נגיף בגוף, חיידק בכיס

משבר הקורונה מעניק לעבריינים הזדמנויות רבות להונאות בקני מידה ניכרים, תוך ניצול אווירת החירום, המירוץ לציוד חיוני ואפילו ההתגייסות לטובת הקורבנות. מדריך מעשי לסכנות העיקריות וכיצד להימנע מהן > יהודה ברלב

המסחר בתרופות מזויפות וגנובות מוערך ב־3.3% מכלל הסחר העולמי בתרופות, דהיינו קרוב ל־400 מיליון דולר בשנה. ההונאות בייצור ובמסחר של מוצרי בריאות מתבצעות בהיקף גדול, המגיע במקומות מסוימים ל־10% מכלל תקציב הבריאות. ישנם אזורים המשמשים מקור למוצרים מזויפים וגנובים, או כיצרנים של הסחורה המזויפת, או כנקודות מעבר לסחורה גנובה ומזויפת

משברים לאומיים מהווים מוקד משיכה לנוכלים. מצד אחד ישנה אוכלוסייה גדולה הנזקקת לסיוע – כספי, רפואי וסיעודי. מצד שני מתבצעת הזרמה ניכרת של משאבים על ידי ממשלות וגופים ציבוריים, המהווים אבן שואבת לעבריינים. בעיתות משבר, לצד תופעות מחממות לב של ערבות הדדית ופעולות סיוע רבות הנעשות בכוונות טובות למען הנפגעים והחברה, ניתן לראות גם מאפיינים של מעשי הונאה, אשר מועצמים בעזרת הטכנולוגיות המפותחות בתחומי התקשורת, הכספים והפצת מידע.

ההונאות במשבר הקורונה אינן שונות מהונאות בעת אסונות אחרים שפקדו מדינות במאה ה־21, אך לאור ההיקף העולמי של המשבר, ישנה העצמה ניכרת של מעשי ההונאה מבחינת הכמות וההיקף הכספי.

הונאות בעידן אסון (Disaster Fraud) זכו להתייחסות נפרדת ואף לטיפול שונה על ידי מדינות שחוו אסונות לאומיים ב־20 השנים האחרונות, כולל מגיפות, רעידות אדמה, שיטפונות ועוד. המקרים הבולטים הם: הוריקן קתרינה (2005) והוריקן סנדי (2012); רעידות האדמה והצונאמי באוקיינוס ההודי (2004), בהאיטי (2010) וביפן (2011); השריפות בקליפורניה (2018–2017), קנדה (2017) ואוסטרליה (2020–2019); התאונות גרעיניות בצ'רנוביל (אוקראינה, 1986) ובפוקושימה (יפן, 2011).

הונאות סיוע ושיקום

לאחר אירועי אסון, גורמים ממלכתיים וממלכתיים־למחצה הזרימו כספים רבים לשיקום האזורים שנפגעו ולסיוע לאוכלוסייה שנפגעה. במספר מקרים, כספים אלה לא הגיעו לייעדם והוסטו על ידי גורמים עבריינים למטרותיהם. ניתן לאפיין הונאות סיוע ושיקום לפי הסוגים הבאים.

הונאת צדקה. אדם או קבוצה מעמידים פנים שהם ישות פילנתרופית לגיטימית המתרימה עבור קורבנות אסון. הם מבקשים מהציבור כסף, שלעולם לא יגיע למקבלים המיועדים. פניות כוזבות לתרומות מתבצעות באמצעות אתרי אינטרנט הנחזים לארגונים לגיטימיים המגייסים כספים לנפגעי אסון. כך לדוגמה, באסון ההוריקן קתרינה, נוכל הקים אתר לגיוס כספים לסיוע בהטסת נפגעי השטפונות אל מחוץ לאזורי הסכנה. את הכסף שנתרם הכניס לכיסו.

כיצד להימנע מכך? עשו שיעורי בית – חפשו באתר של מיפוי ארגוני צדקה את שם הקבוצה שאליהם תרצו לתרום, כגון Guidestar, Charity Navigator או GiveWell. בצעו חיפוש מקוון אחר "תרמית" ושם ארגון הצדקה; חיפוש כזה עשוי להביא לחשיפת התרמית. היזהרו מארגוני צדקה בעלי היסטוריה מועטה ושימו לב לשיטת ההתרמה – מזומן, העברות בנקאיות או צ'קים לאדם בודד. חפשו דרך לתרום לארגון גדול ומוכר יותר באמצעים מקוונים מאובטחים.

הונאת מענק. זמן קצר לאחר הוריקן קתרינה, נחשפו שני עבריינים שהתחזו כעובדי צבא הישע. הם גרמו ליותר מ־2,500 שוטרים, כבאים, צוותי הצלה וסוכני FBI לחשוף מידע אישי. השניים שכנעו את אנשי ההצלה והביטחון לחתום על טפסים לקבלת מענקים, בסך 5,000 דולר לכל אחד, בחסות ענק תקשורת בינלאומי. המטרה הסופית היתה להוציא את כספי הסיוע מהקורבנות בעזרת המידע האישי שנאסף במרמה.

כיצד להימנע מכך? פנו לגוף התורם או הנותן מענק, סביר להניח שהוא כבר מעודכן בעניין ויתריע אם מדובר בהתחזות. כך למשל, פניות של קורבנות לסיפורים כוזבים על מענקים שנותנות חברות רב־לאומיות כנגד הקלקות ברשת, זכו להכחשות מיידיות מצד החברות.

הונאת ספקים וקבלנים. אנשים מתחזים לקבלנים או למשפצים ומבטיחים לתקן נזקים שנגרמו באזורי האסון, ללא כוונה לבצע את השיפוץ או להשלים את המטלה. לעיתים הם מבקשים מקדמות ניכרות במסווה של קניית חומרים מראש, ולאחר מכן נעלמים.

רו"ח יהודה ברלב, ברלב ושות' - ביקורת חקירתית. התמונות: הונאות אופיניות מתקופת הקורונה

כך לדוגמא, באסון ההוריקן צ'רלי בפלורידה ב־2004, כומר לשעבר התחזה לנציג של שתי חברות שיפוצים בעלות רישיון לעבודות בנייה, עם כרטיסי ביקור שלהן. הוא לקח מקדמות בסך חצי מיליון דולר מ־50 בעלי בתים שנפגעו. בחלק מהמקרים ה"משפץ" התחיל לעבוד עם פועלים שהביא ואח"כ נעלם. הוא נעצר מאוחר יותר במדינה אחרת והוסגר לצורך העמדה לדין.

