



מגן

המדריך המשפחתי להגנה מהונאות AI

היום אפשר לזייף בטלפון את הקול של בן משפחה ואפילו שיחת וידאו שלמה, ולכן כבר אי אפשר לסמוך רק על מה ששומעים ורואים. המדריך הזה מסביר איך ההונאות האלה עובדות, ונותן לכם ולהורים שלכם כמה הרגלים פשוטים שעוצרים אותן.

מה תמצאו בפנים: חמישה מקרים מתועדים, פרטוקול משפחתי ברור, כרטיס להדפסה ליד הטלפון של ההורים, ומספרי מוקדי ההונאות של הבנקים בישראל.

למה כתבנו את המדריך, ואיך משתמשים בו

ה-AI מאפשר לנוכלים להישמע ולהיראות כמו מישהו שאתם סומכים עליו, ולכן ההגנה כבר לא יכולה להיות "אני אזהה את הקול". ההגנה היא הרגל משפחתי קבוע: כשמישהו מבקש כסף או קוד בדחיפות, מנתקים ובודקים מולו בדרך אחרת.

כתבנו את המדריך בשביל הורים, סבים וסבתות, וכל מי שאחראי על הכסף בבית או בעסק קטן. אם אין לכם זמן לקרוא הכול עכשיו, תתחילו מעמוד 8, שמסביר מה עושים בדקה הראשונה של שיחה חשודה, ומהכרטיס שבעמוד 11. אחר כך תשובו עם ההורים לעשר דקות ותקבעו יחד מילת קוד.

כל מקרה, נתון ומספר טלפון במדריך מגיע ממקור שמופיע ברשימה בסוף, והמספר בסוגריים המרובעים מפנה אליו. את מספרי הטלפון בדקנו באתרים הרשמיים ב-8 באוקטובר 2026, ובכל זאת כדאי לוודא את המספר של הבנק שלכם גם באפליקציה שלו.

הכלל במשפט אחד

בקשה דחופה לכסף או לקוד, אפילו בקול מוכר, היא סיבה לנתק ולהתקשר בחזרה למספר שאתם כבר מכירים.

מה במדריך

3	איך נראות הונאות AI היום
4	חמישה מקרים מתועדים, ומה אפשר ללמוד מכל אחד
6	שבעה סימנים שמסגירים הונאה
7	מילת קוד משפחתית: איך בוחרים אותה ואיך מתרגלים עם ההורים
8	מה עושים בדקה הראשונה כשמגיעה שיחה חשודה
9	איך מקשים על הנוכלים: הקול שלכם ברשת, וואטסאפ והבנק
10	אם זה כבר קרה: למי פונים ובאיזה סדר
11	כרטיס לתלות ליד הטלפון של ההורים
12	מקורות

איך נראות הונאות AI היום

ההונאות עצמן לא חדשות, וגם לפני עשר שנים נוכלים התקשרו וסיפרו על נכד שעשה תאונה. מה שהשתנה הוא שכלי AI הופכים את הסיפור להרבה יותר משכנע. לפי ה-FBI, הכלים האלה גם מתקנים טעויות שפעם הסגירו את הנוכלים [1]. אלה ארבע הצורות הנפוצות היום:

1 שכפול קול של בן משפחה

לנוכלים מספיק קטע קצר מהקול שלכם, למשל מסרטון ברשת, כדי לייצר קול דומה שאומר כל מה שהם רוצים. חוקרים של McAfee מצאו ב-2023 שבאחת הבדיקות שלהם הספיקו שלוש שניות של הקלטה כדי ליצור שיבוט שתואם למקור ב-85%, לפי מדד הבדיקה שלהם [2]. אחר כך מגיעה שיחה או הודעה קולית, בדרך כלל עם בכי, לחץ ובקשה לכסף מיד. רשות הסחר הפדרלית בארה"ב (FTC) מסכמת את זה במשפט אחד: אל תסמכו על הקול [3].

2 שיחת וידאו מזויפת

אותה טכנולוגיה עובדת גם על פנים, ולכן הנוכלים יכולים להופיע בשיחת וידאו בדמות של מנהל, בן משפחה או נותן שירות, ולדבר בזמן אמת. ראש היחידה להזדהות וליישומים ביומטריים במערך הסייבר הלאומי אמר שמי שמנהל היום שיחת וידאו עם נותן שירות, כמו עורך דין או יועץ משכנתאות, צריך להביא בחשבון שייתכן שמדובר בהתחזות [13].

