

## 5 טיפים – כך תימנעו מתוכנות כופר במחשב שלכם

תוכנות כופר הן בין האיזמים היותר זדוניים של השנים האחרונות – הן חוטפות קבצים במחשב, מצפינות אותם ודורשות בין מאות לאלפי דולרים תמורת שחרורם. החדשות הטובות – קל להימנע מהן וכך תעשו את זה.

האיזמים איתם אנחנו מתמודדים בעולם האבטחה הופכים לרבים, מורכבים ומגוונים יותר. אחד מאותם איזמים שמערימים קשיים על חברות האבטחה, מנהלי רשת וגולשים פרטיים הן תוכנות הכופר הידועות לשמצה, שמצפינות את כל הקבצים על המחשב ודורשות כופר של מאות עד אלפי דולרים כדי לספק את מפענח ההצפנה.

המטרה של איום מהסוג הזה היא "לחטוף" את המידע של המשתמש, בית העסק או הארגון על ידי כך שהוא מצפין אותו ואז לדרוש תשלום ככופר עבור שחרורו.



צילום מסך של הודעת כופר אופיינית.

## איזמים חדשים, שיטות הפצה ישנות

אך למרות המאפיינים המורכבים שמאפיינים את נזקות ה-Ransomware למיניהן אחרי שהם הדביקו את המחשב, השיטות שבהן משתמשים התוקפים על מנת להפיץ אותן הן פשוטות למדי והן כוללות בעיקר הונאות הנדסה חברתית בהודעות דואר אלקטרוני. לפיכך נקטת כמה אמצעי זהירות פשוטים יכולה למנוע הדבקת המחשב בתוכנות כופר.

מעבדת הווירוסים של ESET פרסמה לאחרונה דו"ח העוסק בדרכי ההפצה של סוגים שונים של תוכנות זדוניות, ומצוין בו שהן מופצות בעיקר באמצעות קבצים המצורפים להודעות דואר אלקטרוני.

פתיחת הקבצים המצורפים באותן הודעות דואר אלקטרוני, גורמת להתקנת תוכנת ההצפנה על המחשב של המשתמש אשר תצפין את כל הקבצים בדיסק הקשיח ותציג את דרישת התשלום על מסך הבית - בה היא תנקוב בסכום הכופר המבוקש עבור מפתח ההצפנה הייחודי לאותו מחשב.



[Forward](#) [Forward as Attachment](#) [Reply](#) [Reply All](#) [Message List](#) [Unread](#) [Delete](#)

**Subject:** [Hobson Industries Ltd] 4 pages from +07786690048  
**From:** "Aida Stebbins" <aida.stebbins@hobson.co.uk>  
**Date:** Mon, January 19, 2015 9:16 am  
**To:** <mailto:mediatise@hobson.co.uk>  
**Priority:** Normal  
**Options:** [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#) | [Add to Address Book](#) | [View Message Details](#)

Number: +07786690048  
Date: 2015/01/18 16:16:36 CST  
Pages: 4  
Reference number: AH-BF409986D-5742  
Filename: mediatise.zip

--  
Hobson Industries Ltd  
Aida Stebbins

 mediatise.zip 25 k [Download](#)

Move to:  [Move](#)

קובץ זדוני מצורף להודעת אימייל תמימה למראה

## כך תמנעו מתוכנות הכופר:

**1. אל תורידו קבצים מצורפים –** לעולם אל תורידו קבצים המצורפים להודעות דואר אלקטרוני אם אינכם בטוחים במאה אחוז מהי התשובה לכל אחת מהשאלות הבאות: 1. מי הוא השולח? 2. מה הוא שלח? 3. האם הקובץ אכן מיועד אליי?

השתלטות על חשבונות דואר אלקטרוני במטרה להפיץ הונאות רשת היא לא דבר נדיר. לכן העובדה שאתם כביכול מכירים את השולח לא מספיקה על מנת להבטיח שהקובץ המצורף הוא לא וירוס. לכן דבר מומלץ לקרוא את התוכן של ההודעה כדי לקבל נתונים נוספים. אם משהו עדיין נראה חשוד, עדיף שתיצרו קשר עם השולח על מנת לוודא אם הוא אכן שלח לכם את ההודעה ומה מכיל הקובץ המצורף. מקרים שממש צריכים לעורר את חשדכם הם אנשים שאינכם נמצאים איתם בקשר שפתאום שולחים לכם כל מיני הודעות וקבצים מוזרים.

