משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות לאיסור הלבנת הון ומימון טרור
ISRAEL MONEY LAUNDERING AND TERROR FINANCING PROHIBITION AUTHORITY
سلطة حظر تبييض الأموال وتمويل الإرهاب

מדריך בנושא
הונאות הנדסה חברתית

המדריך נערך ע"י קבוצת ה-Egmont

בה חברה הרשות לאיסור הלבנת הון ומימון טרור

פברואר 2020

מטרת מדריך זה היא להציג בפני רשויות האכיפה וגופים מדווחים מהסקטור הפרטי את השיטות העיקריות וסיכוני הלבנת ההון הקשורים בהונאות הנדסה חברתית (Business Email Compromise / CEO Fraud Schemes). המידע במדריך זה אמור לסייע לרשויות ולגופים המדווחים בזיהוי, דיווח וחקירה של רשתות הונאה מסוג זה וכן בסיכול רשתות פיננסיות עבריינית אלו.

הקדמה

הונאות הנדסה חברתית הן בין איומי פשיעת הסייבר הגדלים במהירות הגבוהה ביותר, הפוגעים במוסדות פיננסיים וחושפים את הסקטור הפיננסי העולמי להפסדים של מיליארדי דולרים. למשל, אחת המדינות זיהתה הפסדים פוטנציאלים של מעל ל-12 מיליארד דולר הנובעים ממעל 78,000 מקרים של הנדסה חברתית המדווחים, במשך תקופה של חמש שנים, בהם היו מעורבים קרבנות מאותה מדינה ומרחבי העולם[1]. מזימות אלו מופנות כלפי עסקים, בעלי מקצוע ואנשים פרטיים ומשתמשות בחשבונות דואר אלקטרוני עסקיים או פרטיים כדי לשלוח (או לגרום לכך שיישלחו) הוראות תשלום כוזבות וכן מידע נוסף בו נעשה שימוש לביצוע הונאה פיננסית.

> **הונאת הנדסה חברתית** כוללת מזימות בהן עבריינים משתלטים על כתובת הדואר האלקטרוני של הקרבנות בכדי: (1) לשלוח הוראות תשלום מזויפות למוסדות פיננסיים או לאנשי קשר עסקיים כדי לגנוב כספים; או (2) לגרום בהונאה לכך שיועבר מידע אשר ישמש לביצוע

מוסדות פיננסיים הינם בעלי יכולת לקחת תפקיד חשוב בזיהוי, מניעה ודיווח על הונאות הנדסה חברתית, וזאת באמצעות עידוד התקשורת ושיתוף הפעולה בין היחידות העסקיות שלהם לבין היחידות הפנימיות למניעת הלבנת הון, למניעת הונאה ולביטחון סייבר.

כיצד פועלות הונאות הנדסה חברתית

הונאות הנדסה חברתית בדרך כלל כוללות התחזות לקרבנות כדי לשלוח למוסדות פיננסיים הוראות לביצוע עסקאות הנחזות כלגיטימיות. למרות שהונאות הנדסה חברתית נבדלות במאפיינים שונים, כולן מתמקדות בשימוש בחשבונות דואר אלקטרוני שנפרצו כדי לגרום למוסדות פיננסיים או ללקוחותיהם לבצע תשלומים ללא הרשאה או כאלו שביצועם הושג במרמה, או לשלוח מידע רגיש לצדדים שלישיים לא מורשים. לאחר מכן, צדדים שלישיים אלו משתמשים במידע כדי לבצע הונאה פיננסית. ניתן לחלק הונאות הנדסה חברתית לשלושה שלבים:

[1] עיין Federal Bureau of Investigation (FBI) Public Service Announcement, *Business Email Compromise: The 12 Billion Dollar Scam*, July 12, 2018, available at https://www.ic3.gov/media/2018/180712.aspx

שלב 1 – פריצה למידע ולחשבון הדוא"ל של הקרבן: ראשית עבריינים פורצים לחשבון הדוא"ל של הקרבן, בדרך כלל תוך שימוש בהנדסה חברתית[2] או תוכנות בפריצה למחשבים. לאחר מכן, העבריינים מנצלים את החשבון שנפרץ כדי להשיג מידע על המוסדות הפיננסיים, פרטי החשבון ואנשי הקשר של הקרבן.

