

מידע כוזב, שמועות והונאות בזמן חירום

מדריך מעשי לציבור בישראל לאימות מידע, צמצום הפצה, זיהוי התחזות והגנה על מידע וכסף

בזמן חירום

אוגוסט 2026

הבהרת אחריות: המידע במדריך הוא מידע כללי, אינו כולל את כל סוגי ההודעות, ההונאות והמצבים האפשריים, ואינו מהווה ייעוץ משפטי, פיננסי או אבטחת מידע אישי. הוא מבוסס על מקורות מוסמכים (פיקוד העורף, מערך הסייבר הלאומי, משטרת ישראל, בנק ישראל והמטה הלאומי להגנה על ילדים ברשת). לפני פעולה בעלת השלכות כספיות, משפטיות או בטיחותיות יש לפנות לגוף המוסמך באמצעות ערוץ שאיתרתם בעצמכם.

בכל מקרה: בזמן חירום יש לפעול לפי הערוצים הרשמיים של הגוף המוסמך הרלוונטי.

איך משתמשים במדריך

המדריך נועד לרגע שבו מתקבלת בזמן חירום הודעה דחופה, מפחידה או מפתה: התרעה, בקשת תרומה, דרישה להעברת כסף, קישור לעדכון, צילום מזירה או הודעה בשם גוף ציבורי. המטרה היא לעצור, לאמת, להגן על מידע וכסף, ולדווח בערוץ המתאים.

למה חשוב להיזהר במיוחד בזמן חירום?

בתקופות חירום גוברים הלחץ, אי-הוודאות והצורך במידע מהיר. גורמים עוינים ועבריינים עלולים לנצל מצב זה להפצת שמועות ומידע כוזב, להתחזות לגופי חירום, לבנקים או לאנשים מוכרים, ולשלוח קישורים ובקשות דחופות לכסף או לפרטים אישיים. גם מידע אמיתי עלול להיות ישן, חלקי ולשמש לצרכים מניפולטיביים. במקביל, בזמן חירום מופץ לעיתים גם מידע אמין, אך סודי ופרטי, כגון מיקום נפילות, או שמות נפגעים. לכן חשוב לעצור לפני פעולה או שיתוף, לבדוק את המקור בערוץ רשמי שאיתרתם בעצמכם, ולבחון גם את סוג המידע, ולא להסתמך על תחושת הדחיפות או על זהות השולח לכאורה.

ארבע שאלות ראשונות

- מי המקור המקורי של ההודעה (ולא מי העביר אותה אליי)?
- האם ההודעה מופיעה גם בערוץ הרשמי של הגוף שמוזכר בה?
- האם מבקשים ממני ללחוץ, למסור קוד, להעביר כסף או לפעול מיד?
- האם שיתוף ההודעה עלול לחשוף מיקום, אדם שנפגע או מידע מבצעי?

חשוב: דחיפות, פחד וסמכות מדומה הם כלי שכנוע נפוצים. אל תבצעו פעולה בלתי הפיכה לפני אימות עצמאי.

1. הכנה מראש

- שמרו קישורים או יישומונים רשמיים של פיקוד העורף, הרשות המקומית, קופת החולים והבנק.
- הפעילו אימות דו-שלבי בחשבונות חשובים והשתמשו בסיסמאות שונות.
- קבעו במשפחה כלל: קוד אימות וסיסמה אינם נמסרים לאדם אחר בטלפון, בהודעה או בצי'ט. מזינים קוד רק באתר או ביישומון רשמי שאיתרתם בעצמכם, ורק לצורך פעולה שאתם יזמתם ושאתם מזהים כלגיטימית.
- הסכימו מי מסייע לאדם מבוגר, לילד או למי שאינו קורא עברית בבדיקת הודעות.
- הכירו את מוקדי הדיווח: מערך הסייבר הלאומי - מוקד 119; משטרת ישראל: 100; המטה הלאומי להגנה על ילדים ברשת - מוקד 105.

2. סולם אימות של חמש פעולות

שלב	פעולה
1. עצרו	אל תלחצו, אל תעבירו ואל תענו מיד.
2. זהו מקור	בדקו מי טוען ששלח, מה מבוקש ומה יקרה אם לא תפעלו.
3. עברו לערוץ עצמאי	פתחו בעצמכם אתר או יישומון רשמי; אל תשתמשו בקישור שבהודעה.
4. השוו	בדקו תאריך, שעה, אזור, ניסוח והאם יש הודעה רשמית תואמת.
5. החליטו	רק לאחר אימות פעלו, שמרו לתייעוד או דווחו.

