



הרשות לפיתוח
כלכלי-חברתי
של המגזר החרדי
במשרד ראש
הממשלה מציגה:

**הרשות
החרדית**
שירותי ממשל בהתאמה חרדית
ורשות לפיתוח כלכלי וחברתי של המגזר החרדי



**מדריך
לנדרשים
לשירותים
דיגיטליים**

הרשות החרדית

שירותי ממשל בהתאמה חרדית
הרשות לפיתוח כלכלי חברתי של המגזר החרדי



מיזמים אסטרטגיים

מבצע:

תלם - אסטרטגיה
שילוב ופרויקטים בע"מ

כתיבת תוכן מקצועי:
מוטי רייך

עריכת תוכן ועריכה לשונית:
עזרא כהן

תוכן העניינים

7.....	על המדריך.....
9.....	חלק א - קבלת שירות ללא אמצעים דיגיטליים.....
10.....	1. אופני קבלת שירות ללא אמצעים דיגיטליים.....
13.....	2. דוגמאות לקבלת שירותים ממשלתיים ללא דיגיטל.....
14.....	3. שירותים עירוניים.....
16.....	4. תחבורה ציבורית.....
17.....	5. שירותי חירום.....
18.....	6. שירותי למידה.....
18.....	7. מימוש זכויות.....
20.....	חלק ב - חלופות דיגטליות לבעלי טלפון כשר.....
21.....	1. פתרונות לאימות דו-שלבי וקבלת SMS.....
25.....	2. פתרונות תקשורת במחשב.....
31.....	3. שאלות ותשובות נפוצות.....
32.....	חלק ג - שימוש בטוח ברשת.....
33.....	1. תעודת זהות חכמה - מהי ולמה היא חשובה.....
35.....	2. שימוש בטוח בעמדות ציבוריות.....
37.....	3. בחירת כתובת מייל ואבטחת חשבון המייל.....
41.....	4. זיהוי והתמודדות עם הונאות דיגטליות.....
45.....	5. הגנה על המשפחה בשימוש בג'ימיל.....
49.....	6. סמלים ואמצעי זיהוי בתקשורת דיגטלית.....
51.....	7. סיכום.....
53.....	נספח - מילון מונחים.....

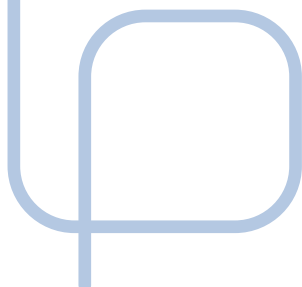
דבר סגן השר הרב אורי מקלב

סגן שר במשרד ראש הממשלה וסגן שר במשרד התחבורה

במסגרת תפקידיה הרבים של הרשות החרדית במשרד ראש הממשלה, היא ממונה גם על הנגשת השירותים הממשלתיים לציבור החרדי וטיוב הממשקים, על מנת לסגור פערים של מחסור במידע ואי מיצוי זכויות ואפשרויות. פערים אלו של אי נגישות לשירותי הממשלה היו גם לפני עידן הדיגיטציה, ונבעו בדרך כלל מחוסר היכרות של מקבלי ההחלטות עם צרכי המגזר או אי התאמה תרבותית. המעבר של רוב שירותי הממשלה לפלטפורמה דיגיטלית לא שיפר את המצב ובמובן מסוים הקשה אף יותר על קבלת שירותי ממשלה באופן מותאם לציבור החרדי, בשל בחירתו להתרחק מאוד מן השימוש ברשת האינטרנט. בלשכתי מתקבלות פניות רבות של אזרחים המלינים על כך שאינם יכולים לקבל שירותים כאלו ואחרים, וזאת במקרים בהם הם מודעים לקיומם של השירותים הללו. אחרים גם אינם יודעים את זכויותיהם או את האפשרויות הקיימות ואינם מתלוננים.

הרשות שוקדת על פתרונות שאינם דורשים שימוש באינטרנט, כגון קבלת אותם השירותים באמצעות הטלפון ודרכים נוספות. אך לצד זאת ועבור מי שמתמש במייל, או באינטרנט מסונן לפי הוראת רבותיו, מוצע מדריך זה. כפי שלימדונו רבותינו, גם בשעה שיש היתר להשתמש, מתקיים העיקרון של "הקל הקל תחילה". מדריך זה, המיועד לנדרשים לשירותים דיגיטליים, פותח בחלופות הלא דיגיטליות, על מנת לאפשר את מלוא השירותים ללא שימוש באמצעים טכנולוגיים. החלק השני עוסק בשירותים טכנולוגיים באמצעות טלפון כשר, והשלישי מספק פתרונות למי שקיבל היתר להשתמש ברשת, על מנת לעשות זאת באופן זהיר ללא סיכונים רוחניים וגשמיים. תפילתנו שלא נבוש ולא ניכשל ולא ניכלם לעולם ועד.

אורי



• דברי ברכה

אני מתכבד לברך על פרסום המדריך המונגש לשירותים דיגיטליים, אשר מהווה אבן דרך נוספת בפעילותה של הרשות לפיתוח כלכלי-חברתי של המגזר החרדי- למען הציבור, ומתוך מחויבות אמיתית לשוויון הזדמנויות.

בעידן שבו העולם הציבורי והממשלתי עובר תהליכי דיגיטציה מואצים, חשוב לזכור שישנם אזרחים שהדיגיטציה הממשלתית אינה מותאמת עבורם על פי אורחות חייהם.

מדריך זה נועד להבטיח כי גם עבורם - קבלת שירותים, מימוש זכויות ונגישות למידע - יהיו זמינים, פשוטים וראויים.

הרשות שמה לה למטרה לצמצם פערים, להסיר חסמים ולפתח מענים מותאמים לאורח החיים החרדי - הן באמצעים טכנולוגיים ייחודיים, הן בחיזוק החלופות הלא-דיגיטליות והן בשיח מכבד עם הקהילה עצמה.

המדריך משקף הבנה עמוקה של השטח ומחויבות לפתרונות אמיתיים. אני מברך את כל השותפים לעשייה, ומייחל שמדריך זה יהיה לכל בית ולכל אזרח חרדי - כלי עזר שימושי ומעצים.

בהערכה ובברכה,

רועי אסף.

ראש הרשות לפיתוח כלכלי-חברתי של המגזר החרדי.

משרד ראש הממשלה.

• דברי ברכה

בשנה האחרונה, בהובלת סגן השר הרב מקלב, ובסיוע מיקצועי של חברת תלם, מיקדה הרשות את האתגרים העומדים לפתחו של מי שאינו משתמש בטלפון חכם, במובנים של צריכת שירותים ציבוריים, בכל מה שקשור לקבלת שירותי ממשלה.

מחקר שערכנו הראה כי האתגר היותר משמעותי לאנשים רבים הוא אתגר ההזדהות, הפעולה של "להכנס לאזור האיש" הופכת מסורבלת למי שאינו יכול לאשר את זהותו. אתגרים נוספים מופו, ונבחרו שני כלים לשימוש הציבור.

כלי אחד העוסק באתגר ההזדהות טרם הושלם, ועל השקתו תבוא הודעה נפרדת.

את הכלי האחר אתם מחזיקים בידכם עכשיו. המדריך לנדרשים לשירותים דיגיטליים כולל בתוכו כלים שימושיים, שיכולים להיות לעזר לאותם שמבקשים לצרוך את השירותים- עם מינימום שימוש בטכנולוגיה מתקדמת.

המדריך הזה הוא הראשון מסוגו, והוא מגלם אמירה- מדינת ישראל מנגישה ותמשיך להנגיש את כלל השירותים שלה לאוכלוסיות בכל רמה טכנולוגית.

אני מודה לחברת תלם על העבודה המקצועית, ובפרט לאיש המקצוע המעולה מוטי רייך, שבהיכרותו את שני העולמות, העולם החרדי ועולם הטכנולוגיה, היה לנו לעזר רב.

ויה"ר שלא תצא תקלה תחת ידינו, ושהמדריך יהיה לעזר רב לנדרשים לו.

בהערכה ובברכה,

הלל ואזנר

ראש תחום בכיר מחקר ואסטרטגיה

על המדריך •

הרשות לפיתוח כלכלי חברתי של המגזר החרדי הוקמה בשנת תש"פ (2020), על מנת לתכלל את המענים לצרכי המגזר החרדי במקום אחד, ועל ידי כך להביא למדיניות מותאמת יותר ופתרונות מדויקים יותר עבור האזרחים החרדיים. הרשות עוסקת בכלל היבטי הממשלה - בריאות, רווחה, הכשרות מקצועיות ועוד.

המעבר של שירותים ממשלתיים לפלטפורמות דיגיטליות מקשה על אלו הבוחרים לצמצם את השימוש באינטרנט.

אתגרים כמו טפסים מקוונים וגישה למידע דיגיטלי מהווים מכשולים יומיומיים. הרשות פועלת להנגשת שירותים ממשלתיים בהתאמה לדפוסי השימוש המקובלים בקהילה החרדית, ולפיתוח פתרונות זיהוי שאינם דורשים אינטרנט או טלפון המקבל הודעות בנוסף לשיחות קוליות.

המדריך שלפניכם נועד לספק מענה מעשי לאתגרי הדיגיטל עבור המגזר החרדי, והוא כולל שלושה חלקים מרכזיים:

חלק א - שירותים ללא אינטרנט: מתמקד בהדגשת החלופות הלא-דיגיטליות לקבלת שירות מלא ללא שימוש באמצעים טכנולוגיים;

חלק ב - חלופות דיגיטליות: מציע חלופות לשירות דיגיטלי לבעלי טלפון כשר, כולל פתרונות לטלפונים כשרים ושימוש בעמדות ציבוריות;

חלק ג - בטיחות ברשת: מספק דגשים על שימוש בטוח בדיגיטל ומניעת סיכונים.

הכל מתוך הבנה עמוקה של צרכי הציבור החרדי ומתוך מחויבות להבטיח שכל אזרח יוכל לממש את זכויותיו ולקבל שירותים באופן התואם את אורח חייו.

המדריך נערך בשיתוף עם רבנים ואנשי מקצוע מהמגזר החרדי במטרה לספק פתרונות מעשיים המתאימים לאורח החיים החרדי

על אף שהעולם
סביבנו הופך
לדיגיטלי, חשוב
שתדעו: החוק מחייב
את הרשויות להמשיך
לספק שירות גם
בדרכים המסורתיות.
רשויות, עיריות וגופים
ציבוריים חייבים על
פי חוק לספק חלופות
נגישות לשירות
הדיגיטלי.

חלק א קבלת שירות ללא אמצעים דיגיטליים



איך מתחילים?

מוקד ממשלתי 1299



שיחה אחת ואתם מקבלים מידע על כל משרד ממשלתי

מוקד טלפוני זה משמש כקו מידע ראשוני עבור כלל משרדי הממשלה בישראל.
דרך שיחה אחת ניתן לקבל מידע עדכני על שעות קבלת קהל, מיקומים של לשכות
וסניפים, סוגי השירותים הניתנים, והדרכים להגשת בקשות.

