קורא יקר,

וירוסים, פרצות וספאם הולכים ומתרבים מיום ליום **באופן מבהיל.** מערכות המחשוב הופכות למורכבות וסבוכות. במקביל, הפס הרחב, הוירטואליזציה, BI - מציעים **הזדמנויות חדשות ומלהיבות** וגם תפקיד מנהלי המחשוב עובר טרנספורמציה **דרמטית ומבטיחה**. כך, לנוכח שטף חידושים וגלי תמורות, שרק מתעצמים ומואצים, קשה להתמקד במה שבאמת חשוב. **למי להאמין? על מי לסמוך?**

תחקירי PCאון מספקים בכל שבוע ריכוז של החדשות החשובות ביותר בעולם המחשוב והתקשורת, יחד עם תחקיר מקצועי שמתמקד בנושא מפתח מרכזי ומשמעותי. הם משרתים חלק גדול ממנהלי המחשוב המובילים של מדינת ישראל. חלקם מנויים לשירות קרוב לשש עשרה שנים כיוון ש:

- PCאון הוא מקור מידע **אמין ותכליתי.** הוא מתמקד רק **בנושאי המפתח** החשובים ביותר בעולם המחשוב והתקשורת, והוא **מדבר בשפתך המקצועית.**
- PCאון כולל את ריכוז **החדשות החשובות** ביותר וגם **מגמות, טיפים, ידע יישומי ושימושי** נוסף. הוא מאפשר בהשקעה של **פחות מ-10 דקות** בשבוע, להיות כל הזמן **עם יד על הדופק.**
- PCאון מביא תועלת בכך שהוא **רלוונטי לבעיות הנוכחיות שלך,** בנוסף לכך, הוא מסייע לך בהערכות מוקדמת בפני **סכנות ואיומים** למערך המחשוב **ו/או ניצול הזדמנויות עסקיות** חדשות.
- ניתן **להתרשם ממנו באופן אישי** באמצעות תחקיר הדוגמא המצורף או להסתמך על למעלה ממאה חוות דעת של מנהלי מחשוב מובילים (ראה - www.pcon.co.il/v5/103.asp).

PCאון נתפס כיום כ**מפתח מוכח להצלחה מהירה,** וככזה גם אתה תוכל ליהנות ממנו בקרוב. כמו ארגונים רבים תוכל להצטרף כמנוי ארגוני ותאפשר לכל העוסקים במחשוב בארגונך, ליהנות מכל היתרונות שלמעלה.

מחירי מנוי השנתי בגין 52 תחקירים:

מספר מנויים	המחיר בדולרים + מע"מ
1	516
5	1270
10	1970
20	3270
50	5970
100	7700
200 ויותר	9700

נכון, אפשר לנסות להתמודד לבד עם כל התמורות. להתעלם או לדגום מאמר אקראי ולקוות לטוב. **תחשוב על התוצאות.** מצד שני ניתן ללכת **בדרך סלולה ובטוחה** שבה הולכים המובילים במחשוב הישראלי, שגם ימשיכו להוביל בבטחה. כדי להצטרף אליהם, ללכת יחד איתם, אפשר לקרוא על תחקירי PCאון ולהצטרף באתר ב- www.pCon.co.il/promo טלפון 03-9667939, פקס 03-9660310 או מייל - sub@pcon.co.il

קובי שפיבק
העורך הראשי של PCאון

נ.ב. על כל תחקירי PCאון חלות כל ההגנות החוקיות של זכויות יוצרים. ביחד עם זה, אנו מתירים לשכפל ולהפיץ את תחקיר זה, **מבלי לשנותו, עד 31.12.2007 ורק יחד עם דף היתר זה!** למנהלים, עמיתים ואנשי מחשוב נוספים, שעשויים לדעתך למצוא בו עניין.

מה אתה מקבל? - מפתחות להצלחה

קורא יקר,

תיזכר ב"נפילה" האחרונה של מערכת בארגון, ב"פספוס" בבחירת טכנולוגיה, בפרוייקט שלא "סיפק את הסחורה". מדמיין? עכשיו קח לך פחות מחצי דקה ותחשוב על מי שקרא תחקיר דומה, לפני כשנה. באינטואיציה פנימית חזקה הוא הבין שמצא פיתרון אמיתי לצורך אמיתי - להיות ממוקד באיומים האמיתיים וההזדמנויות המבטיחות שרלוונטיים לארגון ולתפקיד שלו, למציאות שבה הוא חי. שוב ושוב הוא נוכח מאז, שהוא מתבסס על מקור מידע שמדבר אליו בשפתו, מקור תכליתי ואמין.

כאשר חבר קרוב מתקשר ושואל לחוות דעתו על תחקירי PCאון. "מה הם נותנים לך באופן מעשי?" באופן טבעי הוא נזכר ומספר על כמה מהדוגמאות הבאות:

- **בתחקיר - ה-IT מאיץ חדשנות** - הוא גילה את הטרנספורמציה שעוברת היום כגל סוחף בעולם העסקי. ה-IT הופך מכלי שתומך בעסקים, למנוע שמאיץ חדשנות ופותח הזדמנויות חדשות. התועלת עבורו הייתה דרך הסתכלות חדשה על היבטי ה-IT, כזאת שפתחה בפניו דלת לקידום מהיר...

- **בתחקיר - חוסכים חשמל** - הוא מצא נתונים לפיהם, עלויות החשמל של דטה סנטר בשנה יכולות להיות יקרות יותר מכל עלויות החומרה שבו. הוא גם קרא כיצד השינוי בצריכת החשמל בניידים לוקחת אותנו לעידן חדש. התועלת שהפיק מהתייחסות ויישום הייתה - הרבה כסף לארגון. איך זה נשמע?

- **בתחקיר - כללי אצבע למנמ"ר** - הוא מצא נתונים, מספרים, כללי אצבע ומקורות שחיוני לכל מנהל שעוסק במחשוב להיות מצויד בהם. התועלת שהפיק הייתה קבלת החלטות מהירות יותר, מבוססות ומוצלחות יותר. התוצאות נראות בשטח. מכיר אנשים כאלה?

- **בתחקיר - וירטואליזציה בשרתים** - הוא הבין את המשמעויות המעשיות של מגמה מרכזית שסוחפות כיום את עולם המחשוב, כאשר הוא גילה **איך** וירטואליזציה יכולה להעניק יותר גמישות, חיסכון עצום, שרידות, עבודה קלה ועוד יתרונות נוספים. פתאום הכול התחבר. אתה רואה זאת?