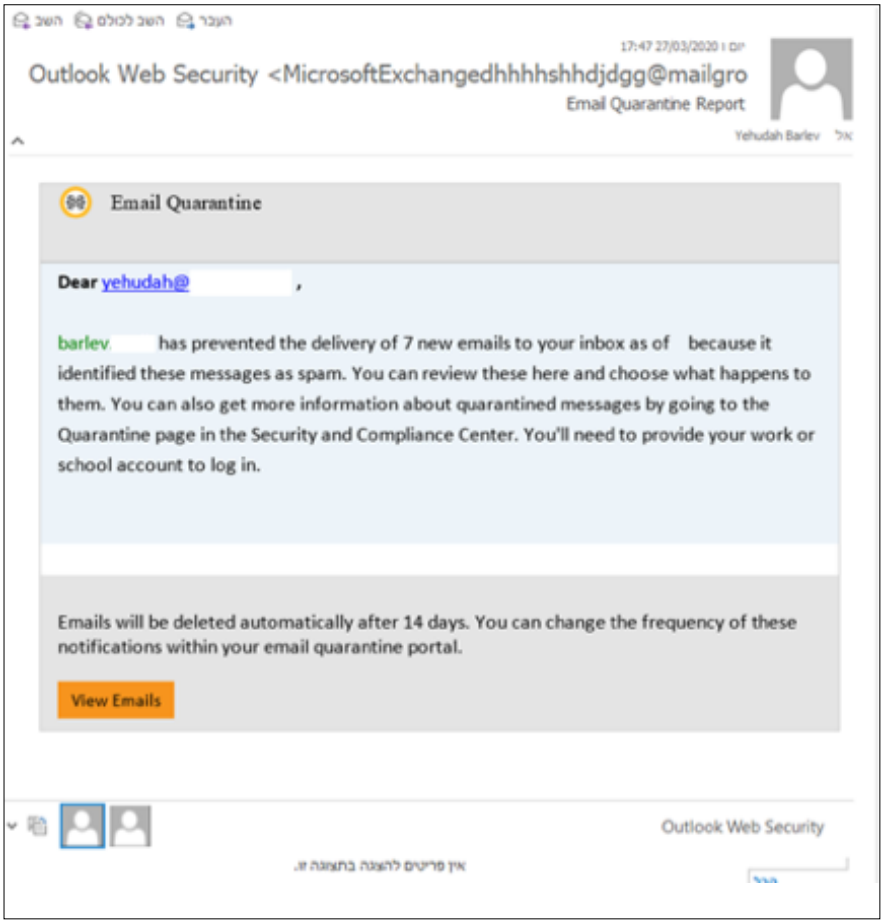
כיצד להימנע מכך? אם הנכס שלכם נפגע באסון טבע, עשו מחקר מקוון כדי למצוא קבלנים אמינים או חברות תיקוני נכסים. חפשו ארגונים בעלי היסטוריה מבוססת של עבודה באזור וקראו ביקורות של לקוחות. פנו ישירות לחברה באמצעות פרטי קשר שפורסמו, ולא דרך אדם שעשוי להתחזות.

הונאות בתביעות ביטוח. לאחר אסון, בעלי הרכוש שנפגע מגישים תביעות לחברות הביטוח בגין הנזק שנגרם לרכוש המבוטח. ישנם אנשים או ארגונים מסוימים הרואים בכך הזדמנות להגיש תביעות מנופחות, או מפוברקות לחלוטין, ואף נעזרים ב"בעלי מקצוע" להגשת תביעות כאלה. חלקם אף פוגעים במכוון ברכוש כדי לקבל תשלום יותר גבוה.

כיצד להימנע מכך? אנשי מקצוע שתפקידם לאתר ולמנוע הונאות בענף הביטוח, צריכים לשים לב במיוחד לתביעות שהוגשו לאחר אסונות גדולים ולחפש אי התאמות או דגלים אדומים. אם בוטיק בגדים בשטח 200 מ"ר מגיש תביעה בגין חומרי ריצוף בשווי 2 מיליון דולר, לא סביר שכמות החומרים תואמת את שטח החנות. למרות שבשלב זה מופעל לחץ רב, גם מטעם השלטונות, לקבלת סכומי התביעה באופן מיידי, על התובעים להיות מסוגלים לספק הוכחה כלשהי לרכישה או לשימוש של הנכס עבורם הם מבקשים פיצויים.

מסחר בתרופות מזויפות

במארס 2020 פרסם OECD דוח על המסחר הלא־חוקי בתרופות מזויפות.[1] מנתוני הדוח עולה, כי ב־2018 הסתכם שוק התרופות העולמי ב־1.2 טריליון דולר, עלייה של 100 מיליון דולר לעומת שנת 2017. בשנים 2014–2018 חלה עלייה ממוצעת של 6.3% בשנה. עוד לפני משבר הקורונה היתה ציפייה ששוק התרופות יגדל ליותר מ־1.5 טריליון דולר בשנה, עד שנת 2023.



הונאת אבטחה
המטרה: להוציא מכם את הסיסמה למחשב שלכם ובמיוחד למערכת הדוא"ל שלכם.
השיטה: שליחת הודעת פישינג (Phishing) עם טענה שהשרת חסם הודעות דוא"ל ושומר אותם. על מנת לשחרר את ההודעות שנמצאות כרגע בבידוד (Quarantined) הינך מתבקש להיכנס לקישור. בקישור הינך נדרש להקיש סיסמא.

המסחר בתרופות מזויפות וגנובות מוערך ב־3.3% מכלל הסחר העולמי בתרופות, דהיינו קרוב ל־400 מיליון דולר בשנה. ההונאות בייצור ובמסחר של מוצרי בריאות מתבצעות בהיקף גדול, המגיע במקומות מסוימים ל־10% מכלל תקציב הבריאות. ישנם אזורים בעולם המשמשים מקור למוצרים מזויפים וגנובים, או כיצרנים של הסחורה המזויפת, או כנקודות מעבר לסחורה גנובה ומזויפת.

המוצרים הגנובים והמזויפים מופצים באמצעות תובלה יבשתית, אווירית וימית, במיכלים או בחבילות קטנות, תוך ניצול פתרונות לוגיסטיקה מודרניים, כמו משלוחי חבילות קטנות או אזורי סחר חופשי. צרכני התרופות אינם מודעים תמיד לבעיית התרופות המזויפות וניתן לשכנע אותם בקלות שמדובר בתרופות מקוריות. למשל, באיטליה 90% מהצרכנים שרכשו תרופות מזויפות, האמינו שמדובר בתרופות מקוריות.

עד לשנים האחרונות היה קיים בלבול לגבי הגדרות של תרופות מקוריות ולגבי זכויות הקניין וייצור התרופות. ב־2017 ארגון הבריאות העולמי (WHO) הגדיר מחדש את המוצרים:

> מוצרי תת־תקן – הנקראים גם "מחוץ

אם בוטיק בגדים בשטח 200 מ"ר מגיש תביעה בגין חומרי ריצוף בשווי 2 מיליון דולר, לא סביר שכמות החומרים תואמת את שטח החנות. למרות שבשלב זה מופעל לחץ רב, גם מטעם השלטונות, לקבלת סכומי התביעה באופן מיידי, על התובעים להיות מסוגלים לספק הוכחה כלשהי לרכישה או לשימוש של הנכס עבורם הם מבקשים פיצויים

לאפיון" ("out of specification"). אלו הם מוצרים רפואיים מורשים, אולם אינם עומדים בתקני איכות או באפיון המוצר, או בשניהם.

> מוצרים שאינם רשומים/מאושרים – מוצרים רפואיים שלא עברו תהליך הערכה או אישור של הגוף המאסדר הלאומי/האזורי המוסמך לאשר תרופות לאזור בו הן משווקות/מופצות, בכפוף לתנאים לשימוש המוסדרים בדרך כלל בחקיקה מקומית או אזורית.

> מוצר מזויף – מוצר רפואי שבמזיד מציג זהות כוזבת או מרכיבי ייצור או מקור כוזבים.

השפעת תרופות מזויפות מורגשת במספר רמות:

> נזק בריאותי למשתמשים. כך למשל, קיימת הערכה, כי בין 72 אלף ל־169 אלף ילדים מתו מדי שנה מדלקת ריאות לאחר שקבלו תרופות מזויפות, ותרופות מזויפות נגד מלריה גרמו למותם של עוד 116 אלף.

> אובדן מכירות ונזק תדמיתי ליצרנים לגיטימיים. חברות תרופות בארה"ב הן הנפגעות העיקריות מסחר בתרופות מזויפות. מדינות נוספות ב־OECD שנפגעות קשות מכך הן שווייץ, גרמניה וצרפת.

> אובדן הכנסות ועלויות למדינות ולמשקים. העלות למדינות האיחוד האירופי מאובדן הכנסות מסחר בתרופות מזויפות מוערכת ב־1.7 מיליארד אירו בשנה.

> עלויות טיפול בחולים הסובלים מנזקים בריאותיים בשל שימוש בתרופות מזויפות.

> זיהום סביבתי כתוצאה מייצור ללא פיקוח, תוך שימוש בחומרים רעילים.

