

בנק הפועלים

מוגש כשירות לציבור מטעם בנק הפועלים.

טיפים פשוטים

לשיפור **Take Away**

האבטחה במרחב האישי

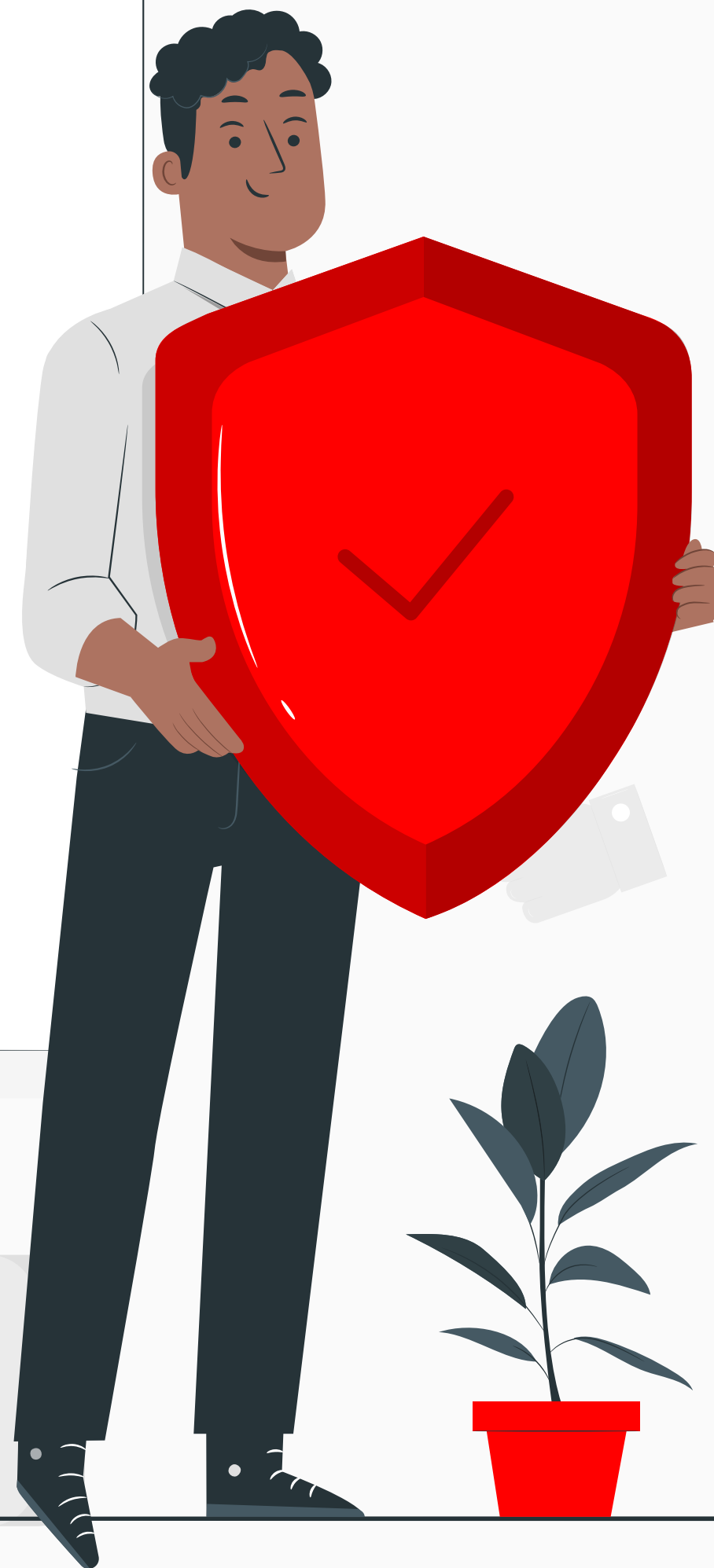
מהדורת אפריל 2024

לתשומת לבכם:

- אבטחת מידע הינה נושא מורכב ומשתנה, וכפוף להוראות דין שונות
- המידע הכלול בעלון זה הינו כללי, ולא הותאם למטרות או דרישות ספציפיות. אין לראות בו ייעוץ מקצועי, משפטי, או אחר
- זכויות היוצרים והקניין הרוחני במידע הכלול שייכות לבנק הפועלים בע"מ

טיפים למשתמש

-
-
-
-



לקוחות יקרים,

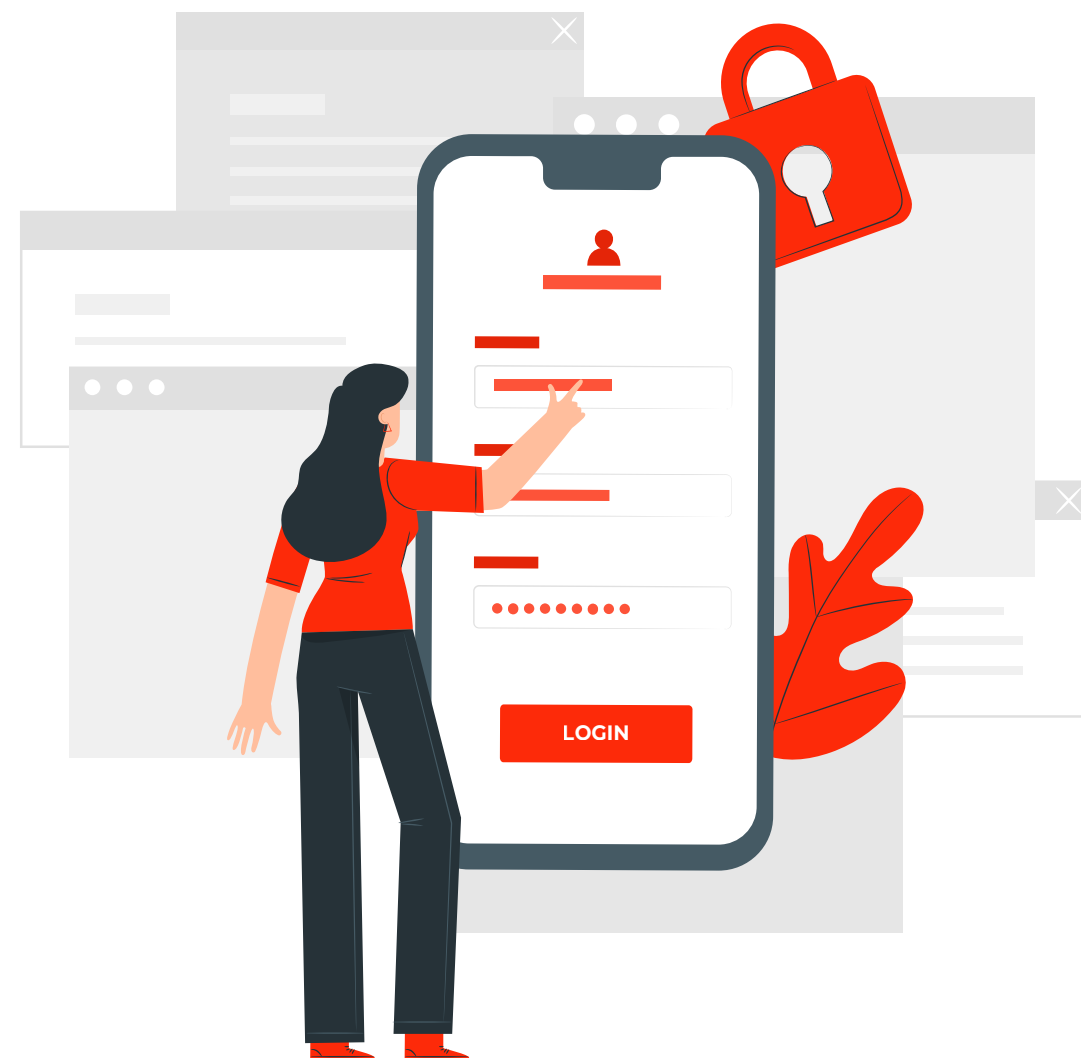
ריכזנו עבורכם טיפים ודרכי התנהלות ליצירת מרחב דיגיטלי אישי מאובטח יותר. ביצוע ההנחיות במדריך זה אינו מחייב רמת הבנה טכנית גבוהה.