- **בתחקיר - Rootkit - חפרפרת במחשב** - הוא קרא כי ברשת הארגונית של כל ארגון חמישי באוסטרליה (וכנראה כך גם בארץ), חבויה כיום תוכנה נסתרת, שיכולה לפתוח דלתות לתוכנות מזיקות. בדרך כלל, לא ניתן לגלות אותה! גניבת מידע, שיבוש נתונים, האזנות, ציטוטים, חדירות, נזקים. חלק מהאיומים יכולים להביא לקריסה. הוא עשה את כל שניתן לטפל בכך וישן טוב בלילה. ואתה?

הוא גם לא היחידי שחושב כך. מאה המלצות נוספות עם מסר חד וברור מדברות בעד עצמן. אחרי הכול, עם הישגים שמוכחים בשטח, קשה להתווכח...

לכן אנו ממליצים לשתף מספר רחב ככל האפשר של חברים, עובדים ומנהלים, בארגון ומחוצה לו, בשימוש בתחקירי PCאון. בדומה לטלפון ופקס, ככל שרבים יותר המשתמשים בהם, כך גם גדלה התועלת. אתה ודאי מכיר זאת.

עכשיו אתה מוזמן לקרוא את התחקיר המצורף, להתרשם באופן בלתי אמצעי ולהתקשר - דרך האתר www.pCon.co.il/promo לטלפן 03-9667939, לפקסס 03-9660310 או מייל - sub@pcon.co.il

אחרי שתצטרף ותסתכל קדימה שנה מהיום, יתכן וגם אתה תחשוב כמוהו? מה דעתך?

PCאון ©

למנהלים ומשתמשי מחשב בכירים

תדרוך מקצועי קצר ומרוכז ● בחדשות ומידע שימושי ייחודי ● למיצוי המחשוב באופן מרבי

והפעם... אל תיפול לפח ה-Hoaxes

מסר אישי

"זהירות!!! מחשבך נגוע בוירוס קטלני! הודעה זו איננה Hoax!!!..". הודעה זו היא כמובן פתיחה אופיינית להונאה מקוונת, המשמשת לפיתוי של גולשים למגוון פעולות מיותרות ומזיקות. כיום משתכללים ערוצי ההונאה שלרשות ה-**Hoaxes**, בזכות השימוש המתרחב ב-**E-Mail** ובאמצעים כ-**Instant Messaging** ושיתוף קבצים. בו בזמן, אין למתגונן תשובה טכנית מלאה לכך בנוסח האנטי וירוס, והוא נאלץ להשתמש בהגיון הבריא ובשורה של הרגלים וכללים מועילים.

מה הם נזקי ה-**Hoaxes** האפשריים? כיצד תזהה **Hoaxes** מבעוד מועד? כיצד להתגונן מפניהם ומה צריך לעשות? על כל זאת ועוד - תקרא בתחקיר שלפניך.

תמצית החדשות בעולם המחשוב טור

תוכן התדרוך השבועי טור

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA

עורך - **ערן דרור**

תחקיר וכתיבה - **עמית לוי**

טלפון - **03-9667939**, פקס - **03-9660310**

דואר - **ת.ד. 2340 ראשון לציון 75121**

E-Mail - editor@pcon.co.il

לתשומת לבך

PCאון© למנהלים ומשתמשי מחשב בכירים

597.11 – חדשות בקצרה

• **סקר נוסף מחזק את ההערכה כי הוצאות IT בכל זאת יעלו השנה, גם אם במידה מועטה בלבד.** סקר **Forrester Research** לגבי צפון אמריקה מצא עלייה של 1.9% בהוצאות ה-**IT** ב-2003, אך חושף גם שארגונים ימשיכו להיות בררנים מאוד לגבי רכישות וכי מעל שליש ממנהלי מחלקות שאינן **IT** מעורבים מאוד בהחלטות רכש אלו.

• **אינטרנט** תהיה מוקד לתחרות בין הבנקים ב-2003, לפי **גרטנר**. לפי תחזיות החברה, נראה כי השנה היישום המקוון המהיר ביותר לצמוח יהיה תשלום חשבונות מקוון, עם צמיחה בת 38% בארה"ב לבדה. אם תחזית זו מדוייקת, הרי ש**האינטרנט** משתלטת סופסוף גם על מעוז השמרנות האחרון בכלכלה האמריקאית - והופכת לכלי כלכלי ממדרגה ראשונה.

• החודש צפויה חברת **Dell** להציג מדפסות ראשונות מתוצרתה ועם הלוגו שלה. בכך היא תיכנס לתחום חזק במיוחד של מתחרתה הגדולה **HP**. המדפסות יוצעו בשלל סוגים ותחומי מחיר, ממדפסות אישיות בסיסיות ועד מדפסות מחלקתיות להדפסה אינטנסיבית.

597.12 – מלינוקס ועד יוניקס

עולם היוניקס / לינוקס אינו קופא על שמריו:

• **אוראקל** ו-**IBM** מנסות כעת לקבל הסמכת בטיחות **ללינוקס** כך שיעמוד בקריטריונים ממשלתיים הנדרשים בארה"ב לתוכנות שבשימוש בתחום הבטחון. קריטריונים אלה יעלו מדרגה בקרוב וכעת מתארגנת קואליציה שתבטיח ש**לינוקס** לא תהיה בעמדת נחיתות מול מערכות הפעלה אחרות בשוק זה.

• פרוייקט הקוד הפתוח **XFree86** שבמסגרת פיתוח ה**לינוקס**, הוציא כעת עדכון המקדם את תמיכת **לינוקס** במעבדים וכרטיסי מסך מודרניים. גרסת **4.3.0** לרכיב ה-**XFree86** מקדמת בין השאר תמיכת **לינוקס** בגרפיקת תלת ממד ובהצגת פונטים משופרת. ראה - xfree86.org

• מספר בנצ'מרקים חדשים עבור מפתחי **לינוקס** זמינים כעת חינם מה-**Open Source Development Lab** (**OSDL**) שבמימון **RedHat**, **SuSE**, **IBM**, **טושיבה**, **אריקסון** ו-**HP**. אלו בדיקות החופפות לבדיקות **TPC**, והן כוללות בדיקת אחזור מידע מ-**Database** על ידי שרת **לינוקס**, הדמיית חנות ספרים מקוונת ושימוש במערכת מלאי. ב - www.osdl.org

• האם השם "**חלונות**" מתייחס רק למערכת ההפעלה המיקרוסופטית? בית משפט חייב כעת את **מיקרוסופט** למסור לחברת **Lindows** מסמכים בעזרתם היא מקווה להוכיח שהתשובה לכך שלילית. זאת במסגרת התגוננותה בתביעת **מיקרוסופט** כלפיה על הפרת סימן המסחרי. (**Lindows** היא מערכת הפעלה מבוססת **לינוקס**, המריצה גם יישומי **חלונות**).