> עלויות חברתיות כתוצאה מהגידול בפשיעה מאורגנת ואובדן מקומות עבודה. קיימת הערכה, לפיה בענף התרופות והשירותים הנלווים באירופה קיים אובדן של 80 אלף משרות.

המסחר בתרופות מזויפות גדל משמעותית כתוצאה מהזינוק בשימוש במשלוחים (דואר, חברות שליחים). ב־95% מההחרמות שבוצעו על ידי שירותי המכס העולמיים בשנים 2014–2016, ממוצע התפיסות של תרופות מזויפות בשירותי דואר ושליחויות אקספרס, היה גבוה משמעותית מהממוצע התפיסות של מוצרים אחרים. מידע חסר על משלוחי דואר מקשה על גילוי וניטור של מוצרים הנשלחים בדואר מכתובת מקומית או זרה. מאחר שהמסמכים הקשורים למשלוח מגיעים בנייר מודפס, ניתן בקלות לשנות ולתת דיווח כוזב למכס.

הגידול האדיר בסחר האלקטרוני, החוצה מדינות ומגדיל משמעותית את כמות הצנכנים הישירים, הפך את המשלוחים הקטנים לדרך אטרקטיבית מאוד לעבריינים. השוק מוצף בחבילות דואר, במספר הולך וגדל. המשלוחים הקטנים מטופלים בעיקר על ידי רשויות דואר וחברות דואר מהיר, בתמיכה פעילה של פלטפורמות מסחר אלקטרוני קמעונאי. הגידול המשמעותי בסחר, שרובו לגיטימי, מקשה על גילוי הסחר הבלתי חוקי. הזייפנים משתמשים בחבילות/מעטפות קטנות בעלות בועות פלסטיק ("פצפצים"), אשר נבלעות בים המשלוחים.

מתוך התרופות המזויפות שנתפסו על ידי גופי המכס בעולם בשנים 2014–2016, היו 35% בתחום האנטיביוטיקה, 15% בתחום המיני, 10% משככי כאבים, ובשיעור דומה תרופות מזויפות נגד מלריה. 3%–5% היו תרופות מזויפות לטיפול בסוכרת, במחלות לב, באלרגיות ותוספי מזון.

ארגון הבריאות העולמי הערין, כי למעלה ממחצית התרופות שנרכשות באינטרנט, מאתרים לא־חוקיים המסתירים את הכתובת הפיזית שלהן, הן מזויפות. מחקר משנת 2008 העלה, כי 62% מהתרופות שנרכשו במהלכו באופן מקוון היו מזויפות או לא תקניות; 95.6% מבתי המרקחת המקוונים שנחקרו פעלו באופן בלתי חוקי; 94% מהאתרים היו ללא שם הבעלים או רוקח שניתן לאמת; 84.5% מבתי המרקחת המקוונים היו וירטואליים (כלומר, לא פעלו ממבנה ניתן לזיהוי); 78.8% מהאתרים הפרו סימנים מסחריים; 90.3% מהאתרים סיפקו תרופות מרשם ללא מרשם רופא.

באותו דוח ביצעו מומחים ניתוח של התרופות ששווקו באופן מקוון, כדי לקבוע את המקוריות שלהן. הם מצאו, כי סביר להניח שרוב הצרכנים לא יוכלו לזהות בעצמם שהמוצרים מזויפים. הרוב המכריע של התרופות המזויפות אינן מכילות את החומרים הפעילים הנכונים במינון הנכון. בנוסף, רבות מהתרופות המזויפות מכילות רכיבים פעילים לא־מוצהרים, שעלולים לגרום להשלכות בריאותיות קשות.

בישראל, שרשרת אספקת התרופות שונה באופן מהותי מהמתואר בדוח. עם זאת, במשבר קורונה, לאור הירידה בהיקף השירותים הרפואיים הלא־דחופים והנטייה לפנות לאפיקים לא־קונבנציונליים בעת מצוקה, פועלת שרשרת אספקה דומה.

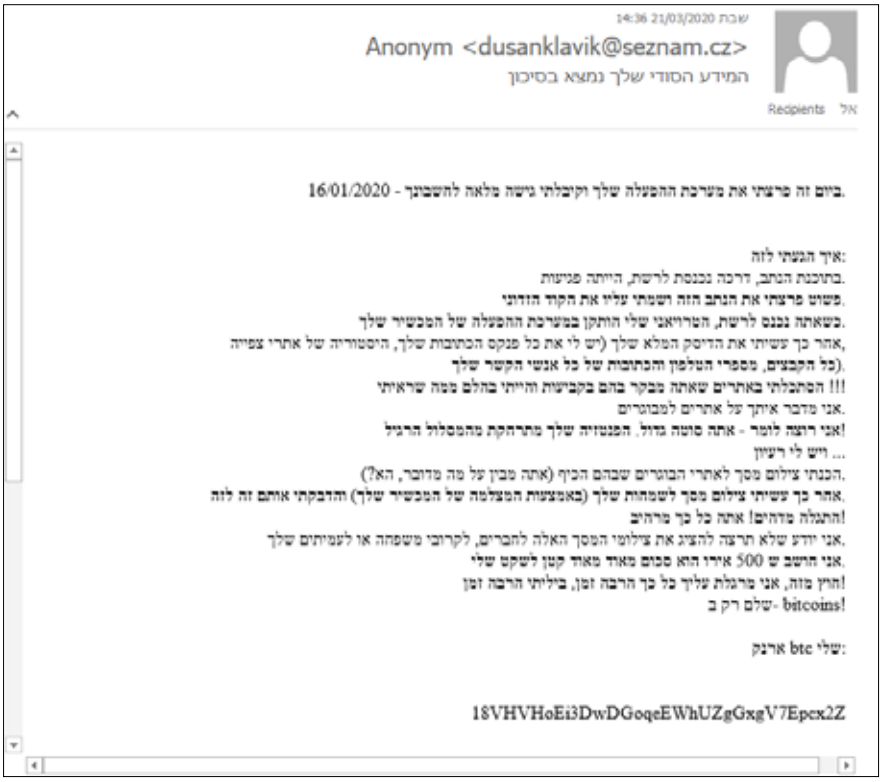
על פי הדוח, שיווק של תרופות מזויפות מצליח כתוצאה מניצול חולשות בשרשרת האספקה, במקטעיה השונים. המרשמים לתרופות ניתנים על ידי רופאים אשר לעיתים נדירות באים במגע עם התרופות, ונמסרים על ידי רוקחים המקבלים את התרופות בדרך כלל ממספר סיטונאים. בארצות הברית, 90% מהתרופות מופצות על ידי חמישה סיטונאים עיקריים, ו־10% הנותרים מסופקים על ידי 7,000 סיטונאים משניים המתמחים ברכישה ומכירה של מוצרים רפואיים מוזלים.

