - ולא התקין רכיבי תוכנה שהם תוכנות פרסומת או ריגול.
5. להוריד רק תוכנות מוכרות וידועות.
6. לא לטייל באתרי אינטרנט "מפוקפקים" שמכילים פורנו, פיצוחים, האקרים וכדומה. באתרים אלו הסיכוי "לחטוף" תוכנת ריגול הוא גבוה פי כמה מהאתרים הסטנדרטיים.
7. במידה ואתם שומעים את המודם שלכם מחייג (הכוונה לחיגוי רגיל של טלפון), ולא הפעלתם חיגוי כלשהו - קודם כל נתקו את הכבל טלפון מהשקע. ייתכן ונכנסה אליכם תוכנת ריגול שהפעילה חיגוי אל טלפון בחו"ל בתשלום, ואתם תחוייבו על כך.
8. במידה והמחשב פועל בצורה מוזרה, איטית יותר, האינטרנט נראה לכם איטי או כל חשד אחר - בצעו סריקה במחשב באמצעות ה-**Ad-Aware** וגם האנטי-וירוס. ייתכן ונכנסה אליכם תוכנת ריגול / טפיל או אפילו וירוס.
9. במידה והאנטי-וירוס או הפיירוול שלכם הפסיקו לעבוד פתאום (יש עליהם למשל סמל של X אדום), קודם כל נסו לכבות ולהדליק את המחשב - ייתכן וזוהי בעייה רגעית. אם הבעייה נפתרה לאחר כיבוי והדלקה, בצעו בדיקת וירוסים וטפילים מייד! אם הבעייה לא נפתרה - נראה שיש לכם במחשב וירוס ויש לטפל בו או להזמין טכנאי.
10. הכי חשוב - בצעו סריקה מדי שבוע של וירוסים ותוכנות ריגול על ידי התוכנות שהומלצו באתר זה. כך תוכלו למנוע לעצמכם הרבה צרות והרבה בעיות שאני בטוח שאין לכם צורך בהן

כיצד להיפטר מתוכנות הריגול ?

א. סגירת פרסומות קופצות :

1. סגירת החלון של הפרסומת על ידי ה- שבפינת החלון. במידה ואין או שהחלון מכסה את כל המסך, יש ללחוץ רצוף על מקש **ALT** ולהוסיף לחיצה בודדת (תוך כדי) על מקש **F4** במקלדת. צרוף המקשים הנ"ל יסגור את החלון.
 2. במידה ומותקנת במחשב תוכנת Firewall שיש לה יכולת לחסום גם פרסומות (הסבר יובא בחלק של תוכנות פריצה), יש להגדיר לה לחסום חלונות של פרסומות (AD-Blocking).
 3. להתקין במחשב תוכנה שחוסמת פרסומות מסוג Pop-Up כגון: [Pop-Up Stopper](#), [Stop The Pop](#) וכדומה. תוכנות אלו הן בעלות יעילות מוגבלת - התוכנה תסגור חלונות פרסומת שהוגדרו לה במאגר המידע שלה כפרסומות. חלונות פרסומת שלא הוגדרו בתוכנה לא ייסגרו על ידיה. בנוסף, לעתים תוכנות אלו חוסמות גם חלונות "קופצים" סטנדרטיים שיש צורך בהם.
 4. להתקין תוכנה שסורקת את המחשב וה-Windows ומוחקת כל פריט שגורם לפתיחה של חלונות פרסומת. ישנן מספר תוכנות מאוד מוצלחות בתחום זה, אך המפורסמות ביותר הן: [Ad-aware](#), [Spybot](#)
-