• מחקר **IDC** מגלה כי ברבעון האחרון של 2002 היו **HP** ו-**IBM** מובילות בשוק שרתי ה**יוניקס** עם נתח שוק של 30% כל אחת. **SUN** החזיקה בנתח שוק בן 28%, אם כי היא הובילה בסיכום השנתי.

597.13 – על האלחוט

המחשוב שואף לחופש וממשיך לצמוח ללא חוטים:

• למרות ירידה חודשית בת 2.4% במכירות השבבים בינואר השנה, נתוני **Semiconductor Industry Association (SIA)** מגלים גידול שנתי בן 22%. הצפי הוא להמשך הגידול השנה, כשאחד הגורמים המדרבנים לכך צפוי להיות הביקוש לשבבים אלחוטיים.

• מחשבים ניידים מבוססי טכנולוגיית ה-**Centrino** של **אינטל** צפויים לצאת בחודשים הקרובים. הטכנולוגיה מחדשת במעבד הבנוי מהיסוד למחשוב נייד, ביכולת לעבוד עד 5 שעות רצוף ללא טעינה ובתמיכת אלחוט משופרת.

• **Dell** הכריזה על שני מחשבי מחברת חדשים "מוכנים לשימוש אלחוטי", הכרזה המבטאת את הפופולריות הגואה של התחום: **Inspiron 1100** (**$900**) ו-**Inspiron 5100** (**$2,000**), כוללים חיבור **FireWire** ותאימות לתקן האלחוטי **802.11b** (**Bluetooth**) באופן מובנה.

• **H.A.T** - חברה מקומית - השיקה דיבורית אוניברסלית לרכב בשם **One**. הפתרון מתאים לכל סוגי החברות והמכשירים הסלולריים, בעזרת עריסות מתחלפות. הוא כולל מיקרופון, רמקול וחיבור לאנטנה ומאפשר הוספת צג חיצוני בגודל **3.7** (*999* ש"ח). המחיר: **699** ש"ח, כולל דיבורית, עריסה, התקנה ואחריות לכל החיים. ב - www.hat-int.com

597.14 – אינטרנט משנה פניה ?

אינטרנט - ה"יבשת" הטכנולוגית החדשה - מתפתחת ללא הרף ומשנה פניה. אך כמו בכל מסע ליבשת חדשה, חשוב להתעדכן קודם כל בסכנות:

• חוק הגנת הפרטיות מגן עליכם לכאורה מפני פרסום פרטיכם הפרטיים השמורים במאגר מידע, על ה**אינטרנט**, אך לאחרונה חשף אתר **נענע** כי ישנו ב**אינטרנט** מאגר נתונים מפורט על אזרחי המדינה הזמין לכניסה ולחיפוש. העלאת מאגר כזה ל**אינטרנט** אינה חוקית וממשרד הפנים נמסר כי הנושא בבדיקה. הלקח: הזהרו מכתובות צדדיות לא מאובטחות.

• ה-**Spam** הגיע לממדי מגיפה, אך גם הפתרונות עבורו מתרחבים: כעת נכנסה לתחום גם יצרנית האנטי וירוס **TrendMicro** עם **Spam Prevention Service**. לפרטים הכתובת - www.trendmicro.com

• ומסכנות לתלונות: תוצאות סריקת פורומים שמבצעת חברת יחסי הציבור **גוב קרטין** מצביעה על עליה נוספת בתלונות צרכנים כנגד אתרי מכירה ברשת. בפברואר נרשמה עליה חודשית בת 2% בתלונות עם עליה משמעותית (5%) בתלונות כנגד החברות הסלולריות. ירידה בת 7% נרשמה בקטגוריית "הטעיית צרכנים". במקום הראשון (19%) נמצא נושא השרות הלקוי ובשני המוצר הפגום (18%). לפרטים ☎ 03-6962286.

• החיפוש ב**אינטרנט** מהווה כיום עזר חיוני ביותר להתמצאות והפתרון המוביל **Google** קיבל כעת פטנט על שיטת קביעת רלוונטיות תוצאות חיפוש על פי מספר האתרים המקשרים אליו. פתרונות החיפוש מתחילים להתקדם לכיוון פרוש חכם יותר לטקסט, המתייחס גם לקונטקסט לשם זיהוי ישויות כמו אנשים, מקומות ושמות. דוגמא למוצר כזה הוא **MindServer** של **Recommind**. ראה - www.recommind.com

597.21 – הונאה בקוונה תחילה

סקר איגוד צרכנים אמריקאי מגלה שכשני שליש מהאוכלוסיה לא מאמינים לחלק ניכר מהכתוב באתרי אינטרנט שונים. משום מה, ב-**E-Mail** זה עובד קצת אחרת. קיבלת אזהרה דחופה בדואר מחבר לגבי וירוס מסוכן שהאנטי וירוס שלך עוד לא מסוגל לגלות! מומלץ שתבדוק מייד בעזרת שם הקובץ אם נדבקת. ואכן - אתה מוצא קובץ זה בספריית **Windows**! מוחק אותו מיידית ומפעיל את המחשב מחדש והמחשב לא עולה! כעת תוציא על כך התמיכה הטכנית לא מעט זמן. **Hoaxes** או הונאות **E-Mail** הן חלק ממגיפת דואר בלתי רצוי הפושטת בארגונים. הן מוסיפות לווירוסים ול-**Spam** נדבך של נזק אבטחתי והפסד כספי נוסף. כפי שהדגמנו, דואר מטעה במכוון עשוי להתבטא בנזקים ישירים מפעולה על סמך האמור בו, ובהטרדה גוזלת זמן. לכך מתווספים גם נזקי עומס יתר על מערכות דואר ואף חשיפה מוגברת ל-**Spam**. יש המנסים להפיץ **Hoaxes** גם ביישומי **Instant Messaging** (**ICQ** במיוחד) ושיתוף הקבצים, אך התחום המוביל הוא הפצתם ב-**E-Mail**.