3 הודעה מבן משפחה "עם טלפון חדש"

ההודעה מגיעה בוואטסאפ או ב-SMS ממספר לא מוכר, ומי שכותב אותה טוען שהוא הבן או הבת ושהטלפון שלו התקלקל. אחרי כמה הודעות מגיעה בקשה דחופה להעביר כסף. בגרסה אחרת כותבים לכם "שלחתי לך קוד בטעות, תוכל להעביר לי אותו?", ולפי מערך הסייבר זו הדרך הנפוצה להשתלט על חשבונות וואטסאפ. מי שהשתלט על החשבון יכול לפנות בשמכם לחברים ולמשפחה ולבקש גם מהם כסף [15].

4 מודעת השקעה עם ידוען מזויף

ברשתות החברתיות רצות מודעות שבהן אדם מוכר ממליץ על השקעה, אבל הסרטון נוצר ב-AI. הקישור מוביל לקבוצת וואטסאפ שבה "מומחים" דוחפים לקנות מניה מסוימת. לפי רשות ניירות ערך, בהתחלה המשקיעים לפעמים אפילו רואים רווח, ולכן הם משקיעים עוד, עד שהמניה צונחת וההפסד גדול [12].

לפי סקר של McAfee בקרב יותר מ-7,000 מבוגרים בשבע מדינות, אחד מכל ארבעה נתקל בהונאת קול כזו בעצמו או מכיר מישהו שנתקל בה, ו-77% ממי שנפלו בה הפסידו כסף [2].

חמישה מקרים מתועדים, ומה אפשר ללמוד מכל אחד

בחרנו מקרים שתועדו בתקשורת או בהודעות רשמיות, ובכל אחד יש לקח שאפשר ליישם בבית.

הונג קונג • ינואר 2024

שיחת הווידאו שעלתה 25 מיליון דולר

עובד במחלקת הכספים של הסניף בהונג קונג של Arup, חברת הנדסה בריטית גדולה, קיבל הודעה שנראתה כאילו נשלחה מסמנכ"ל הכספים של החברה בבריטניה, ובה בקשה לבצע עסקה סודית. בהתחלה הוא חשד, אבל אז הוזמן לשיחת וידאו שבה ראה ושמע את סמנכ"ל הכספים ועוד כמה אנשים מהחברה. כל המשתתפים בשיחה, חוץ ממנו, היו זיופים שנוצרו ב-AI. לפי משטרת הונג קונג, במשך שבוע הוא ביצע 15 העברות לחמישה חשבונות בנק, בסך 200 מיליון דולר הונג קונגי (כ-25.6 מיליון דולר אמריקאי), והבין שמדובר בהונאה רק כשבדק מול המטה בבריטניה.

מה לומדים מזה: שיחת וידאו כבר לא מוכיחה שמישהו הוא מי שהוא נראה. לפני שכסף זז, מאמתים מול האדם בערוץ אחר, כזה שאתם יזמתם.

מקורות: [5] [6]

אריזונה, ארה"ב • אפריל 2023

הבת "נחטפה", אבל בכלל הייתה בטיול סקי

ג'ניפר דסטפנו ענתה לשיחה ממספר לא מוכר ושמעה את בתה בת ה-15 בוכה ואומרת "אמא, פישלתי". הבת הייתה באותו זמן בטיול סקי. אחר כך גבר לקח את הטלפון, אמר שהבת אצלו ודרש כופר: קודם מיליון דולר, ואחר כך 50 אלף דולר במזומן. בזמן שהיא ניהלה איתו משא ומתן, הורים אחרים שהיו לידה התקשרו למשטרה, והיא הצליחה להשיג את הבעל ואת הבת ולשמוע שהבת בסדר. ביוני 2023 היא העידה בסנאט האמריקאי ותיארה את השיחה כהונאה שבה שוכפל הקול של בתה.

מה לומדים מזה: הנוכלים מנסים להשאיר אתכם על הקו, לבד ובפאניקה. מה שעצר את ההונאה היה אדם נוסף שבדק במקביל, ושיחה ישירה לבת.

