סיכוני אבטחה בשירות לקיצור קישור (Link)

1. מבוא

קישור (Link) לכתובת של אתר במרשתת (להלן: "**קישור**", "**כתובת**", "**כתובת URL**" או "**כתובת אתר**") עשוי להיות ארוך, מורכב ולא קריא למשתמש (להלן: "**משתמש**" או "**גולש**").
במטרה להקל על המשתמש קמו מספר שירותים אשר מקצרים קישור ארוך, ומציעים במקומו קישור קצר, קריא ונוח, ויודעים להפנות את דפדפן המרשתת מהקישור הקצר אל הכתובת המקורית של האתר המבוקש.[1]

לשירות לקיצור קישור (ידוע גם כשירות לקיצור כתובת אתר) מספר יתרונות אפשריים, הן לבעלי הכתובת המלאה (בין אם מדובר בגישה לקובץ, לנתוני מיקום או לכתובת אתר אינטרנט; להלן: "**בעלי האתר**"), והן למשתמש בקישור, במקרים בהם קיימת מגבלת תווים על מלל או דרושה המרת פרמטר ארוך בקישור למלל קריא והגיוני. לצדם, קיימים יתרונות נוספים, כגון האפשרות ליצירת קישור זמני, שפג לאחר פרק זמן שנקבע מראש.

אולם, כדאי לדעת שלצד היתרונות האמורים, בשימוש בקישור מקוצר יש חסרונות וסיכונים, הן למשתמש והן לבעלי האתר, ובהם חשיפת הקישור ברשת, פגיעה בפרטיות המשתמש, וסיכון להכוונת המשתמש לאתרים שיש בהם סיכוני אבטחה משמעותיים לגולש. חסרון נוסף, הוא חשיפת מיקום קבצים של בעלי האתר. חשיפה זו עלולה להוביל לשימוש בלתי מורשה בקבצים, ללא ידיעת בעלי האתר.

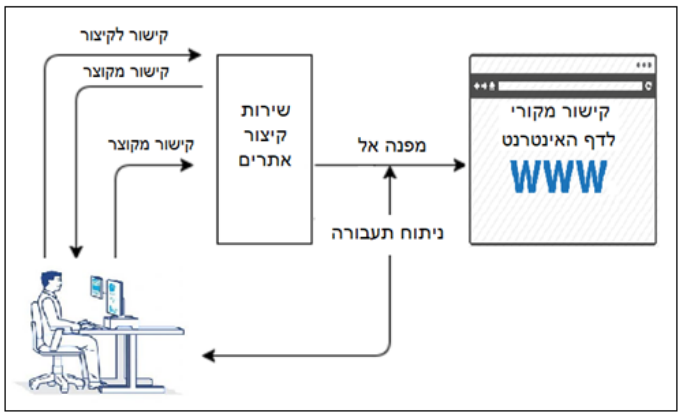
מטרת מסמך זה היא להציג את הסיכונים שבשירות לקיצור קישור, ולהציע מספר המלצות כדי להתגונן מפניהם.

2. מהו שרות לקיצור קישור?

בפשטות, שירות לקיצור קישור מציע המרה של הקישור המקורי הארוך לקישור מקוצר. השירות מספק דרך נוחה למשתמש לשתף קישור ארוך וקשה לזכירה, באמצעות שירות המרה של כתובת אינטרנט (URL) ארוכה בכתובת מקוצרת.

המרת הכתובת מתבצעת בשרתים של החברה נותנת השירות (להלן: "**החברה**"). כך, כאשר המשתמש לוחץ על קישור מקוצר, נוצר קשר עם שרת החברה, וזה מצדו "מחזיר" למשתמש את הכתובת המלאה, באופן המאפשר למשתמש להגיע אל היעד המבוקש. כלומר, השדר עובר דרך החברה, שהיא צד שלישי בתקשורת בין המשתמש לבין אתר האינטרנט.

[1] ראה דוגמה לשירות קיצור קישור של ויקיפדיה: https://en.wikipedia.org/wiki/Wikipedia:URLShortener



איור 1. סכמת שירות לקיצור קישור

שירות לקיצור קישור אינו שירות חדש, ולמעשה רבים מהשירותים הללו קיימים כבר למעלה מעשור. הוא מהווה חלופה המאפשרת למשתמש להגיע לאותה נקודה בדיוק, ללא מאמץ בהקלדת הכתובת, וללא צורך בידיעת הכתובת המקורית הארוכה. הקישור המקוצר מכיל שם מתחם (Domain), המאפשר לזהות את השירות ולהבין שמדובר בקישור מקוצר.

