מניעת הונאה

עורך: דוד מסיקה מנהל תחום מניעת הונאה

לפני שנתחיל


0 34096630
עאמר
אמגד
פלאח
רנה
סעיד
21.05.1996 כ"ב במאיו התשנ"ד
ישראל
זכר
הזרחות ישראלית
כפר קאסם
10.03.2015 י"ג באדאר התשע"ד
10.03.2025 באדאר התשפ"ד

מטרות ההדרכה

- איתור וזיהוי לקוחות מתחזים
- מתן מידע לאחר זיהוי מתאים
- הצפה של מקרים חריגים
- אופן טיפול בעת חשד למתחזה

מה מתחזים יכולים לחפש בחברת תקשורת?

- ❑ איתור פרטים של כרטיסי אשראי לצורך שימוש לרעה
- ❑ איתור מידע על לקוחות (כתובת, מייל, טלפון, שם פרטי ושם משפחה)
- ❑ גניבת מספרים יפים (פלטינום, זהב, כסף) לדוגמא: 051-5555555
- ❑ פתיחה לשימוש לחול וגניבת סים
- ❑ פרטי משתמש נוספים

איך נשמעות שיחות מעוררות חשד:

- ❑ זירוז לפעולה מהירה
- ❑ לא מתעניין במחירים
- ❑ מגמגם
- ❑ קול עולה ויורד
- ❑ כאשר מוסר את פרטי תעודת הזהות נשמע שמקריא
- ❑ מתבלבל במסירת נתונים
- ❑ התעקשות יתר לרכישה

הנחיות למניעת הדלפת מידע

המטרה: להקשות על המתחזה לקבל פרטים

פעולות שננקוט:

1. אימות פרטים / אימות מחמיר – חובה על הלקוח לומר את פרטי ת.ז + אמצעי תשלום + שם החשבון המלא והמדויק!!!!
2. לשאול עם מי מדברים – בלקוחות עסקיים לוודא שמדובר באיש קשר
3. לשים לב לדברים או מלל שאומר "הלקוח" והאם מתאים למציאות – לדוגמא: כדי לתת לך ת.ז אני צריך ללכת למשרד..
4. אין לתת או לכוון את הלקוח למציאת הפרטים, עליו להשיגם בעצמו
5. ביצוע זיהוי ובירור שמו המלא של הלקוח בתחילת השיחה
6. לקוח שלא זוכר פרט מזהה, לציין כי לא ניתן לתת פרטים ללא זיהוי
7. במידה ובמהלך השיחה ממשיך לטעון שאינו זוכר – יש לציין כי לצערנו לא ניתן לבצע את הפעולה וכי הינו מוזמן להיכנס לאזור האישי באתר.
8. גם במידה ומסר מידע חלקי נכון, אין להתקדם לביצוע פעולות ללא זיהוי מלא של ת.ז + 4 ספרות + שם מלא של החשבון

יש לזכור

אנחנו מובילים את השיחה ולא הלקוח!

- במידה ולקוח מעוניין במספר ספציפי יש לבדוק זמינותו – יש לשים לב אם הלקוח מנחה אתכם לחיפוש ומראה היכרות עם המערכות
- במקרה של חשד, יש לציין בפני הלקוח כי אנו ננתק את השיחה ונתקשר למספרו (של איש הקשר)
- במקרה של צורך באישור של בעל החשבון, או לביצוע העברת בעלות – חובה שהנציג יעלה את הגורם השלישי ולא הלקוח שהתקשר + לזהות מחמיר ולעשות ביניהם וועידה.
- בכל פנייה בה נדרש לשוחח עם צד ג' יש להוציא שיחה ללקוח מקו נוסף (לא בוועידה) לצורך זיהוי ולאחר מכן לחבר לוועידה לצורך אישור הפעולה.
- הסרת "נעילת ניוד" לא מאופשרת על מספרים מסוג פלטינום או זהב ובמקרים חריגים יש להתייעץ עם גורם מוסמך להסרת החסימה.
- גניבת מספר על ידי פעולה של "ריפלייס סים" – לקוח מתקשר עם סים חדש ומחליף – במקרה זה חובה לזהות מחמיר + אימות התקשרות למנהל החשבון

כלל הנציגים והמנהלים חייבים להיות ערניים לבקשות מוזרות / מפתיעות מצד הלקוחות לטובת מניעת הונאות בעתיד ולהציפן בזמן אמת

במה מדובר?