מקורות: [7]

איטליה • יולי 2024

שאלה אחת על ספר עצרה זיוף מצוין

מנהל בכיר בפרארי קיבל הודעות וואטסאפ שנראו כאילו נשלחו מהמנכ"ל, בנדטו ויניה, על עסקת רכישה גדולה וסודית. ההודעות לא הגיעו מהמספר הרגיל שלו, אבל הופיעה בהן תמונה של המנכ"ל. אחר כך הגיעה שיחה בקול שחיקה את ויניה היטב, כולל המבטא שלו. המנהל שם לב לכמה צלילים מכניים, ולכן אמר שהוא צריך לזהות את בן שיחו ושאל מה שם הספר שויניה המליץ לו עליו כמה ימים קודם. השיחה נותקה מיד.

מה לומדים מזה: שאלה שרק האדם האמיתי יודע לענות עליה עוצרת גם זיוף טוב מאוד. זה בדיוק הרעיון של מילת קוד משפחתית.

מקורות: [8]

איטליה · פברואר 2025

הקול של שר ההגנה ביקש מיליון יורו

אנשי עסקים בכירים באיטליה קיבלו שיחות ממי שהציגו את עצמם כשר ההגנה, גואידו קרוזטו, וכאנשי הצוות שלו. הם ביקשו כמיליון יורו לחשבון בהונג קונג, כדי לשחרר עיתונאים איטלקים שנחטפו במזרח התיכון. לפחות אחד מהם, מסימו מוראטי, הבעלים לשעבר של קבוצת הכדורגל אינטר, העביר כמעט מיליון יורו. הוא הגיש תלונה, ולפי רויטרס המשטרה איתרה את הכסף בחשבון בהולנד והקפיאה אותו.

מה לומדים מזה: גם אנשים מנוסים נופלים כשהסיפור משלב סמכות, מטרה טובה ודחיפות. וכדאי לדווח מיד ובלי להתבייש, כי לפעמים עוד אפשר לעצור את הכסף.

מקורות: [9] [10]

ישראל · אפריל עד יולי 2025

הנגיד "המליץ" על מניה, ומשקיעים הפסידו מאות אלפי שקלים

בפייסבוק ובאינסטגרם רצו מודעות ממומנות עם סרטוני דיפ-פייק של אנשים מוכרים, ובהם נגיד בנק ישראל פרופ' אמיר ירון, ראש הממשלה, אייל גולן ונועה קירל, שכביכול המליצו על השקעה. מי שלחץ הגיע לקבוצות וואטסאפ שבהן "מומחים" דחפו לקנות מניה אמיתית שנסחרת בנאסד"ק. המניה עלתה בהתחלה, ובתחילת יולי 2025 קרסה. לפי ynet, אחד המשקיעים דיווח שהפסיד 250 אלף שקלים, ומשקיע אחר דיווח על הפסד של 150 אלף שקלים.

מה לומדים מזה: אנשי ציבור אמיתיים לא ממליצים על מניות במודעה ממומנת. לפני כל השקעה בודקים אם למי שממליץ יש רישיון מרשות ניירות ערך.

מקורות: [11] [12]

ומה קורה בישראל?

- לפי דוח של מערך הסייבר הלאומי מספטמבר 2025, במערך התקבלו בשנה שלפני כן 250 דיווחים על סרטוני דיפ-פייק ברשת, ורובם התחזו לאנשים מוכרים [13].
- ביולי 2026 הזהיר מערך הסייבר מפני הונאות טלפוניות נגד מבוגרים דוברי רוסית, וציין שבחלק מהמקרים הנוכלים משתמשים בזיוף קול ב-AI כדי להישמע כמו בן משפחה [14].
- בגלל ריבוי ההונאות, בנק ישראל חייב את הבנקים להפעיל מוקד הונאות עם מענה אנושי בכל שעות היממה, והחובה בתוקף מ-31 במאי 2026 [17] [18].

שבעה סימנים שמסגירים הונאה

זיוף טוב אי אפשר לזהות באוזן או בעין, ולכן כדאי להסתכל על מה שמבקשים מכם ולא על מי שנראה שמבקש. כמעט בכל המקרים במדריך הופיעו לפחות שניים מהסימנים האלה:

1 דחיפות

אומרים לכם שצריך לפעול עכשיו ושאין זמן להסביר, כי הלחץ נועד למנוע מכם לעצור ולבדוק.