1. הגנה על האינטרנט הביתי



4

2. אבטחת המחשב והסמארטפון/הטאבלט



7

3. התנהלות בטוחה בגלישה באינטרנט



14

1. הגנה על האינטרנט הביתי

מרבית הפעילויות שאנו מבצעים באינטרנט במרחב האישי שלנו מתאפשרות באמצעות הרשת הביתית שברשותנו, אם בשימוש ברשת ה-Wi-Fi או ע"י חיבור כבל פיסי.

תוקפי סייבר יכולים להתחבר לרשתות Wi-Fi פרטיות ע"י פריצת סיסמת ה-Wi-Fi הביתית או ע"י חדירה לנתב (ראוטר) שברשותנו. התחברות זדונית לרשת הביתית עלולה להוביל לגניבת מידע אישי ולנזקים נוספים.

חולשת אבטחה התגלתה במיליוני נתבים

חולשה ברכיב שנמצא בראוטרים של חברות כמו TP-Link, D-Link ו-Netgear מאפשרת להאקרים לחדור לרשתות ולקבצים אישיים. החדשות הטובות: לא ידוע על מקרים של ניצול של החולשה. איך בדיוק זה עובד וכיצד אפשר להתגונן?

8 תגובות

רועי האן | 11.01.22 | 16:10

חברת הסייבר SentinelOne מדווחת על גילוי מדאיג המצוי בנתבי רשת רבים, שעשוי לפגוע במאות אלפי משתמשים ברחבי העולם ולהעניק לפושעי הסייבר חלון כניסה קל למערכות הרשת של משתמשים פרטיים וארגונים ולמידע האישי שלהם.



מחקר: יותר מ-70% מרשתות ה-Wi-Fi במדינה נפרצות בקלות

לפי חוקרי סייברארק, "בעידן העבודה מהבית, פריצה לרשת Wi-Fi ביתית מהווה סכנה לא רק למשתמשים, קורבנות התקיפה, ולפרטיותם, אלא עלולה להפוך, בנוסף, לאיום על הרשת הארגונית של מקום עבודתו"



יוסי הטוני | 26/10/2021 15:00

אנשים ומחשבים

בפרק זה נציג לכם מספר פעולות פשוטות שניתן לבצע באופן עצמאי או בסיוע ספק האינטרנט, אשר ישפרו באופן משמעותי את רמת ההגנה של הרשת הביתית שלכם.

רשת ה-Wi-Fi

התחברות לרשת ה-Wi-Fi הביתית מחייבת להכיר את שם הרשת ואת הסיסמה. בכדי למנוע מתוקפי סייבר להתחבר לרשת הביתית, יש לוודא ששם הרשת אינו קשור או מרמז על שם המשפחה שלנו ושסיסמת הרשת לא תהיה קלה לניחוש.

שם רשת ה-Wi-Fi

ככל שנגדיר שם שקשה לקשר אותו אלינו, כך נקשה על תוקפי סייבר להתמקד ברשת שלנו ולתקוף אותה. רצוי להגדיר שם רשת שאינו מקושר לשם המשפחה שלנו.

סיסמת רשת ה-Wi-Fi

שימוש במספר טלפון נייד של אחד מבני הבית כסיסמת התחברות לרשת הביתית הוא סטנדרט ישראלי מוכר, המקל על תוקפים לאתר את המספרים באינטרנט ולהתחבר לרשתות פרטיות. רצוי לקבוע סיסמת Wi-Fi ייחודית המשלבת אותיות, ספרות ותווים מיוחדים, שתקשה מאוד על התוקפים.