המוקד פועל בימים א'-ה', בשעות 08:00 - 19:00, ומאויש על ידי נציגים מוסמכים
אשר יכולים להפנות אתכם ישירות למוקד הרלוונטי או להדריך אתכם כיצד לפעול.

1. אופני קבלת שירות ללא אמצעים דיגיטליים:



א. פנייה ישירה למשרדי הרשויות

כדי לקבל שירות פיזי ממשרדי ממשלה ורשויות, מומלץ **לקבוע תור מראש, להביא תעודה מזהה ומסמכים מקוריים** רלוונטיים. לבירור אופן זימון התור, כתובת הסניף המבוקש ושעות הפעילות יש לפנות למוקד המידע הממשלתי **1299**.



ב. מוקדי שירות טלפוניים

הטבלה הבאה מרכזת עבורכם את המוקדים הטלפוניים של השירותים הציבוריים השונים בהתאם לנושאי הפניות בהן מטפל כל מוקד.

המוקד	סוג שירות		נושאי פנייה
1299		מידע ממשלתי כללי	מידע על כל משרדי הממשלה, שעות פעילות ומיקומי סניפים
*3450		רשות האוכלוסין	חידוש תעודות זהות ודרכונים, הנפקת ספחי תעודת לידה או פטירה
*4954		רשות המיסים	בקשת החזרי מס, הגשת דוחות שנתיים, טיפול בעיקולים וחובות מס
*5678		משרד התחבורה	חידוש רישיונות נהיגה, תשלום אגרות רישוי רכב, עדכון בעלות רכב
*8787		תחבורה ציבורית	מידע על קווים, תחנות ועמדות טעינת רב-קו
106		מוקד עירוני	כל השירותים העירוניים, דיווח על מפגעים
100		משטרה	מצבי חירום, פריצות, תאונות

* מספר 106 פועל בעיקר בערים ויישובים מרכזיים. במועצות אזוריות ויישובים קטנים לרוב אין 106, ויש לפנות במספר טלפון ייעודי.

המוקד	סוג שירות	נושאי פנייה
101	 מגן דוד אדום	מקרי חירום רפואיים
102	 נבואה השירות הראשי לרפואה	שריפות ומצבי סכנה
104	 פיקוד העורף	הנחיות בשעת חירום
*8840	מוקד מידע לאזרחים וותיקים	עזרה לאזרחים וותיקים
1-800-800-818	 נציבות שוויון בעבודה	אפליה בעבודה
*5400	 מוקד "קול הבריאות" של משרד הבריאות	זכויות רפואיות
*6552	 משרד החינוך	רישום למוסדות חינוך בירורי סטטוס זכאות/קבלה
*5442	 משרד הבינוי והשיכון	זכאות לדיוור ציבורי וסיוע בשכר דירה
*2994	 משרד העלייה והקליטה	סיוע לעולים חדשים
*9276	 נציבות שירות מדינה	פרסום מכרזים ומידע על תפקידים פתוחים
*2496	 יד מכוונת ייעוץ והכנה למוסדות לביטוח לאומי	ייעוץ והכנה לוועדות הרפואיות בחינם



ג. עמדות שירות עצמי

עמדות שירות עצמי פזורות ברחבי הארץ ומאפשרות לכם לבצע מגוון פעולות בקלות ובמהירות, ללא צורך בהמתנה בתור במשרדי הממשלה. באמצעות העמדות תוכלו לעדכן פרטים אישיים, להדפיס אישורים, לשלם אגרות ולקבל מידע - בזמנכם הפנוי ובהתאם לשעות הפתיחה של מיקום העמדה. פשוט הגיעו לעמדה הקרובה למקום מגוריכם, הזדהו באמצעות תעודת זהות או רישיון נהיגה, ובצעו את הפעולה המבוקשת במהירות ובנוחות.

■ היכן מוצאים עמדות שירות עצמי?

- במשרדי ממשלה וגופים ציבוריים
- בקניונים ומרכזי קניות, כמו למשל בחלק מסניפי סופר-פארם במרכזי הערים
- בסניפי דואר נבחרים
- במוקדי עירייה

■ מה אפשר לעשות בעמדות?

שירותי זיהוי ומרשם אוכלוסיין: הנפקת ספח תעודת זהות, הנפקת תמצית רישום (לצורכי רישום נישואין), שינוי מען.

שירותי רכב ונהיגה: חידוש רישיונות נהיגה ורכב, ביורר מצב נקודות חובה לנהג, היתר נהיגה לנהג חדש, קבלת פרטים מעודכנים על רכב, היסטוריה ובעלויות.

תשלומים ואגרות: תשלום אגרות רישיון, תשלום קנסות, תשלום עבור דרכון ביומטרי.



שירותי מידע: כניסה לאתר 'כל זכות' המרכז את כל הזכויות, ההטבות והשירותים לאזרחי ישראל, וכולל את מערכת 'כל שאלה' - צ'אטבוט חכם המספק מענה מיידי בתחומי זכויות אזרח וממשל זמין בכל שעות היום, וכניסה לאתר-gov.il המאפשר גישה ישירה לשירותים ממשלתיים דיגיטליים, הגשת בקשות, מעקב אחר סטטוס טיפול וקבלת אישורים ותעודות מול משרדי הממשלה.



2. שירותים בדואר רגיל

חלק ממושרדי הממשלה מאפשרים הגשת פניות באמצעות דואר, כך שניתן לקבל שירות ללא צורך בהגעה פיזית למשרד. לשליחת בקשה: השיגו את הטופס הרלוונטי דרך המוקד הטלפוני, מלאו אותו בקפידה, צרפו צילום תעודת זהות עם ספח ואישורים נדרשים, חתמו במקומות המסומנים ושלחו בדואר רשום. הקפידו לציין פרטי התקשרות ושמרו את אישור המשלוח למעקב.

2. דוגמאות לקבלת שירותים ממשלתיים ללא דיגיטל



1. איך לחדש דרכון?



1. חיגו **3450*** וקבעו תור לסניף רשות האוכלוסין הקרוב לביתכם
2. הכינו את המסמכים הדרושים:
 - תעודת זהות
 - דרכון ישן (אם יש)
 - תמונת פספורט עדכנית
 - אמצעי תשלום לאגרה
3. הגיעו לסניף במועד שנקבע עם כל המסמכים
4. שלמו את האגרה במקום ותקבלו אישור על הבקשה
5. הדרכון החדש יישלח לביתכם בדואר רשום (או תינתן לכם אפשרות לאיסוף עצמי)



2. איך להגיש בקשה להחזר מס בדואר?

1. השיגו את הטופס הנדרש - טופס 135:
 - בקשו במוקד הטלפוני **4954*** לשלוח לכם את הטופס בדואר או קחו טופס מודפס ממשרד השומה האזורי
2. מלאו את הטופס בעזרת המסמכים הבאים:
 - תלושי משכורת שנתיים, אישורי הפקדות לפנסיה/קופות גמל, קבלות רלוונטיות להוצאות מוכרות
3. צרפו צילום תעודת זהות וצ'ק מבוטל
4. שלחו את המעטפה בדואר רשום למשרד השומה באזור מגוריכם
5. בדקו סטטוס הבקשה בטלפון **4954*** כעבור 4-6 שבועות



איך לחדש רישיון נהיגה?

- **בסניפי הדואר:** הציגו תעודת זהות ושלמו את האגרה
- **בעמדות שירות עצמי של משרד התחבורה:** הכניסו תעודת זהות ועקבו אחר ההוראות
- **בסניפי משרד הרישוי:** הגיעו עם תעודת זהות ורישיון נהיגה ישן

3. שירותים עירוניים



דרכי פניה לעירייה*

מוקד 106 - מענה אנושי 24/7 לכל סוגי הפניות

ביקור במשרדי העירייה - קבלת קהל בשעות הפעילות במחלקות הרלוונטיות

* מספר 106 פועל בעיקר בערים ויישובים מרכזיים. במועצות אזוריות ויישובים קטנים לרוב אין 106, ויש לפנות במספר טלפון ייעודי.





קבלת שירותים נפוצים בעירייה ללא דיגיטל

קטגוריה	סוג שירות	אופני קבלת השירות
תשלומים עירוניים	ארנונה ומים	תשלום בקופת העירייה במזומן, צ'ק או כרטיס אשראי
		תשלום בסניפי הדואר כנגד הצגת השובר המקורי
		תשלום בהוראת קבע באמצעות הגשת טופס חתום במחלקת הגבייה
הנחות וסיוע כלכלי	הנחות בארנונה	הגשת בקשה ידנית במחלקת הגבייה
	פריסת תשלומים	פנייה למחלקת הגבייה ותיאום הסדר תשלומים
שירותי חינוך	רישום למוסדות חינוך	מילוי טפסים במחלקת החינוך בתקופת הרישום
שירותי רווחה	פנייה לעובד/ת סוציאלי/ת	תיאום פגישה טלפונית דרך מחלקת הרווחה
	הגשת בקשות לסיוע	מילוי טפסים ידנית במשרדי הרווחה או שליחה בדואר
דוחות וקנסות	תשלום דוחות	תשלום במחלקת האכיפה/חניה בעירייה או תשלום בסניפי הדואר עם השובר המקורי
	ערעור על דוחות	הגשת ערעור בכתב במשרדי העירייה או שליחת מכתב ערעור בדואר רשום

4. תחבורה ציבורית



1. איך להטעין את כרטיס הרב-קו?

1. בעמדות פיזיות שנמצאים ב:

- תחנות מרכזיות ותחנות רכבת
- מרכזי קניות
- כספומטים של כספונט
- חנויות נבחרות ועמדות "נדירים פלוס" בבתי הכנסת

2. בטעינה טלפונית:

- חייגו **03-720-7406**
- הקישו את מספר הרב-קו (מופיע על גב הכרטיס)
- בחרו את הפרופיל המתאים (רגיל/נוער/אזרח ותיק)
- הזינו את סכום הטעינה ושלמו באשראי
- שימו לב! הטעינה הטלפונית נשמרת זמנית במערכת, וצריך לסנכרן אותה פיזית לכרטיס הרב-קו באמצעות תיקוף במכשיר טעינה בעמדת שירות או בעת עלייה לאוטובוס עם קורא רב-קו.