3. כללים לזיהוי מידע כוזב ושמועה

- אין מקור ראשוני ברור, מזהה ומוסמך.
- הצילום או הסרטון שהופצו אינם מלווים בתאריך, מקום והקשר הניתנים לבדיקה.
- כותרת דרמטית אינה תואמת את תוכן ההודעה או את ההודעה הרשמית.
- מתבקשים "להעביר לכולם" לפני שניתן לבדוק.
- המידע מערבב עובדה נכונה עם מסקנה לא מבוססת.
- היזהרו במיוחד כשהודעה מדווחת על אירוע "כדחוף" או כזה שהתרחש "עכשיו", מבלי שמתלווים לה פרטים ניתנים לאימות.
- זכרו שגם תוכן אמיתי עלול להיות מזיק כאשר הוא ישן, חלקי, מוצא מהקשרו או חושף מידע רגיש. המבחן אינו רק "אמיתי או מזויף", אלא האם המידע עדכני, מלא ומותר להפצה.

4. לזהות התחזות והונאה

- בקשה למסור סיסמה, קוד חד-פעמי, מספר כרטיס, צילום תעודה או פרטי כניסה.
- בקשה להזין קוד. לפני שמזינים קוד, קוראים את ההודעה המלאה ובודקים איזו פעולה הקוד מאשר, מה הסכום ולמי הוא מועבר. קוד שהגיע בלי שיזמתם פעולה הוא סימן לעצור ולפנות לבנק.
- קישור שכתובתו דומה אך אינה זהה לאתר הרשמי.
- מספר שמופיע על הצג בשיחה נכנסת, גם אם הוא נראה כמספר של בנק, משטרה או גוף ממשלתי, אינו מוכיח את זהות המתקשר. מנתקים וחוזרים למספר הרשמי שמצאתם בעצמכם.
- דרישה להעביר כסף ל"חשבון בטוח", למשך מזומן, להתקין יישום שליטה מרחוק או לשלם מקדמה.
- בקשת תרומה לחשבון פרטי או לקישור שאינו ניתן לאימות.

- התחזות לבן משפחה באמצעות קול, וידאו או הודעה, **בצירוף לחץ לא לשתף אחרים**. אם מתעורר חשד, מפסיקים את השיחה ויוצרים עם האדם קשר מחדש במספר המוכר השמור אצלכם. אפשר לשאול שאלה שרק הוא או היא אמורים לדעת להשיב עליה. אין להסתמך רק על הקול, התמונה או מספר הטלפון.

חשוב: בנק ישראל והמשטרה מזהירים כי גורם פיננסי לגיטימי לא יבקש מכם למסור קוד אימות שנשלח אליכם. מספר שמופיע על הצג אינו הוכחה לזהות המתקשר.

5. אם לחצתם או מסרתם מידע

- נתקו קשר עם הפונה ואל תמשיכו לבצע הוראות.
- פנו מיד לבנק או לחברת כרטיסי האשראי באמצעות מספר שמצאתם בעצמכם, ובקשו לעצור פעולות חשודות. יש לבדוק גם עסקאות, העברות, מוטבים חדשים ושינויים בפרטי החשבון. יש להמשיך לעקוב אחר פעילות חריגה בימים שלאחר האירוע.
- שנו את הסיסמה ממכשיר שאתם סומכים עליו ושלא הותקנה בו תוכנת שליטה מרחוק. נתקו חיבורים שאינכם מזהים והפעילו אימות דו-שלבי. אם אינכם בטוחים שהמכשיר בטוח לשימוש, בקשו סיוע מקצועי.
- דווחו למערך הסייבר הלאומי במוקד 119 על דיוג, התחזות, חטיפת חשבון או דף מתחזה.
- שמרו צילומי מסך, כתובות, מספרים, תכתובות ואסמכתאות.
- אם הועבר כסף, נעשה שימוש בפרטים, בוצעה התחזות או שיש חשד לעבירה, יש להגיש תלונה למשטרה. במקרה של סכנה מיידית מתקשרים למוקד 100.

חשוב: אל תמחקו תיעוד לפני ששמרתם עותק. אל תשלמו "דמי שחרור" נוספים ואל תיענו לגורם שמבטיח להשיב את הכסף תמורת תשלום.

6. לפני שמעבירים מידע

- כללים אלו נוגעים גם למידע מפוקפק, וגם למידע שאומת, שמטעמי סודיות ופרטיות אין להעבירו בערוצי מדיה:
- בדקו אם המידע מופיע בערוץ רשמי ועדכני.
 - הסירו מיקום מדויק, פנים, מספרי רכב, מסמכים ופרטים רפואיים.
 - אל תפרסמו מידע נפגעים, נעדרים או חללים לפני הודעה מוסמכת למשפחה.
 - אל תשתפו תמונות של זירות, כוחות, מערכות הגנה או תנועת כוחות בזמן אמת.
 - כאשר אינכם בטוחים לגבי המידע, או אם אינכם יודעים כיצד להסוות פרטים שפוגעים בסודיות, אל תעבירו. אפשר לדווח לגוף המוסמך.