מרכזיותן של מערכות המחשוב בעולם המודרני, הופכת אותן למטרה לניצול לרעה, כולל הונאות שונות כמו שימוש בכרטיסי אשראי גנובים, התחזות וכוונות זדון בשימוש של הקווים. מסוכן במיוחד האיום הפנים ארגוני של מעילות עובדים, מהיותם בעלי גישה למידע רב ונהנים מאמון המערכת. במקביל, התרחבות עולם המחשוב לכיוונים חדשים, מציגה בפני הפושעים מגוון הזדמנויות חדשות.

לדוגמא:
עסקאות אשראי, שבשנים האחרונות מתבצעות יותר ויותר מרחוק, ללא הצגת כרטיס אשראי. התוקפים מנצלים זאת וארגונים רבים ניזוקים. כאשר הונאה פעילה היא מסבה לחברה נזק כספי מתמשך.

מחלקת מניעת הונאה בחברה פועלת רבות על מנת לזהות את כל סוגי ההונאות האפשריות.

גניבת פרטי אשראי
סרטון לדוגמא

https://youtu.be/2z2kOpOm8qI

כיצד מחלקת מניעת הונאה יכולה לסייע?

מחלקת מניעת הונאה מעורבת בניטור שוטף, בלימת נזקי הונאות, התראות, ניהול סיכונים, איסוף מידע וניתוח. למעשה, מנהל מערכות המידע מעורב בכך בעקיפין, מאחר שהיבטים רבים של אבטחת מערכות המחשוב, מסייעים גם לטיפול בהונאות.


0 5745552 9
רחמים
יאיר
יעקב
אביבה
יוסף
24.08.1985 ז' באלול התשנ"ג
ישראל
זכר
אזרחות ישראלית
חדרה 24.07.2017 א' באב התשע"ז
24.07.2027 י"ט תמוז התשפ"ז
מדינת ישראל
משרד הפנים
ספח לתעודת זהות
0 5745552 9
רחמים


0 6559666 0
סמואל
אורן
יעקב
אביבה
יוסף
24.08.1985 ז' באלול התשנ"ג
ישראל
זכר
אזרחות ישראלית
חדרה 24.07.2017 א' באב התשע"ז
24.07.2027 י"ט תמוז התשפ"ז
מדינת ישראל
משרד הפנים
ספח לתעודת זהות
0 6559666 0
סמואל
אורן
הרצל
158
19
חדרה

איך נגן על הלקוחות מפני הונאות?

לעתים, הונאות פוגעות גם בלקוחות החברה. למשל, במקרה של נוכל שפונה אליכם, תוך התחזות ללקוח אחר עם פרטי זהות גנובים של לקוח קיים.
מודעות, יכולת תגובה מהירה, ותיעוד פרטים מדויקים, עשויים לצמצם נזקים של מקרים כאלה, ללקוח ולחברה ומונעים גם נזקי תדמית.

מהי מעילה ?

מעילה זהו סוג נוסף של הונאה, שכולל היבט של הפרת אמון מיוחד שניתן לעובד שמתבטא פעמים רבות בהרשאות גישה למערכות מחשוב רגישות.

גישה נרחבת של עובדים למידע ארגוני רגיש כמטרה להונאות, הופכות את מקום העבודה שלנו מ"מועדון סגור" ל"מועדון פתוח".

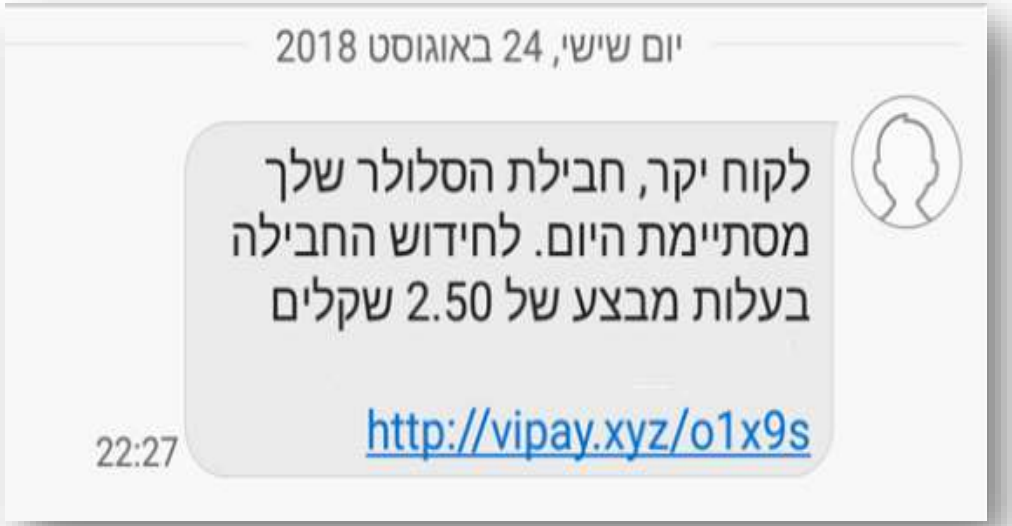
הונאות באמצעות מערכות החברה, עשויות להתבטא בין השאר במשלוח מייל מטעה, הקמת לקוחות פיקטיביים, הונאות פיננסיות לסוגיהן, גניבת זהות, שיבוש מידע במערכות הארגון, Fake news והונאות ברשתות החברתיות.