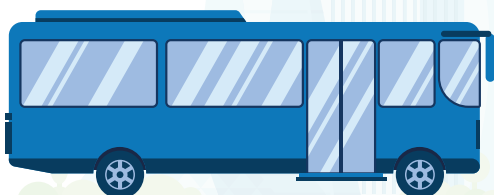
2. איך להתעדכן על שינויים בתחבורה ציבורית:

- מוקד מידע כללי: ***8787**
- מוקד מידע בזמן אמת: **1700-70-70-50**
- מודיעין בתחנות מרכזיות



3. מוקדים לבירורי תלונות והחזרים:

- במוקד ***8787** ניתן לפנות בנוגע לאיכות השירות, בעיות בלוחות זמנים, בעיות עם נהגים, נגישות לנכים ובקשות להחזרים כספיים.
- גם בעמדות "נדירים פלוס" בבתי הכנסת ניתן להגיש פניות בנושאים אלו ישירות למשרד התחבורה



5. שירותי חירום



מקורות למידע בחירום:

- מוקד מידע של פיקוד העורף: **104**
- מוקדי מידע עירוניים: **106 / 108**
- **גל שקט בשבתות וחגים בזמני חירום:**
 - רדיו כאן מורשת משמיע התרעות של פיקוד העורף מכל רחבי הארץ בתדרים **90.5 / 90.8 / 92.5 / 100.7 FM**
 - רדיו קול חי בתדרים **92.8 / 93 / 102.5 FM** משמיע התרעות של פיקוד העורף באזור השידור
 - רדיו קול ברמה - משמיע התרעה של פיקוד העורף ממוקדת לפי אזור בתדרים **92.1 / 104.3 / 105.7 / 107.6 FM**



מספרי חירום חיוניים:

- משטרה: **100**
- מגן דוד אדום: **101**
- כיבוי אש: **102**
- פיקוד העורף: **104**
- מוקד סיוע בתחומי הרווחה: **118**
- מוקד פניות של חברת חשמל: **103**
- מוקד סיוע לאזרחים ותיקים: ***8840**
- מוקד סיוע לנפגעי טראומה על רקע לאומי: **1800-363-363**



6. שירותי למידה



שירותי למידה טלפוניים - "קו ידע - שמע"

הרשות לפיתוח כלכלי-חברתי של המגזר החרדי יזמה ופיתחה שירות למידה טלפוני חדשני המיועד לציבור החרדי. "קו הידע שמע" הוא מערכת למידה זמינה לכל אחד ובכל זמן, המאפשרת רכישת ידע מקצועי וכישורים בעולם העבודה המשתנה באמצעות הטלפון בלבד.

המערכת מציעה קורסי תעסוקה מגוונים הכוללים: כישורים בעולם העבודה משתנה, כתיבת קורות חיים, מיתוג עצמי, והכנה לראיון עבודה. הקורסים מוגשים על ידי מיטב המומחים, מותאמים לאורח החיים בקהילה החרדית, ומאפשרים למידה נגישה ללא צורך באמצעים דיגיטליים. לקבלת מידע נוסף ופרטים על השירותים הזמינים, ניתן לפנות לקו בטלפון: **079-520-5235**

7. מימוש זכויות



פורטל "כל זכות"

פורטל "כל זכות" הינו מאגר מידע מקיף המרכז עבורכם את כל הזכויות האזרחיות במגוון תחומי חיים: בריאות, דיור, תעסוקה, רווחה, משפחה ועוד. המידע מוצג בשפה ברורה ונגישה, ומספק הכוונה מעשית למימוש הזכויות. באתר קיימת מערכת מקוונת המספקת מענה לשאלות בתחום מיצוי זכויות ושירותי ממשל. בפיתוח: ממשק טלפוני לאתר 'כל זכות' ולשירות כל שאלה. קיימת גישה פתוחה לפורטל בכל העמדות לשירות עצמי.



איך לפנות במקרה של הפרת זכויות:

נציבות שוויון הזדמנויות בעבודה

- **מוקד טלפוני: 1800-800-818** - לדיווח על מקרי אפליה או בירור זכויות
- **פנייה בכתב:** שליחת מכתב מפורט באמצעות הדואר המתאר את פרטי המקרה

משרד הפנים (רשות האוכלוסין וההגירה): *3450

- **שעות פעילות:** ימים א'-ה' בין השעות 08:00 עד 16:00
- **שי"ל (שירות ייעוץ לאזרח): 104** (מוקד משרד הרווחה)

נציבות פניות הציבור: 03-675-1596

המוסד לביטוח לאומי: 02-675-1596

- **שעות פעילות:** ימים א'-ה' בין השעות 08:00 עד 17:00
- **"יד מכוונת"** - ייעוץ והכנה לוועדות הרפואיות בחינם *2496

הלשכה לסיוע משפטי (משרד המשפטים): 1700-70-60-44 (שלוחה 4)

- **שעות פעילות:** ימים א'-ה' בין השעות 08:00 עד 16:00 .





חלק ב חלופות דיגיטליות לבעלי טלפון כשר

בחלק זה המדריך מציע פתרונות מעשיים המאפשרים גישה לשירותים דיגיטליים חיוניים, ללא צורך בטלפון חכם לא-כשר, עם הקפדה מיוחדת על פרטיות ואבטחת מידע, ובליטוי המלצות מותאמות למציאות הייחודית של המגזר החרדי בעידן הדיגיטלי.

1. פתרונות לאימות דו-שלבי וקבלת SMS



1.1. מספר וירטואלי

מהו מספר וירטואלי?

מספר וירטואלי הוא מספר טלפון שאינו קשור פיזית למכשיר ספציפי. הוא פועל ב"ענן" ומאפשר קבלת הודעות SMS והעברתן אליכם בדרכים חלופיות.

■ כיצד משתמשים במספר וירטואלי?

המספר הווירטואלי מאפשר קבלת קודי אימות בשתי דרכים עיקריות:

1. המרת SMS למייל:

- פתרון זה מחייב גישה לדואר אלקטרוני
- ההודעה שנשלחת למספר הווירטואלי מועברת אוטומטית לתיבת הדואר האלקטרוני שלכם
- אתם קוראים את קוד האימות מהמייל ומזינים אותו בשירות הנדרש

2. המרת SMS לשיחה קולית:

- זהו פתרון אידיאלי למי שאין לו גישה לאינטרנט כלל
- המערכת מתקשרת לטלפון הכשר שלכם
- הקוד שהגיע בהודעת SMS מוקרא בשיחה הקולית



שלב 1:

בחירת ספק ורכישת מספר וירטואלי

- בדקו ספקים אמינים המספקים שירותי מספרים וירטואליים או שירותי טלפוניה בענן לעסקים. חשוב לבדוק האם הספק פועל ברישיון, האם יש לו חוות דעת חיוביות מלקוחות עסקיים, ומהי רמת התמיכה והשקיפות שלו בתמחור ובתנאי השימוש.
- ודאו שהספק מציע את האפשרויות הרצויות: המרת SMS למייל או לשיחה, וניתוב שיחות.
- הירשמו לשירות ורכשו מספר וירטואלי (לרוב בעלות חודשית)

שלב 2:

הגדרת ניתוב והמרה

- הגדירו את המייל שאליו יישלחו ההודעות או את מספר הטלפון הכשר
- הגדירו העברת שיחות מהמספר הווירטואלי למספר הכשר
- בדקו את ההגדרות באמצעות שליחת הודעת ביקורת או ביצוע שיחת ניסיון

שלב 3:

רישום לשירות הדיגיטלי

- בעת הרישום לשירות הדיגיטלי, הזינו את המספר הווירטואלי כמספר הטלפון שלכם
- בחרו באפשרות של אימות דרך SMS (בידיעה שתוכלו לקבל את הקוד דרך מייל או שיחה)

שלב 4:

קבלת ושימוש בקוד האימות

- המתינו לקבלת הקוד במייל או בשיחה קולית
- הזינו את הקוד בשירות הדיגיטלי להשלמת תהליך האימות

■ שימושים נוספים למספר וירטואלי:

המספר הווירטואלי יכול לשמש לא רק לאימות דו-שלבי, אלא גם:

- קבלת הודעות שירות מבנקים וחברות אשראי
- קבלת עדכונים שוטפים משירותים דיגיטליים

■ יתרונות השימוש במספר וירטואלי לאימות דו-שלבי:

- **פתרון נגיש לבעלי טלפונים כשרים:** מאפשר שימוש בשירותים דיגיטליים הדורשים אימות דו-שלבי, גם ללא תמיכה ב-SMS במכשיר
- **שמירה על פרטיות:** מאפשר להימנע מחשיפת מספר הטלפון האישי לשירותים שונים
- **גמישות:** מאפשר בחירה בין אפשרויות שונות לקבלת קוד האימות (מייל או שיחה)

■ שימו לב! נקודות חשובות לבדיקה

- **עלויות:** בדקו את העלויות של שירות המספר הווירטואלי, כולל עלויות חודשיות ועלויות עבור המרת הודעות וניתוב שיחות
- **אמינות הספק:** בחרו ספק אמיין ומקצועי המבטיח שירות יציב ותמיכה טכנית
- **אבטחה ופרטיות:** ודאו שהספק נוקט באמצעי אבטחה מתאימים לשמירה על פרטיות המידע
- **תמיכה בשירותים:** בדקו האם השירות הדיגיטלי הספציפי תומך במספרים וירטואליים
- **ניתוב שיחות:** הגדירו ניתוב שיחות מהמספר הווירטואלי למספר הטלפון הכשר למקרים בהם השירות הדיגיטלי עשוי ליצור קשר טלפוני בעתיד



1.2. שימוש בקו סים של סטיק לקבלת הודעות SMS

■ מהו פתרון הסטיק?

סטיק (התקן נייד) סלולרי USB הוא התקן המשמש בדרך כלל לחיבור למייל או לאינטרנט מסונן במחשב. היתרון הגדול הוא שהוא כולל כרטיס SIM עם מספר טלפון שמאפשר קבלת הודעות SMS

■ כיצד עובד הפתרון?

קו סלולרי עצמאי: הסטיק כולל כרטיס SIM עם מספר טלפון ייחודי, המאפשר קבלת הודעות SMS בדומה לטלפון רגיל. ההבדל המרכזי הוא שהודעות אלו מתקבלות ומוצגות דרך תוכנת ניהול הסטיק במחשב ולא במכשיר טלפון. את מספר הטלפון של הסטיק ניתן לזהות דרך החשבונית החודשית של חברת הסלולר שאליה משויך הסיים.

■ איך תקבלו גישה להודעות SMS:

1. חברו את הסטיק למחשב
 2. פתחו את תוכנת הניהול של הסטיק
 3. נווטו לחלק שמציג הודעות SMS
 4. קראו את ההודעות שהתקבלו במספר ה-SIM
- שימוש בקוד האימות: כאשר קוד האימות מתקבל, הוא יופיע בממשק התוכנה. תוכלו להעתיק אותו ולהזין בשירות הדיגיטלי שדורש את האימות.

■ יתרונות השימוש בקו של הסטיק

- **נגישות פשוטה ובטוחה:** מאפשר קבלת SMS בקלות ובפרטיות, ללא צורך בטלפון חכם
- **התאמה לשימוש באינטרנט מסונן:** פתרון שמותאם במיוחד למשתמשים המחוברים לאינטרנט המסונן
- **עלות נמוכה יחסית:** מאחר והקו כבר כלול בחבילת האינטרנט המסונן, אין צורך בתשלום נוסף עבור שירות נפרד
- **פרטיות מלאה:** מספר ה-SIM של הסטיק משמש רק לצרכי קבלת SMS ואימותים, ואינו נחשף לשימושים אחרים. תוכן נוסף בנושא פרטיות ראו בחלק ג'.

■ חסרונות ופתרונות לשימוש בסטיק

תלות במחשב:

קבלת ה-SMS מתאפשרת רק כאשר הסטיק מחובר למחשב עם התוכנה.

הפתרון

תכננו מראש את זמני האימות ודאגו להיות ליד המחשב כאשר נדרשת פעולה זו

כיסוי סלולרי

ייתכנו אזורים שבהם כיסוי הרשת חלש.