השירות מסייע למנוע את 'שבירתן' של כתובות אתרים ארוכות בעת העתקתן (כלומר, העתקה חלקית שלא תאפשר הגעה לעמוד המבוקש); מאפשר הכלתן של כתובות אתרים ארוכות ללא מעברי שורה; ומסייע להצגה אסתטית יותר של תכנים המכילים קישור.

קיים פן נוסף לשימוש בקישור מקוצר, שייתכן שאינו מוכר לרוב הציבור. שימוש בקישור מקוצר מאפשר גם **תיעוד ומעקב** של פעילות המשתמש ביחס לקישור, על-ידי החברה נותנת השירות. זאת, **בנוסף** לניטור ותיעוד ומעקב המבוצעים על-ידי בעלי האתר, או חברות המתמחות באיסוף מידע במרשתת.

כך, קישור מקוצר מאפשר לעקוב אחר הגישה לכתובת האתר ולנהל אותה, בעזרת תכונות שונות, כמו ניתוח הקשות. ביכולתו של הקישור המקוצר לתמוך בפרמטרים המשמשים גורמים עסקיים למעקב (UTM[2]) אחר אפקטיביות של קמפיינים שיווקיים מקוונים, אחר מקורות תנועה במדיות פרסום שונות ועוד.

דוגמאות לשירותי קיצור קישור:

- **"Bitly"** – אחד מהכלים הנפוצים לקיצור קישורים. השירות החינמי מאפשר לקצר קישורים באמצעות שם המתחם Bit.ly. שירות הפרימיום בתשלום מאפשר להשתמש בשם דומיין המותאם אישית. לשירות Bitly בתשלום ישנו תכונות נוספות, למשל, מיקוד על קישורים.

[2] UTM – Urchin Tracking Module. ראה:
https://support.google.com/urchin/answer/28307?hl=en

המיקוד מאפשר לעקוב אחר קישורים בודדים, לקבל ניתוחים לגביהם בלוח מחוונים אישי (Dashboard) ולמדוד ביצועי קמפיינים שיווקיים באופן ספציפי.

- **"TinyURL"** – השירות מציע פתרון לקיצור כתובות אתרים לשימוש אנונימי. הוא מאפשר להתאים באופן אישי את המחרוזת שתוצג בכתובת האתר המקוצרת. TinyURL הוא אנונימי לחלוטין – אין צורך ליצור ולהתחבר לחשבון. עם זאת, הוא אינו מציע ניתוחים או תכונות מתקדמות אחרות.
- **"Ow.ly"** - כלי נוסף לקיצור כתובות אתרים המונגש כחלק מחבילת תוכנה בשם Hootsuite[3], המשמש לקיצור קישורים עבור המשתמשים ברשתות חברתיות.
- **"Rebrandly"** – השירות מציע טכנולוגיית קיצור קישור מתקדמת עמוסה בתכונות, ליצירת קישורים קצרים המותאמים אישית, כגון, בניית קישור קצר לשיתוף ברשתות חברתיות.
- **"T2M"** – כלי נוסף ברשימת מקצרי קישורים, המאפשר להקל על מעקב אחר כתובות אתרים. הכלי בעל שני לוחות מחוונים נפרדים: האחד מיועד לניתוח מיקום, והשני מיועד לזיהוי מכשיר או פלטפורמה. בנוסף, השירות מאפשר יצירת קוד QR עבור הקישור המקוצר.

לצד היתרונות בשימוש בקישור מקוצר, כתובות אתרים מקוצרות עלולות להוביל את הגולשים, המקישים עליהן, לאתרים המכילים סיכוני האבטחה, וחושפות אותם לפגיעה בפרטיותם. בנוסף, שימוש בקיצור מקושר חושף גם את בעלי האתר, המבקשים לעשות בו שימוש, לסיכוני אבטחה ולפגיעה בפרטיותם. להלן, נמנה בקצרה את הסיכונים האמורים.

3. <u>סיכוני אבטחה ופרטיות הטמונים בשימוש בקישור מקוצר</u>

3.1 סיכון סייבר למשתמש – לאן מוביל הקישור?