הודעות הצטרפות / חידוש חבילה

באמצעות הודעות שנשלחות על ידי נוכלים, מנסים לשכנע את הלקוחות שחבילת הגלישה שלהם נגמרה ועליהם להזין פרטי אשראי כדי לשנותה

- לקוחות חברות הסלולר לעיתים מקבלים הודעות SMS בפורמט דומה לשל ספקית הסלולר, שלפיהן חבילת הגלישה שלהם עומדת להיגמר - ועליהם להקליק על לינק, בו התבקשו להזין פרטי אשראי כדי להרחיב את החבילה מחדש. מאחורי ההודעות עומדת מערכת אוטומטית להפצת, SMS אותה מפעילים פושעי "סייבר" שמנסים לקבל את פרטי האשראי.
- הודעות אלה נשלחות כמעט בכל יום, אך לרוב זוכות להתעלמות; ואולם, במקרים מסוימים עצם הלחיצה על הלינק מסכנת את המכשיר ובמקרים אחרים, עלול הלקוח ליפול קורבן לריגול או לנזקים אחרים.
- גניבת זהות ברשת הינה פרקטיקה ותיקה, נפוצה ומוכרת. הנוכלים מתחזים למקורות לגיטימיים, אך מנסים לגרום לכם להקליק על לינקים "נגועים" - לינקים שבמקרים רבים, אין סיבה שהמקור הלגיטימי ישלח.

כשלקוח מתקשר להתלונן בנושא



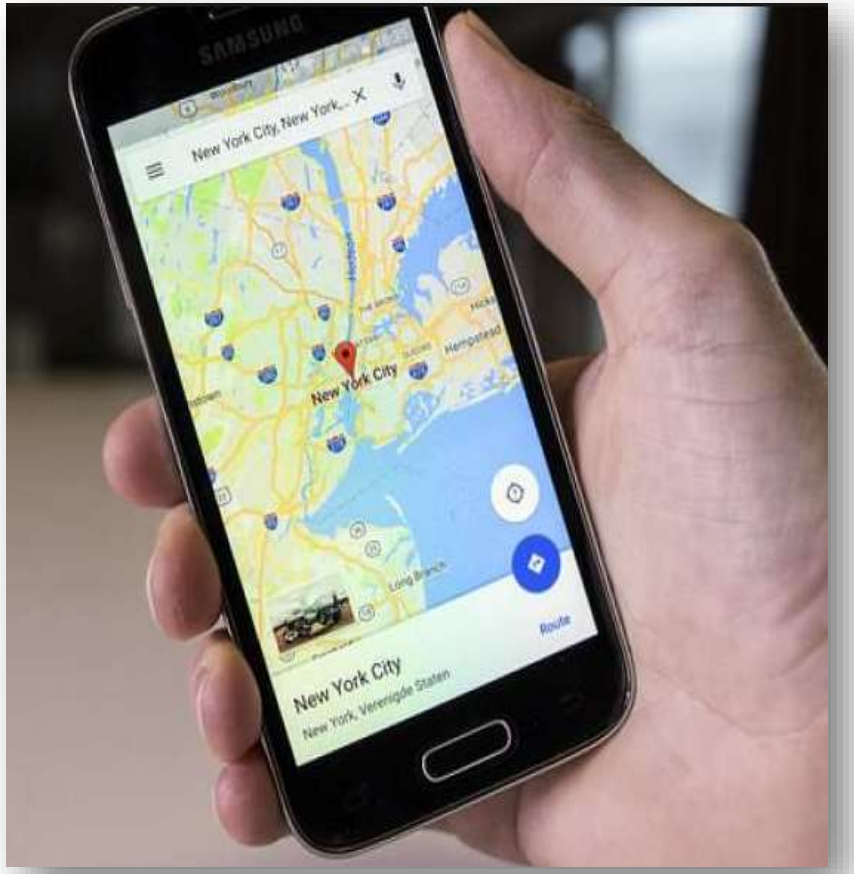
כך נאמר ללקוח:

נציגי המכירות שלנו היו פונים אליכם על מנת לנסות לשכנע אתכם להצטרף או לשנות חבילה. בנוסף, במקרים בהם נשלחות הודעות ב-SMS מהחברה עצמה, תתבקשו להזין סיסמא שנשלחת אליכם לכתובת המייל או לנייד ולא את פרטי האשראי המלאים.

ככל הנראה מדובר בנוכלים שמנסים לפרוץ לטלפונים שלכם. לחברתנו יש את פרטי האשראי שלכם, כך שאין שום היגיון בכך שתתבקשו להזין אותם מחדש.

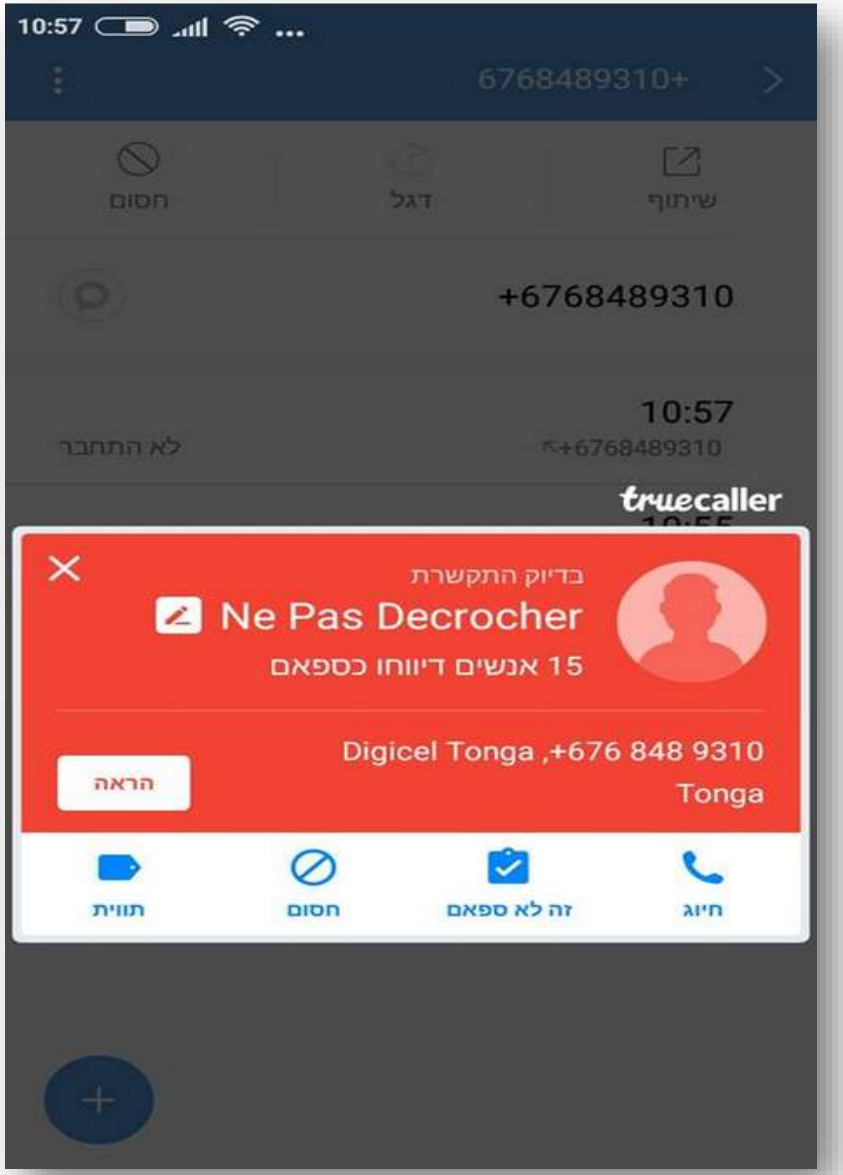
https://youtu.be/K-oo65W-8rQ

הונאה בשיחות טלפון מחו"ל



הונאה טלפונית מוכרת מהעולם עשתה עליה לארץ ישראל, ונוכלים מתקשרים אליכם באמצע הלילה ממספר מוזר.