הספקים המשניים ממלאים את הביקוש במקרים של מחסור, ומשמשים כמקור הכנסה נוסף עבור הסיטונאים העיקריים. הספקים המשניים רוכשים במחירים מוזלים מלאי עודף מיצרנים, סיטונאים, בתי מרקחת ולעיתים ממתווכים חסרי מצפון. הם מוכרים את המוצרים למפיצים גדולים או לקמעונאים גדולים אחרים. גודלם הקטן מאפשר

מאפייני הסחר בתרופות מזויפות

הגורם המדרבן	התנאים המיטיבים לזיוף תרופות	המצב הנוכחי
מאפייני השוק		
רווחיות	שיעור רווחיות גבוה ליחידה או נפח גדול	יכולה להיות גבוהה מאוד, במיוחד אם הרכיבים זולים
גודל השוק	שוק פוטנציאלי גדול	שוק הפארמה גדול מאוד (1.2 טריליון דולר) וממשיך לגדול
חוזק המותג	רמה גבוהה של הכרת המותג	עוצמת מותג חזקה
ייצור, טכנולוגיה והפצה		
ההשקעה הנדרשת	ציוד פשוט וזול	עלות ייצור זיופים גולמיים יכולה להיות צנועה ומכבש ייצור לגלולה עשוי להספיק
טכנולוגיה נדרשת	לא מתוחכמת, קלה להשגה	אתגרים משתנים של טכנולוגית ייצור, אריזה וסימון מוצרים. יכול להיות אתגר מורכב או פשוט, תלוי במוצר
לוגיסטיקה	פשוטה וזולה	הוצאות הובלה נמוכות; אזורי סחר חופשי מאיצים סחר בזיופים
שיווק ומכירת המוצרים	קל להקים מערך שיווק או לחדור לקיים	קשה לחדור לשרשרת מערך שיווק של ספקים מקוריים. קל יותר בשכבה השנייה של קמעונאים. האינטרנט מאיץ סחר בזיופים
היכולת להסתיר הפעולות	קל להסתיר פעולות בלתי חוקיות	כאשר הפעולות הבלתי חוקיות בהיקפים קטנים, קל להסתירן
היכולת לרמות את הצרכנים	קל לרמות צרכנים	קשה יותר לרמות את גורמי הפיקוח ומניעת ההונאות של השלטונות ושל היצרן המקורי
מאפיינים מוסדיים		
מסגרת חוקית ומאסדרת	חקיקה חלשה	במדינות רבות מצבים מורכבים מקשים על העמדה לדין
אכיפה	אכיפה חלשה	רמת האכיפה משתנה ממדינה למדינה. זייפנים מתוחכמים בדרך כלל מצליחים לעקוף אותה ולהתחמק
עונשין	עונשים קלים	ברוב המדינות הסנקציות פליליות, עם קנסות בגובה של עלות עסקית נסבלת לעומת הרווח האפשרי

מומחים ניתחו תרופות ששווקו באופן מקוון, כדי לקבוע את המקוריות שלהן. הם מצאו, כי סביר להניח שרוב הצרכנים לא יוכלו לזהות בעצמם שהמוצרים מזויפים. הרוב המכריע של התרופות המזויפות אינן מכילות את החומרים הפעילים הנכונים במינון הנכון. בנוסף, רבות מהתרופות המזויפות מכילות רכיבים פעילים לא־מוצהרים, שעלולים לגרום להשלכות בריאותיות קשות



הונאת הפריצה הזדונית
<u>המטרה</u>: תשלום באמצעות Bitcoin או מטבע וירטואלי אחר.
<u>השיטה</u>: הצגה לכאורה של פריצה למחשב שלך והוצאת חומר מביך. "אם לא תשלם נציג חומר מביך" והערה: אין שום הצגה של חומר מביך. "הכל דיבורים").

להם לנצל שינויים בשוק ולהתרכז בתרופות ספציפיות בעלות ביקוש גבוה בזמנים ובאזורים מסוימים.

הבעיות במעקב ובפיקוח מתעוררות במעבר של מוצרים רפואיים מקוריים ממדינה למדינה, כאשר יבואנים, קמעונאים ומפיצים לגיטימיים נכנסים לתמונה. האריזה מחדש שמתבצעת בתהליך זה, מספקת הזדמנות להחדיר תרופות מזויפות לשרשרת האספקה, תוך הסוואת הגורמים המבצעים. הערכת האטרקטיביות לזייפנים לייצור וסחר בתרופות מזויפות מובאת בטבלה המצורפת.


שלום רב, לצורך תשלום מקדמה על חשבון גמלת אבטלה, עליך לעדכן את פרטי חשבון הבנק בקישור הבא: btl.gov.il/f2196722. לאחר עדכון פרטי חשבון הבנק, התשלום יופקד בחשבונך באופן אוטומטי. המוסד לביטוח לאומי.

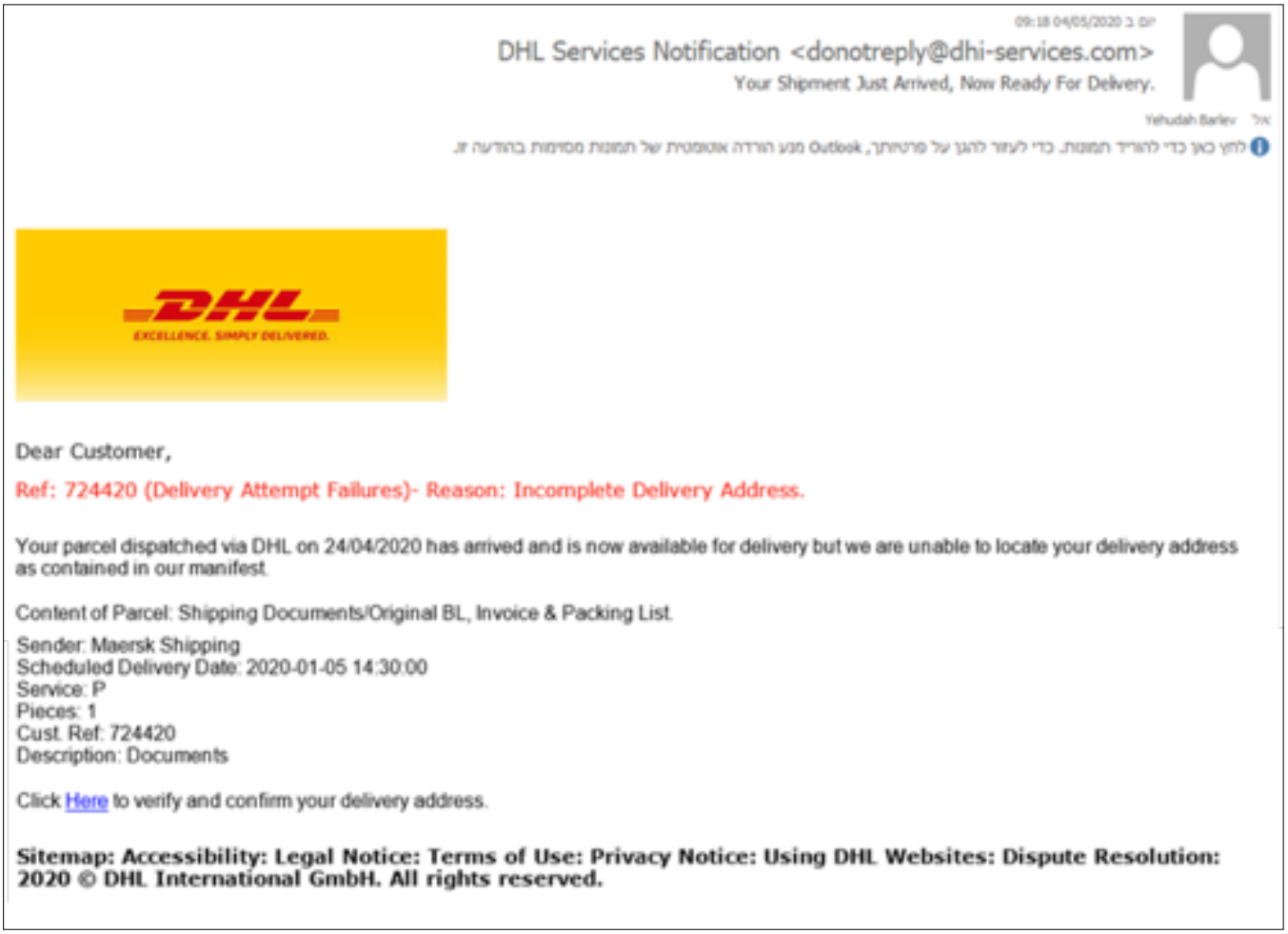
זהו דוא"ל אמיתי של הביטוח הלאומי. נפלו בו טעויות העלולות לרמז על מירמה: לא קיימת "גימלת אבטלה" ושמו של הנמען אינו מופיע