בשונה מהקלקת כתובת מלאה של אתר (למשל, בתוצאה שעולה במנוע חיפוש או קבלת מסרון עם קישור לכתובת אתר ממכר), שמבחינה פשוטה שלה ניתן לראות האם מדובר באתר מאובטח (עם תחילית https, או אתר ממשלתי (עם סיומת gov.il למשל) או מוכר למשתמש, אחד מסיכוני האבטחה הבסיסיים ביותר הגלומים **בלחיצה על קישור מקוצר** הוא **שלא ניתן לדעת לאן מופנית הקריאה עם הלחיצה עליו**. לכן ייתכן שלחיצה על קישור מקוצר שנחזה על פניו להיות תמים (כי כולל למשל שם של חברה מוכרת), יוביל למעשה ליעד זדוני (למשל – אתרים המארחים תוכנות זדוניות, כסוסים טרויאניים ודומיהם; אתרים הבנויים לנצל סיכוני אבטחה בדפדפן או במערכת ההפעלה; אתרי דיוג ("פישינג") מתחזים לצורך גניבת מידע אישי; או אתרים המשמשים למתקפות Spam).

אם כן, למעשה, בעת לחיצה על קישור מקוצר, המשתמש נאלץ לסמוך על אמינותו של שולח הקישור. לנוכח התגברותן של מתקפות דיוג והתחזות למטרת גניבת מידע אישי, מדובר בסיכון

[3] ראה: https://www.hootsuite.com

ממשי. לכן, ישנם ארגונים אשר מנחים את עובדיהם להימנע מהקשה על קישורים מקוצרים, וחוסמים כל גישה באמצעותם, במסגרת מדיניות האבטחה הארגונית.

3.2 סיכון לפרטיות המשתמש

קישור מקוצר מאפשר לעקוב אחר הגישה לכתובת האתר ולנתח את מרכיביו השונים, כגון ניתוח הקשות בדף האתר, תדירות ביקורים באתר ועוד. ביכולתו לתמוך בפרמטרים המשמשים גורמים עסקיים למעקב (UTM[4]) אחר אפקטיביות של קמפיינים שיווקיים מקוונים, לעקוב אחר מקורות תנועה במדיות-פרסום שונות ועוד.

משמעות הדבר היא ששימוש בשירות מקוצר מאפשר ניטור של פעילות המשתמש ואיסוף נתונים רבים על פעילותו ביחס לקישור, **על-ידי צד שלישי**. זאת, מבלי שהמשתמש נתן הסכמתו לכך, ואף מבלי שהמשתמש מודע לכך. לנתונים האמורים, הנאספים בידי החברות המספקות את שירות הקישורים המקוצרים, יכול להיות ערך כספי רב, והמידע שנאסף עלול להגיע לידי גורמים נוספים תמורת תשלום.

3.3 סיכונים לפרטיות בעלי האתר

בעל האתר עשוי לסבור בטעות כי השם החדש שניתן לקישור, במסגרת יצירת הקישור המקוצר, מגן מפני גישה לא מורשית לכתובת הקישור המלאה. זאת, מאחר שהקישור מעורבל (ערבול הוא המרת מחרוזת הקישור ויצירת מחרוזת אקראית וייחודית שמסתירה את הפרמטרים בה), ולכאורה המידע מוגן. ואולם, בשיתוף קישור מקוצר, אף אם הוא מעורבל, ללא הגנה נוספת על מקור המידע שהקישור מוביל אליו, יש משום סיכון לפרטיות בעלי האתר. לכן, מדובר למעשה בתחושת ביטחון בלבד, מבלי שניתנת הגנה לפרטיות בעלי האתר בפועל, מאחר שעצם יצירת הקיצור אינה מאבטחת את המסמכים או את תוכנם. כך, קיימות דוגמאות רבות להשלכות החמורות על האבטחה והפרטיות בשירותי ענן, במקרים בהם קישור מקוצר הפנה למסמך או למקור מידע מקוון, אשר שותף על ידי משתמש בשירות ענן, וחשף אותו לכלל ציבור הגולשים.

הסיכון נובע מכך שבפועל, כל מי שמחזיק בקישור המעורבל יכול להמיר אותו לאחור (Reverse engineering) ולחלץ ממנו את הקישור המקורי, ובהמשך לכך להגיע למידע השמור בקישור. זאת, באמצעות תכונת "תצוגה מקדימה" ששירות קיצור הקישור מציע, שמאפשרת לצפות בכתובת האתר המלאה (לדוגמה, בהקשה על פקד preview בשירות tinyurl או בהקשה על פקד '+' בשירות bit.ly).