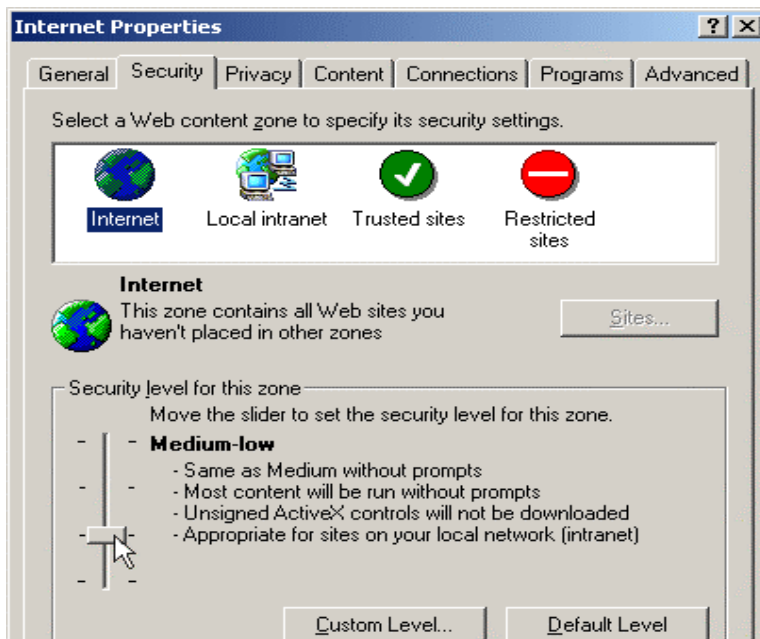
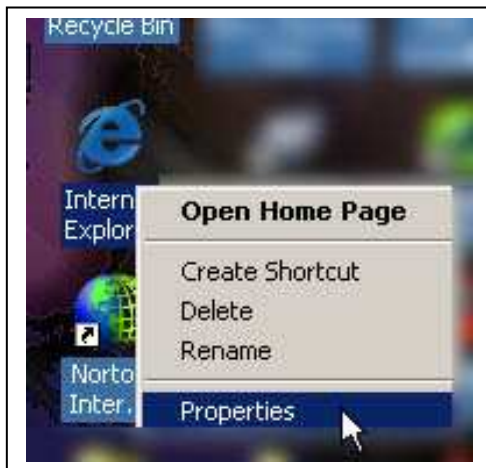
ב. מניעת התקנה של Plug-ins לא רצויים

על מנת להעלות את רמת הבטחון שלנו בעת גלישה ברשת האינטרנט, ניתן להעלות את רמת האבטחה של הדפדפן (Internet Explorer). העלאת רמת האבטחה תגרום לכך שפחות חלונות ייפתחו באופן אוטומטי, ואנו נתבקש לאשר ידנית את ההורדה של תוכנות תוסף (Plug-Ins) מהאינטרנט.

החסרון בהעלאת רמת האבטחה של הדפדפן הוא בכך שיייתכן שאם רמת האבטחה גבוהה מדי, חלק מהאתרים לא יוצגו כראוי או לא יוצגו כלל. נתקלתי, לדוגמה, בבעייה שבה המשחקים באתר וואלה לא פעלו, אלא אם הגדרתי את רמת האבטחה כנמוכה ביותר. מיותר לציין, שברמה כזו, כל תוכנה ותוסף שרוצים להתקין את עצמם בתוך המחשב - מצליחים ולעיתים גם לא מציגים לנו איזושהי אינדיקציה שנכנס לתוך המחשב שלנו משהו חדש (ומזיק...).

ובכל זאת : כיצד משנים את רמת האבטחה של הדפדפן

ההסבר יובא עבור Internet Explorer



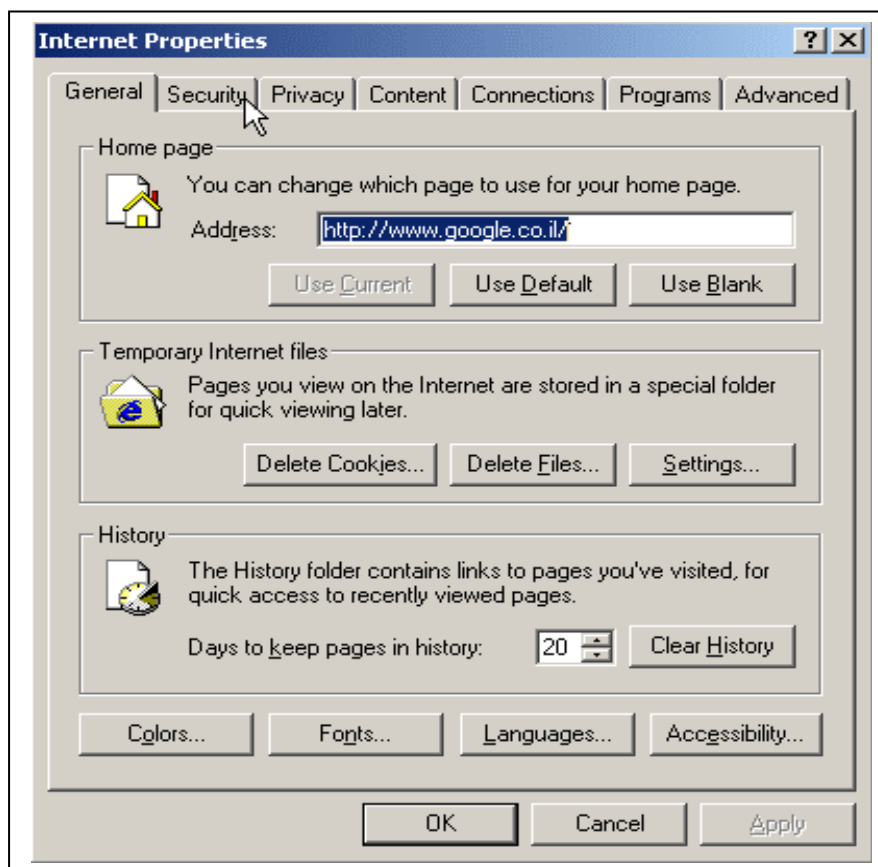
. יש להגיע לשולחן העבודה של ה-Windows (המסך ההתחלתי שנפתח עם הדלקת המחשב)