הונאות בהשקעות ובמכירות

משבר הקורונה יצר לעבריינים הזדמנויות רבות. סגירת הגבולות, מגבלות תנועה וחשש ממפגשים אישיים הביאו לשימוש נרחב בטכנולוגיות מתקדמות. ניהול מו"מ, ביצוע עסקאות ואף חתימות על הסכמים מתבצעים באמצעים טכנולוגיים מרחוק, ולא באופן ישיר כמקובל. מצב זה, תוך ניצול הפאניקה בקרב הציבור, מהווה כר פורה להוצאת כספים במרמה או למעשי הונאה אחרים. אנו מבחינים בהונאות בתחומים הבאים:

הונאות בהשקעות מסוג "לשאוב ולהשליך" (investment pump-and-dump scams). העבריינים מפיצים המלצות לרכוש מניות של חברות שפורסם לגביהן שיש להן פתרונות זמינים או עתידיים לחיסון או לטיפול בקורונה, או מוצרים המתאימים למשבר (למשל: מוצרים לתקופות סגר בבית, טכנולוגיות יישומיות לעבודה בסגר, רעיונות "מהפכניים" להקלה על האוכלוסייה). הפצת המידע הכוזב על החברה ומניותיה נעשית בדרכים שונות, כולל: שמועות, דוא"ל שלכאורה נשלח בטעות, הודעות לעיתונות ואף מאמרים, כולל ברשתות החברתיות.

מחיר המניות מזנק כתוצאה מהביקוש והעבריינים, שרכשו קודם את המניות במחירי רצפה, מוכרים אותן ברווחים נאים. אחרי מספר ימים מחיר המניה מתרסק, כשמתברר שהמניות אינן מייצגות שווי כלשהו. בנוסף, קיימת סכנה, כי כתוצאה מההונאה יופסק המסחר במניות והרוכש לא יוכל לממש השקעתו, אף לא בחלקה. עד סוף אפריל פרסמה רשות ניירות הערך האמריקנית (SEC) הודעות אזהרה[2] והשעתה מהמ־



החבילה שלא הגיעה
המטרה: לקבל פרטים מוכמנים.
השיטה: פנייה לעדכון פרטים עבור החבילה שלא הגיעה בשל העדר כתובת מתאימה, תגרום למשתמש לפתוח את הקובץ המצורף ולהעביר פרטים מוכמנים. המייל נחזה להיות של חברת משלוחים בינלאומית מוכרת.

סחר למעלה מ־25 חברות.

לדוגמא, במקרה של Predictive Technology Group הודיעה הרשות, כי היא משעה את המסחר במניות החברה מאחר שעלו שאלות לגבי אמינות והתאמה של המידע שהופץ בשוק. מדובר בשלוש הודעות לעיתונות במהלך מארס–אפריל בשם החברה, המצהירות על יכולתה להפיץ באופן מיידי כמויות גדולות של בדיקות סרולוגיות לגילוי נוכחותו של קורונה בנוגדנים.

המסחר במניות SpectrumDNA הושעה לאור חששות בקשר להתאמה ודיוק במידע הזמין לציבור בנוגע לחברה, כולל מצבה הכספי ופעולותיה, אם בכלל. זאת, לאור העדר גילוי כלשהו מהחברה לציבור מאז שנת 2015 ובשל החשש שהמשקיעים מבלבלים בינה לבין חברה פרטית בשם דומה, המייצרת מכשירים לאיסוף דגימות רוק ומעוררת התעניינות תקשורתית רבה במהלך הקורונה. מאותה סיבה הושעה המסחר במניות Zoom Technologies, בשל השם הזהה לזה של מפעילת שירות הפגישות הוויטוראלי, שמניותיה זינקו מאז תחילת המשבר.

מכירות דמה על פלטפורמות מכירה לגיטימיות. אלו מתפרסמות על גבי אתרי מכירה מקוונים, כולל מוצרים, מחירים וזמן אספקה אטרקטיביים, כאשר הספק אינו חלק מפלטפורמת מכירה מקוונת ואינו קשור אליה, אלא רק "אורח". בפועל, המוצר אינו תואם את התיאור באתר או שלא מתבצע אספקה. התשלום מתבצע מראש ואין החזרה של הכסף, בכל מצב.

בעיתות משבר, כשהציבור משווע למוצרים מסוימים, במיוחד אם הם במחסור (למשל: מסכות, חומרי חיטוי, חיסונים), קל יותר להניע אותו לבצע רכישה עם בטחונות מינימליים או בלא בטחונות כלל. ככל שהמחיר יהיה נמוך יותר, כך רמת הסיכון שהקונה

העבריינים מפיצים המלצות לרכוש מניות של חברות שפורסם לגביהן שיש להן פתרונות זמינים או עתידיים לחיסון או לטיפול בקורונה, או מוצרים המתאימים למשבר. הפצת המידע הכוזב על החברה ומניותיה נעשית בדרכים שונות, מחיר המניות מזנק כתוצאה מהביקוש והעבריינים, שרכשו קודם את המניות במחירי רצפה, מוכרים אותן ברווחים נאים

הונאת אמצעי בטחון שהופרו
המטרה: להוציא מכם את הסיסמה למחשב שלכם ובמיוחד למערכת הדוא"ל שלכם. או: השתלת תוכנה זדונית/וירוס.
השיטה: לגרום למשתמש ללחוץ על הקישור.

יהיה מוכן לקחת על עצמו תהיה גבוהה יותר.

הפקעת מחירים. בעיתות משבר יש המנצלים את מצוקת הציבור ונכונותו לשלם כל מחיר על מוצרים מניעתיים. השלטונות וגופים מאסדרים פועלים למנוע תופעות כאלה, אולם לעיתים יש קושי בהוכחת ההפקעה. לדוגמא, במקרה שהיה באסון הוריקן וילמה, אדם הועמד לדין על שרכש גנרטורים בצפון קרוליינה ב־529.99 דולר ו־279.99 דולר ומיד לאחר מכן מכר אותם במיאמי ב־900 דולר ו־600 דולר.

הונאות סייבר

הונאות סייבר קיימות מזה שנים, אולם במשבר הקורונה חלה עלייה ניכרת בהיקף התופעה, כפי שמתריעים על כך גופי מחקר בתחום. ככל שמתרחב השימוש במכשירים ניידים למסחר אלקטרוני, כך מתרבים הניסיונות לחדור ולשבש עסקאות. ניתן לראות לא מעט אתרים של רשויות וגופים מסחריים המפרסמים אזהרות לגבי אתרים וקישורים חשודים ומתריעים מהונאות הסייבר.[3] באחד הפרסומים נכתב שנרכשו למעלה מ־4,000 כתובות, ככל הנראה לשימוש אתרי הונאות סייבר, בינואר–פברואר השנה לבדם. אלו המאפיינים בהונאות סייבר בעידן הקורונה:

דוא"ל שנשלח לקורבן המתחזה להודעות מגוף מוכר, כגון ארגון הבריאות העולמי, משרד הבריאות, הביטוח הלאומי, נותני שירות כמו אתרי סחר מקוון, משרדי עורכי דין ועוד. המלל בדוא"ל מתייחס ל"עדכונים" או זיהוי לצורך הטבה/מענק או בדיקה כלשהי ומכיל קישור זדוני לאתר הנחזה להיות אתר של גורם אמיתי. זאת במטרה לקבל פרטים מוכמנים (כגון סיסמאות, פרטי חשבון, כתובת) שיאפשרו חדירה לאמצעים של הקורבן. לאחר מסירת הפרטים, מקושר הקורבן לאתר האמיתי ואינו יודע שנפל קורבן.