7. התאמות לאוכלוסיות ייחודיות

ילדים ובני נוער

- הסבירו שלא משתפים סרטונים קשים ושלא לוחצים על קישור שמבטיח פרס, מידע בלעדי או תמונה.
- פגיעה, איום או סחיטה ברשת מדווחים למוקד 105 ובמקרה של סכנה מיידית, גם למוקד 100 של המשטרה.
- אין להאשים ילד שלחץ או שיתף; עצירה מהירה ושמירת תיעוד חשובות יותר.

אזרחים ותיקים, אנשים ללא אוריינות דיגיטלית

- קבעו אדם קבוע לבדיקה ואימות, בלי לקחת מן האדם את השליטה בהחלטותיו.
- הדפיסו מספרים רשמיים של הבנק, הקופה והרשות.
- השתמשו בכלל פשוט: שיחה נכנסת מסתיימת; החזרה נעשית למספר רשמי שנמצא בנפרד.
- אל תעבירו מידע רפואי או פרטי ללא הסכמה, גם כאשר הכוונה לסייע.

דוברים שאינם שולטים היטב בעברית

- קבעו אדם קבוע לבקיה ואימות, בלי לקחת מהאדם את השליטה בהחלטותיו.
- העדיפו ערוצים רשמיים בשפה ובפורמט נגישים.
- ודאו שהתרגום מתייחס לאותה גרסה ולא להודעה ישנה.

תזכורת: מה אסור לעשות

- לא ללחוץ על קישור רק משום שהוא נשלח בידי אדם מוכר; ייתכן שחשבוננו נפרץ.
- לא למסור קוד אימות, סיסמה או פרטי כרטיס למי שפנה אליכם.
- לא להתקין יישום שליטה מרחוק לפי הוראת מתקשר.
- לא להעביר כסף לחשבון "בטוח" או לאדם שמגיע לאסוף מזומן.
- לא לפרסם מידע מזהה על נפגעים או מידע מבצעי.
- לא להפיץ הודעה בתוספת "לא יודע אם נכון". ההסתייגות אינה מונעת את הנזק.
- לא להתעמת עם חשוד בהונאה בערוץ מדיה או לנסות לחקור אותו בעצמכם.

8. נקודות החלטה

מצב	הפעולה המתאימה
מידע לא מאומת ללא בקשת פעולה	לא מעבירים; בודקים בערוץ רשמי.
הודעה עם קישור או בקשת פרטים	עוצרים, סוגרים ועוברים לערוץ עצמאי.
נמסרו פרטים או בוצעה העברה	פונים מיד לבנק/ספק, משנים גישה, מדווחים למוקד 119 ולמשטרה לפי הצורך.
איום, סחיטה או סכנה מיידית	מתקשרים למוקד 100; במקרה של ילדים ונוער גם למוקד 105.
תוכן שחושף זירה או אדם	מפסיקים הפצה, שומרים תיעוד ומדווחים לפלטפורמה ולגורם המוסמך.

9. דף פעולה קצר להדפסה:

• עצרו - אל תלחצו ואל תעבירו. • זהו - מי המקור ומה מבקשים מכם. • אמתו - עברו בעצמכם לאתר או ליישומון הרשמי. • הגנו - אל תמסרו קוד, סיסמה, כסף או מידע אישי. • תעדו - שמרו צילום מסך, קישור, מספר ושעת הפנייה. • דווחו - 119 לסייבר; 100 לסכנה או עבירה דחופה; 105 לפגיעה בילדים ברשת; הבנק במקרה פיננסי.

פרסום עצמאי: מדריך זה פותח במסגרת מיזם "הבית ערוך". הוא אינו מופק, מאושר או מופעל בידי הגופים המוזכרים בו.

המקורות נבדקו באוגוסט 2026. יש לבדוק הודעות וערוצי דיווח עדכניים בזמן האירוע.

מקורות מרכזיים

[פיקוד העורף. לא מעבירים מידע ברשת.](#)

[מערך הסייבר הלאומי. התרעה מפני הפחדה, התחזות והפצת מידע כוזב. 2026.](#)

[מערך הסייבר הלאומי. דיווח על אירוע סייבר.](#)

[מערך הסייבר הלאומי. המדריך להגנה ממתקפות פשינג.](#)

[משטרת ישראל. הגשת תלונה למשטרת ישראל.](#)

[בנק ישראל. אזהרה לציבור מפני הונאות על ידי התחזות. 2024.](#)

[בנק ישראל. הונאות פיננסיות — פשינג.](#)

[המטה הלאומי להגנה על ילדים ברשת. ארגז כלים דיגיטלי למצב חירום.](#)