לפי סיכומי ה-**National Fraud Information Center** האמריקאי לינואר-יוני 2002, 8% מההונאות ב**אינטרנט** התחילו באמצעות **E-Mail**. רק 5% מהנפגעים (המדווחים) היו מחוץ לארה"ב וקנדה, אך הנזק הממוצע היה **484$** והכולל הגיע ל-**7,209,196$**.

קל ליצור הונאות אלה, כפי שיודע אמן ההונאה המתוחכם וגם הילד המשועמם הממחזר תבנית **Hoax** מוכרת ופשוטה. קל גם ליפול בפח, אך נדגיש שבהחלט לא מסובך למנוע זאת ברמה הארגונית. במקרה (אליו אין כלל צורך להגיע!) בו נפגעת, תוכל אף לפנות למשטרה, אם מדובר בהונאה שאתה בטוח שנעשית בזדון - אך ברוב המקרים תקבל את ה-**Hoax** דווקא ממכר או עמית שקיבל אותו ורוצה בתמימות רק לעזור.

<u>לסיכום - דווקא בעת מיתון, אסור לארגון לבזבז זמן, כסף ומשאבים על הונאות סרות טעם. הפתרון: יצירת מודעות, זהירות ושימוש בנוהל מוגדר לחשד לוירוס.</u>

597.22 – מי ומי ב-Hoax ?

אלו סוגי ההונאות השונים בהם אתה עשוי להיתקל:

- **Hoaxes** - זהו המונח הכללי שבו מתייחסים לכמה סוגי הודעות שקריות הנשלחות לאנשים ב-**E-Mail**. לשם הנוחות נשתמש בתחקיר בעיקר במונח זה. **Hoaxes** מגיעים פעמים רבות כ**אזהרות מפני וירוסים מתוחכמים ודמיוניים לגמרי**, סוסים טרויאניים, תולעי **אינטרנט** וכדומה. דוגמא מפורסמת היה "וירוס" ה-**Good Times**. צורת **Hoax** נפוצה נוספת הן **הבטחות לתמורה כספית** מחברה ידועה אם רק תפיץ דואר זה הלאה. ואחרון: **בקשות לסיוע כספי** למישהו הנמצא כביכול בצרה.
- **רמאויות** - השולחים ינסו להוציא ממך מידע רגיש כמו פרטי כרטיס אשראי, באמצעי רמייה. דוגמא נפוצה היא פניה מחברה המוכרת לך, למשל ספק **אינטרנט**, המודיעה על תקלה ומבקשת להזין שם משתמש וסיסמא וכדומה.
- **שמועות / אגדות עירוניות / מיתוסים** - **Urban Legends** או מיתוסים הן שמועות דמיוניות על סכנות האורבות לך (זהירות! סיכות במושבים בבתי קולנוע!) ואסונות שקרו כביכול לאנשים או לעתים לחיות. זה יכול להיות גם משעשע (בתנאי שלא נופלים בפח), כמו בהודעה על סגירת **אינטרנט** לרגל "ניקיון". ראה -
pcon.co.il/smartmanager3/headlines_rej.asp?id=82
- **בדיחות / הונאות** - אלו הודעות שדווקא אינן מתאמצות להישמע אמינות, אלא בודקות עד היכן יצליחו למתוח אותך. למשל: סיפור "הבננות הטורפות", המזהיר ממשלוח בננות הנגועות בחיידק "טורף בשר".
- **מכתבי שרשרת** - **Chain Letters**, בדומה לגרסתם המוכרת מהדואר הרגיל, הם מכתבים המעודדים אותך להפיצם הלאה לשיפור מזלך. מובן, שאם תתעקש ולא תעשה כן, צפוי לך למרבה הצער עתיד איום ונורא.

597.23 – כך תזהה ותיזהר

אלו "הסימנים המרשיעים" בעזרתם תזהה הונאות:

1. **מראה דרמטי** - הודעות אלה מתאפיינות בתווים וצבעים המושכים תשומת לב ויוצרים מראה דרמטי. מדובר בעיקר בשימוש רב בסימני קריאה, באותיות גדולות ומודגשות ואף בצבעים עזים.
2. **תוכן מפחיד** - התוכן כולל אזהרות על סכנה חמורה במיוחד: וירוס שאי אפשר לאתר! אם לא תפעל מיידית הדיסק הקשיח שלך יקבל התקף לב והמעבד יישרף! כל זאת עשוי להיות מגובה בהסבר טכני מצוץ מהאצבע.
3. **שמות גדולים ליצירת אמינות** - ההודעה תכלול לרוב גם הסתמכות על שמות גדולים כמו **IBM**, **McAfee** או **מיקרוסופט** להגברת תחושת האמינות. מצד שני, היא לא תספק שום קישור ממשי לגופים אלה או לאתר אבטחה כלשהוא לשם האימות.
4. **הצעות פעולה קיצוניות וחשודות** - הצעות הפעולה תהיינה קיצוניות למדי. לגבי וירוסים מדובר ב"טיפול" פרימיטיבי (ללא אנטי וירוס כמובן) בעזרת מחיקת קובץ מסוים, כיבוי המחשב, ניתוק מ**אינטרנט** או פירמוט הכונן הקשיח. בהונאות אחרות מדובר על מתן כסף או פרטים אישיים רגישים.
5. **שמות מוזרים לווירוסים** - סוג ה-**Hoax** הפופולרי המזהיר מפני וירוסים דמיוניים עשוי להשתמש לשם כך בשמות מוזרים למדי לאותם לוירוסים. אין צורך לומר שבקובץ העזרה בתוכנות האנטי וירוס שלך לא תמצא התייחסות לשם זה ולא בגלל שהוא כל כך "חדשני".
6. **קריאה להפיץ הלאה** - בכל **Hoax** תמצא כאלמנט הפצה קריאה להפיץ אותו הלאה לכל מי שאתה מכיר. זכור שללא שיתוף פעולה זה מצידך, הודעות אלו לא ימשיכו בדרכן הלאה. בניגוד לתולעי ה**אינטרנט** הנפוצות כיום, **Hoaxes** לא מפיצים עצמם לבד דרך ספר הכתובות שלך, אלא תלויים בשיתוף פעולתך האדיב.