יצירת רשת Wi-Fi ייעודית לאורחים

רוב הנתבים מאפשרים הקמה של יותר מרשת אלחוטית אחת ולכל רשת כזו, ניתן להגדיר שם וסיסמה ייחודיים. הרעיון הוא לייצר הפרדה בהתחברות לרשת הביתית בין המכשירים הביתיים ומכשירי האורחים. לדוגמה, ניתן להקים שתי רשתות ביתיות שיחולקו באופן הבא:

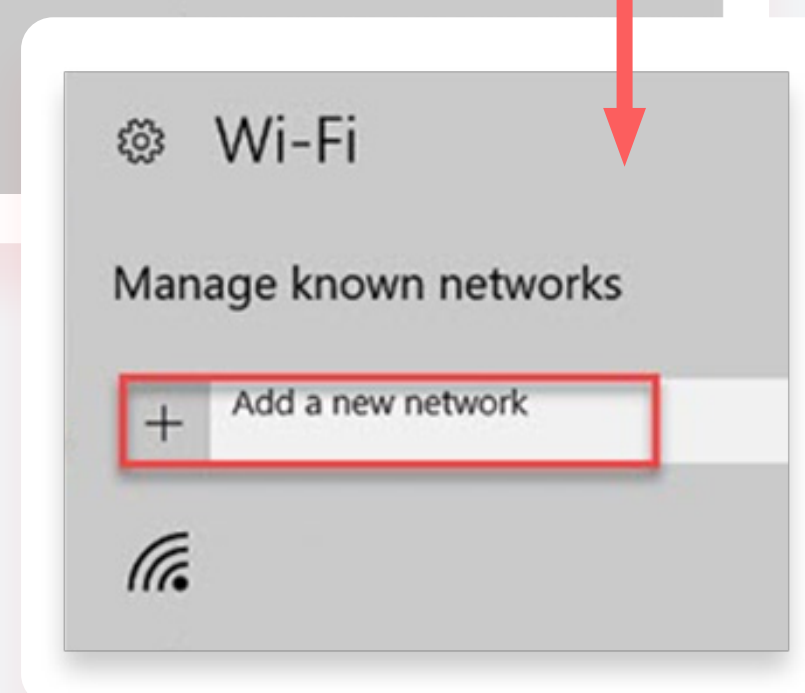
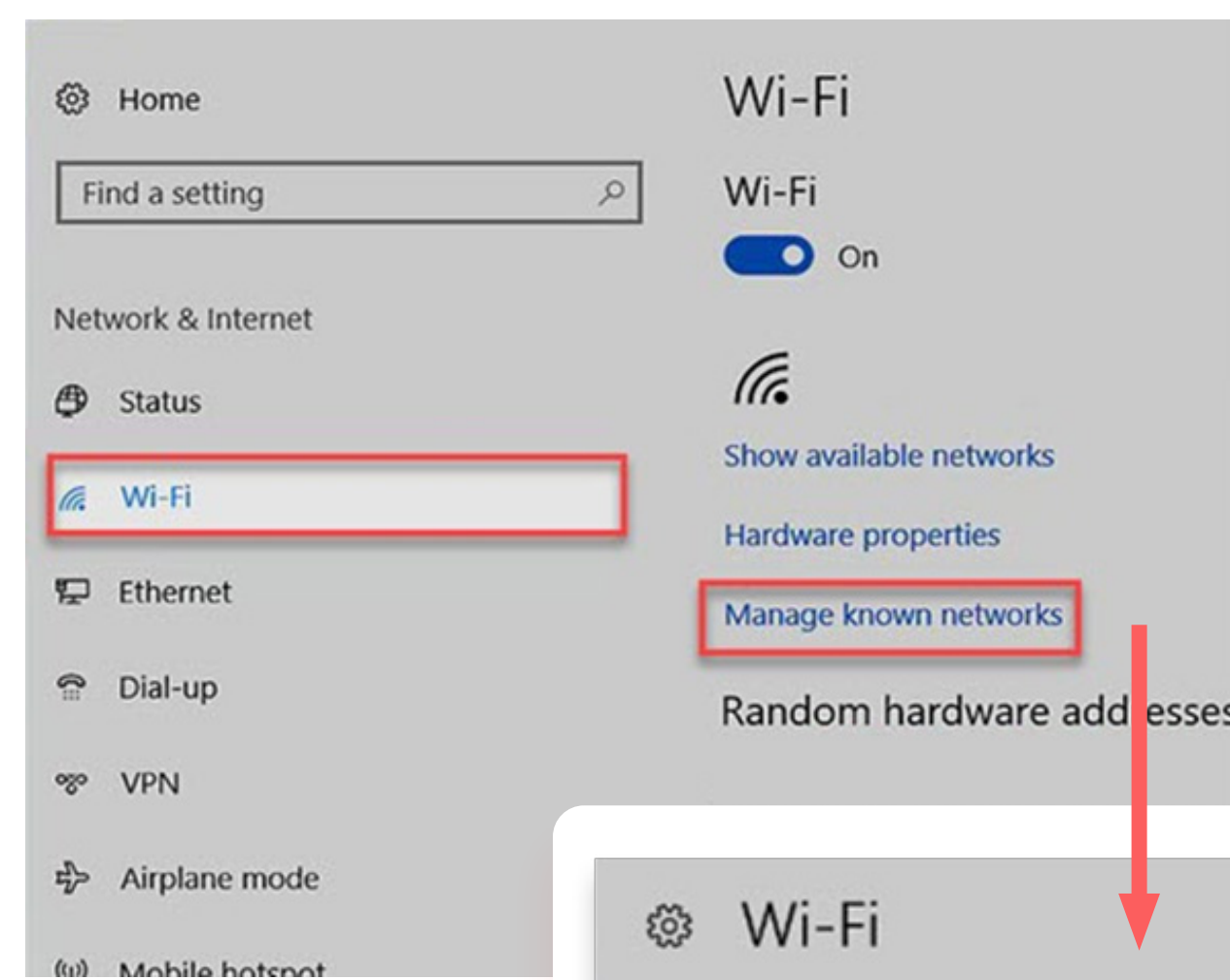
רשת A - למכשירים הביתיים כדוגמת מחשבים ומכשירים סלולריים, טלוויזיה חכמה, מצלמות אבטחה, i-robot ודומיהם.