ניסיונות חדירה והשתלטות על מחשב של קורבן, לשימושים שונים: שימוש ברשתות חברתיות לגיוס כספים לסיוע לנזקקים ל"מלחמה בקורונה", כך למשל הטמנת מלכודות לקורבנות שנכנסים לאתרים של עבריינים, או לקישורים לטפסים, סרטונים ותמונות שמאפשרים כניסה למחשבים שלהם, או למכשירים טכנולוגיים אחרים (טלפונים חכמים, טבלטים), או חושפים את הקורבנות למעשי מרמה.

שיטות נוספות להשתלטות על חשבון המחשב של הקורבן:

- רכישת פרטי התחברות ברשת האפילה.
- דחיסת אישורים, תוך ניצול העובדה שמרבית המשתמשים עושים שימוש חוזר בסיסמא ושם משתמש, או משתמשים באותו מבנה להבנייתם, באתרים רבים

המשמשים אותם. על בסיס הנחה זו מריץ התוקף אינספור ניסיונות עם הסיסמא/שם משתמש שכבר בידו. ממחקר שנערך עלה, כי 81% מהמשתמשים עשו שימוש בסיסמא אחת בשניים או יותר אתרים.

› שימוש בהונאת משלוח. פצחן משתלט על מחשב הקורבן, אולם שומר על כתובת הלקוח למשלוח, למניעת חשיפה. לאחר שהמשלוח יצא לדרכו הוא מיורט באתר המשלח תוך שינוי בכתובת הנמען.

› הנדסה חברתית – טכניקות שונות המשמשות לתמרון קורבנות לביצוע פעולות או חלוקת מידע סודי. לדוגמא: העברין מתחזה לגורם אחר לצורך מתן הנחיות, כמו שינוי חשבון ספק. הוא רוכש כתובת של www.ternbel.na. חיבור האותיות r ו־n נראה כמו m והקורבן מניח שהכתובת היא של ספק שלו: www.tembel.na. אילוזיה דומה מתקבלת משילוב האותיות v ו–v ומשילובים נוספים.

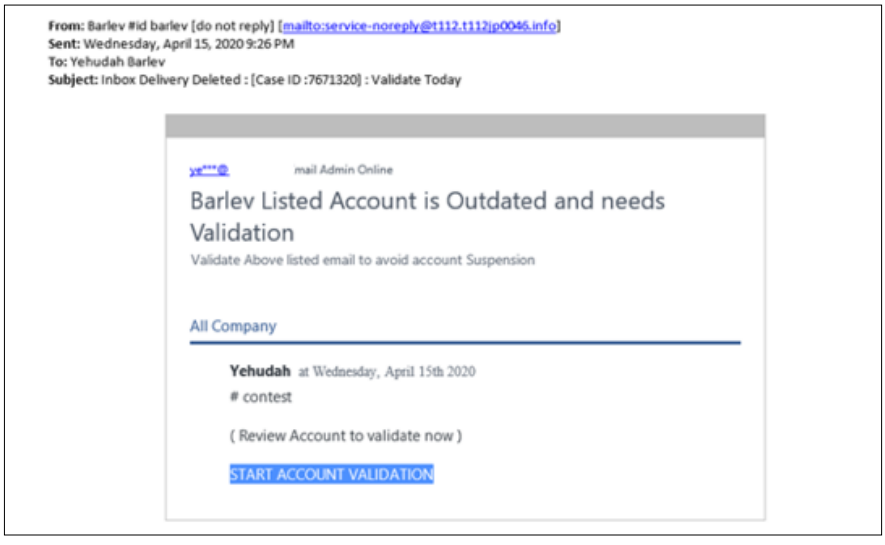
› הונאות על רקע רומנטי – בן/בת הזוג משלטים על המחשב של בת/בן הזוג והסימאות המשמשות אותו.

פעולות זדוניות אלו נועדו, בין השאר, להחדרת סוס טרויאני.[4] כך למשל, בינואר־פברואר השנה נשלח ביפן דוא"ל שנחזה להיות מארגון סעד יפני ועסק בהתפשטות מקרי הקורונה. צורפה אליו תוכנת סוס טרויאני שהיתה אמורה לתת לקורבן מידע נוסף. פתיחת הצרופה גרמה לתוכנת הסוס הטרויאני EMOTET[5] להיטען לתוך מערכת המחשב של הקורבן.

שימוש בבוטים. באתרי מסחר מקוון קיימת מגמה של שימוש בבוטים.[6] כשליש מהם, כך מניחים, מיועדים למטרות זדוניות. אחרי תחום הפרסום והתקשורת, המסחר המקוון הוא הענף השני עליו ממוקדים בוטים זדוניים במשבר הקורונה. כבר בפברואר 2020 מגזר המסחר המקוון היה עד לעלייה בלתי צפויה בתנועת הבוטים הזדוניים.

בתקופת משבר הקורונה, אתרים רבים זוהו כמוקדים של פעולות זדוניות. אלו משכו את הקורבנות להתחבר אליהם באמצעות קיום דיונים מקוונים על הנגיף בפרט ועל משבר הקורונה בכלל, כמו גם אתרים כוזבים הטוענים למכירה של מסכות רפואיות, חיסונים וערכות בדיקה ביתיות לאיתור הווירוס. כך למשל, האתר vaccinecovid-19.com שנוצר בפברואר 2020 ונרשם ברוסיה,

הונאה בכיסוי של WHO
המטרה: הוצאת פרטים מוכמנים.
השיטה: דוא"ל במסווה של ארגון הבריאות העולמי נשלח עם קישור (לינק) לרשימת אמצעי הגנה נגד הקורונה. הכניסה לרשימה מחייבת לעבור דרך דף עם זיהוי כתובת דוא"ל וסיסמה. לאחר השארת פרטים הקורבן מופנה לאתר האמיתי של WHO. הפרטים נשמרים לשימוש עתידי של העבריינים.



אימות ותקפות החשבון
המטרה: גביית כסף "לחידוש" החשבון.
השיטה: הודעה לקורבן הפוטנציאלי כי תוקף החשבון עבר ויש לחדש אותו. החידוש כרוך בתשלום קטן יחסית והחשבון יתחדש לפרק זמן נוסף.

בעיתות משבר, כשהציבור משווע למוצרים מסוימים, במיוחד אם הם במחסור (למשל: מסכות, חומרי חיטוי, חיסונים), קל יותר להניע אותו לבצע רכישה עם בטחונות מינימליים או בלא בטחונות כלל. ככל שהמחיר יהיה נמוך יותר, כך רמת הסיכון שהקונה יהיה מוכן לקחת על עצמו תהיה גבוהה יותר

הונאת המצילנו מידו
המטרה: ניצול אמון הציבור בכח נעלה.
השיטה: תתרום ונתפלל עבורך שלא יאונה לך שום רע.

הציע למכירה את "הבדיקה המהירה והיעילה ביותר לאיתור וירוס קורונה" במחיר הפנטסטי של 19 אלף רובל (בערך 300 דולר).

בינואר–מארס השנה נרכשו יותר מ־100 אלף שמות של אתרים חדשים באינטרנט המכילים הטיות שונות של המילה covid, virus או corona. ניתן להניח מכך שהעבריינות ברשת, בעיקר בסחר המקוון, תלך ותתגבר בתקופת המשבר.

בבדיקה של הפעילות התעבורתית הקשורה לאתר אירופי מוביל למסחר מקוון, המכיל הצעות למכירה של חומרי ניקוי ידיים ומסיכות פנים, עלה, כי ככל שהפחד מפני קורונה מתגבר, כך גדל החיפוש של בוטים אחרי מסיכות פנים וחומרי חיטוי. אותרו התקפות אוטומטיות שנועדו למנוע גישה למלאי, על מנת להפנות לאתרים דומים שפועלים עם תוכנות זדוניות שמטרתם להונות, או לבצע רכישות בשוק השחור.