2 סוד

מבקשים מכם לא לספר לאף אחד ולא לערב את המשפחה. לפי מערך הסייבר, זה סימן אזהרה מובהק [14].

3 מספר חדש או ערוץ לא רגיל

הפנייה מגיעה ממספר שלא שמור אצלכם, עם הסבר כמו "הטלפון שלי התקלקל". כך התחיל גם הניסיון בפרארי [8].

4 בקשה לקוד, לסיסמה או לפרטי אשראי

נציג אמיתי של בנק, משטרה או משרד ממשלתי לא יבקש מכם בטלפון קוד חד-פעמי או סיסמה [14].

5 בקשה להתקין אפליקציה או ללחוץ על קישור

מבקשים מכם להתקין משהו, ללחוץ על קישור, לשתף מסך או לתת גישה לטלפון או למחשב. זה סימן אזהרה ברור [14].

6 דרך תשלום חריגה

מבקשים לתת מזומן לשליח שבא לאסוף, להעביר כסף ל"חשבון בטוח", או לשלם בקריפטו או בכרטיסי מתנה [3] [14].

7 הבטחה שנשמעת טוב מדי

מבטיחים רווח גבוה בלי סיכון, מדברים על "אלגוריתם סודי" ולוחצים עליכם להחליט מהר. כך רשות ניירות ערך מתארת הצעת השקעה תרמיתית [12].

ומה עם סימנים בסרטון עצמו? ה-FBI ממליץ לשים לב לידיים או לשיניים מעוותות, לצללים לא הגיוניים, להשהיות ולתנועות לא טבעיות [1]. הזיופים משתפרים מהר, ולכן אל תסתמכו רק על זה.

מילת קוד משפחתית

מילת קוד היא מילה או משפט שרק בני המשפחה הקרובה מכירים. אם מישהו מתקשר בקול של הבן שלכם ומבקש כסף בדחיפות, אתם שואלים אותו מה מילת הקוד, והזיוף לא יודע לענות. ה-FBI המליץ על זה רשמית בדצמבר 2024 [1], ובבריטניה בנק Starling הפך את זה לקמפיין ארצי אחרי שסקר שלו מצא ש-28% מהבוגרים בבריטניה חושבים שניסו להונות אותם בשכפול קול בשנה האחרונה [4].

איך מתרגלים עם ההורים

עדיף לשבת איתם פנים מול פנים ולהגיד משהו כמו:

"יש היום תוכנות שיודעות לחקות את הקול שלי. אם פעם אתקשר ואבקש כסף בדחיפות, תשאלו אותי מה המילה שלנו. אם לא אענה, תנתקו ותתקשרו אליי למספר הרגיל."

אחר כך עושים תרגיל אחד: מתקשרים אליהם ממספר אחר, מבקשים כסף ובודקים שהם זוכרים לשאול. כדאי לחזור על התרגיל פעם בכמה חודשים.

איך בוחרים מילה טובה

- משהו שקל לזכור גם בלחץ, אבל שאי אפשר לנחש. לא שם של כלב, רחוב או תאריך לידה, כי את כל אלה אפשר למצוא ברשת.
- צירוף מצחיק של שתי מילים שלא קשורות זו לזו עובד טוב, למשל "חביתה כחולה". רק אל תבחרו בדוגמה הזו.
- אומרים אותה רק בעל פה. לא כותבים אותה בוואטסאפ, במייל או על פתק במקרר [4].
- אם יש חשש שמישהו זר שמע אותה, מחליפים.

ומה אם ברגע של לחץ שכחו את המילה?

זו בדיוק הסיבה שמילת הקוד היא רק חצי מהפרוטוקול. החצי השני עובד גם בלי לזכור שום דבר: מנתקים ומתקשרים בחזרה למספר שכבר שמור בטלפון. במקום מילת קוד אפשר גם לשאול שאלה שרק האדם האמיתי יודע את התשובה עליה, כמו שעשה המנהל בפרארי [8].