רשת B - לאורחים (למשל, חברים או מבקרים זמניים).

הסתרת רשת ה-Wi-Fi

במידה ואינכם מעוניינים ששכנים או עוברי אורח יוכלו לנסות להתחבר לרשת האלחוטית הביתית שלכם, ניתן להגדיר שם הרשת שלכם יוסתר ולא יופיע בעת ביצוע חיפוש רשתות אלחוטיות זמינות.

במידה והרשת שלכם מוסתרת ותרצו לחבר אליה מכשיר חדש, ניתן לעשות זאת באמצעות חיפוש ייזום לשם הרשת ולבצע אימות רגיל באמצעות הסיסמה שהגדרתם.



אבטחת הנתב (ראוטר)

הרשת הביתית מתאפשרת באמצעות הנתב (ראוטר). בעת ייצור הנתב במפעל, מוגדרת לו סיסמת ברירת מחדל במטרה להקל על טכנאי האינטרנט בשלב ההתקנה הראשונית או הטיפול. במידה ולא קבעתם שם משתמש וסיסמה ייחודיים לנתב שלכם, ניתן לפרוץ אליו בקלות יחסית מכל מקום בעולם ולהשיג דרכו גישה לרשת הביתית

עדכון סיסמת הנתב הביתי שברשותכם

רצוי לקבוע שם משתמש וסיסמה ייחודית המורכבת מספרות, אותיות ותווים מיוחדים.

עדכוני קושחה (Firmware) לנתב הביתי

בדומה לעדכונים המותקנים מעת לעת במחשב או בסמארטפון שלנו בכדי לאבטח אותם, כך גם נדרש לעדכן מעת לעת את הנתב הביתי. מומלץ לבדוק באופן תדיר אם יש לנתב עדכוני קושחה ולהתקינם. נתבים מיושנים שכבר אינם נתמכים ע"י היצרן אינם מקבלים עדכוני קושחה ובכך חושפים את הרשת הביתית למתקפות סייבר פוטנציאליות. מומלץ לוודא שהנתב שברשותכם עדכני, נתמך ומקבל עדכוני קושחה. ניתן לבדוק זאת באופן עצמאי באינטרנט ע"י הקלדת שם ודגם הנתב שברשותכם.