שלב 2 – העברה בתרמית של הוראות לביצוע עסקאות: בהמשך, העבריינים משתמשים במידע שנגנב מהקרבן כדי לשלוח בתרמית למוסדות פיננסיים הודעות דוא"ל הכוללות הוראות לביצוע תשלומים או להעברת מידע, כך שהן נחזות להיות מהקרבן. למטרה זו, העבריינים ישתמשו בחשבון הדוא"ל של הקרבן, אשר עליו הם השתלטו, או יפתחו חשבון מזויף הדומה לחשבון הקרבן. כדי לתמוך בהוראותיהם ולחזק את מהימנותם, העבריינים לפעמים מספקים מסמכים תומכים, אשר זויפו למטרה זו.

שלב 3 – ביצוע עסקאות לא מורשות: עבריינים מרמים את העובד או את המוסד הפיננסי של הקרבן כדי לבצע העברה כספית הנחזית כלגיטימית אך היא למעשה בוצעה ללא הרשאה או שיסודה בתרמית. ההוראות מורות על העברת תשלומים לחשבונות של העבריינים במוסדות פיננסיים מקומיים או זרים. מוסדות פיננסיים במזרח ודרום-מזרח אסיה, בנוסף למדינות במערב ובמזרח אירופה, הם יעדים שכיחים לעסקאות תרמית אלו. אולם יש לציין כי עבריינים מסוגלים לשנות את תכניותיהם כך שמדינות היעד עשויות להשתנות במהירות.

תרחישים לביצוע הונאות הנדסה חברתית

הונאות הנדסה חברתית בדרך כלל מתמקדות במוסדות פיננסיים או בלקוחותיהם, כולל עסקים ואנשים פרטיים, אשר מבצעים עסקאות גדולות באמצעות מוסדות פיננסיים, נותני אשראי, חברות נדל"ן ומשרדי עורכי דין. לצורך המחשה, פעמים רבות מבוצעות הונאות ההנדסה החברתית באופנים הבאים:

תרחיש 1 – עבריין מתחזה ללקוח עסקי של מוסד פיננסי: עבריין פורץ ומשתמש בחשבון דוא"ל של עובד של חברה א' כדי לשלוח למוסד פיננסי של חברה א' הוראות לביצוע העברה בנקאית.[3] בהתבסס על בקשה זו, חברה א' מבצעת העברה בנקאית ושולחת כספים לחשבון שבשליטת העבריין.

בתרחיש זה, העבריין המתחזה ללקוח של המוסד הפיננסי גורם למוסד הפיננסי לבצע העברה בנקאית בלתי מורשית.

תרחיש 2 – עבריין מתחזה למנהל בכיר ("הונאת מנכ"ל"): עבריין פורץ ומשתמש בחשבון דוא"ל של מנהל בכיר בחברה ב' כדי לשלוח לעובד של חברה ב' שאחראי על עיבוד והנפקת תשלומים הוראות לביצוע העברה כספית. העובד, המאמין שהוראות המנהל הן לגיטימיות, מורה למוסד הפיננסי של חברה ב' לבצע את ההעברה.

[2] הנדסה חברתית מתייחסת לטקטיקות של אינטראקציה אנושית הנועדות להונות אנשים כדי לגלות מידע.
[3] בכל התרחישים האלו, במקום לפרוץ לחשבון, העבריין יכול גם לפתוח חשבון המחקה בצורה מאוד קרובה את כתובת הדוא"ל של הגורם המבקש.