הפתרון

בדקו את איכות הכיסוי באזורים לפני הרכישה

ממשק מורכב

חלק מתוכנות הניהול אינן ידידותיות למשתמשים חדשים.

הפתרון

פנו לספק האינטרנט או לאנשי תמיכה טכנית כדי לקבל עזרה בהגדרה ראשונית

2. פתרונות תקשורת במחשב



2.1 שימוש בווטסאפ (WhatsApp) ללא טלפון חכם

למי שנזקק לשירותי ווטסאפ, ישנם פתרונות המאפשרים שימוש גם ללא טלפון חכם, דרך המחשב.

■ פתרון 1:

שימוש בווטסאפ-ווב (WhatsApp Web): עם עזרה ראשונית מחבר

פתרון זה מאפשר להתקין את ווטסאפ במחשב ולהפעילו עם מספר טלפון כשר או קווי. הדבר מצריך סיוע חד-פעמי ממכר שהינו בעל טלפון חכם.

■ איך תבצעו שלב-אחר-שלב:

שלב 1:

הכנת המחשב

- הורידו את תוכנת WhatsApp Desktop מאתר WhatsApp או היכנסו לגרסת ווב בכתובת web.whatsapp.com
- התקינו את התוכנה לפי ההוראות

שלב 2:

קבלת עזרה ממכר (חד-פעמי)

- פנו למכר בעל טלפון חכם
- בקשו ממנו להוריד את אפליקציית ווטסאפ לטלפון שלו
- הרשמו עם המספר שלכם (טלפון כשר או קווי)

שלב 3:

תהליך האימות

- בחרו באפשרות אימות קולי (במקום SMS)
- קבלו שיחה לטלפון הכשר/קווי שלכם עם קוד האימות
- הזינו את הקוד שקיבלתם בשיחה

שלב 4:

סריקת קוד QR

- בעזרת הטלפון החכם של החבר, סרקו את קוד ה-QR שמופיע במחשב שלכם
- לאחר הסריקה הראשונית, תוכלו להשתמש בוואטסאפ באופן עצמאי מהמחשב

הערה חשובה: אם לחבר שעוזר לכם כבר יש ווטסאפ על הטלפון שלו, אל תבקשו ממנו להתנתק מהחשבון שלו. במקום זאת, בחרו באחת מהדרכים הבאות:

אפשרות 1 - ווטסאפ עסקי:

אם אתם מעוניינים להשתמש בווטסאפ עסקי, החבר יכול להוריד את האפליקציה "WhatsApp Business" (נפרדת מהוואטסאפ הרגיל) ולעזור לכם להגדיר אותה. כך שני הוואטסאפים יעבדו יחד על אותו טלפון.

אפשרות 2 - יישומים משוכפלים:

ברוב הטלפונים החכמים החדשים יש אפשרות להפעיל שני ווטסאפים על אותו מכשיר. חפשו בהגדרות הטלפון את האפשרות "יישומים משוכפלים", "שכפול אפליקציות" או "חשבון כפול". באמצעות זה ניתן להתקין ווטסאפ נוסף.

אפשרות 3 - משתמש אורח:

החבר יכול ליצור "משתמש אורח" בטלפון שלו, להוריד ווטסאפ תחת המשתמש החדש, לעזור לכם להגדיר, ואחר כך למחוק את המשתמש האורח. כך הווטסאפ שלו לא יושפע בכלל. כל השיטות הללו מבטיחות שהחבר יוכל להמשיך להשתמש בווטסאפ שלו כרגיל.

■ פתרון 2:

התקנת סימולטור אנדרואיד במחשב

סימולטור אנדרואיד מדמה טלפון חכם על גבי המחשב ומאפשר להתקין ולהפעיל אפליקציות אנדרואיד, כולל ווטסאפ.

■ שלב-אחר-שלב:

שלב 1:

התקנת הסימולטור:

- הורידו אחת מהתוכנות המומלצות (BlueStacks/ NoxPlayer/LDPlayer)
- התקינו את הסימולטור לפי הוראות ההתקנה
- הפעילו את הסימולטור והשלימו את ההגדרה הראשונית

שלב 2:

התקנת ווטסאפ:

- פתחו את חנות האפליקציות Google Play בתוך הסימולטור
- חפשו "WhatsApp" והתקינו את האפליקציה
- פתחו את ווטסאפ והקלידו את מספר הטלפון שלכם (כשר/קווי)

שלב 3:

אימות המספר

- בחרו באפשרות של אימות קולי ולא SMS
- קבלו שיחה למספר שהזנתם ורשמו את קוד האימות
- הזינו את הקוד בווטסאפ להשלמת הרישום

שלב 4:

הגדרת הפרופיל

- ניתן להוסיף תמונת פרופיל הגדירו את שמכם
- התחילו להשתמש בווטסאפ על המחשב

הערות חשובות

- **עדכונים עתידיים:** הפתרונות המוצעים נכונים לעת כתיבה זו, אך ייתכן שישתנו בעתיד בהתאם למדיניות של WhatsApp או מערכות ההפעלה
- **אבטחה:** בכל אחד מהפתרונות, ודאו שאתם שומרים על אבטחת המידע שלכם: אל תשתפו את קוד האימות עם גורמים זרים, ועדכנו סיסמאות באופן קבוע
- **חוקיות השימוש:** שימוש בסימולטור אנדרואיד הוא אפשרות חוקית, אך יש לשים לב לתנאי השימוש של WhatsApp
- ישנן קהילות המתירות שימוש בוואטסאפ באישור רבני הקהילה בלבד, מדריך זה הינו מדריך טכני בלבד.



2.2 שימוש זהיר בשירותים פרטיים לתקשורת דיגיטלית

שירותים פרטיים לשליחת וקבלת הודעות ווטסאפ דרך המייל

בנוסף לפתרונות שהוזכרו, קיימים גם **פתרונות חלופיים** המאפשרים לעקוף את המגבלות הקיימות ולספק פתרונות מהירים לצרכים דיגיטליים. שירותים אלה מציעים ממשק המחבר בין וואטסאפ למערכות דואר אלקטרוני, ומאפשרים למשתמשים לקבל הודעות וואטסאפ ישירות לתיבת המייל שלהם או לשלוח הודעות וואטסאפ באמצעות שליחת אימייל.

חשוב לציין שאלו אינם שירותים רשמיים של וואטסאפ אלא פתרונות צד שלישי המפעילים טכנולוגיות גישור כמו API או אוטומציה. בעוד שהם עשויים להציע פתרון חלופי, הם פותחים פתח לסיכונים אבטחה שכדאי לקחת בחשבון. המידע העובר דרך שירותים אלה נחשף למפעילי השירות, ומידת האבטחה של המידע תלויה באמינותם ובמקצועיותם. ולכן חשוב להדגיש שהשימוש בפתרונות אלו מצריך **זהירות רבה**.

למה כדאי להיזהר?

- **חשיפה למידע אישי:** שירותים מסוימים, במיוחד אלו הפועלים ללא פיקוח ברור, עלולים לאבטח בצורה לא מספקת את המידע האישי המוזן בהם
- **כוונות טובות, ביצוע בעייתי:** גם אם שירות מסוים פותח בכוונה לעזור לאנשים עם צרכים ייחודיים, אין זה מבטיח שהשירות תוכנן מתוך הבנה מעמיקה של הסיכונים האפשריים
- **מי עוד חשוף למידע שלך?** שירותים לא רשמיים עשויים לנתב את המידע דרך צדדים שלישיים, מה שמעלה את הסיכון שגורמים לא רצויים יקבלו גישה למידע רגיש

איך לוודא שאתם מוגנים?

- **בדיקת אמינות:** השתמשו רק בשירותים מספקים מוכרים ואמינים, עם המלצות מוכחות וסקירות חיוביות
- **שימוש במידע מינימלי:** אל תמסרו יותר מידע אישי ממה שנדרש
- **הימנעו משירותים מפוקפקים:** שירותים שאינם נראים רשמיים או כאלה שאינם מספקים מדיניות פרטיות ברורה - עדיף להימנע מהם
- **תמיד שאלו שאלות:** אם יש ספק - אל תהססו לשאול את נותן השירות לגבי אמצעי האבטחה ומדיניות הפרטיות

לסיכום: זהירות לפני הכול

בעידן הטכנולוגי של היום, קל להתפתות לפתרונות שנראים קלים ומהירים. המידע האישי שלכם הוא בעל ערך רב - השקיעו זמן לבדוק את מידת הבטיחות של כל שירות. גם אם הפתרון נראה זמין ונגיש, לא תמיד המחיר שווה את הסיכון. אם אינכם בטוחים - פנו לאנשי מקצוע מוסמכים לקבלת ייעוץ והכוונה.



2.3. פתרון לשיחות ועידה ווידאו

שיחות ועידה הפכו לכלי חיוני לפגישות עסקיות, לימודים מרחוק ופעילויות קהילתיות. ישנן מספר פלטפורמות עם אפשרויות גישה מגוונות, המתאימות גם למשתמשי טלפונים כשרים.

■ גישה רב-אמצעית לשיחות ועידה

"גישה רב-אמצעית" מאפשרת להשתתף בשיחות בדרכים שונות - דרך מחשב, טלפון רגיל או טלפון כשר - כך שכל משתתף יכול להתחבר באמצעי הנוח והמתאים לו.

פלטפורמות עיקריות ואופן החיבור מטלפון כשר

להלן פירוט של שלוש הפלטפורמות המרכזיות המאפשרות הצטרפות באמצעות טלפון רגיל או כשר:

תהליך החיבור הכללי לשיחות ועידה

לכל הפלטפורמות (זום, גוגל מיט ומיקרוסופט טימס), תהליך החיבור דומה:

1. בקשו מהמארגן את מספר הטלפון להתקשרות המתאים לפלטפורמה ואת הקוד הייחודי לפגישה
2. חייגו למספר הישראלי של הפלטפורמה:

• זום: **+972-3-978-6688**

• גוגל מיט: **+972-2-378-6688**

• מיקרוסופט טימס: **+972-3-763-0431**

המתינו להנחיות הקוליות והזינו את קוד הפגישה בהתאם לבקשה
הזינו סיסמה או קוד גישה נוסף אם נדרש
בחלק מהמקרים תתבקשו להקליט את שמכם לפני הכניסה לשיחה

■ טיפים יעילים למשתתפי שיחות וועידה טלפונית:

הכנה מראש:

- קבלו מראש את החומרים הרלוונטיים לפגישה (במייל, פקס או בדואר)
- הכינו את השאלות והנקודות שתצטוו להעלות
- התקשרו 5 דקות לפני תחילת הפגישה

שמיעה אופטימלית:

- השתמשו באוזניות לשיפור איכות השמע
- בחרו מקום שקט ללא רעשי רקע
- דברו ברור ובקול רם

השתתפות אפקטיבית:

- הציגו את עצמכם בתחילת כל דיבור ("זה יעקב מדבר")
- היו תמציתיים וממוקדים בדבריכם
- השתמשו בפקודות הטלפון להשקעה כשאינכם מדברים

3. שאלות ותשובות נפוצות

■ אימות דו-שלבי ו-SMS

ש: האם אפשר להשתמש במספר וירטואלי לכל שירות שדורש אימות דו-שלבי?