ריכזנו לכם את הטיפים להגברת האבטחה ברשת הביתית. כל סעיף שתשלימו ותסמנו בו ✓, יגביר את רמת האבטחה של הרשת הביתית שלכם:

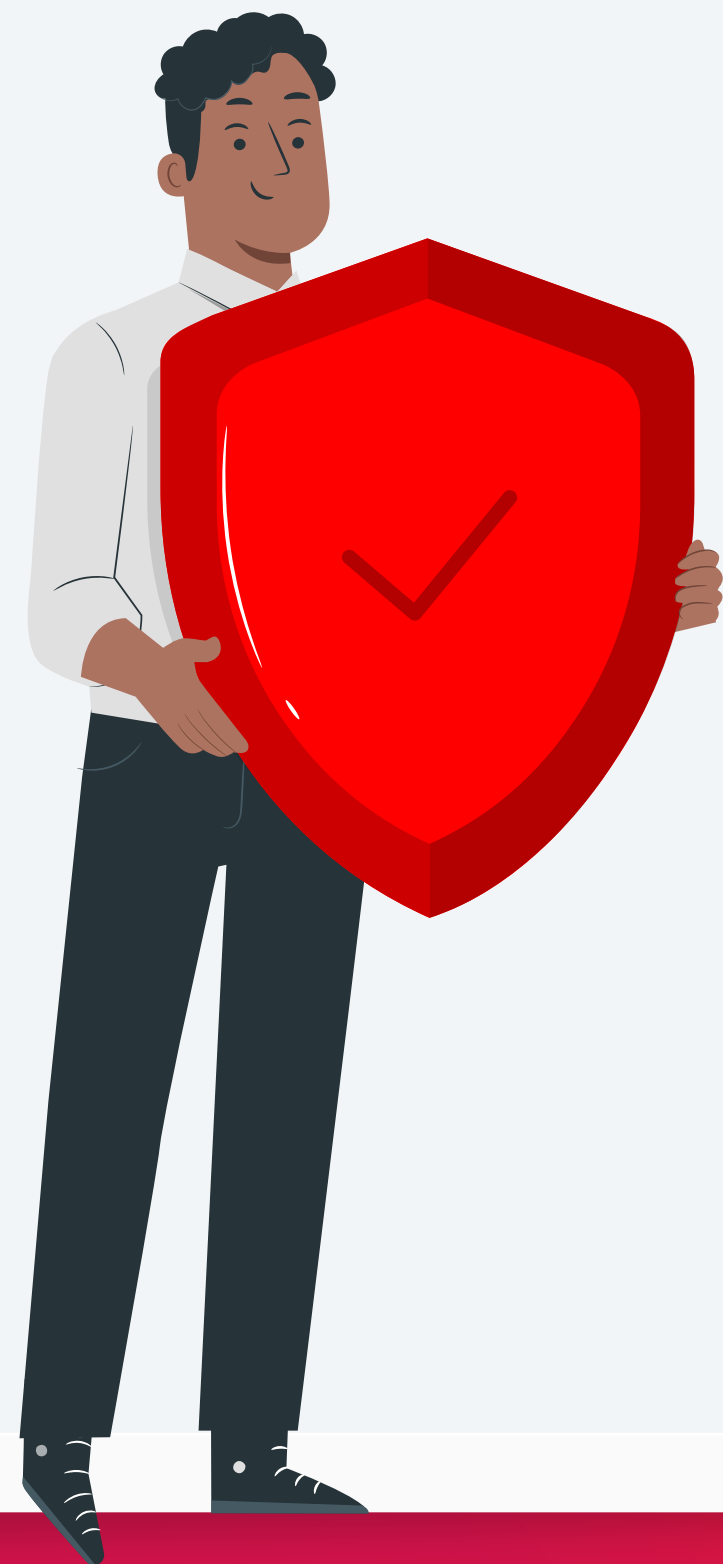
החלפתי את שם הרשת לשם שאינו מקושר לשם משפחתי