בתרחיש זה, העבריין המתחזה למנהל בכיר בחברה מטעה עובד כדי שיאשר העברת כספים לחשבון בשליטת העבריין. גרסאות שונות של תרחיש זה עלולות לכלול עבריין המתחזה למנהל בכיר בחברה כדי להטעות עובד על מנת שישלח לו מידע רגיש על שכר או עסקאות אשר בו יוכל העבריין לעשות שימוש בהונאה פיננסית עתידית.

תרחיש 3 – עבריין מתחזה לספק: עבריין מתחזה לספק של חברה ג' או לנותן שירותים מקצועיים (כמו מתווך נדל"ן, חברת נאמנות או עורך דין) כדי לשלוח מייל ולהודיע לחברה ג' שעליה לשלוח תשלומים עתידיים למספר חשבון חדש. בהתבסס על מידע שקרי זה, חברה ג' מעדכנת את המידע שיש לה לגבי אופן התשלום לספק זה ומעבירה למוסד הפיננסי הוראות חדשות לביצוע תשלומים, כך שהכספים מועברים לחשבון בשליטת העבריין.

בתרחיש זה, העבריין מתחזה לספק או לנותן שירות ושולח הוראות שקריות לגבי אופן התשלום על-מנת להטעות את עובד החברה כך שיעביר כספים לחשבון שבשליטת העבריין.

תרחיש 4 – העבריין מתמקד בשירותי נדל"ן: עבריין פורץ לחשבון דוא"ל אמיתי של מתווך נדל"ן או של אדם הרוכש או מוכר נדל"ן, כדי לשנות הוראות תשלום ולהפנות אליו את כספי העסקה הנדל"נית. לחלופין, עבריין פורץ ומשתמש בכתובת הדוא"ל של מתווך הנדל"ן כדי ליצור קשר עם חברת נאמנות ומורה לה להעביר עמלות שהסוכן מרוויח מהעסקה לחשבון בשליטת העבריין.

בתרחיש זה, העבריין מתחזה לסוכן נדל"ן או לשחקן מרכזי אחר בעסקת נדל"ן ומספק לצד הנגדי הנחיות שקריות בנוגע לאופן ביצוע תשלומי מקדמות ותשלומים אחרים כך שהם יועברו לחשבון בשליטת העבריין.

תבחינים לזיהוי הונאת הנדסה חברתית ("דגלים אדומים"):

הצלחה בזיהוי ועצירת מזימות הנדסה חברתית מחייבת בדיקה זהירה ואימות של הוראות הלקוח לביצוע עסקאות תוך לקיחה בחשבון של הנסיבות הקשורות להוראות אלו. מכיוון שסממנים מסוימים המזוהים עם הונאת הנדסה חברתית יכולים לשקף פעילות פיננסית לגיטימית, יש להזכיר ***כי אין שום סממן יחיד שמורה בהכרח על פעילות חשודה***. על מוסדות פיננסיים לבחון סממנים נוספים ואת עובדות ונסיבות המקרה, כמו ההיסטוריה של הפעילות הפיננסית של הלקוח והאם הלקוח מראה מספר סממנים, לפני הקביעה כי עסקה היא חשודה. על מוסדות פיננסיים לעשות בדיקות וחקירות נוספות במידת הצורך.

הסממנים הבאים יכולים להעיד על הונאות הנדסה חברתית:

סממני חשבון הקרבן

דפוסים כלליים של עסקאות חשודות

- הלקוח שולח הוראות אשר מורות לשלם למוטב ידוע, אך פרטי חשבון המוטב שונים מהעבר.
- הלקוח שולח הוראות אשר מורות לשלם למוטב עמו אין ללקוח שום היסטוריה של תשלומים או קשר עסקי מתועד, והתשלום בסכום דומה או גבוה מתשלומים שנשלחו בעבר על ידי הלקוח למוטבים.