ת: רוב השירותים תומכים במספרים וירטואליים, אך ישנם שירותים (במיוחד בנקים ושירותים פיננסיים) שעשויים לחסום מספרים וירטואליים. בדקו מראש עם השירות הספציפי.

ש: כמה עולה מספר וירטואלי?

ת: העלות משתנה בין ספקים. בדרך כלל מדובר בעלות חודשית של 5-20 ש"ח ותשלום נוסף לפי כמות ההודעות/שיחות. חלק מהספקים מציעים תקופת ניסיון חינם.

■ ווטסאפ ללא טלפון חכם

ש: כמה זמן נשאר החיבור של ווטסאפ ווב פעיל במחשב?

ת: לרוב החיבור נשאר פעיל כל עוד אתם משתמשים בדפדפן ולא מתנתקים. בגרסת דסקטופ, החיבור נשאר עד שמתנתקים במפורש. עם זאת, לעתים נדרשת סריקה מחדש של קוד QR לאחר תקופה מסוימת או לאחר עדכונים.

ש: האם סימולטור אנדרואיד בטוח לשימוש?

ת: סימולטורים מחברות מוכרות בטוחים לשימוש, אך חשוב להוריד אותם מהאתרים הרשמיים בלבד ולהימנע מהתקנת אפליקציות לא מאומתות. כמו כן, הקפידו לעדכן את הסימולטור באופן תדיר.

■ אבטחה ופרטיות

ש: כיצד ניתן לדעת אם שירות מספרים וירטואליים אמין?

ת: בדקו את הנקודות הבאות:

- האם החברה קיימת מספר שנים?
- האם יש ביקורות חיוביות מלקוחות?
- האם יש מדיניות פרטיות ברורה?
- האם הם תומכים בהצפנה ואבטחת מידע?
- האם יש שירות לקוחות זמין?

ש: כיצד ניתן להגן על המידע בסטיק הסלולרי?

ת: הקפידו להגן על הסטיק הפיזי, הגדירו סיסמה לתוכנת הניהול, עדכנו את התוכנה לגרסה האחרונה, ומחקו באופן קבוע הודעות SMS לאחר קריאתן.



חלק א שימוש בטוח ברשת

העולם הדיגיטלי טומן בחובו סיכונים. שימוש נכון ומושכל ברשת יכול להגן על המידע האישי שלנו ולשמור על פרטיותנו. עלינו להכיר את הסיכונים ולדעת כיצד להתגונן מפניהם. בפרק זה נעסוק בדרכים לשמור על בטיחות דיגיטלית, במיוחד עבור אוכלוסיות המסתמכות על עמדות ציבוריות ושירותים דיגיטליים, ונעניק כלים מעשיים להתמודדות עם האתגרים השונים.

1. תעודת זהות חכמה - מהי ולמה היא חשובה



מהי תעודת זהות חכמה?

בשנים האחרונות, הונפקה תעודת זהות ביומטרית חכמה לכלל האוכלוסייה, והיא משמשת כאמצעי זיהוי דיגיטלי מאובטח. תעודה זו מאפשרת גישה לשירותים ממשלתיים

ומערכות דיגיטליות בצורה בטוחה ונוחה.

יתרון מיוחד לציבור החרדי: התעודה מספקת פתרון מעשי להזדהות בעמדות שירות ובמחשבים, תוך התגברות על מגבלות כמו חוסר גישה לקודי SMS במכשירים כשרים.

שימושים עיקריים של תעודת זהות חכמה

1. הזדהות במערכת הזדהות לאומית - גישה למאות שירותים ממשלתיים ואחרים
2. קבלת שירותים דיגיטליים כמו הנפקת מסמכים וביצוע תשלומים באופן מאובטח ללא צורך באימות נוסף כמו SMS.

סיסמה אישית של התעודה

הסיסמה האישית של תעודת הזהות החכמה היא קוד בן 4 ספרות שמונפק יחד עם התעודה בעת הוצאתה ברשות ההגירה והאוכלוסין. הסיסמה משמשת לאימות הזהות שלך במערכות הדיגיטליות ומאפשרת גישה לשירותים ממשלתיים בצורה בטוחה.

חשוב לדעת: הסיסמה האישית היא אחד האמצעים החשובים ביותר לשמירה על פרטיותך ולהגנה על המידע האישי שלך



■ טיפים חשובים לשימוש בתעודת זהות חכמה

הסבר	פעולות
ודאו שתעודת הזהות הופעלה לאחר קבלתה, כדי שתוכלו להשתמש בה בשירותים הדיגיטליים	הפעלת התעודה
במקרה ששכחתם את הקוד, תוכלו להגיע ללשכת האוכלוסין הקרובה לביתכם ללא תור ולקבל קוד חדש באופן מיידי	שחזור סיסמה
במידה ויש לכם קורא כרטיסים חכם, ניתן להתחבר לשירותים ממשלתיים ופיננסיים על ידי חיבור הקורא למחשב, התקנת תוכנת רשות האוכלוסין, הכנסת התעודה והזנת קוד PIN	שימוש בקורא כרטיסים
הקפידו לשמור את הסיסמה במקום בטוח ולהימנע משיתוף שלה עם אחרים	שמירה על פרטיות

■ כיצד להשתמש בתעודת זהות חכמה בעמדות שירות?

1. הכינו את התעודה
 - ודאו שהתעודה מעודכנת ושיש ברשותכם את הסיסמה האישית
2. בחרו עמדות בטוחות
 - העדיפו להשתמש בעמדות מוכרות ומוסדרות כמו ספריות ציבוריות או מרכזים קהילתיים
3. שמרו על פרטיותכם
 - במהלך השימוש, ודאו שאחרים אינם יכולים לצפות במידע שאתם מזינים
4. וודאו שהתנתקתם בסיום
 - חשוב לוודא שהתנתקתם מכל החשבונות בהם השתמשתם והוצאתם את התעודה מהעמדה

2. שימוש בטוח בעמדות מחשבים ציבוריות

שימוש בעמדות ציבוריות, כמו ספריות, עמדות שירות מפקחות בקהילה או מרכזי מידע, הוא דרך נוחה לבצע פעולות דיגיטליות למי שאין ברשותם מחשב אישי או קורא כרטיסים בבית. עם זאת, השימוש בעמדות אלה עלול לחשוף את המשתמשים לסיכוני אבטחה ופרטיות.

לדוגמה: אברהם השתמש בעמדת מחשב בספרייה ציבורית כדי לבדוק את חשבון הבנק שלו. הוא לא התנתק מהחשבון כשסיים, והאדם הבא שהשתמש במחשב יכול היה לגשת למידע הפיננסי האישי שלו.

■ המלצות לפני השימוש

בחירת סוג עמדה

- מומלץ להשתמש אך ורק בעמדות שירות רשמיות, כמו אלה המצויות בספריות ציבוריות או במרכזים קהילתיים
- במידה ואתם משתמשים בחדרי מחשבים ציבוריים, הקפידו על כללי הזהירות המפורטים

בדיקת העמדה לפני השימוש

- ודאו שהעמדה נראית תקינה ושאין בה התקנים חשודים כמו מצלמות נסתרות או התקני USB לא מוכרים

תכנון מראש

- הכינו את כל המסמכים או המידע שתצטרכו מראש
- תכננו את הפעולות שתצטרכו לבצע כדי למזער את זמן השימוש

■ המלצות במהלך השימוש

שמירה על פרטיות

- בעמדות ציבוריות קיים סיכון שמידע אישי כגון סיסמאות או נתוני אשראי ייחשפו לעיניים זרות. יש להיזהר מכך.

הימנעו משמירת פרטים רגישים

- אל תשמרו סיסמאות, מסמכים או מידע אישי על מחשבים ציבוריים, גם אם זה נראה נוח
- אל תסמנו "זכור אותי" או "התחבר אוטומטית" בדפדפן

בדיקת כתובת האתר

- השתמשו רק באתרים מאובטחים (HTTPS)
- ודאו שכתובת האתר תואמת לשירות בו אתם משתמשים
- שימו לב לסימן המנעול בשורת הכתובת של הדפדפן

שימוש זהיר במסמכים

- אם אתם נדרשים להעלות או להוריד מסמכים רגישים, הקפידו למחוק אותם מיד לאחר השימוש
- מומלץ להשתמש בכונן נידד (דיסק און קי) אישי לשמירת מסמכים במקום לשמור על המחשב

■ המלצות בסיום השימוש

התנתקות מלאה

- הקפידו להתנתק מכל השירותים בהם השתמשתם לפני עזיבת העמדה
- לחצו על "התנתק"/"Logout" ולא רק לסגור את החלון

מחיקת נתונים זמניים

- בשימוש במחשבים ציבוריים קיים סיכון שמידע אישי יוותר על המחשב בו השתמשנו ויהיה חשוף לאנשים זרים. על מנת להימנע מכך אנו ממליצים על הצעדים הבאים:
- יש לנקות את היסטוריית הגלישה, הקבצים הזמניים וכל מידע אישי שהוזן במהלך השימוש
- למחיקת נתוני הגלישה:
- לחצו על תפריט 3 הקווים בדפדפן
- בחרו "הגדרות" ואז "פרטיות ואבטחה"
- בחרו "נקה נתוני גלישה"

שימוש במצב גלישה אנונימי

- מומלץ להשתמש במצב גלישה אנונימי בדפדפן (גם נקרא "חלון גלישה בסתר")
- להפעלת מצב אנונימי:
- לחצו על שלוש הנקודות בפינת המסך
- בחרו "חלון גלישה בסתר" או "חלון פרטי חדש"

ודאו שלא נשארו מסמכים

- בדקו היטב שלא נותרו קבצים אישיים בשולחן העבודה או בתיקיות של העמדה
- חפשו גם בתיקיית "הורדות" ו"מסמכים"

דיווח על בעיות

- אם נתקלתם בבעיה או בחשד לפעילות לא רגילה, דווחו למנהל המקום או לגורם האחראי על העמדה

3. בחירת כתובת מייל ואבטחת חשבון המייל

כתובת המייל שלנו היא אחת הדרכים המרכזיות שבהן אנו מזדהים ומשתמשים בשירותים דיגיטליים. בחירה נכונה של כתובת מייל ואבטחתה היא צעד חשוב בשמירה על הפרטיות והביטחון הדיגיטלי שלנו.

חשוב לדעת: בחירה לא מתאימה או שימוש בכתובת לא פעילה עלולים לחשוף אותנו לסיכונים כמו אובדן מידע, פגיעה בפרטיות, או קשיים בקבלת שירותים.



בחירת כתובת מייל מתאימה

הימנעו משימוש בפרטי זיהוי רגילים

מה לא לכלול בכתובת המייל:

- מספר טלפון מלא
- מספר זהות
- שם מלא
- תאריך לידה

דוגמה לסיכון: אנשים שהשתמשו במספר טלפון ככתובת מייל (לדוגמה: 0501234567@gmail.com) נחשפו להטרדות טלפוניות כאשר כתובת המייל שלהם הופיעה בקבוצות או פורומים ציבוריים.