הסיכון החמור ביותר הוא חשיפת הקישור – והמידע השמור בו – ברשת, אף אם מקפידים לערבל את הקישור המקוצר למקור-המידע ולשתפו רק עם משתמשים מורשים. יש לקחת בחשבון **שקיים סיכון ממשי כי הקישור המקוצר (ובצמוד לו הקישור המלא), ייחשף ברשת,**

[4] ראה הערת-שוליים 2.

באופן פומבי, ויוכל להגיע לידיהם של גורמים לא רצויים. כתוצאה מכך, ייתכן שלכל גורם תהיה גישה למידע בכל נקודת זמן, וזאת גם לאחר שיפוג תוקפו של הקישור המקוצר. זאת, לנוכח פעילות למפתוח (מפתוח, בלעז index, הוא יצירת מפתח שמאפשר גישה מהירה לרשומת מידע) על-ידי מנוע חיפוש או זחלן רשת (web crawler – תוכנה לסריקת רשת באופן אוטומטי ושיטתי).

כך, כל קישור שנשלח בהודעה מבעל המידע למשתמש אחר, עשוי להישלח הלאה למשתמשים נוספים; כל הקשה על קישור מקוצר למסמך המאוחסן באתר של Google, תתועד במערכות האתר או השירות בו נוצר הקישור, ברשת בה המשתמש גולש, ובדפדפן שלו. הכתובת למסמך תתועד וכל מי שרשאי לגשת לדוחות האתר, השירות או הדפדפן, יוכל לפתוח את המסמך, ללא כל הזדהות נוספת. כיום, קיימים כלי חיפוש,[5] שמנצלים חולשה זו, וסורקים את הרשת במטרה לאתר קישורים מקוצרים. לבסוף, קישור מקוצר הוא ייחודי, ולכן עלול לזהות את יוצרו. גורם זדוני אשר ביכולתו להצליב מידע, עלול לזהות קשר אפשרי בין הקישור המקוצר הייחודי לבין מי שהשתמש בו.

קיימות דוגמות לאירועי אבטחה שבהם תיעוד קישור מקוצר הוביל לחשיפת הכתובת המלאה וכתוצאה מכך לדליפתו של מידע רגיש לרשת, וזאת ללא ידיעת בעל השליטה במאגר המידע, וממילא מבלי שניתנה הסכמת נושאי המידע לחשיפת מידע כה רגיש אודותיהם באופן פומבי, ולהפסקת השימוש בקישורים מקוצרים כתוצאה מכך:

- בשנת 2016 נחשף, כי כאשר מדובר בשירותי אחסון ענן כמו מיקרוסופט OneDrive או גוגל דרייב, הקישור המקוצר עלול להוביל לדליפתו של מסמך רגיש. בנוסף מתאפשרת הזרקת תוכן זדוני לחשבונות פרטיים נעולים, אשר משוכפל אוטומטית לכל המכשירים של בעל החשבון.
- לדוגמה, במקרה של שירותי מיפוי מקוונים כמו מפות Google, כתובות אתרים מקוצרות שימשו כנקודות מוצא לחשיפת נתונים ומידע נוסף של משתמשים. משתמשים שיתפו קישורים מקוצרים אשר כללו הוראות ניווט למתקנים רפואיים; למרכזי הפלות; למרכזי בריאות הנפש; למוקדי טיפול בהתמכרות; לבתי כלא ובתי מעצר לנוער; לבתי תפילה; ולמקומות רגישים אחרים. באמצעות הצלבת מידע זה עם מידע אחר שפורסם באופן ציבורי, ניתן היה להגיע למסקנות בדבר זהות המשתמשים וקשריהם החברתיים, ולחשיפת מידע אישי ורגיש אחר.
- עם חשיפת חורי אבטחה בשירות OneDrive, מייקרוסופט השביתה את קיצור כתובות אתרים מבוסס bit.ly, ופעלה לשינוי מבנה כתובות ה-URL שלה, במטרה למנוע גישה לא

[5] ראה Grayhatwarfare Short Url Serch Engine tool:
https://shorteners.grayhatwarfare.com/

מורשית מכתובת מקוצרת. כך נמנעה כל אפשרות לאחזור נתונים של משתמש אחד בידי משתמשאחר.