גם בעסק: אותו עיקרון עובד בעבודה. קובעים מראש שכל העברה גדולה, או כל שינוי בפרטי חשבון של ספק, מאושרים בשיחה יזומה למספר שמור ועל ידי שני אנשים. ככה בקשה דחופה מ"המנכ"ל" בוואטסאפ לא מספיקה כדי להוציא כסף.

מה עושים בדקה הראשונה כשמגיעה שיחה חשובה

מערך הסייבר הלאומי מסכם את זה בשלוש מילים: עוצרים, מנתקים ומאמתים [14]. בפועל זה נראה כך:

1 עוצרים

לא מבטיחים כלום ולא עושים שום פעולה בזמן השיחה, גם אם הצד השני לוחץ. מותר להגיד "אני חוזר אליך בעוד חמש דקות" ולנתק.

2 שואלים את מילת הקוד

אם קבעתם מילה, זה הזמן לבקש אותה. מי שלא יודע אותה, או מתחמק, הוא לא מי שהוא אומר שהוא.

3 מנתקים ומתקשרים בעצמכם

מתקשרים למספר שכבר שמור אצלכם: לבן המשפחה, לבנק דרך המספר שבאפליקציה או בגב הכרטיס, או למשרד. לא חוזרים למספר שהתקשר ולא למספר שנשלח בהודעה, אלא רק למספר שאתם כבר מכירים [1] [3] [14].

4 לא נשארים לבד עם זה

אם לא מצליחים להשיג את האדם, מתקשרים לבן משפחה אחר או לשכן שיעזור לבדוק [14]. כך נעצרה ההונאה בסיפור של דסטפנו [7].

מה אף פעם לא עושים בטלפון

- לא מוסרים קוד חד-פעמי, סיסמה או פרטי אשראי, גם לא למי שמציג את עצמו כבנק, כמשרה או כבן משפחה [14].
- לא מתקינים אפליקציה, לא לוחצים על קישור ולא משתפים מסך כי משהו ביקש בשיחה [14].
- לא מעבירים כסף ל"חשבון בטוח" ולא מוסרים כסף או תכשיטים לשליח שבא לאסוף [14].
- לא שומרים את השיחה בסוד. מספרים מיד לבן משפחה או לחבר קרוב [14].

ואם התברר שהכול היה אמיתי? אז הפסדתם חמש דקות, וזה מחיר קטן לעומת מה שעלול לקרות אם זו הונאה.

איך מקשים על הנוכלים

אי אפשר להיעלם מהרשת, אבל אפשר להקשות על מי שמנסה להתחזות אליכם. ה-FBI ממליץ לצמצם את כמות הקול והתמונות שלכם שזמינים לכולם ברשת, ולהפוך את החשבונות ברשתות החברתיות לפרטיים [1].

הקול והפנים שלכם ברשת

- הופכים את הפרופילים באינסטגרם, בפייסבוק ובטיקטוק לפרטיים, ומשאירים כעוקבים רק אנשים שאתם מכירים [1].
- חושבים פעמיים לפני שמעלים לפרופיל פתוח סרטונים ארוכים שבהם מדברים אתם, הילדים או ההורים, כי מהם אפשר לשכפל קול [2] [4].

וואטסאפ: חמש דקות שחוסכות הרבה צרות

- מפעילים אימות דו-שלבי: **הגדרות** ← **חשבון** ← **אימות דו-שלבי**, ובוחרים קוד PIN בן שש ספרות. מעכשיו גם מי שהשיג את הקוד מה-SMS לא יוכל להיכנס לחשבון בלי ה-PIN [15] [19].
- מוסיפים כתובת מייל לשחזור החשבון, תחת **הגדרות** ← **חשבון** ← **כתובת אימייל** [15].
- לא מעבירים לאף אחד את הקוד בן שש הספרות שוואטסאפ שולחת ב-SMS, גם לא לחבר שכותב שהוא "שלח אותו בטעות" [15].

הבנק, המייל וההשקעות

- מפעילים אימות דו-שלבי גם במייל, ברשתות החברתיות ובאפליקציית הבנק [15].
- שומרים כבר עכשיו באנשי הקשר את מספר מוקד ההונאות של הבנק שלכם (הרשימה בעמוד הבא), כדי שברגע אמת לא תצטרכו לחפש אותו.
- לפני השקעה בודקים שלמי שממליץ יש רישיון, ברשימת בעלי הרישיון באתר של רשות ניירות ערך. במודעה ממומנת בגוגל אפשר גם לבדוק מי המפרסם במרכז השקיפות של גוגל, כמו שהרשות ממליצה [12].