■ שימוש בכתובת מייל רשמית לשירותים ממשלתיים

- בחרו כתובת מייל פעילה שתשמש אתכם למטרות רשמיות בלבד
- ודאו שתוכלו לגשת לכתובת זו בקלות ובאופן תדיר
- דאגו שכתובת זו תהיה מעודכנת בכל המערכות הרשמיות

טיפ: כדאי ליצור תיקייה מיוחדת במייל עבור הודעות מגופים רשמיים, כך שתוכלו למצוא אותן בקלות.



■ עדכניות הכתובת

- בדקו באופן תקופתי שהגישה לחשבון המייל שלכם תקינה
- אם אתם מחליפים כתובת מייל, דאגו לעדכן את כל השירותים והמערכות הרלוונטיים
- כאשר מקבלים הודעות חשובות, בצעו גיבוי שלהן לתיקייה במחשב או הדפיסו אותן



■ סיכונים בשימוש במייל לא מתאים

■ מסירת מייל לא פעיל לגופים רשמיים

- אובדן מידע חשוב כמו הודעות רשמיות, קודי אימות לשחזור גישה
 - החמצת הזדמנויות או התראות חשובות (תמיכה, הטבות, מלגות, החמצה של עדכונים בנושאים דרושים כגון פרטי מכירה שכוונתית, דרישות לתשלום וכדו)
 - אי-יכולת לשחזר חשבונות מקוונים במקרה של שכחת סיסמה
- מקרה לדוגמה: צעירים רבים מוסרים כתובות מייל שאינן בשימוש סדיר, ומגלים רק מאוחר מדי שפספסו הודעות חשובות על זכויות או חובות.**

■ סיכונים בשימוש בכתובת זמנית או לא מאובטחת

- חשיפה לפריצת חשבון וגניבת מידע אישי
- אובדן גישה לשירותים מקוונים המקושרים לכתובת המייל
- קושי בשחזור חשבונות במקרה של תקלה



■ אבטחת חשבון המייל

■ בחירת סיסמה חזקה וייחודית

- צרו סיסמה באורך של לפחות 12 תווים
- שלבו בסיסמה:
 - אותיות גדולות וקטנות
 - מספרים
 - תווים מיוחדים (!, @, #, \$ וכדומה)
- הימנעו משימוש במילים, תאריכים אישיים, או רצפים פשוטים כגון 1234
- השתמשו בסיסמה שונה מזו שאתם משתמשים בשירותים אחרים

■ הפעלת אימות דו-שלבי (2FA)

- אימות דו-שלבי מספק שכבת הגנה נוספת מעבר לסיסמה
- אופן הפעלת האימות הדו-שלבי:
 1. היכנסו להגדרות האבטחה של חשבון המייל
- חפשו את האפשרות "אימות דו-שלבי" או "Two-Factor Authentication"
- 2. עקבו אחר ההוראות להפעלת התכונה

שימו לב! משתמשי טלפון כשר נדרשים לבחור בהגדרת האימות דו-שלבי באפשרות של אימות באמצעות שיחה קולית. אם הגדרתם אימות דו-שלבי דרך SMS, ודאו שהקוד נשלח למספר טלפון נגיש ולא למספר וירטואלי שמעביר את ההודעות למייל עצמו, כדי שלא ימנע מכם הגישה לחשבון.



■ מעקב אחר פעילות חשודה

- בדקו מדי פעם את היסטוריית ההתחברות לחשבון המייל שלכם
- שימו לב להתראות על התחברות ממכשיר או מיקום לא מוכר
- בדקו שלא בוצעו שינויים בהגדרות החשבון ללא ידיעתכם

■ עדכון פרטי שחזור

- הגדירו מייל חלופי לשחזור במקרה של אובדן גישה
- אם אפשרי, קשרו מספר טלפון לצורך שחזור (רצוי מספר טלפון של בן משפחה במקרה שאתם משתמשים בטלפון כשר)
- שמרו את פרטי השחזור במקום בטוח ומעודכנים

■ המלצות לשימוש בטוח במייל

- הימנעו מלחיצה על קישורים חשודים המופיעים בהודעות מגורמים לא מזוהים
- רחפו עם העכבר מעל הקישור כדי לראות את כתובת היעד האמיתית לפני לחיצה

■ זהירות בפתיחת קבצים מצורפים

- אל תפתחו קבצים מצורפים ממיילים חשודים
- בדקו שמקור הקובץ מהימן
- בדקו את סוג הקובץ לפני פתיחתו (היזהרו במיוחד מקבצי .exe, .bat, .vbs)

■ שמירה על פרטיות המייל

- ישנם אתרים המנסים להשיג את כתובת המייל של המשתמש בהם מתוך כוונות זדון. פריצה ושימוש בכתובת המייל עלולה להסב נזק כספי ועוגמת נפש. **אל תשתפו את כתובת המייל שלכם, או את פרטי ההתחברות שלכם, כגון סיסמאות, באתרים לא מהימנים.**
- אל תענו להודעות "שרשרת" או הודעות ספאם

4. זיהוי והתמודדות עם הונאות דיגישליות

בעידן הדיגיטלי, הונאות ברשת הולכות ומתרבות, והן נעשות מתוחכמות ומותאמות אישית יותר. מספר הנפגעים מהן עולה מדי שנה, ולעיתים רבות, קורבנות ההונאה אינם מודעים לכך שהם נפלו בפח עד שנגרם נזק ממשי.

- חשוב לדעת: אחת ההונאות הנפוצות ביותר היא פשינג (Phishing), תהליך שבו גורמים זדוניים מנסים להונות משתמשים למסור מידע אישי או רגיש על ידי התחזות לגוף מהימן.



סוגי הונאות נפוצות

פשינג (Phishing)

פשינג הוא תהליך שבו נשלחות הודעות דוא"ל, הודעות טקסט או שיחות טלפון המתחזות לגופים רשמיים ואמינים. מטרת ההונאה היא לשכנע את הקורבן למסור פרטים אישיים כמו סיסמאות, פרטי אשראי או מספרי זיהוי.

דוגמה: קיבלתם הודעת דוא"ל שנראית כאילו היא מהבנק שלכם, ובה בקשה לעדכן פרטי חשבון באמצעות לחיצה על קישור. האתר אליו תגיעו נראה בדיוק כמו אתר הבנק אך נועד לגנוב את הפרטים שאתם מזינים.

התחזות לגופים רשמיים

מדובר בהונאה שבה גורמים מתחזים לשירותי ממשלה, בנקים, חברות אשראי או ספקי שירותים אחרים. המתחזים יוצרים קשר דרך שיחות טלפון, הודעות טקסט או מיילים.

דוגמה: שיחה שמגיעה ממספר לא מוכר שבה נטען שאתם חייבים סכום כסף על חבילה, עם איום על צעדים משפטיים אם לא תשלמו מיד.

קישורים זדוניים

זוהי הונאה שנעשית באמצעות קישורים שנשלחים בהודעות או במיילים ומובילים לאתרים זדוניים. אתרים אלו יכולים להיראות אמינים אך בפועל מטרתם לאסוף מידע רגיש, להתקין תוכנות זדוניות או לשבש את פעילות המכשיר.

דוגמה: הודעה שמודיעה על זכייה בפרס יוקרתי ומבקשת ללחוץ על קישור כדי לאסוף את הפרס.

■ הונאות טלפוניות

הונאות שנעשות באמצעות הטלפון כמו שיחות שמגיעות ממספרים לא מוכרים, שבהן המתקשרים מנסים לשכנע אתכם למסור פרטים אישיים, לבצע תשלומים או להתקין אפליקציה במכשיר. דוגמה: שיחה בה נאמר שחשבון הבנק שלכם נפרץ ושעליכם למסור את פרטי הגישה לצורך תיקון הבעיה.



■ כיצד לזהות הונאות?

■ בדקו את מקור ההודעה

- כתובת מייל אמינה תסתיים בדרך כלל בדומיין של החברה (לדוגמה: support@bankleumi.co.il) ולא בסיומות כלליות (כמו: bankleumi.support@gmail.com)
- מספרי טלפון של בנקים וגופים רשמיים בדרך כלל יופיעו כמספרים קבועים ומוכרים

■ חשד במידע לא צפוי

- היו חשדנים אם קיבלתם הודעה על זכייה בפרס שלא השתתפתם בתחרות לקבלו
- תהיו ערניים לבקשות דחופות למסור פרטים אישיים ללא סיבה מוצדקת
- הצעות שנשמעות טובות מדי כדי להיות אמיתיות - כנראה שאינן אמיתיות

■ שגיאות לשוניות או עיצוביות

- הודעות מזויפות רבות מכילות שגיאות כתיב, ניסוחים מוזרים או עיצוב לא מקצועי
- חפשו סימנים כמו לוגו באיכות נמוכה, פונטים לא אחידים, או ניסוחים שאינם מקובלים בתכתובת רשמית

■ בדיקת קישורים לפני לחיצה

- רחפו עם העכבר מעל הקישור (בלי ללחוץ) כדי לראות את כתובת היעד האמיתית
- חפשו כתובות אתרים שנראות דומות אך לא זהות לאתרים הרשמיים (למשל: bankleumi-verify.com במקום bankleumi.co.il)



כיצד להתגונן מהונאות?

■ היעזרו ברשות הסייבר הלאומית

- הרשות מספקת מידע וכלים להתמודדות עם איומים דיגיטליים
- בקרו באתר הרשות (www.gov.il/he/departments/israel_national_cyber_directorate) לקבלת עדכונים והנחיות מעודכנות
- במקרה של חשד להונאה, ניתן לפנות למוקד 119 או לדווח באתר הרשות

■ אל תמסרו קוד דו-שלבי (2FA)

- קוד האימות הדו-שלבי נועד לשימושכם האישי בלבד
- לעולם אל תמסרו את הקוד, גם אם הפונה מתחזה לנציג רשמי או גורם אמין אחר
- אף גורם לגיטימי לא יבקש מכם את קוד האימות הדו-שלבי

■ אימות מול הגורם הרלוונטי

- אם קיבלתם הודעה או שיחה חשודה, עצרו את הפעולה
- צרו קשר ישיר עם הגוף הרלוונטי דרך מספר הטלפון הרשמי שלו (שמופיע בגב כרטיס האשראי, באתר הרשמי או בחשבונות הרשמיים)
- לעולם אל תסמכו על פרטי יצירת הקשר שמסופקים בהודעה החשודה
- גם אם הבקשה לקוד מגיעה מאדם שאתם מכירים - אל תיענו. ייתכן שפרצו לחשבוננו, וכעת מנסים בעזרתו להשתלט גם על שלכם. זו טכניקה נפוצה של גניבת זהות.