2. יש ללחוץ לחצן ימני של העכבר על גבי סמל ה-Internet Explorer שעל גבי שולחן העבודה. לחיצה על לחצן זה צריכה לפתוח תפריט עם מספר אפשרויות. מהאפשרויות שנפתחו יש לבחור באפשרות **מאפיינים** או **Properties**. (התחלונה בתפריט זה) - ראה תמונת דוגמה משמאל.

במידה ולא מופיעה האפשרות "מאפיינים" או "Properties", יש להיכנס לתפריט זה דרך לחצן **התחל-הגדרות-לוח הבקרה ו- הגדרות אינטרנט**

או באנגלית : **Start <- Settings <- Internet Options <- Control Panel**

3.1 בתפריט שנפתח נבחר בכרטיסייה העליונה של **אבטחה** או **Security**.



4. לאחר שהתחלף תוכן הכרטיסייה, לכרטיסיית **Security** או **אבטחה**, יש לבחור באמצעות העכבר את רמת האבטחה הרצויה של הדפדפן. הבחירה נעשית על ידי גרירת תיבת הבחירה למעלה או למטה (כמתואר בתמונת המסך שמשמאל).

במידה ולא מופיעה תיבת הגרירה, יש ללחוץ על גבי לחצן ה- **Default Level** (ברירת מחדל) ואז תופיע התיבה.

אני אישית ממליץ על רמת אבטחה של **Medium-low**, היות ורמה זו מספקת הגנה ברמה בסיסית ועם זאת היא אינה פוגעת בחווית הדפדוף ברוב האתרים. במידה ואתר אינטרנט מסויים לא נטען כראוי ברמת אבטחה זו, ניתן להוריד את רמת האבטחה לרמה **Low** "נמוכה", ולנסות להיכנס שוב לאתר. מומלץ, עם זאת, להעלות שוב את רמת האבטחה לאחר היציאה מאתר זה.

העלאת רמת האבטחה ל- **Medium** היא בטוחה יותר, וזוהי גם ברירת המחדל, אך ייתכן שיותר אתרים לא ייטענו כראוי. ניתן גם לבחור כמובן ברמת האבטחה הגבוהה ביותר, אך זאת במחיר של חוסר פונקציונליות מסויימת באתרים רבים.

5. לאחר בחירת רמת האבטחה הרצויה יש ללחוץ על **OK** או **אישור** בתחתית המסך.

ניתן לבצע שינויים אלו גם תוך כדי הגלישה, ואין צורך להתנתק מהאינטרנט לטובת שינוי הגדרות רמת האבטחה.

ג. הסרת תוכנות ריגול שהותקנו במחשב כתוצאה מהתקנת תוכנה אחרת



חלק מתוכנות הריגול שנכנסות לתוך המחשב שלנו ניתן להסיר בצורה פשוטה יחסית, על ידי תפריט הוספה והסרה של תוכניות אשר בלוח הבקרה של ה-Windows.

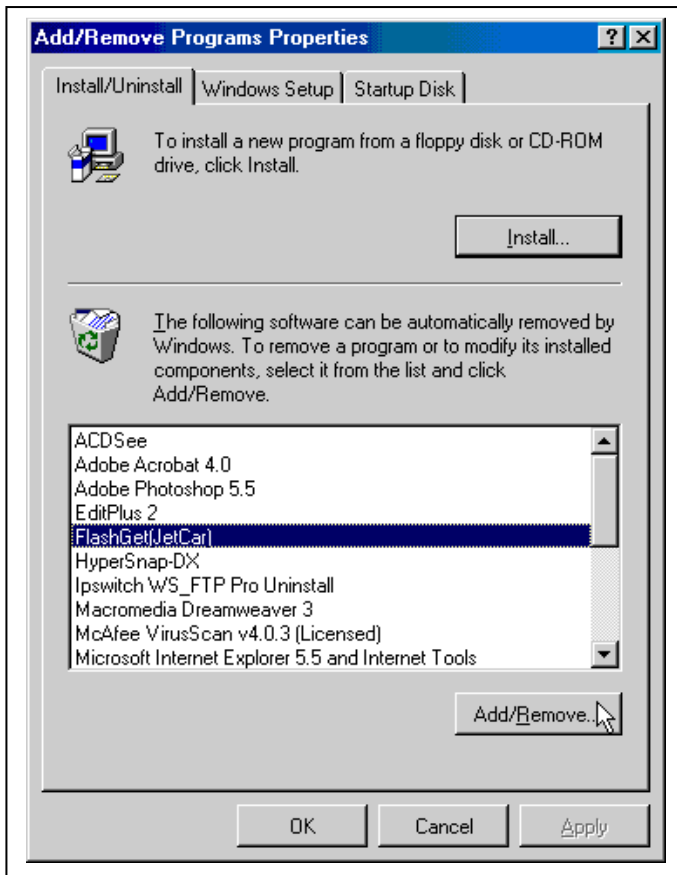
1. נכנסים לתפריט הוספה והסרה של תוכניות דרך :