- הלקוח שולח בקשה לביצוע תשלומים נוספים מיד לאחד תשלום מוצלח לחשבון שאליו לא שלח הלקוח לפני כן תשלום לספקים. התנהגות זו יכולה להעיד על ניסיון עברייני לבצע תשלומים לא מורשים נוספים לאחר שהצליח ניסיון ראשון להשיג תשלום במרמה.
- הלקוח שולח הוראות אשר מסווגות את העסקה כ"דחוף", "סודי" או "חסוי".
- הלקוח שולח הוראות בצורה שמשאירה למוסד הפיננסי זמן ואפשרות מוגבלים לוודא את אוטנטיות הבקשה.
- הלקוח שולח הוראות להעביר תשלומים למוסד פיננסי זר אשר מתועד בתלונות לקוחות כיעד חשוד לעסקאות כוזבות.
- הוראות הלקוח הנחזות כלגיטימיות כוללות שפה, עיתוי וסכומים שונים מבקשות מאושרות ואוטנטיות קודמות.
- מקור ההוראות בכתובת דוא"ל דומה לכתובת הדוא"ל הידועה של הלקוח, אך הכתובת שונה במקצת על ידי הוספת, החלפת או מחיקת אותיות; למשל:
  כתובת דוא"ל לגיטימית: john-doe@abc.com
  כתובת דוא"ל מזויפת: john-doe@bcd.com , john_doe@abc.com
- מוסד פיננסי מקבל הוראות מעובד של הלקוח, אשר רק לאחרונה אושר כמורשה חתימה בחשבון, או אשר היה מורשה חתימה אך לא שלח הוראות תשלום בעבר.
- עובדו או נציגו של הלקוח שולח הוראות למוסד פיננסי בשם הלקוח אשר מבוססות באופן בלעדי על תכתובת דוא"ל עם מנהלים בכירים, פרקליטים או מיופי כוחם, אולם עובדו או נציגו של הלקוח אומר כי לא הצליח לאמת את העסקאות עם אותם מנהלים בכירים, פרקליטים או מיופי כוח.

מדינות בסיכון גבוה להונאות הנדסה חברתית

- חשבון הנהנה שייך לחברת חוץ או מוחזק אצל מוסד פיננסי הנמצא במדינה בסיכון גבוה, כפי שנקבע על ידי המוסד הפיננסי והרשויות המוסמכות במדינה בה נמצאת המוסד הפיננסי.

שימוש במסמכים וחשבוניות מזויפים

- עבריינים שולחים מסמכים או חשבוניות מזויפים לעובדי הקרבן כדי לאמת את העסקה. מסמכים וחשבוניות מזויפים יכולים להיות באיכות גבוהה ואף יכולים לכלול מסמכים אמתיים אשר שונו כדי לגרום להעברת כספים לחשבון העבריין.

סממנים הקשורים לחשבון של עבריינים החשודים בהנדסה חברתית

דפוסים כלליים של עסקאות חשודות

- לאחר מתקפה על חשבון או חברה, כספים נמשכים מהמוסד הפיננסי, מועברים מהמוסד הפיננסי או מועברים לחשבונות מרובים בתוך המוסד הפיננסי.
- המוסד הפיננסי מקבל העברה בנקאית לזיכוי חשבון אבל בהעברה מצוין מוטב אשר אינו הבעלים של אותו חשבון. במקרה מסוג זה קרבן שולח העברה בנקאית לחשבון חדש, שאת פרטיו קיבל מעבריין המתחזה לספק ידוע, בעודו חושב כי החשבון שייך לאותו ספק, כפי שהוסבר למעלה

בתרחיש 3. את סממן זה יכולים לזהות מוסדות פיננסיים המקבלים ממוסדות פיננסיים אחרים העברות בנקאיות הנובעות מהונאת הנדסת חברתית.

סכום ההעברה

- סכום ההעברה שהתקבל בחשבון המוטב אינו תואם את אפיון הלקוח.