■ שימוש באימות דו-שלבי (2FA)

- הפעילו אימות דו-שלבי בכל חשבונותיכם החשובים (מייל, חשבונות בנק, רשתות חברתיות)
- כך, גם אם סיסמתכם נגנבת, יהיה קשה יותר לגורמים זדוניים לגשת לחשבון שלכם
- אם אתם משתמשים בטלפון כשר, היעזרו בפתרונות המוצגים בחלק ב' של המדריך לקבלת קודי אימות

■ עדכוני תוכנה שוטפים

- עדכנו את מערכות ההפעלה, הדפדפנים והתוכנות במכשירים שלכם באופן קבוע
- עדכונים אלה כוללים "טלאי אבטחה" שסוגרים פרצות אבטחה ידועות
- הפעילו עדכונים אוטומטיים במידת האפשר

■ הכירו את ניסיונות גניבת הזהות

- גורמים זדוניים משתמשים בטכניקות מתוחכמות כדי לגנוב את זהותכם
- היו חשדנים כלפי בקשות לא צפויות למידע אישי
- לא להתקין תוכנות ממקור לא ידוע
- לא לאשר באגרים קופצים
- זכרו: בנקים, רשויות ממשלה וחברות אמינות לעולם לא ישלחו הודעות המבקשות את הסיסמה שלכם
- אל תגיבו לבקשות בהודעות לקבלת מידע אישי, קוד אימות או העברת כספים. גם אם הן מגיעות ממקור מוכר לכאורה. עצרו, בדקו וודאו מול הגורם ישירות.

■ הימנעו ממסירת פרטים רגישים

- לעולם אל תמסרו סיסמאות, פרטי אשראי או מידע אישי אחר דרך הטלפון או במייל
- מידע רגיש יש למסור רק באתרים מאובטחים (עם סמל של מנעול בשורת הכתובת והכתובת מתחילה ב-https)



■ מה לעשות במקרה של הונאה?

■ שינוי סיסמאות

- אם נחשפתם להונאה, החליפו מיד את הסיסמאות של החשבונות שהיו מעורבים
- השתמשו בסיסמאות חזקות וייחודיות לכל חשבון

■ דיווח לגורמים מוסמכים

- דווחו לרשויות החוק (משטרת ישראל - 100) על האירוע
- דווחו לבנק שלכם או לחברת האשראי אם נחשפו פרטים פיננסיים
- דווחו למוקד הסייבר הלאומי (119)

■ מעקב אחר חשבונות

- עקבו אחר הפעילות בחשבונות הבנק ובחשבונות הדיגיטליים שלכם
- חפשו פעולות חשודות או לא מוכרות
- הגדירו התראות על פעילות חריגה בחשבונות הבנק והאשראי שלכם

■ היעזרו במומחים

- אם אינכם בטוחים כיצד לטפל במצב, פנו לעזרה מקצועית
- פנו למוקדי התמיכה של הבנק/חברת האשראי/שירות הרלוונטי
- במקרים מורכבים, שקלו לפנות למומחה סייבר או תמיכה טכנית מקצועית

5. הגנה על המשפחה בשימוש בג'ימייל Gmail

ג'ימייל Gmail הוא כלי מרכזי עבור משפחות רבות, המציע אפשרויות כמו צ'טים אישיים, קבוצות תפוצה, ותכונות אינטגרציה מגוונות. למרות הנוחות הרבה, ישנן סכנות רוחניות וגשמיות ופוטנציאל לשימוש לא נכון, במיוחד כאשר משתמשים אינם מכירים את כל הכלים הקיימים במערכת.

חשוב לדעת: כאשר פותחים חשבון ג'ימייל, מקבלים גישה אוטומטית למגוון שירותים נוספים של גוגל, שחלקם עשויים להיות בעלי סיכונים פוטנציאליים אם לא משתמשים בהם כראוי.



מודעות לסיכונים בג'ימייל Gmail

■ חוסר מודעות לכלים נוספים בג'ימייל

- כאשר מצטרפים לג'ימייל, משתמשים רבים אינם מודעים לכך שהם מקבלים גישה לסט רחב של כלים נוספים. יצוין כי מערכות סינון שונות חוסמות חלק מהשירותים המוצעים בג'ימייל מטעמי כשרות.
 - Google Chat - מערכת צ'טים אישיים וקבוצתיים
 - Google Groups - קבוצות דיון ותפוצה
 - Google Drive - אחסון קבצים ושיתוף מסמכים
 - Google Photos - אחסון ושיתוף תמונות
- זוהי רשימה חלקית. כלים אלו מקלים על התקשורת והניהול, אך עלולים להוות פתח לסיכונים אם לא מגדירים אותם כראוי.

■ סכנות בצ'טים פתוחים

- צ'טים אישיים וקבוצתיים בג'מייל עשויים להיות פתוחים לאנשים זרים
- כאשר הצ'ט פעיל לכל מי שיש לו את כתובת המייל שלכם, זרים עלולים לשלוח הודעות לא רצויות
- אנשים עלולים לנסות ליצור קשר למטרות פוגעניות או זדוניות

שימו לב: אם כתובת המייל שלכם מבוססת על מספר הטלפון האישי (לדוגמה 0501234567@gmail.com) זרים יכולים לנצל זאת כדי ליצור קשר טלפוני לא רצוי או לקשר בין זהותכם לחשבונות אחרים ברשת.



■ הצטרפות לקבוצות וצ'טים קבוצתיים גדולים

- Google Groups וצ'טים קבוצתיים מאפשרים הצטרפות למרחבים בהם משתתפים רבים
- בקבוצות גדולות לא ניתן לדעת מי המשתתפים האחרים, מה שפותח פתח לפעילות פוגענית או לא ראויה
- מידע אישי שנחשף בקבוצות כאלה עלול להגיע לגורמים לא רצויים

סיכון מיוחד למשתמשים צעירים: נוער וילדים לעיתים נוטים להצטרף לקבוצות או צ'טים מתוך סקרנות, מבלי להבין את הסכנה שבחשיפת המידע שלהם לאנשים זרים.



הדרכת בני משפחה בשימוש בטוח בג'מייל Gmail

■ ניהול הגדרות פרטיות בגוגל צ'ט Chat

הגדרת מי יכול לפנות אליכם:

- היכנסו ל-Google Chat (באמצעות אייקון הצ'אט בתיבת הג'מייל או ישירות ב-chat.google.com)
- 1. לחצו על הגדרות (אייקון הגלגל שיניים)
- 2. בחרו באפשרות "הגדרות צ'אט"
- 3. תחת "אפשרויות צ'אט", בחרו באחת מהאפשרויות:
- "קבל הזמנות צ'אט רק מאנשים שיש לך את כתובת המייל שלהם"
- "קבל הזמנות צ'אט רק מאנשי קשר"

דיווח על תוכן פוגעני:

- גופי בטיחות ברשת ממליצים לפקח על שימוש ילדים ובני נוער במחשב. יש מגוון תוכנות שזה תפקידן. ישנן תוכנות שנועלות את המחשב, מגבילות את שעות השימוש בו, או את השימוש ברשת. תוכנות אחרות מתריעות בעת ניסיון כניסה לאתרים שמוגדרים מראש.
- עודדו את בני המשפחה לדווח על הודעות חשודות או פוגעניות באופן מיידי
- לדיווח: לחצו על שלוש הנקודות ליד ההודעה ובחרו "דווח"

כללי הצטרפות לקבוצות תפוצה

בדיקה לפני הצטרפות:

- בדקו היטב לפני שאתם או בני משפחתכם מצטרפים לקבוצה בגוגל גרופס
- בררו:
 - מי מנהל את הקבוצה?
 - מהי מטרת הקבוצה?
 - האם הקבוצה ציבורית או פרטית?
 - מה סוג התוכן שמשותף בקבוצה?

■ הנחיות לבני המשפחה:

- הגדירו לבני המשפחה להצטרף רק לקבוצות מוכרות ומהימנות
- הסבירו את הסיכונים בחשיפת מידע אישי בקבוצות ציבוריות
- הדריכו אותם לא לקבל הזמנות מגורמים לא מוכרים

■ ניהול חשבונות וכלים משותפים

הסבר על כלים אינטגרטיביים:

- הציגו בפני בני המשפחה את הכלים האינטגרטיביים שמגיעים עם ג'ימיל
- הדגו כיצד לשתף מסמכים בצורה בטוחה ב-Google Drive
- הסבירו את ההבדל בין שיתוף פרטי, מוגבל וציבורי

■ חיזוק אבטחת החשבון:

- ודאו שכל בני המשפחה משתמשים באימות דו-שלבי (2FA)
- עזרו להם להגדיר שאלות אבטחה ואפשרויות שחזור מתאימות
- שקלו להשתמש במנהל סיסמאות משפחתי

■ סכנות בשימוש במייל שמבוסס על מספר טלפון

- הסבירו את הסיכונים בשימוש בכתובת מייל הכוללת מספר טלפון
- עודדו בני משפחה להשתמש בכתובות מייל שאינן חושפות מידע אישי
- אם יש כבר חשבון כזה, שקלו ליצור חשבון חדש עם כתובת אנונימית יותר

■ הדרכה למניעת פשינג והתחזויות

סימנים לזיהוי הודעות פשינג:

- כתובת שולח חשודה או שגויה
- שגיאות כתיב ודקדוק
- בקשות דחופות לפעולה
- קישורים חשודים
- בקשות למידע אישי או פרטי התחברות

■ הנחיות פרקטיות:

- למדו את בני המשפחה לבדוק תמיד את כתובת השולח
- הדריכו אותם לריחוף העכבר מעל קישורים לפני לחיצה עליהם
- קבעו כלל משפחתי: "לעולם לא מוסרים סיסמאות במייל או בטלפון"

6. סמלים ואמצעי זיהוי בתקשורת דיגיטלית

בעת רכישת מוצרים טכנולוגיים, לעיתים איננו מודעים לפונקציות תקשורת נסתרות כמו Wi-Fi או Bluetooth. פונקציות אלה יכולות להועיל, אך גם לסכן את פרטיותנו ואבטחת המידע שלנו. מכשירים רבים מגיעים עם יכולות תקשורת פעילות כברירת מחדל, גם בלי ידיעתנו.



פונקציות תקשורת נסתרות וסיכונים

■ חיבור Wi-Fi

- מוצרים עם חיבור Wi-Fi: נגני מדיה, מצלמות, שעונים חכמים, צעצועים, מכשירי חשמל
- סיכון: חשיפה לפריצות ואיסוף נתונים אישיים ללא ידיעתכם
- טיפ: חפשו סמלי Wi-Fi על האריזה ובדקו הגדרות חיבור במכשיר

■ Bluetooth

- שימושים: חיבור לאוזניות/רמקולים, העברת קבצים, חיבור לאביזרים, סנכרון נתונים
- סיכון: חשיפה לגישה לא מורשית, במיוחד במקומות ציבוריים
- טיפ: כבו את ה Bluetooth כשאינו בשימוש

■ סמלי תקשורת עיקריים

סיכון פוטנציאלי	משמעות	סמל	
חשיפה לרשתות לא מאובטחות	חיבור רשת אלחוטית		Wi-Fi
גישה לא מורשית, העברת מידע ללא ידיעה	חיבור למכשירים קרובים		Bluetooth

Cloud		שירותי ענן/ גיבוי	אחסון מידע בשרתים חיצוניים
GPS		מיקום גיאוגרפי	מעקב אחר מיקומכם
NFC		תקשורת טווח קצר	חשיפת מידע למכשירים בקרבתכם



הימנעות מחשיפה לא רצויה

לפני הרכישה

- שאלו: האם המכשיר מתחבר לאינטרנט Wi-Fi/Bluetooth/סלולרי?
- ברו: אילו נתונים נאספים? האם ניתן לכבות פונקציות תקשורת?
- בדקו: האם יש הגדרות פרטיות שכדאי לשנות?