- יחד עם זאת, סריקה שהתבצעה לאחרונה על כתובות אתרים מקוצרים הניבה 227,276 מסמכי OneDrive נגישים לציבור, כולל עשרות אלפי קבצי PDF ו-Word, גיליונות אלקטרוניים, קבצי מדיה וקבצים בינאריים, שניתנים להפעלה (Executables).
סריקה דומה של 100,000,000 קיצורים אקראיים בני שבעה תווים של bit.ly הניבו 1,105,146 מסמכי OneDrive נגישים לציבור, שרבים מהם הכילו מידע פרטי או רגיש.[6]
הסריקה הוכיחה, כי 7% לערך מתיקיות OneDrive שנחשפו בסריקה התירו גישה מלאה לכתיבה. הרשאה זו מאפשרת לשתול בתיקיה תוכנות זדוניות, אשר משוכפלות אל המכשירים השונים של המשתמש, המחוברים לחשבון ה-OneDrive.
בנוסף, אין צורך לנחש את ערכי הפרמטרים של כתובת ה-URL כדי לקבל גישה לשאר קבצי המשתמש המאוחסנים ב-OneDrive. בהשגת כתובת ה-URL של מסמך אחד, ניתן לנצל את מבנה התחביר של שאר ה-URL ב-OneDrive כדי לסרוק את היררכית הספריות של החשבון ולבצע אינומרציה[7] לחשיפת שאר התיקיות והקבצים.

אשר על כן, לצד היתרונות הגלומים בקיצור הקישורים, טבוע בו סיכון ממשי לפגיעה בפרטיות נושאי מידע, שבעלי האתרים בהם מוחזק אותו מידע, יצרו עבורם קישור מקוצר. זאת, מאחר שגם אם בעליו של המידע דאג לא לפרסם את הקישור המקוצר, ולשתפו רק באופן פרטי, עתה באמצעות מנועי חיפוש ודומיהם, הקישור הופך להיות גלוי והמידע מאחוריו חשוף לציבור.

אם כתובת הקישור המקוצרת מובילה למידע שאינו מאובטח כיאות, כלומר, אינו מוגבל בהרשאות גישה, אינו מוצפן או אינו נעול בסיסמה, המידע עשוי להיחשף ולהפוך לנחלת הכלל.

בהתאם להוראות חוק הגנת הפרטיות ותקנותיו, **קישור למידע המהווה חלק ממאגר מידע, בין אם מקוצר ובין אם לאו, חייב להיות מוגן ומאובטח ולמנוע מגורם לא מורשה גישה למידע**.

4. <u>המלצות להגברת האבטחה וההגנה על נכסי המידע</u>

4.1 המלצות לבעלי האתרים

4.1.1 המלצת הרשות העיקרית היא להמעיט בשימוש בשירותי קיצור קישורים, ככל הניתן. זאת, כאמור, בשל העובדה שכתובות אלו מתועדות על ידי צדדים שלישיים.

4.1.2 יש להימנע משימוש בכתובת מקוצרת לאתר בו נדרשת הזדהות בכניסה אליו. זאת, כאמור, מכיוון שברגע בו המשתמש הקיש על הקישור המקוצר, תעבורת הרשת

---

[6] ראה:
https://www.pcmag.com/news/url-shorteners-convenient-but-a-potential-security-risk

[7] אינומרציה - מונח המשמש בדרך כלל במתמטיקה ובמדעי המחשב כדי להתייחס לרישום של כל היסודות בסט מסוים. זוהי פעולת ספירה בדגש על קביעת מספר האלמנטים שמכילה ערכה, ליצירת רשימה מלאה ומסודרת של כל הפריטים באותה ערכה לצורך יצירת מפתוח (Index).

עוברת דרך השרת של נותנת השירות, שהיא צד שלישי למשתמש ולאתר, ויכולה לנטר את פרטי ההזדהות של המשתמשים.

4.1.3 במידה והתקבלה החלטה להשתמש בקישור מקוצר, יש להתריע לציבור המשתמשים לאן היא מובילה (ואפילו להוסיף לצידה את הכתובת המלאה, לשימוש המשתמשים החוששים). יש לזכור – פושעי סייבר משתמשים בכתובות מקוצרות על מנת להפנות משתמשים ברשת לאתרי דיוג, לגנוב מהם מידע אישי ולשתול תוכנות זדוניות במחשביהם.