שימוש בבלדרים

- עליה פתאומית בהיקף העסקאות והיתרות של לקוח העוסק בתיווך יכולה להעיד על השתתפותו כבלדר בהונאות הנדסה חברתית. בלדרים[4] משמשים כמתווכים עבור עבריינים וארגוני פשיעה. במקרים מסוימים, הקרבנות אינם מודעים כי הם משמשים לביצוע העברת מרמה לעברייני סייבר. עבריינים בדרך כלל משתמשים בבלדרים כדי לבצע הונאות הקשורות להנדסה חברתית. לבלדרים יש בדרך כלל יתרות נמוכות ופעילות פיננסית מוגבלת טרם שנעשו מעורבים בהונאה.

הפחתת סיכונים

תהליך אימות רב-שלבי יכול לעזור למוסדות פיננסיים במניעת הונאות הנדסה חברתית. למשל, מוסדות פיננסיים יכולים לאמת את האוטנטיות של הוראות תשלום חשודות עד ידי תקשורת עם הלקוח דרך אמצעים שונים (דוג' טלפון, חשבון דוא"ל חלופי), או על ידי פנייה לאחרים בחברת הלקוח אשר מורשים לבצע עסקאות. ההצלחה של הונאות הנדסה חברתית תלויה באפשרות של עבריינים לבצע עסקאות שנחזות כלגיטימיות אך אינן מורשות. עסקאות אלו הן בדרך כלל בלתי הדירות ולכן מוסדות פיננסיים אינם יכולים לבטל או להחזיר את הכספים. לכן, זיהוי הוראות תשלום שקריות לפני העברת התשלום הכרחי למניעת ולהפחתת עסקאות לא מורשות.

תגובה לתקריות הנדסה חברתית והשבת כספים

תגובה מהירה מצד הקרבנות, המוסדות הפיננסיים וגורמי האכיפה היא קריטית להשבה מוצלחת של כספי הקרבן. שיעור החזרת הכספים יורד בצורה ניכרת לאחר 24 השעות הראשונות.

כדי לעזור בחקירת מקרי הונאה חברתית ובהשבת כספי הקרבן, מומלץ למוסדות פיננסיים לבצע פעולות אלו[5]:

1. <u>פנייה מידית לגורמי אכיפה ולרשויות הרלוונטיות</u>

א. <u>*דיווח מידי על העבירה*</u> – יש חשיבות עליונה לכך שהקרבן, המוסד הפיננסי, גורמי האכיפה, רגולטורים והרשויות למודיעין פיננסי במדינות המעורבות יפעלו במהירות כדי להשיב את הכספים שהועברו. כדי לעשות זאת, הקרבן או המוסד הפיננסי של הקרבן חייבים לדווח על הפשע באופן מידי ולבקש סיוע מרשויות האכיפה ומהרשות למודיעין פיננסי[6].

[4] זהותם של בלדרים משמשת כדי לפתוח חשבונות במוסדות פיננסיים, להשיג כרטיסי בנק עם קוד, ולהשיג גישה לשירותי תשלום מקוונים. הבלדרים מעבירים מידע זה או את הגישה לשירותים המקוונים לחברים אחרים בארגוני פשיעה לשם שימוש עברייני. בלדרים בדרך כלל אינם מכירים את התמונה המלאה של הפשע בו הם לוקחים חלק, ומקבלים רק סכום זעום בגין "שירותיהם".

[5] סדר הפעולות אינן בהכרח ברצף כרונולוגי, משום שרבות מהפעולות יכולות להתבצע במקביל או בסמיכות. כאמור לעיל, תגובה מהירה ושיתוף פעולה עם הגורמים הרלוונטיים, כולל גורמי אכיפה ורשויות למודיעין פיננסי, הם מפתח להשבת כספים שאבדו עקב מזימות הונאה חברתית.