לאחר הרכישה

- קראו את מדריך ההפעלה בקפידה
- בדקו את תפריט ההגדרות
- כבו חיבורים אוטומטיים לא נחוצים
- התאימו הגדרות פרטיות וביטחון למינימום הנדרש

רכישות למשפחה

- ודאו שבני משפחה מבינים את פונקציות המכשיר
- הסבירו סיכונים והדגישו שימוש בהגדרות אבטחה
- עדכנו ילדים על סכנות בשיתוף מידע

בדיקת תקנים

- חפשו תקני אבטחה מקובלים (CE, FCC, ISO)
- העדיפו חברות מוכרות עם מוניטין טוב באבטחה
- קראו סקירות מקצועיות לפני רכישה

דוגמא מעשית לחשיפה לא רצויה

■ מצלמה עם חיבור לענן

- סיכון: שמירת תמונות וסרטונים בענן וחשיפת תוכן פרטי
- פתרון: בדיקת מיקום שמירת תמונות, ביטול גיבוי אוטומטי לענן

■ המלצות למשפחות

כללים משפחתיים לשימוש

- קביעת כללים ברורים למכשירים מחוברים
- הגדרת מטרות חיבור לכל מכשיר
- שיתוף בהחלטות רכישה של מוצרים עם יכולות תקשורת

ניהול זמן מסך

- הגבלת זמן שימוש, במיוחד לילדים ובני נוער
- וידוא שימוש חיובי (לימודים, תקשורת)
- הצבת מכשירים במקומות משותפים

בדיקה ועדכון שוטפים

- בדיקת הגדרות אבטחה ופרטיות באופן קבוע
- עדכון תוכנות וקושחה
- מעקב אחר מכשירים המחוברים לרשת הביתית

תקשורת פתוחה

- שיח משפחתי על טכנולוגיה
- עידוד דיווח על חוויות חשודות
- הקשבה לחששות ושאלות בנושאי פרטיות ואבטחה

7. סיכום

הגנה דיגיטלית היא לא רק טכנולוגיה, אלא גם אחריות אישית ומשפחתית. על ידי הקפדה על הכללים וההמלצות שהוצגו במדריך, תוכלו להפחית את הסיכונים, לשמור על ביטחון המידע האישי,

ולשתמש בטכנולוגיה בצורה חכמה ובטוחה. האחריות הראשונה לשמירה על הביטחון הדיגיטלי של המשפחה מוטלת עליכם, והכלים שבידיכם יכולים לעשות את ההבדל.



נקודות חשובות לשמירה על בטיחות דיגיטלית

■ זיהוי והזדהות בטוחים

- השתמשו בתעודת זהות חכמה לצורך הזדהות בשירותים ממשלתיים
- שמרו בקפידה על הקוד האישי של התעודה החכמה
- היזהרו ממסירת פרטים אישיים או קודי אימות

■ שימוש בטוח בעמדות ציבוריות

- בחרו עמדות מאובטחות ומוכרות
- אל תשמרו מידע אישי על מחשבים ציבוריים
- הקפידו להתנתק בסיום השימוש ולמחוק נתוני גלישה

■ אבטחת חשבונות מייל ותקשורת

- בחרו כתובת מייל שאינה חושפת פרטים אישיים
- הפעילו אימות דו-שלבי בכל החשבונות החשובים
- היו ערניים לניסיונות פשינג והונאה

■ הגנה על המשפחה

- הדריכו את בני המשפחה בנושאי בטיחות דיגיטלית
- נהלו שיח פתוח על סיכונים ברשת
- עקבו אחר התנהגות חשודה או לא רגילה

■ התמודדות עם טכנולוגיה חדשה

- בדקו אפשרויות תקשורת במוצרים חדשים לפני הרכישה
- כבו פונקציות תקשורת שאינן בשימוש
- עדכנו תוכנות ומכשירים באופן שוטף

■ המלצות לשימוש יומיומי

- בדקו באופן שוטף את חשבונותיכם ופעילותם
- עדכנו סיסמאות לפחות פעם בחצי שנה
- הימנעו משמירת פרטים רגישים על מכשירים שאינם מאובטחים
- דווחו על פעילות חשודה לגורמים הרלוונטיים בהקדם

■ מספרי חירום ומוקדי סיוע בנושא בטיחות ברשת

- מוקד הסייבר הלאומי: 119
- משטרת ישראל: 100
- מוקד חירום לאומי להגנה על ילדים ובני נוער מפני פגיעות ברשת: 105 (פעיל 24/7 ומספק סיוע מידי במקרי בריאות, סחיטה או הטרדה מקוונת)
- הרשות להגנת הפרטיות: 02-646-7590



נספח
מילון
מונחים

בלוטוס (Bluetooth)

טכנולוגיה המאפשרת חיבור אלחוטי בין מכשירים קרובים. למשל, חיבור בין מכשיר שמיעה לטלפון. כמו "גשר אווירי" קטן בין שני מכשירים.

דפדפן

תוכנה המאפשרת לנו לראות אתרי אינטרנט. כמו מדריך שמוביל אותנו בין "רחובות" האינטרנט. הדפדפן מתרגם את השפה הטכנית של האינטרנט למשהו שאנחנו יכולים לראות ולהבין.

הזדהות בשוחה

תהליך שבו אנחנו מוכיחים למערכת שאנחנו באמת מי שאנחנו טוענים שאנחנו. כמו כשמגיעים לבנק ומציגים תעודת זהות. בעולם הדיגיטלי, זה יכול להיות באמצעות תעודת זהות חכמה או סיסמה.

הצפנה

שיטה להגנה על מידע על ידי הפיכתו לקוד מוצפן שרק מי שיש לו את המפתח המתאים יכול לקרוא. כמו כתב סתרים מתוחכם - רק מי שידוע את השיטה יכול להבין את המסר.

מספר וירטואלי

מספר טלפון שקיים רק במחשב, לא במכשיר פיזי. משמש בעיקר לקבלת הודעות SMS במחשב. כמו שיש "תא קולי" בטלפון רגיל, אבל זה תא שמקבל הודעות כתובות במחשב.

אבטחת מידע

מערכת של כללים ופעולות השומרת על המידע האישי שלנו מפני גניבה או שימוש לרעה. בדומה למערכת אבטחה במוסדות חינוך - יש שומר בכניסה, מצלמות, ונהלים ברורים מי יכול להיכנס ומתי.

אימות דו-שלבי (2FA)

שיטת הגנה הדורשת שני סוגי זיהוי שונים כדי להיכנס לחשבון. למשל: סיסמה קבועה + קוד חד-פעמי שנשלח לטלפון. זה דומה לכספת בבנק - צריך גם מפתח פיזי וגם לדעת את הקוד כדי לפתוח אותה. בעולם הדיגיטלי, זו דרך להבטיח שגם אם מישהו השיג את הסיסמה שלנו, הוא עדיין לא יוכל להיכנס לחשבון בלי הקוד הנוסף.

אינטרנט מסונון

חיבור לאינטרנט העובר דרך מערכת סינון מאושרת על ידי רבנים, המונעת גישה לתכנים לא ראויים. החיבור המסונן מאפשר גישה רק לאתרים ושירותים הכרחיים ומאושרים.

אתר אינטרנט

מקום וירטואלי ברשת שבו מוצג מידע או ניתנים שירותים. בדומה לחנות או משרד, אבל במרחב הדיגיטלי. לדוגמה: אתר של קופת חולים מאפשר לקבוע תורים ולראות תוצאות בדיקות.

למסור פרטים אישיים למי שפונה אלינו, גם אם נראה אמין.

קורא כרטיסים

מכשיר קטן המתחבר למחשב ומאפשר לקרוא כרטיסים חכמים כמו תעודת זהות חכמה. כמו "מכשיר כרטיס אשראי" בחנות, אבל במקום לקרוא כרטיס אשראי, הוא קורא תעודות זהות חכמות.

רב-קו

כרטיס חכם המשמש לתשלום בתחבורה ציבורית. כמו "כרטיסייה" דיגיטלית שאפשר לטעון בה כסף או לקנות מנוי חודשי. הכרטיס מכיל שבב אלקטרוני שמאחסן את המידע על הכסף או המנוי שיש בו.

שירותי ענן

מקום אחסון דיגיטלי באינטרנט. כמו "מחסן" וירטואלי שבו אפשר לשמור קבצים, תמונות ומסמכים. במקום לשמור הכל במחשב האישי, שומרים באינטרנט וכך אפשר לגשת למידע מכל מחשב מורשה.

תעודת זהות חכמה

תעודת זהות עם שבב אלקטרוני המכיל את המידע שלנו בצורה מאובטחת. כמו תעודת זהות רגילה, אבל עם יכולות דיגיטליות - אפשר להשתמש בה כדי להזדהות באופן בטוח באינטרנט או בעמדות שירות ממשלתיות.

תוכנה זדונית

תוכנה מזיקה שנועדה לפגוע במחשב או לגנוב מידע. כמו "גנב" דיגיטלי שמנסה להיכנס למחשב שלנו. חשוב להתקין תוכנות הגנה ולא להוריד קבצים ממקורות לא מוכרים.

מערכת הפעלה

התוכנה הראשית במחשב שמאפשרת לו לעבוד. כמו המנהל של בית ספר - מפקח על כל הפעילות ומוודא שכל הדברים עובדים יחד בצורה נכונה.

מצב גלישה אנונימי

מצב גלישה מוסתר הוא אפשרות מיוחדת בדפדפן שמונעת שמירת היסטוריית גלישה, סיסמאות ופרטים אישיים במחשב בו אתם משתמשים. כדי להפעיל אותו, לחצו על שלוש הנקודות בפינה השמאלית העליונה של הדפדפן ובחרו ב"חלון גלישה בסתר חדש" (בדפדפן כרום), "חלון גלישה פרטי חדש" או "חלון פרטי חדש". כשתסיימו את הגלישה וסגרו את החלון, לא יישאר שום מידע על הפעולות שביצעתם במחשב.

סטיק (התקן נייד) סלולרי

מכשיר קטן בצורת מפתח USB המתחבר למחשב ומאפשר גישה לאינטרנט מסונן. כמו "שער כניסה" נייד לאינטרנט המסונן.

עמדת שירות עצמי

מכשיר ציבורי המאפשר לבצע פעולות ממשלתיות ותשלומים בלי צורך בפקיד. כמו מכונה אוטומטית למכר כרטיסי רב-קו, אבל עם הרבה יותר אפשרויות - הנפקת תעודות, תשלום חשבונות וכדומה.

פישינג

ניסיון הונאה שבו מתחזים לגוף אמין (כמו בנק או משרד ממשלתי) כדי לגנוב מידע אישי. כמו "גנב" שמתחזה לגבאי צדקה מוכר כדי לקבל תרומות. חשוב להיזהר ולא