ככל שאיום הנגיף מתעצם, הבוטים ימשיכו להיות כלי יעיל עבור פושעי הרשת. ההשפעה של מידע ברשת – אמיתי או כוזב – מתעצמת בעידן של פחד, אי ודאות ובלבול. מכיוון שערוצי התקשורת מגוונים ובלתי נשלטים, גם לא על ידי השלטונות, יכולתם של עברייני הסייבר גדלה.

החזרי מס ומענקי ביטוח לאומי. בעקבות הפרסומים על הטבות מס ומענקים ממשלה לאזרחים ולעסקים שנפגעו במשבר הקורונה, חלה עלייה בפשיעה סביב הטבות אלה. במקרה של בריטניה, השילוב של קורונה עם הברקזיט יצר פתח רחב לפעילות עבריינית בתחום פשיעת הסייבר, ובלבול בקרב הציבור כיצד לנהוג וכיצד לאתר ניסיונות של פעולות זדוניות. משרד הפנים הבריטי יצא בפרסום מקיף, המדריך כיצד להגן על אזרחים ועל עסקים מהונאה ופשיעת סייבר.[7] כך נכתב במדריך:

"הצעדים שהוכרזו במהלך השבועות האחרונים להתמודדות עם קורונה שינו דרסטית את חיי היום־יום ואנו נמצאים יותר ויותר בבתים ובתקשורת מקוונת. העבריינים ינצלו כל הזדמנות שביכולתם להונות אנשים תמימים ואת עסקיהם. העבריינים מומחים בחיקוי אנשים, ארגונים ומשטרה. הם משקיעים שעות רבות במיפוי וחקירה של הקורבנות האפשריים, בתקווה שאתם תשמטו ולו רק לרגע את אמצעי ההגנה שלכם.

"העבריינים יכולים ליצור עימכם קשר בטלפון, דוא"ל, מדיה חברתית או באופן אישי. הם ינסו לשכנע אתכם להיפרד מכספכם, ממידע אישי, או רכישת מוצרים ושירותים שאינם קיימים. גופי אכיפה, ממשלה ותעשייה פועלים ביחד על מנת להגן עליכם ועסקיכם מפני עבריינים אלה, על ידי איתור אתרים כוזבים, מניעת דוא"ל זדוני, חסימת מספרי טלפון והעמדה לדין של האחראים".

בהמשך ניתנו כללים בסיסיים להגנה:

> שקלו אם זה יכול להיות מזויף. זה בסדר לדחות, לסרב או להתעלם מבקשות שונות; רק עבריינים ינסו להאיץ בכם, או לזרוע בכם בהלה.

> המשטרה או הבנק לעולם לא יורו לכם למשוך כספכם או להעביר אותו לחשבון אחר. הם לעולם לא יבקשו מכם לגלות סיסמאות מלאות או מספר סודי.

> אל תלחצו על קישורים או צרופות בטקסטים לא צפויים או דוא"ל.

> ודאו שהבקשות אמיתיות. התקשרו למספר טלפון הידוע לכם או לכתובת דוא"ל הישירה של הארגון שפנה אליכם, לכאורה.

> אם אתם חושבים שנפלתם קורבן למעשה הונאה, דווחו מיידית לבנק ולמשטרה.

הונאת מוצרים מצילי חיים
המטרה: הוצאת כספים.
השיטה: הצגת מוצרים "מצילי חיים" (מסיכות, אלכוג'ל) לאספקה מיידית, במחירי מבצע.
למשל מסכות במחיר של $0.99 במקום $9.99 (בדוק זמינות המוצרים ומחירים באתרים אחרים.
אם זה too good to be true אזי זה כנראה לא קיים).

> ודאו שאתם משתמשים בתוכנות, אפליקציות, ומערכות הפעלה עדכניות בטל־פון, בטבלט ובמחשב. כוונו את המכשירים לעדכונים אוטומטיים על מנת לחסוך דאגה.

> אם אתם מקבלים פנייה לתשלום מיידי, להחלפת פרטי חשבון ספק, או למתן פרטים פיננסיים – עצרו וקחו זמן למחשבה. זו יכולה להיות פנייה כוזבת. ודאו את כל התשלומים ופרטי הספקים ישירות בשיחת טלפון המוכר לכם עם אדם המוכר לכם.

> בדקו אם כתובת השולח אינה זהה לכתובת המקורית. למשל: הכתובת של רשות המיסים הבריטית (HMRC) היא xxx@hmrc.gov.uk, בעוד עבריינים משתמ־שים בכתובת דומה כמו refunds@hmrc.org.uk שנועדה להטעות.

> עבריינים יכולים גם לזייף את כתובת השולח כך שתראה אמיתית.

> אם אינכם בטוחים ב־100% שהשולח אמיתי, אל תפתחו את הדוא"ל. אם פתחתם ואתה מתלבטים, אל תלחצו על הקישורים ואל תבצעו הורדה/גיבוי (download).

> גוף ממלכתי לעולם לא יודיע לכם על החזר ממס, יציע לכם תשלום, יבקש מכם לגלות מידע אישי כגון כתובת, פרטי חשבון בנק, יתן לכם כתובת דוא"ל אישית לחזור אליה, יבקש מכם מידע פיננסי כמו נתונים מספריים ספציפיים, חישובי מס, אלא אם נתתם הסכמה לכך.

> העבריינים דורשים פעולה מיידית. לכן, היזהרו מדוא"ל הכולל פניות כמו "יש לך שלושה ימים לענות" או "נדרשת פעולה מיידית".

> היזהרו מפני אתרים מזויפים שהעב־ריינים יוצרים אליהם קישורים והם נראים כמו דף הבית של אתר רשמי. גם אם הדף נראה אמיתי, אין זה אומר שהוא כזה. לעי־תים קרובות אתרים מזויפים מכילים קישו־רים לבנקים או מכילים שדות וטפסים המב־קשים למלא מידע פרטי כמו סיסמאות, פרטי כרטיס אשראי, או פרטי חשבון בנק. לעיתים העבריינים כוללים קישורים אמיתיים לדפים באתר האמיתי, על מנת לתת תדמית אמי־תית לאתר שלהם.

חלק מהתרגילים המתוארים לעיל אינם ישימים בסביבה העסקית בישראל. עם זאת, יש מקום להסתכל על ההנחיות לפעולות מניעה במשקפיים ישראליות. זאת, לאור "גיוור" פעולות ההונאה לישראל, ואף פניות ישירות מחוץ לארץ לקורבן פוטנציאלי ישראלי.

כללי הגנה נוספים

קיימים אתרי אינטרנט רבים המתריעים מפני הונאות בחסות משבר הקורונה. הנה כמה כללי "עשה ואל־תעשה" מאתרים נבח־רים ותוספות משל הח"מ.

> היזהרו מאנשים המציעים או מוכרים:

"אנו נמצאים יותר ויותר בבתים ובתקשורת מקוונת. העבריינים ינצלו כל הזדמנות שביכולתם להונות אנשים תמימים ואת עסקיהם. העבריינים מומחים בחיקוי אנשים, ארגונים ומשטרה. הם משקיעים שעות רבות במיפוי וחקירה של הקורבנות האפשריים, בתקווה שאתם תשמטו ולו רק לרגע את אמצעי ההגנה שלכם"

הונאת נטפליקס
המטרה: קבלת פרטים מוכמנים.
השיטה: כניסה לקישור הנחזה להיות של נטפליקס להשארת פרטים.

האוצר שבדרך
המטרה: קבלת פרטי חשבון וזכויות חתימה.
השיטה: יצירת קשר של שותפים למרמה וקבלת פרטי חשבון. עריכת "ניסיון" שהתקשורת עובדת וקבלת פרטים לצורך שימוש עתידי לסחיטה (הערה: שיטה משודרגת של "מכתב ניגרי").