כשלקוח מתקשר להתלונן בנושא



למה מתקשרים דווקא אלי?

איש לא מחפש אתכם אישית, הם כנראה מגרילים מספרים.

הם באמת מטונגה וקונגו?

לא בהכרח. ההונאה מגיעה מכל מיני מדינות קטנות, וייתכן שרק מנתבים דרכן את השיחות.

מה עושים?

לא עונים לשיחה. לא חוזרים למספר. אם זה סמס - לא חוזרים אליו. אפשר גם לחסום מספר שמתקשר אליכם שוב ושוב. ברוב המכשירים החכמים - ביומן השיחות שלא נענו, מסמנים את המספר הסורר ולוחצים על חסימה.

זהו?

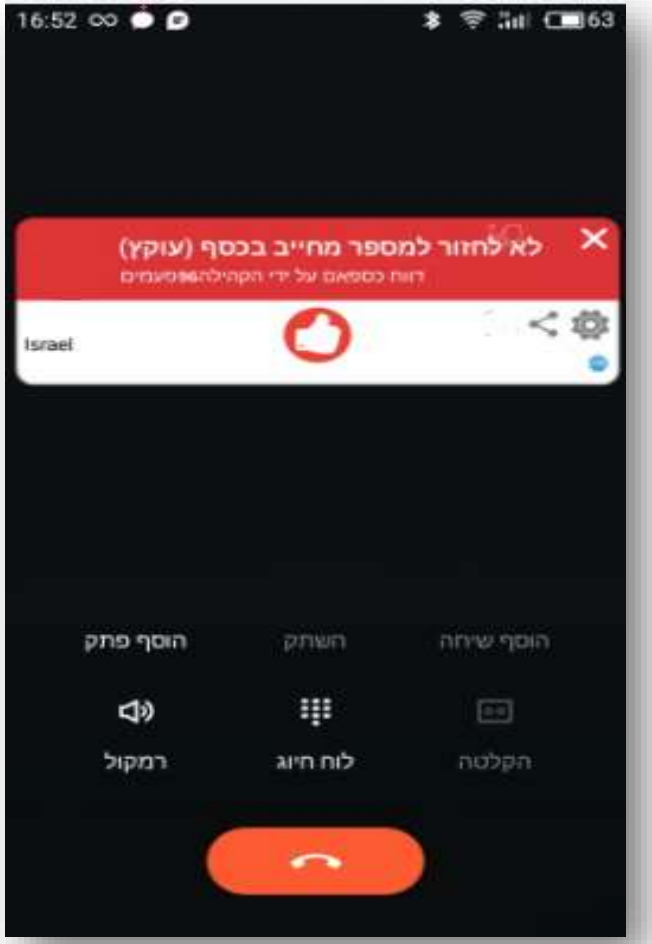
כן. זה די פשוט. לא עונים ולא חוזרים למספר. חוסמים אם צריך. אם זה מספר מחו"ל (טונגה או מדינה אחרת) ואתם לא מצפים לשיחה הזאת - אל תענו.

אם עניתי?

תנתקו כאשר הבנתם שזו טעות במספר או הונאה. הנוכלים לא ייעלבו. אם שומעים מישהו מדבר אתכם בשפה לא מוכרת - זה חלק ידוע מההונאה על מנת למשוך זמן אוויר.

ואם חזרתי למספר?

תנתקו את השיחה מיד, אבל כנראה תצטרכו לשלם עליה בחשבון החודשי – יש ליידע את הלקוח בעלויות ולשאול אם ברצונו **לחסום את הקו שלו לשיחות לחו"ל.**



כדאי להוריד אפליקציות לזיהוי מספרים?

לא נגיד "כדאי" אלא "אפשר"- לבחירתכם. האפליקציות יעילות בזיהוי ספאם וחסימה שלו, אבל בתמורה הן רוצות את רשימת אנשי הקשר שלכם. תחשבו אם שווה לכם למסור אותה.

חברת אקספון- WE 4G עושה משהו בנידון?

בהחלט- חברתנו פועלת לחסום שיחות מהסוג הזה בזמן אמת 24 שעות.

שאלות ?