[6] סמכויות ופעולות גורמי האכיפה, הרשויות למודיעין פיננסי ורשויות מוסמכות אחרות משתנות בהתאם למדינה. אמנם חלק זה מדגיש את חשיבות נקיטת הפעולה כדי להתריע בפני גורמי אכיפה ורשויות למודיעין פיננסי במקרים של הנדסה

ב. *<u>הודעה למוסד הפיננסי המוטב</u>* – על המוסד הפיננסי המחזיק בחשבון הקרבן להודיע מיד למוסד הפיננסי המוטב על החשד להונאה.

ג. *<u>סימון העברות נכנסות חשודות</u>* – המוסד הפיננסי של העבריין או המוטב הראשוני של הכספים שמקורם בתרמית עלול לחשוד בהונאה אם יש ספק לגבי המקור החוקי של הכספים הנכנסים. במקרה כזה, על המוסד הפיננסי לפנות מיד לגורם הרגולטורי המוסמך, לגורמי האכיפה ולרשות למודיעין פיננסי כדי להתריע בפניהם על עסקה חשודה.

על הגורם המדווח לשלוח לרשות למודיעין פיננסי דיווח על פעילות בלתי רגילה/חשודה. אם ההעברה נעשתה בתוך 72 השעות האחרונות, על המדווח להדגיש את דחיפות המקרה.

2. <u>עצירת תנועת הכספים</u>

הימנעות מביצוע עסקאות חשודות – חובה על המוסד הפיננסי המוטב אשר יש לו מידע (דוג' הודעת SWIFT על ביטול העברה) כי נעשתה בחשבון אחד מלקוחותיו העברה במרמה, לנמנע מביצוע העברת המשך שעלולה לגרום לאבדן הכספים. כדי להעריך את תוקף ההעברה הנכנסת, על המוסד הפיננסי המוטב לפנות לגורמי האכיפה ולרשות למודיעין פיננסי.

3. <u>תפיסה והשבה של הנכסים</u>

א. *<u>הודעה לרשויות הרלוונטיות על מקום הימצאות הנכסים</u>* – כדי להגדיל את סיכויי השבת הנכסים, על מוסדות פיננסיים לשתף פעולה עם גורמי האכיפה ועם הרשות למודיעין פיננסי, ולשתף כל מידע מבוקש. על מוסדות פיננסיים להודיע לרשות למודיעין פיננסי ולגורמי האכיפה לפני ביצוע כל העברה, אם הכספים עדיין נמצאים בחשבון. בנוסף, עליהם לשתף מידע על היעד הבא של הכספים אשר הועברו מהחשבון.

ב. *<u>צווי הקפאה</u>* – על מוסדות פיננסיים לשתף פעולה עם הרשות למודיעין פיננסי או עם גורמי האכיפה במקרה של צווי הקפאה שהוצאו על-ידי הרשויות המוסמכות.

דיווח על העברות חשודות

מוסדות המדווחים על חשד להונאות הנדסה חברתית באמצעות דיווחי פעילות בלתי רגילה מתבקשים לכלול את כל המידע הרלוונטי בפירוט מרבי, ובמיוחד את הפרטים הבאים:

<u>פרטי ההעברה הבנקאית</u>:

- התאריכים והסכומים של ההעברות החשודות;
- פרטי זיהוי של המעביר, מספר חשבון ומוסד פיננסי;
- פרטי זיהוי של המוטב, מספר חשבון ומוסד פיננסי; וכן
- פרטי המוסדות הפיננסיים הקורספונדנטים והמתווכים, אם רלוונטי.

חברתית, אך על קרבנות ומוסדות פיננסיים לשקול את הסמכויות הרלוונטיות בהתאם לדין המקומי כדי לקבוע מיהו הגורם המוסמך אליו יש לפנות.

פרטי ההונאה:

- סממני סייבר, כמו כתובת הדוא"ל הרלוונטית, כותרות טכניות (headers) של הודעות דוא"ל, כתובות IP עם ציוני המועד (timestamps); וכן
- תיאור ועיתוי של תכתובת חשודה.