

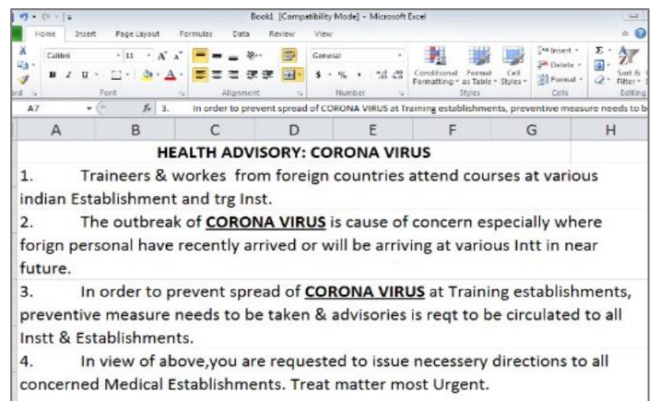
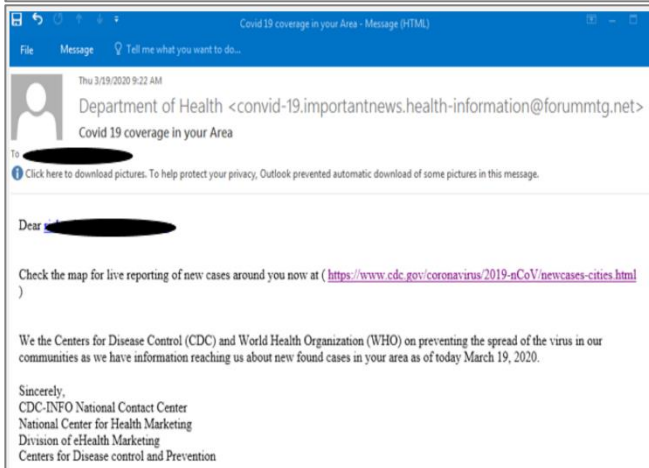
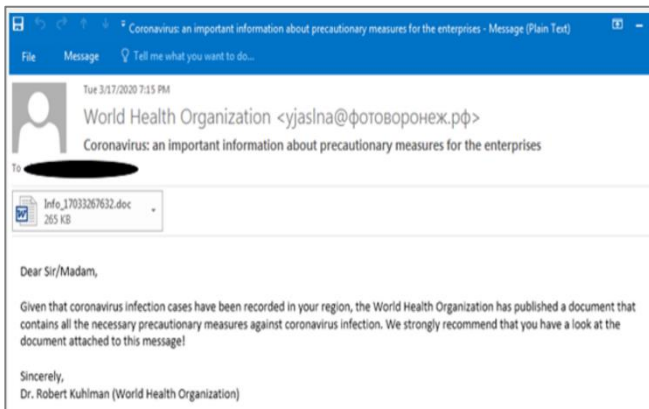


## רחבי העולם

### מתקפות דיוג העוסקות כביכול בנגיף הקורונה, מפיצות נזקות ברחבי העולם

מתקפות נוספות המנצלות את בהלת הנגיף, מפיצות הודעות דוא"ל כביכול מטעם ארגוני בריאות מקומיים ובינלאומיים. ההודעות מציעות מידע אודות הנגיף ומכילות צרופות או קישורים דוונים, אשר פתיחה שלהם מורידה למחשב הקורבן נזקות כגון Ostap/Trickbot המשמשות לאיסוף מידע רגיש, וכן נוזקות כופר ותולעים (worm).

אחת המתקפות מיוחסת להאקרים מפקיסטאן - ככל הנראה מקבוצת התקיפה APT36 – ומפיצה הודעות דוא"ל הנשלחות כביכול מממשלת הודו וכוללות המלצות רפואיות להתמודדות עם הנגיף. ההודעות מכילות צרופה מסוג RTF, המורידה נזקה להשתלטות מרחוק המכונה Crimson RAT. הנוזקה מנצלת חולשה מוכרת (CVE-2017-0199) ב-Microsoft Office וב-Notepad. הרחבה בקישור.



### אתרי הונאה ב-Dark Web

אתרי אינטרנט הפועלים ב-Dark web, מציעים למכירה מסיכות, ציוד רפואי וחיסונים. התשלום על המוצרים הינו בביטקוין ולאחר הרכישה המוכר נעלם והמוצרים לא מגיעים ליעדם. בין אתרים אלה, נמנים גם אתרים המציעים למכירה קיט תקיפה של קורונה בעבור פחות מ-1000 דולר. במסגרת חקירה שביצע האינטרפול, נתפסו כ-34,000 מוצרים מזויפים ולא תקינים.



## המלצות התגוננות

- לקבלת מידע מהימן ומעודכן אודות התפשטות הנגיף, יש להשתמש אך ורק באתרים רשמיים, כגון אתר משרד הבריאות.
- אין להשיב למסרונים הנשלחים כביכול ממשרד הבריאות אולם מכילים פנייה כללית. מסרונים לגיטימיים הנשלחים מטעם משרד הבריאות, תמיד יכילו את שמו המלא של הנמען.

<p>2. הודעה למי שאותר כמגע של חולה: [שם פרטי] שלום לפי חקירה אפידמיולוגית היית בתאריך [==/==/==] ליד חולה קורונה. עליך להיכנס מייד לבידוד עד [==/==/==] להגנה על קרוביך והציבור. אם יש לך חום, שיעול וכו' נא להתקשר למד"א - 101. מידע נוסף בקישור <a href="https://go.gov.il/corona">go.gov.il/corona</a> לאימות ניתן לחייג *5400 המידע ישמש רק למטרה זו וימחק בתום הצורך. בברכה שירותי בריאות הציבור</p>	<p>1. הודעה לחולה בקורונה [שם פרטי] שלום, בהתאם לתוצאות הבדיקה, לפיה חלית בקורונה, מבוצעת חקירה אפידמיולוגית כדי לאתר אנשים שנחשפו אליך. לצורך השלמת החקירה משתמשים באמצעים טכנולוגיים, לפי תקנות שעת חירום. המידע ישמש את משרד הבריאות רק למטרה זו וימחק בתום הצורך. מידע בקישור: <a href="https://go.gov.il/corona">go.gov.il/corona</a> לאימות ניתן לחייג *5400 בברכה שירותי בריאות הציבור</p>
---	---

- אין לפתוח קישורים או להוריד קבצים אשר התקבלו מגורם שאינו מוכר או שאמינותו מוטלת בספק.
- אין למסור מידע אישי כגון סיסמאות או פרטי חשבון ואין להשיב להודעות המבקשות פרטים מסוג זה.
- הודת יישומונים יש לעשות אך ורק מהחנויות המקוונות הרשמיות.
- בעת ביצוע רכישה מקוונת, יש לגשת ישירות לאתר ולא ללחוץ על מודעות וקישורים לקידום מכירות.
- יש להשתמש במוצרי הגנה כגון אנטי-וירוס וסינון דוא"ל.
- המלצות נוספות ניתן למצוא בהתראה שהפיץ מערך הסייבר הלאומי, בנושא מתקפות סייבר המנצלות את בהלת הקורונה.

מידע נוסף מופץ באופן תדיר באמצעות מערכת סייברנט במבזקי הסייבר והתרעות בתפוצה ממוקדת.