התחל <- הגדרות <- לוח הבקרה <- הוספה והסרה של תוכניות

או באנגלית :

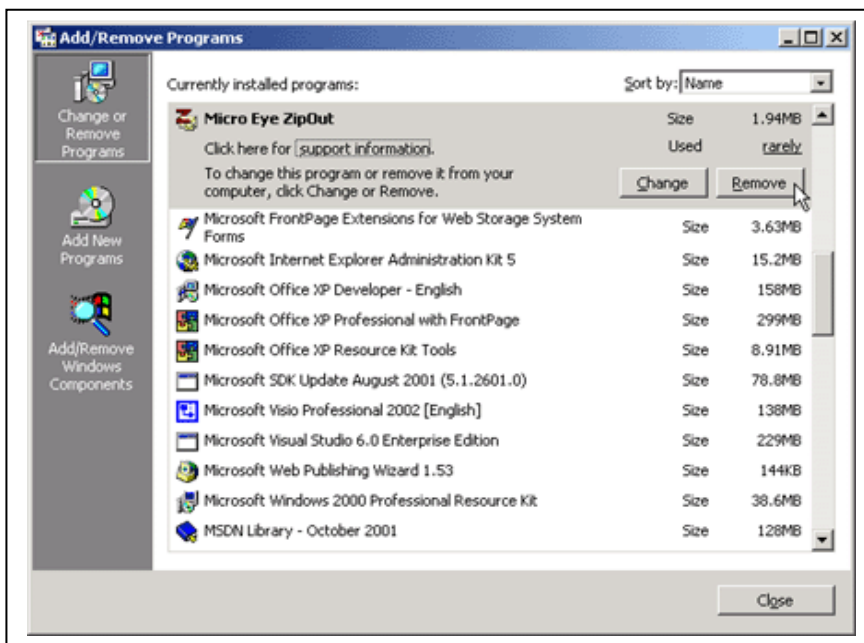
Control Panel <- Settings <- Start <- Add/Remove Programs <-

2. בחלון הבא שייפתח יש לבחור את התוכנה שרוצים להסיר מהמחשב, ולהסירה על ידי לחצן Add/Remove בחלונות 95/98 או לחצן Remove בחלונות 2000 או XP ומעלה.



Windows Me/2000/XP

יש לסמן את התוכנה שרוצים להסיר מרשימת התוכנות באמצעות העכבר, וללחוץ על גבי לחצן **Remove** שמימין לשם התוכנה. על המסך תיפתח תוכנת הסרה אשר תסיר את התוכנה.



הבעייה : לעתים על מנת להסיר כראוי את תוכנת הריגול צריך להוריד תוכנת הסרה מהאינטרנט. במהלך ההורדה של תוכנה ההסרה תתבקשו מספר פעמים לאשר שאתם באמת רוצים לבצע **Uninstall** (הסרה) לתוכנה. יש לקרוא בעיון רב את ההוראות להסרת תוכנות אלו, ולשים לב לכל שמסתתר בתוכנת ההסרה, מכיוון שלחיצה לא זהירה על אפשרות כלשהי עלולה לא רק להשאיר את תוכנת הריגול בתוך המחשב שלכם, אלא גם להוסיף לה עוד תוכנות נוספות!

בעייה נוספת : איך יודעים אילו תוכנות מהרשימה הן תוכנות ריגול ואילו לא ?

1. אם בטעות התקנו תוכנת ריגול ושמנו לב לשמה - מה טוב. נוכל למצוא את שמה בתוך רשימת ההסרה של התוכניות ולהסיר אותה בקלות יחסית.

2. אם לא, יש במספר אתרים רשימה ארוכה של תוכנות המוגדרות כתוכנות ריגול. טיפים מאוד חשובים לקרוא בעיון רב.

שי טיב

SysAdmin- MCSE

Shay_ti@malam.com

Shay_ti@bezeqint.net