שים לב לעוד כמה נקודות: האם מופיע הביטוי "זה לא **Hoax**"? (זה בהחלט כן), מה היא זהות השולח (האם אתה מכיר אותו?) מה היחס בין אופי ההודעה למקורה ולחומרתה (האם חברת **X** המכובדת תשלח ללקוח אזהרת חרום שנראית כך ועוד ב-**E-Mail**?).

PCאון© למנהלים ומשתמשי מחשב בכירים

597.31– מחיר הפיתוי

אלו נזקי ה-Hoaxes העיקריים לארגון:

1. **זמן עובדים** - גם אם כל עובד יוציא דקה לקריאת הודעות דואר מורכבות אלו, בארגון גדול זה יצטבר לבזבוז זמן לא מבוטל. הוסף לכך את אי הוודאות לגבי אמיתות העניין, שמעמיסה זמן בירורים, ותגיע לכמה וכמה שעות יקרות בחודש.
2. **עומס על מערכות דואר** - הודעת טקסט קטנה וטרוויאלית לכאורה עשויה להתפתח למטרד אמיתי לשרת הדואר. אם כל משתמש בארגון גדול ייפול בפח וישלח את ה-**Hoax** ל-10 חברים טובים ואז כל אחד בתורו יעשה כן הלאה - תוך כמה "דורות" ייתפח המשלוח למימדי מטרד תעבורה של ממש. מטרד זה יפגע בתפקוד המערכת ואף עשוי להביא לנפילתה.
3. **חשיפה ל-Spam** - מפיצי דואר זבל מסויימים למדו שניתן להעזר במשלוח **Hoaxes** כמקור לאיסוף כתובות דואר, למטרת משלוח **Spam**. לאחר כמה דורות משלוח יקבל הספאמר אוסף כתובות איכותיות (שתקפותן וזמינות בעליהן אושרו בעצם השימוש בהן).
4. **נזקי הנפילה בפח** - פעולה ישירה על סמך המומלץ בהונאות (ומודגש לרוב כ"דחוף!") תביא לנזקים מיידיים כמחיקת קבצי מערכת, שייגזלו זמן עובדים נוסף לתיקונם. כאן כבר מדובר על זמן העובד (הנפגע מהשבתת המחשב שלו) + זמן אנשי התמיכה הטכנית.
5. **הטעיית העובדים** - העברת המיקוד מסיכונים אמיתיים לאיומים דמיוניים תגזול זמן עובדים ותפגום בתגובותיהם הרצויות מול שיבושי מערכת שונים (המחשב נתקע? בטח בגלל הוירוס המיסתורי עליו קראתי בדואר!).

597.32– ממטרד לאיום אבטחה

מרבית ה-Hoaxes מהווים מטרד המבזבז בעיקר משאבי זמן ארגוניים, אך ישנם גם כאלה שמאחוריהם כוונת זדון בעלת השלכות אבטחה חמורות. גם כשהונאה בודדה כזו "מצליחה", הנזק האבטחתי עשוי להיות משמעותי ביותר. מעשי הונאה שונים משתמשים לפיתוי אנשים לתת מידע אישי רגיש דרך **אינטרנט**. לאחרונה קיבלו מנויי **Yahoo** הודעות שהתחזו להודעות רשמיות משרות הלקוחות, בנסיון להוציא מהם פרטים שכללו בין השאר פרטי כרטיסי אשראי. דבר דומה קרה ללקוחות שרות התשלומים **PayPal** ועשוי להתבטא גם בחשיפת מידע ארגוני רגיש כסיסמאות, אפילו באמצעות דואר המגיע כביכול ממנהל המחשוב או מסניף אחר של אותו ארגון.

סיכון אבטחה נוסף הדגים **Klez.E Worm Immunity Hoax** שהתחזה לדואר המבטיח לך "חיסון" מפני הוירוס הפופולרי **Klez**. עם הפעלת מה שנראה כקובץ **Bat** מצורף **(Class.bat)** הוא הופעל כקובץ ויז'ואל בייסיק שלמעשה הדביק מחשבים באותו הוירוס!

תיאוריית **FUD (Fear, Uncertainty and Doubt)** מסבירה ששיטות אלו עובדות היטב, מאחר וניתן לגרום לאנשים לעשות דברים שונים ומשונים תוך הסתמכות על אלמנטים כפחד, אי-וודאות וספק המצויים בכולם. הלחץ לביצוע פעולה המתוארת כדחופה מעודד לפעולה לא שקולה והאווירה המקצועית שבהודעות מעודדת אמון ומצמצמת התייעצות עם גורמים מקצועיים בארגון. זהו עיקרון בסיסי של **Social Engineering**, המתבטא בכל הכנת **Hoax**. (עוד ב-**597.52**).

דגש – המחשב כאומן הונאה

מעניין לציין שהמחשב האישי מספק לא רק מדיה ידידותית להפצת ההונאות, אלא גם עזר מעולה למפיק ההונאות החובב. הונאה היא אמנות עתיקה המבוססת על דמיון ונזקקת למימושה לטכנולוגיה מתקדמת ולטכניקה מיומנת. במקרה שלנו כל זאת זמין לחובב ה-**Hoaxes** במחשב האישי ובשפע. חומרי גלם לטקסטים? תמונות? יש בשפע ב**אינטרנט** וקל להורידם. כלי עריכת טקסט ותמונה? כנ"ל. דוגמה מפורסמת: זיוף תמונת תייר שכביכול הצטלם על מגדלי התאומים לפני האסון כשמטוס מאחוריו -
www.museumofhoaxes.com/photos/wtcphoto.html

אתר **C|Net** מגדיל לעשות ומספק לך **Net-Hoax Generator** - כלי מקוון ליצירת **Hoaxes** וכמה דוגמאות -
www.cnet.com/techtrends/0-1544318-7-1580533.html

597.33– מקורות מסייעים

אלו כמה אתרים בעזרתם תרחיב ידיעותיך על ה-Hoaxes:

- **Symantec** - מציעה רשימה מתעדכנת של **Hoaxes**, ב - **securityresponse.symantec.com/avcenter/hoax.html**
- **Panda** - באתר חברת האנטי וירוס **Panda Software** תמצא מידעון על **Hoaxes**. בחלון החיפוש תוכל לאתר במהירות מידע על **Hoax**. מתחתיו תמצא את רשימת המובילים - **www.pandasoftware.com/virus_info/hoaxes**
- **Purportal** - אתר זה מציע חיפוש נרחב במיוחד לבירור מידע על **Hoaxes** שונים. עוד תמצא בו מאמרים בנושא, חדשות אחרונות וקישורים. - **www.purportal.com**
- **Sophos** - דף **Hoaxes** באתר חברת האנטי וירוס לארגונים **Sophos**, מאפשר חיפוש אלפאביתי לפי שמותיהם, צפיה ברשימת האחרונים, מונחון ומדיניות ארגונית לדוגמא - **www.sophos.com/virusinfo/hoaxes**
- **Internet 101** - באתר זה תמצא רשימת קישורים מעולה ונרחבת במיוחד לאתרים המתמחים במידע **Hoaxes** כללי, מיתוסים, הונאות ב**אינטרנט** ומכתבי שרשרת. - **www.internet-101.com/hoax**
- **Vmyths** - אתר **Vmyths** מתמחה במיתוסים, אגדות עירוניות ו-**Hoaxes**. בדף הראשי שלו תראה חלון חיפוש, המלצות טיפול בארגונים, הרשמה ל-**NewsLetter**, חדשות ומשאבים נוספים - **www.vmyths.com**
- **McAfee** - באתר **McAfee** תמצא רשימת **Hoaxes** המתמקדת בוירוסים (אזהרות כביכול עליהם או **Hoaxes** הנגועים בוירוס). מומלץ כמקור קל התמצאות ל-**Hoaxes** המסוכנים יותר - **vil.mcafee.com/hoax.asp**
- **ICQ** - באתר **ICQ** תמצא דף הדרכה בנושא הפצת הודעות **E-Mail** מטעות, פנימית במסגרת **ICQ**. התוכן כולל חלק הומוריסטי חביב, אך גם הנחיות מעשיות במסגרת החלק **Stop The Chain Letters** - **www.icq.com/support/urge.html**

597.41– מדברים על זה

המומחים הבאים חלקו איתם כמה תובנות נוספות:

עו"ד **בועז גוטמן**, בעבר אחראי על חקירות עבירות מחשב במשטרה, כיום מרצה לדיני מחשבים ויועץ ל**אינטרפול** (☎ 03-6357444) אומר שאנשים התבגרו קצת ב**אינטרנט** וכבר פחות מפיצים הלאה הודעות על **Hoaxes**. לדבריו, אין תרופה לתופעה זו, אך ניתן לפחות לצמצם נזקים. ישנם אנשים הנופלים בפח מדי פעם, אם כי לא בסכומים גדולים. כמעט כל יחידות האכיפה בעולם נגד רמאות (כמו ב-**FBI** או ב**אינטרפול**) מזהירות מכך כל הזמן ועובדות על הסברה ומניעה. **בועז** אומר שכמויות ה-**Hoaxes** רבות מכמויות הווירוסים ויש פשוט לעקוב. המלצתו: לא לקבל **E-Mail** ממי שלא מכירים.

צבי נתיב, מנכ"ל **נץ מחשוב** (☎ 03-9027777) מדגיש כי סימן ההיכר המובהק ל-**Hoax** זו ההזמנה לשלוח הלאה. מנסיונו, ברגע שאתה רואה אותה - תוכל להניח שהסיפור בדוי ב-**99.999%**. **צבי** אומר כי דווקא מנהלי מערכות שהיו אלה שצריכים לבלום זאת, הם המפיצים הגדולים ביותר והם גורמים לארגונים שלהם לא מעט נזק. הסיבה היא הרצון להיות **On the safe side** כשלא בטוחים באמיתות ההודעה, אך בפועל גם אם ההודעה אמיתית ולא העברת אותה הלאה, לא עשית נזק לאיש. אם כבר שולחים הלאה, **צבי** מציין שמשלוח לנמענים רבים תוך הסתרת הכתובת (בשורת **BCC**) ימנע איסופם לרשימות דיוור ל-**Spam**.

זמיר סיון, מנהל טכני ב**פיינזילבר הנדסה** (☎ 09-8859611) אומר כי נושא ה-**Hoaxes** מהווה בהחלט סוגייה בארגונים. בגלל הפחד מווירוסים מעבירים הודעות כאלו (שכביכול מזהירות מפניהם) מהר מאוד וכך נוצרת תעבורת דואר פנים ארגונית מיותרת בכמויות. המצב חמור יותר כשבהודעה מוזכרת פעולה לביצוע. זה לרוב לא גורם לנזקים גדולים אלא למטרד דוגמת שחזור קבצי מערכת ההפעלה, אך ככל שהארגון גדול, כך גדל גם המטרד. למנהל המחשוב שארגונו מתמודד עם תופעות כאלה **זמיר** מייעץ קודם כל להשתמש במוצר אבטחת תוכן כלשהיא שיודעת לסנן דברים כאלה, וכמובן להיות מודע ל-**Hoaxes** שמסתובבים בשטח ולדעת מה אמיתי ומה לא.

597.42– טיפים לטיפול במצב

העזר בטיפים אלה למיצוי ההתמודדות מול מטרדי ואיומי ההונאות ב-E-Mail:

- **זהה Hoax במהירות** - קיבלת הודעה חשודה ולא בטוח אם תוכנה אמיתי או **Hoax**? לא זוכר היכן קישוריך לבירורים בנושא זה? העתק חלק קטן מגוף המסר שקיבלת, שים במרכאות וחפש בגוגל (מוטב יחד עם המילה **Hoax**). אם אכן מדובר ב-**Hoax**, תגלה זאת מייד בעזרת תוצאות החיפוש.
- **הגבל המשך הפצה** - בהגדרות שרת הדואר הגבל אפשרויות משתמשים לשלוח הודעות **E-Mail** לכמויות נמענים גדולות (לדוגמא: הפצת דואר לכל נמעני הארגון). כך תגביל משמעותית התפשטות **Hoax** פנימית וגם תתרום למניעת הפצתו הלאה.
- **קח עדכון חינם** - חברת **Sophos** תאפשר לך להציג באתרך בחינם רשימת **Hoaxes** הפעילים ביותר כעת. העזר בכך בכדי לאפשר לעובדים להתעדכן לבד בהונאות העדכניות - www.sophos.com/virusinfo/infofeed
- **אל תפספס בחדשים** - הקפד על עדכון עובדים חדשים בהתגוננות מהונאות דואר, מאחר ובלי משים דווקא הם עלולים "ליפול בין הכיסאות". קבע כדף בית בדפדפן שלהם אתר בנושא **Hoaxes** (ראה ידיעה **597.32**). גם אם הם ישנו אותו אחר כך, עדיין יהיה לזה ערך ראשוני שידגיש את התדרוך שנתת להם
- **היזהר מווירוסים** - מאחר ונזקי וירוסים הם גדולים כל כך, **נדגיש כי אם יש לך שמץ ספק שמא זהו וירוס, הנח שאכן זה כך ופעל בהתאם.** כעיקרון מומלץ תמיד להיעזר בחוות דעת של בעלי ניסיון ובלפחות שני אתרים המדווחים על **Hoaxes**, בכדי להצליב מידע.

597.43– לא ליפול בפח

העזר בהנחיות הבאות להכנת הארגון ואנשיו להתמודדות עם מטרדי וסכנות Hoaxes:

1. **חסום בכניסה** - ברכישת תוכנות אנטי וירוס או סינון תוכן לארגון, וודא שיש להן גם התייחסות לנושא ה-**Hoaxes**. לדוגמא: מוצר **E-Mail Content Filtering** בשם **NetIQ MailMarshal** כולל גם סקריפט לזיהוי **Hoaxes** גנריים. יש בו גם אפשרות ליצור סקריפט משלך עם אשפים מתאימים וכך תוכל להוסיף למשל סקריפט בעברית. (מחירו החל מ-**$924** לשנה ל-25 משתמשים. **פיינזילבר הנדסה** ☎ 09-8859611).
דוגמא נוספת: כל מוצרי האנטי וירוס מ- **McAfee** מטפלים גם בנושא **Hoaxes**, אליו הם מתייחסים כווירוס, כולל עדכוני חתימות מ**אינטרנט** (**Network Associates** ☎ 09-7643585).
2. **הגדר ממונה** - קבע בבירור מי הכתובת הארגונית לנושא **Hoaxes**. ממונה זה יהיה מעודכן במיוחד ב-**Hoaxes** האחרונים וזמין לפניית כל עובד שירצה לשאול לגבי דואר חשוד שקיבל. הממונה ידאג גם להפעיל כל עזר שמציעות תוכנות ניהול הדואר וסינון התוכן בארגון, לשם חסימה מוקדמת ככל האפשר של הודעות מסוג זה. במקרה ויש הודעה מטרידה במיוחד, שאינה נחסמת באמצעים הרגילים, הוא יוכל לכתוב אפילו סקריפט מתאים במיוחד לחסימתה.
3. **הדרך עובדים** - הפץ הסבר מפורט לעובדים ותלה עותק ממנו בלוח מודעות ארגוני ובאתר **אינטרה-נט** ארגוני. הקפד לרענן זאת מדי פעם, בכדי לשמור על מודעות לנושא. למשיכת תשומת לב העובד ולהמחשה מומלץ להעזר בדוגמא מעניינת מבין הרבות שבוודאי תמצא.
4. **התעדכן ועדכן** - התעדכן שבועית ב-**Hoaxes** הבולטים האחרונים ואם הוגדר ממונה - וודא שהוא מתעדכן. העבר מידע זה לעובדים באמצעות **אינטרא-נט** ארגוני או לוח מודעות. התייחס שם גם ל-**Hoaxes** ה"מסתובבים" כרגע בארגון או עלולים להגיע אליו (כאלה הפעילים כרגע אצל מכותבים עיקריים כמו לקוחות ראשיים וספקים).
5. **גלה וטפל** - עם גילוי הודעת **E-Mail** החשודה כ-**Hoax**, הפעל שלבי טיפול אלה: וודא במה מדובר בעזרת קישורים לאתרי עזר (קישורים שיהיו זמינים לעובדים ב-**Bookmarks** וב**אינטרה-נט**), אל תעביר אותה הלאה, הודע לשולח במה מדובר ושאין צורך להכנס לפאניקה ושמור אותה לטובת הארגון כולו לעיון עתידי.

597.51 – סוד "ההצלחה" !

אלו הסיבות העיקריות להצלחת ה-Hoaxes:

- **קלות יצירה** - ה-**Hoaxes** קלים מאוד ליצירה. בניגוד לווירוסים, הם אינם דורשים ידע טכני כלשהוא או אפילו התעמקות בנדרש לשימוש בערכות פיתוח וירוסים. כל הדרוש לכתיבת **Hoax** מצליח זמין לכל משתמש מחשב ממוצע: חשבון דואר, רעיון המבוסס לרוב על דוגמא קיימת וזמן מינימלי להכנסת שינוי קל בדוגמא.
- **קלות הפצה** - בדומה ל-**Spam**, הודעות **Hoax** מוצאות במערכות ה-**E-Mail** ערוץ הפצה המוני מעולה. כמויות הדואר שרבים מקבלים כיום מעודדות מיון מהיר ושגוי.
- **חוסר וודאות** - בניגוד למשתמש המודע לנושא ומתורגל למחוק כל מה שנראה כ-**Hoax**, הנמען הממוצע מוצא עצמו בחוסר וודאות. תגובתו הופכת להיות התגובה הרצויה לכותבי ה-**Hoax** - "ליתר בטחון" הוא עשוי להזדרז ולהפיץ את הדואר הלאה או אף לבצע פעולות שונות ה"מומלצות" בו.
- **קושי בהתגוננות** - לא רק המשתמשים, גם כלי התגוננות ארגוניים אינם ערוכים היטב מול אתגר ה-**Hoax**. בשונה מהמצב עם כלים לטיפול בווירוסים, כאן אי הוודאות בזיהוי גדולה במיוחד.
- **חוק ללא שיניים** - מערכת החוק כמעט ואינה פועלת לאיתור יוזמי **Hoaxes** ולהענשה הפרופורציונלית לנזק המצטבר שגרמו. יוצאי דופן הן כמובן הונאות כספיות בודדות בסדר גודל של העוקץ הניגרי (ראה **597.53**).