**2. אל תלחצו על קישורים מפוקפקים –** למרות שרוב מתקפות הכופר מקורן בקבצים המצורפים להודעות דואר אלקטרוני, קיימות שיטות התקפה נפוצות נוספות. אחת מהן היא לכלול קישורים בתוך ההודעה, שיובילו את הקורבן להתקנת התוכנה הזדונית ממקור מרוחק ברשת האינטרנט. בדומה לסעיף 1, אם אינכם יודעים מי שלח לכם את הקישור ולמה – אל תלחצו עליו.

התוקפים עלולים לשלוח מיילים המתחזים לשירותים מוכרים כמו PayPal, אתר הבנק שלכם ועוד, ועליכם להיות ערניים מאוד על מנת להבחין שמדובר בהתחזות, אבל אם יש אפילו ספק קל שבקלים – אל תלחצו! עדיף להתקשר לשירות הלקוחות של הגוף שכביכול שלח לכם את ההודעה ולברר, מאשר ללחוץ על הקישור ולהצטער.

**3. שמרו על מערכת הפעלה, תוכנות ואפליקציות מעודכנות –** עדכוני תוכנה הם חיוניים במלחמה נגד תוכנות זדוניות. התוכנות החשובות ביותר לעדכון הן מערכת ההפעלה שלכם, תוכנת הג'אווה, דפדפנים, תוכנת הפלאש ועוד.

בנוסף, ולא פחות חשוב, עליכם לוודא שהתוכנות המותקנות במחשב שלכם או במחשבי העסק שלכם הן חוקיות ואותנטיות – גם אם מדובר בתוכנה חנימית. תוכנות לא חוקיות לא מקבלות עדכונים ולכן עלולות להכיל פרצות אבטחה דרכן ניתן להדביק אתכם בתוכנות זדוניות.

**4. ודאו שקיימת תוכנת אבטחה על כל מחשב בבית –** אנחנו חייבים להדגיש את החשיבות בשימוש בתוכנת אבטחה – במיוחד בהקשר של תוכנות כופר. חשוב לוודא שתוכנת האנטי וירוס שלכם בתוקף, שהיא מעודכנת בחתימות הווירוסים העדכניות ביותר ושהיא מוגדרת בצורה נכונה.

**גם באנדרואיד –** בתקופה האחרונה נרשם זינוק לתוכנות כופר למכשירי אנדרואיד, לכן מומלץ להצטייד באפליקציית אבטחה שתמנע הדבקה של המכשיר הנייד שלכם.

5. **בצעו גיבוי תקופתי לכל המידע שלכם** – ככל שהעולם הופך טכנולוגי יותר, כך גיבוי הופך לדבר חיוני יותר – ולא רק בעולם העסקי. עסקים וחברות גדולות כבר הכירו מזמן בצורך בגיבוי והנסיבות, לצערנו, מכתיבות לנו מציאות שבה כל אדם צריך לעשות גיבוי של המידע שלו – לכל צרה שלא תבוא.

במקרה של תוכנות כופר החשיבות של גיבוי עולה בעשרות מונים, כיוון שללא מפתח ההצפנה אין אפשרות להשיב את הקבצים והאדם נשאר עם אפשרויות בודדות בלבד – לשלם או לאבד את הקבצים שלו לנצח - גיבוי היה פותר את הדילמה הזו.

## ESET אודות

חברת ESET היא חלוצת האנטי וירוס וחברת האבטחה ה-5 בגודלה בעולם, המגנה בזמן אמת על יותר מ-100 מיליון משתמשים מפני נזקות, גניבת זהויות ופישנינג, התקפות אינטרנט מקוונות והאקרים. מוצריה מתאפיינים בטכנולוגית זיהוי פורצת דרך, בצריכת משאבים מזערית ובחווית-משתמש מעולה.

בישראל מיוצגת ESET על ידי חברת קומסקיור, המפעילה בארץ מרכז שירות המציע תמיכה טכנית בעברית לכל הלקוחות. כיום ESET היא מוצר האנטי וירוס הביתי הנמכר בישראל, ובין לקוחותינו בשוק העסקי ניתן למצוא חברות טכנולוגיה ואינטרנט, מכללות ואוניברסיטאות, גופים ביטחוניים, מוסדות עירוניים וממשלתיים.