אם תעשו רק דבר אחד מהעמוד הזה, **תשבו עשר דקות עם ההורים**: תקבעו מילת קוד, תפעילו להם אימות דו-שלבי בוואטסאפ ותתלו את הכרטיס מעמוד 11 ליד הטלפון.

אם זה כבר קרה: למי פונים ובאיזה סדר

אין סיבה להתבייש. ההונאות האלה הצליחו גם מול מנהלים בחברות ענק ומול אנשי עסקים מנוסים. מה שחשוב עכשיו הוא לפעול מהר, כי לפעמים עוד אפשר לעצור את הכסף [10].

1 הבנק או חברת האשראי, מיד

מבקשים לחסום את הכרטיסים ואת הגישה לחשבון, ושואלים אם אפשר לעצור את ההעברה או להחזיר אותה. לפי הוראה של בנק ישראל, המוקד זמין בכל שעות היממה, גם בשבת, וזמן ההמתנה לנציג לא אמור לעלות על שש דקות, למעט חריגים [18].

2 משטרת ישראל: 100

מתקשרים אם העברתם כסף, מסרתם פרטים או קיבלתם איום, וגם אם שליח בדרך לאסוף מכם כסף [14].

3 מערך הסייבר הלאומי: 119

זמין בכל שעות היממה, לדיווח על השתלטות על וואטסאפ, הודעות פייסינג ואתרים מתחזים. המערך נותן מענה ראשוני ולא מחליף תלונה במשטרה [16].

מייל: 119@cyber.gov.il
צ'אט CyBot בוואטסאפ: 050-6251119

4 מנקים, מזהירים ושומרים ראיות

מוחקים אפליקציה שהתקנתם בעקבות השיחה, מחליפים סיסמאות ומפעילים אימות דו-שלבי. מספרים לחברים ולמשפחה כדי שלא יפלו באותה הונאה, ושומרים צילומי מסך, מספרים, הודעות וקישורים [14] [15].

מוקדי ההונאות של הבנקים וחברות האשראי, 24/7

לפי הרשימה של בנק ישראל [17]

הפועלים	*9391	לאומי	*5946	מזרחי טפחות	*8860
דיסקונט	076-8050010	הבינלאומי	*3009	מרכנתיל	076-8050009
יהב	*2638	מסד	03-5130016	וואן זירו	03-3767424
ישראכרט	03-6364400	כאל	03-5723666	מקס	03-6178800

במזרחי טפחות מקישים שלוחה 6. באתר של הבינלאומי מופיע למוקד ההונאות גם המספר *5120 [20]. הבנק שלכם לא ברשימה? חפשו "מוקד הונאות" באפליקציה שלו או התקשרו למספר שבגב הכרטיס.

מעל גיל 65? מי שנפל קורבן לעושק או לניצול

כלכלי יכול לקבל ייעוץ וייצוג משפטי בחינם מהסיוע המשפטי של משרד המשפטים, בטלפון *6405 [14].

הונאת השקעות? אפשר לדווח לרשות ניירות ערך

דרך טופס הקו הישיר באתר שלה, גם בלי להזדהות [12].

מבקשים מכם כסף או קוד בדחיפות?

גם אם הקול נשמע בדיוק כמו של מישהו שאתם מכירים

- 1 לא מוסרים לאף אחד קוד, סיסמה או פרטי אשראי.
- 2 לא מתקינים אפליקציה ולא לוחצים על קישור.
- 3 שואלים את מילת הקוד שלנו.
- 4 מנתקים ומתקשרים בחזרה למספר ששמור אצלנו.
- 5 לא שומרים את השיחה בסוד, ומספרים לבן משפחה.

הבן או הבת:

בן משפחה נוסף:

מוקד ההונאות של הבנק:

משטרה 100 **מערך הסייבר 119**

אל תכתבו על הכרטיס את מילת הקוד עצמה. AI בדקה

AI בדקה • מגן