597.52 – הנדסה חברתית

תופעת ה-Hoaxes מתבססת במידה רבה במיוחד על מה שמכונה "הנדסה חברתית" - אותה גישה להפצת קוד עויין המוכרת היטב דווקא מעולם הווירוסים. **Social Engineering** מבוססת על תמרון המשתמש, בתור שער כניסה מעולה לארגון. האמון הבסיסי שנותנת המערכת הארגונית במשתמש הופך אותו - במידה ותצליח להטעותו - לסוס טרויאני פוטנציאלי מושלם. אם תפתה אותו להאמין ב-**Hoax** שהגיע ב-**E-Mail**, מייד תזכה להפצה מהירה לחבריו, הבוטחים בו וממהרים לראות מה הוא שלח הפעם. ה"מהנדס" מסתמך לשם כך על חולשות אנושיות בסיסיות כסקרנות (כנוגדן למחיקת הדואר), חששות (מפני ווירוסים), תאוות בצע (אם רק תרוויח) ונטיה למתן אמון בכל דבר המוצג בבטחון רב כמקור סמכותי. לניצול נטיה זו מצטרפים לעתים גם "מומחים" שונים מטעם עצמם ולא מתוך כוונות זדון. **False Authority Syndrome** מתייחס למצב בו אדם מציג עצמו כמומחה לתחום בו יש לו ידע בסיסי בלבד או תחום החורג מעט מתחומו. לדוגמא: מנהל הרשת אינו מומחה לווירוסים ומשתמש שנדבק בווירוס **X** איננו מוסמך ליעץ למשתמשים אחרים המקבלים דואר המעודד לטפל בו במהירות על ידי מחיקת קובץ **Y**. שניהם עלולים לסייע בלי כוונה להתפשטות **Hoax**, בכך שיקבלו את תוכנו ברצינות ולא יהיו מודעים לאפשרות שזו הונאה. הדוגמא הקלאסית היא העלאת רמת ה"פניקה" סביב התפשטות וירוס חדש ומסוכן כביכול.

דגש – הפן המשעשע

לא רק ש-Hoaxes אינן הודעות רציניות, לפעמים הן אפילו משעשעות. לדוגמא: האם כבר הצטרפת למחאה ה**אינטרנטית** כנגד אתרו של היפני מניו יורק, המגדל חתולי בונסאי? לידיעתך - **Bonsai Kittens** הם חתולים גמדיים המגודלים בשיטות עתיקות ואקזוטיות, אם כי לא ידידותיות במיוחד לחתלתולים. האם שמעת על הודעת **מיקרוסופט** ו**הוותיקן** כי **מיקרוסופט** מתכוונת לרכוש את הכנסיה הקתולית? בקרוב תוכל לצפות לשרות דרשות מקוונות ולגרסת בטא של **Microsoft Church** - תוכנת טעינה אוטומטית לחסדי שמיים. ולסיום הנה **Hoax** שנוסח במיוחד כשילוב נוסחים נפוצים להשכלתך. אם קראת אותו, קראת את כולם! - www.stiller.com/badday.htm

597.53 – הונאות בכותרות

ישנן דוגמאות מפורסמות ל-Hoaxes הממחישות את היקף התופעה והצורות שהיא מקבלת. מפורסמת ומצליחה במיוחד היא ההונאה המכונה "העוקץ הניגרי". אתה מקבל **E-Mail** מ"בכיר בממשלת ניגריה" (ברי המזל זוכים לדואר מהמלך בכבודו ובעצמו..), הזקוק בדחיפות להפקיד באופן זמני כמה מיליוני דולרים בחשבון הבנק שלך. הסיבה? לעקוף כמה ענייני בירוקרטיה פנימית בניגריה. מובן ש"תתוגמל היטב בעד עזרתך". בפועל, תפותה "לסייע" קודם בכמה סכומים סמליים לצורך דחוף כלשהוא וכמובן לא תראה בחשבונך גרוש. נדגיש כי הונאה זו עובדת היטב וקיימת בשטח מזה שנים. ארגון **419 Coalition** מעריך שהיא הוציאה מאנשים **כחמישה מיליארד דולר** ומהווה תעשיה של ממש בניגריה. ראה - www.police.gov.il/ezrat_haziboor//msirat_meyda_modiini/xx_oketz.asp

The Good Times Hoax הייתה הונאה שהזהירה מפני וירוס הגורם לדיסק להיהרס. בנוסף, המעבד ייכנס ל-**nth-complexity infinite binary loop** (שים לב לשפה הטכנית כביכול - לשם השיכנוע) ועם הזמן יהרס אף הוא.

ועוד כיוון ל"יצירתיות" בהונאה: **מיקרוסופט** ו-**CNN** דיווחו כי אתר מזויף התחזה לדף חדשות של **CNN** וזייף בצורה משכנעת "ידיעה חדשותית" לפיה רכשה **מיקרוסופט** את חברת משחקי המחשב **Vivendi Universal**.

ארבעה **Hoaxes** המוגדרים כמובילים יספקו עוד דוגמאות:

1. **JDBGMGR** - טוען שבכדי להיפטר מהווירוס **Bugbear** יש למחוק קובץ (מערכת) בשם **jdbgmgr.exe**. ההטעיה מסתייעת בעובדה שליישום ה-**jdbgmgr** אייקון בצורת דובון (**Bear**).
2. **WTC Survivor** - הודעה המזהירה מפני פתיחת כל דואר שהוא המתייחס לאסון מגדלי התאומים (**World Trade Center**). מומלץ דווקא לשמוע להמלצה ולהתעלם גם מהודעה מטרידה זו, אך להתעלם מהקריאה הנרגשת להפיצה לכל.
3. **Budweiser frogs screensaver** - דואר המזהיר מפני הורדת שומר המסך החביב מאתר חברת הבירה באדוייזר, הכולל פרסומת ידועה עם צפרדעים. הקובץ כביכול נגוע בווירוס, אך בפועל - לא צפרדעים ולא יער! אל תבלע זאת!
4. **Hotmail Hoax** - בכדי לצמצם בחשבונות דואר לא פעילים, תתבקש להעביר הודעה זו ל-10 בעלי חשבונות המוכרים לך. זאת בכדי "להקל על מערכת הדואר ב-**Hotmail**". אם לא תעשה כך, "חשבונך ינוטרל עד שתפנה לתמיכה הטכנית".