

19 מרץ 2020
כ"ג אדר תש"פ
סימוכין: ב-ס-1040

ניצול מגפת הקורונה לביצוע מתקפות סייבר

תקציר



קבוצות תקיפה שונות עושות שימוש במגפת הקורונה על מנת לתקוף בשיטות של הנדסה חברתית בערוצים שונים. התקיפות מתבססות על העניין המוגבר והטבעי של המשתמשים בנושא לאור המשך התפשטות המגפה.

מומלץ מאד להתעלם מפניות אלו, ולצרוך את המידע בנוגע למגפת הקורונה מגורמים רשמיים בלבד.

פרטים

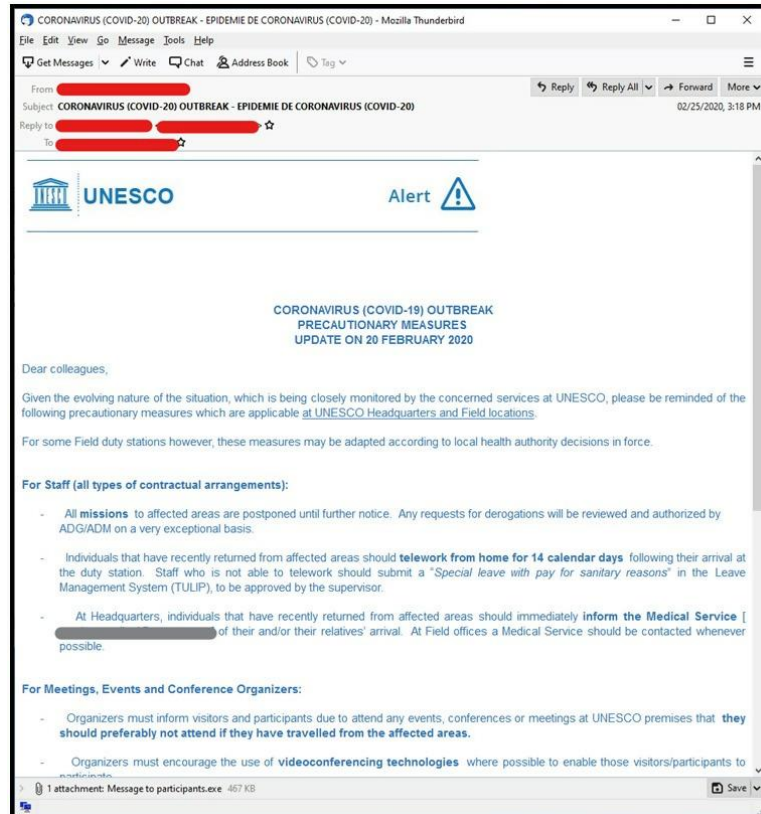


1. פניות התוקפים לציבור המשתמשים נעשות באמצעי תקשורת שונים (דוא"ל, רשתות חברתיות, סמס וואטסאפ וכד').
2. נושא הפניה עוסק בוירוס הקורונה (ייתכן בשמו הרפואי COVID-19) מהיבטים שונים - המלצות התמגנות ושיטות טיפול, מידע על היקף נפגעים במדינה/בעולם, הבטחות לאספקת חיסון תמורת תשלום, בקשה לתרומות לנפגעים מהמגפה, הפניה למפות חיות המציגות את קצב ההתפשטות של המגפה, וכד'.
3. הקישור או הצרופה שיצורפו לפניה יכולים לשמש להדבקה ישירה, להפנות לאתר המשמש לגניבת נתוני הזדהות, או אף לאתר המשמש לקליטת נתוני כרטיסי אשראי, לכאורה כתשלום עבור תרופה/חיסון לנגיף. במקרים רבים, שם הדומיין אליו מופנה המשתמש יכלול את המילה CORONA או COVID-19.

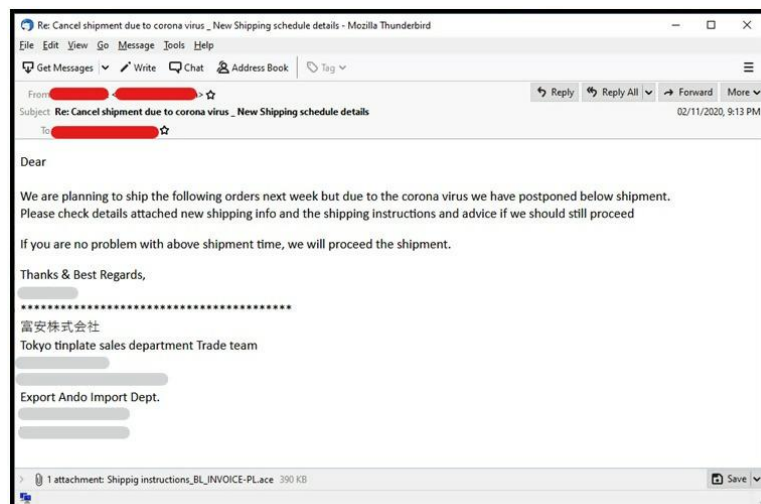
ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

4. ייתכן שימוש בשירותי קיצור URL כגון bit.ly, אשר יסתירו את היעד אליו מופנה המשתמש.

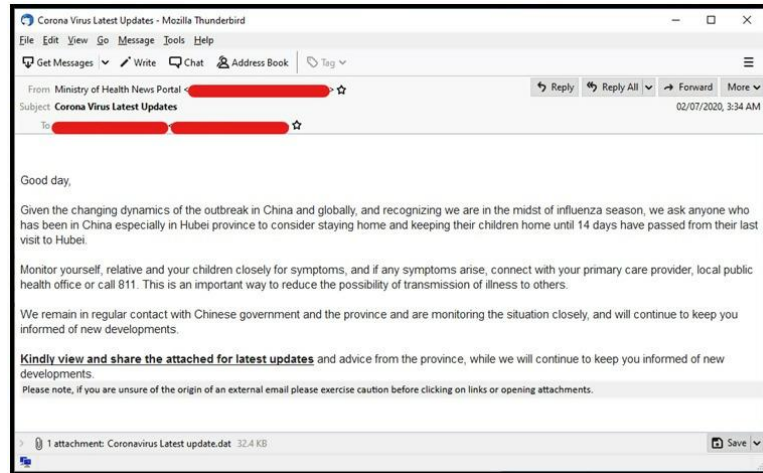
5. להלן מספר דוגמאות של תקיפות מסוג זה (מהבלוג של טרנד מיקרו):



6.



ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים



הודעת וואטסאפ מזויפת (מתוך ערוץ הטלגרם של משרד הבריאות):



1. **מומלץ מאד להתעלם מפניות אלו, ולצרוך את המידע בנוגע למגפת הקורונה מגורמים רשמיים בלבד (משרד הבריאות, רשויות מקומיות וכד').**

2. לרשותכם מידע בערוצים השונים המופעלים על ידי משרד הבריאות:

https://www.gov.il/he/departments/ministry_of_health

<https://govextra.gov.il/ministry-of-health/corona/corona-virus/>

ערוץ המשרד בטלגרם <https://t.me/s/MOHreport>

ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים



שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