ערכות לבדיקת קורונה שלא בידי גופים מוכרים (קופות חולים, מד"א, בתי חולים, משרד הבריאות); חיסונים למניעת קורונה, שלא על ידי גופים מוכרים; מוצרים במחיר מופקע להגנה מפני קורונה, כגון מוצרים אנטי"בקטריאליים ומוצרי חיטוי; שירותי חיטוי שאין בהם תועלת ממשית; שירותי ניקיון נגד קורונה.

› שמרו על עצמכם ועל ואחרים מפני החלטות נמהרות. אם זה נשמע טוב מלהיות אמיתי – אזי זה לא אמיתי.

› אל תפעלו תחת לחץ. רכשו רכוש מוצרים רק מקמעונאים המוכרים לכם או למקורבים לכם, וחשבו פעמיים לפני שאתם נפרדים מכספכם. אל תסיקו שכולם אמיתיים; זה תקין לדחות, לסרב או להתעלם מבקשות. אם מישהו טוען שהוא פועל מטעם גוף צדקה, בקשו אמצעי זיהוי (גם תעודת זהות). היו חשדנים כלפי תשלום מראש.

› יש להיענות לבקשות לשינוי חשבון רק לאחר אימות מול הספק פנים אל פנים או בתקשורת ישירה אחרת, ולא בדוא"ל.

› אם נפלתם קורבן, דווחו למשטרה והודיעו לבנק שלכם.

› אל תלחצו על קישורים ואל תפתחו צרופות לדוא"ל חשוד.

› אל תענו להודעות ממקורות בלתי מוכרים המבקשות פרטים אישיים או פיננסיים.

› אם אתם מבצעים רכישה מחברה או אדם שאינם מוכרים, בצעו מחקר על המוכר ובדקו מראש בקרב חברים ומכרים. ●

הערות

1. OECD/EUIPO (2020), Trade in Counterfeit Pharmaceutical Products, Illicit Trade, https://doi.org/10.1787/a7c7e054-en.

2. introduction-investing/general-/resources/news-alerts/alerts-bulletins/investor-alerts/look-out

3. למשל:

› האתר של ארגון הבריאות העולמי: https://www.who.int/about/communications/cyber-security

› האתר של רשות ההגבלים האמריקנית:

https://www.ftc.gov/news-events/press-releases/2020/03/ftc-fda-send-warning-letters-seven-companies-about-unsupported

› האתר של רשות ניירות הערך האמריקנית:
https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/look-out

› SRA – הגוף המאסדר של עורכי דין באנגליה ו־ווילס: https://www.sra.org.uk/sra/news/press/cyber-awareness-during-lockdown

› מרכז מידע משותף לגופי משטרה בבריטניה:
https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month

4. סוס טרויאני – כינוי לתוכנת מחשב מזיקה המנסה לחדור למחשב, תוך התחזות. מופיעה בדרך כלל כקובץ המצורף לדואר אלקטרוני, או כתוכנה חופשית להורדה

5. EMOTET היא תוכנה זדונית הנשלחת באמצעות הודעות דואר אלקטרוני שמטרתה איסוף נתונים פיננסים, אנשי קשר וכתובות דוא"ל, פרטי הזדהות לחשבונות שונים, היסטוריית גלישה ושימוש במחשב הקורבן לביצוע מתקפות מניעת שירות.

6. בוט (bot, קיצור של המילה רובוט) הוא תוכנה של משתמש פיקטיבי במערכת מחשב (נייח או נייד, כולל טלפון חכם). היא מאפשרת לבצע פעולות אוטומטיות של איסוף מידע, הפצתו וביצוע פעולות מוגדרות, בדרך של חיקוי משתמש. בבוט נעשה שימוש זדוני במספר וירוסי מחשב שמריצים בוט מתוך המחשב אליו הם פורצים.

7. https://www.gov.uk/government/publications/coronavirus-covid-19-fraud-and-cyber-crime/coronavirus-covid-19-advice-on-how-to-protect-yourself-and-your-business-from-fraud-and-cyber-crime

וגם: https://takefive-stopfraud.org.uk

גם אם הדרך נראה אמיתי, אין זה אומר שהוא כזה. לעיתים קרובות אתרים מזויפים מכילים קישורים לבנקים או מכילים שדות וטפסים המבקשים למלא מידע פרטי כמו סיסמאות, פרטי כרטיס אשראי, או פרטי חשבון בנק. לעיתים העבריינים כוללים קישורים אמיתיים לדפים באתר האמיתי, על מנת לתת תדמית אמיתית לאתר שלהם

איטליה - שיאנית ההונאות במשבר הקורונה

באיטליה, אחת המדינות שנפגעה בצורה הקשה ביותר ממגפת הקורונה, ניתן לראות ריכוז של טכניקות הונאה.

תחת מעטה מצב החירום הלאומי, גורמים עבריינים פנו לאזרחים בבקשה להכניס נתונים אישיים לאתרים כוזבים של מוסדות בנקאיים. זאת, למרות שהבנקים באיטליה אינם שולחים דוא"ל, מסרונים או פניות טלפוניות על מנת לברר סיסמאות גישה או לקבלת אימות למידע אישי.

העבריינים שולחים מסרונים משירותי לקוחות של מוסדות בנקאיים, לכאורה, המזמינים את הקורבן הפוטנציאלי לשנות את סיסמת ההתחברות שלו. הלקוח מתבקש להקיש את הסיסמא שלו כדי להיכנס לאתר הנחזה להיות אתר הבנק. האתר המזויף מתקיים למספר שעות בהן הוא קולט את הסיסמאות, ואז נעלם עד להופעתו בשרת אחר בחיפוש אחר קורבנות נוספים.

הונאות נוספות מתבצעות סביב גיוס כספים. לאור מצוקת בתי החולים בתקופת המשבר, התארגנו רשויות מקומיות לגייס תרומות לטובת יחידות לטיפול נמרץ בבתי חולים מקומיים. עבריינים עשו שיבוט לאתרי גיוס הכספים, שעוצבו בכישרון רב כמו אתרי המקור. האתרים המשובטים יירטו כספים שגויסו מתורמים נדיבים. מעשי תרמית אלו נחשפו לאחר שהכספים לא הגיעו לתעודתם. בעקבות כך, הונחו התורמים לפנות לבית החולים ולוודא מראש את נתיב גיוס הכספים המדויק.

האיטלקים חוו גם הצפה של אתרי פישינג, המציעים "מבצעים של ביטוחים רפואיים עדכניים" לכיסוי הקורונה. באמצעות אתרים אלו הצליחו עברייני רשת להשיג פרטים אישיים מוכמנים לשם גניבת זהויות וכספים. דוא"ל נשלח לקורבן ובו הצעה להוסיף לפוליסת הביטוח שלו כיסוי חדשני לנזקי הקורונה. הקלדה על מעין כפתור כניסה מעבירה את הקורבן לטופס "עדכון תשלום", והקורבן מקליד נתונים מוכמנים לאתר הפישינג. בחלק מן המקרים נשלחה בתגובה פנייה כוזבת של "מנכ"ל חברת הביטוח", בה הוא משבח את הקורבנות על בחירתם ומודה להם על האמון.

היצירתיות של העבריינים באיטליה נמשכת לתלושים מזויפים למרכולים ולזכיות כוזבות בתחרויות פרסים. העבריינים מנצלים את החולשות והקשיים של אזרחים רבים ומזמינים אותם להיכנס לאתרים כוזבים ולהשאיר פרטים או לשלם, על מנת להבטיח לכאורה תלושי שי, קופונים להנחות או פרסים.

הוקמו גם אתרים כוזבים העוסקים במכירה מקוונת בשם רשתות פיקטיביות. באתרים "מוכרים" תרופות קסמים, ערכות למניעת וירוסים, ציוד מגן כמו מסיכות וכפפות, במחירים מוזלים – מוצרים שלא קיימים ולא יסופקו לעולם.