4.1.4 יש לוודא כי המידע באתר מוגן מפני גישה לא מורשית, וכי לכל משתמש ישנה הרשאת גישה המתאימה למידע אודותיו, כאשר על מנת לממשה יידרש המשתמש להזדהות ברמה העונה על סיכוני האבטחה ומידת רגישות המידע.

4.2 המלצות למשתמשים

4.2.1 אם קיבלתם קישור מקוצר אשר אתם סומכים על מקורו, השתמשו בתכונת התצוגה המקדימה של שירות הקיצור, כדי לצפות בתצוגה מקדימה של כתובת האתר המלאה. לשם כך, הקלידו את כתובת האתר המקוצרת בשורת הכתובת של דפדפן האינטרנט והוסיפו את התווים או המילים המוצגים להלן:

- preview - לתצוגה מקדימה בשירות tinyurl.com יש להוסיף את המילה preview בין מקטע ה-"http://" לבין מקטע ה-"tinyurl". לדוגמה: http://preview.tinyurl.com/znt7xnzu
- בשירות bit.ly יש להוסיף בסוף המחרוזת של כתובת האתר את התו "+" (plus). לדוגמה: http://bit.ly/2lgKepi+

4.2.2 יש לנסות ולהזין את כתובת האתר הקצרה באתר בדיקה. זאת, במטרה לצפות בכתובת האתר המלאה. להלן מספר אתרי בדיקה:
getlinkinfo.com; unshorten.it; urlxray.com.

4.2.3 אמצעי אבטחה נוסף, שעשוי להגן על המשתמש טרם הקשתו על הקישור, הוא בדיקת כתובת הקישור המקוצרת באמצעות סורק וירוסים דוגמת VirusTotal.[8]

4.2.4 <u>אם אין ביטחון מוחלט במהימנות הקישור המקוצר אין להקיש עליו!</u>
לבסוף, המלצתנו העיקרית לגולש היא להגן על המידע שלו בשעה שהוא מתחבר לשירותים מקוונים. מומלץ להקפיד על האמצעים הבאים:

א. **סיסמה חזקה** – סיסמה חזקה, ארוכה ושונה לכל חשבון, והחלפתה בתדירות גבוהה.[9]

---

[8] ראה: https://www.virustotal.com/gui/home/upload

[9] ראה: https://he.wikipedia.org/wiki/%D7%97%D7%95%D7%96%D7%A7_%D7%A1%D7%99%D7%A1%D7%9E%D7%90%D7%95%D7%AA

ב. **אימות דו-גורמי** – אימות דו-גורמי בכניסה לכל חשבון, ובמידת האפשר אבטחת החשבון בהתקן אימות חומרה (מפתח פיזי), שנתמך על ידי חברות תוכנה. [10] באופן כללי, התקן זה מגן גם על הגישה למחשבים, לרשתות ולשירותים מקוונים, התומכים בסיסמאות חד-פעמיות (OTP).[11]

5. <u>השורה התחתונה</u>

לצד היתרונות הגלומים בשימוש בקיצור קישורים, אל לנו לשכוח כי הוא גם בעל חסרונות, שבראשם הפגיעה בפרטיות בעלי האתרים והמשתמשים. זאת ועוד, יש לקחת בחשבון שכתובות אתרים מקוצרות עלולות להוביל את הגולשים המקישים עליהן, לאתרים המכילים סיכוני האבטחה.

לכן מומלץ להימנע משימוש בשירותי קיצור קישורים, ככל הניתן. אם לא ניתן, מומלץ לשקול חלופות אחרות, טרם יצירת כתובת מקוצרת או שיתופה.

לבסוף, המלצתנו לגולש היא להשתדל להשתמש באמצעים קיימים במטרה להגן על המידע שלו בשעה שהוא מתחבר לשירותים מקוונים.

---

[10] ראה:
https://he.wikipedia.org/wiki/%D7%AA%D7%A7%D7%9F_FIDO

[11] ראה סיסמה חד-פעמית:
https://he.wikipedia.org/wiki/%D7%A1%D7%99%D7%A1%D7%9E%D7%94_%D7%97%D7%93-%D7%A4%D7%A2%D7%9E%D7%99%D7%AA