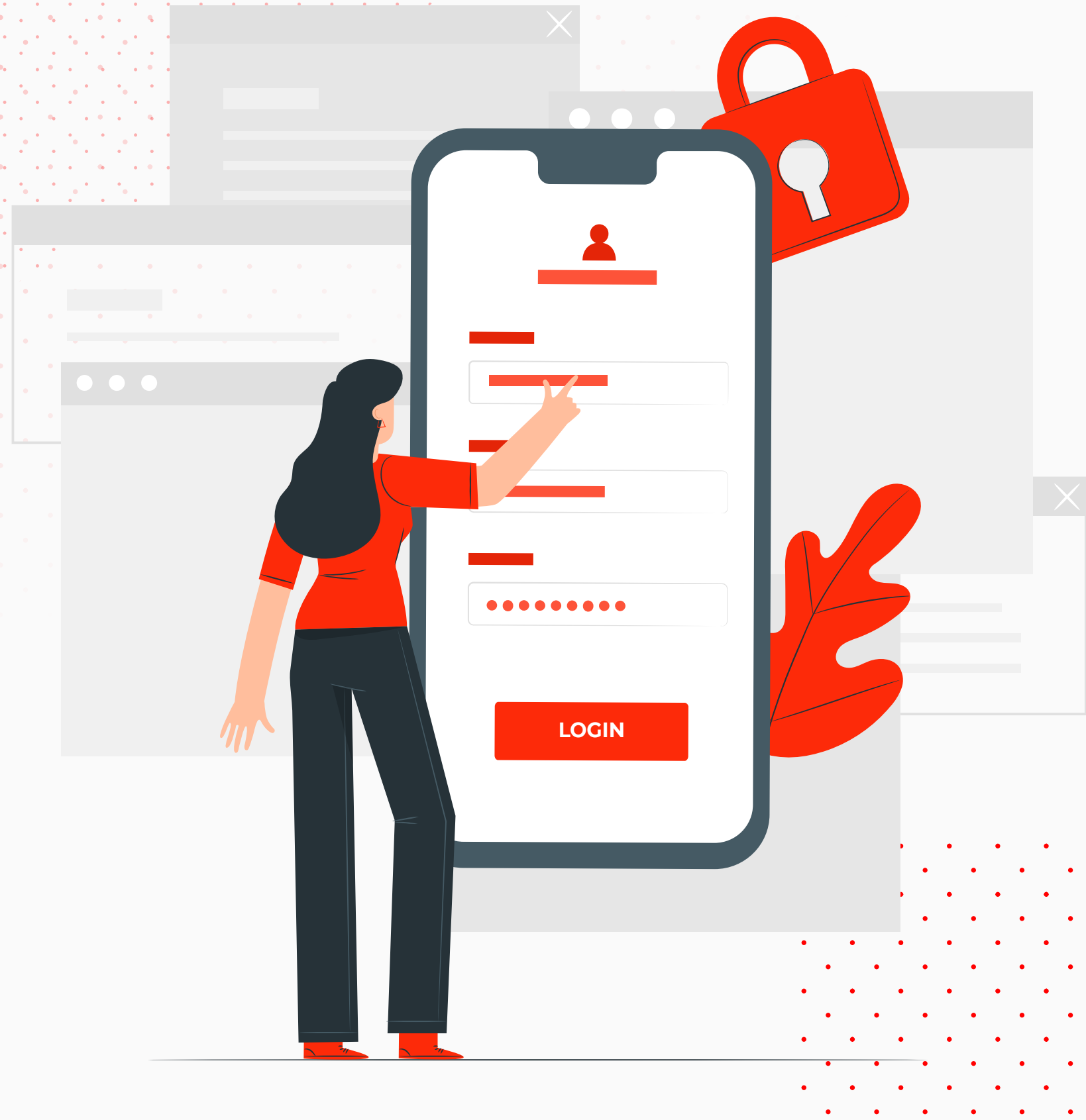
קבעתי סיסמה ייחודית ומורכבת לכניסה לרשת ה-Wi-Fi הביתית

עדכנתי בנתב הביתי שם משתמש וסיסמה ייחודית המורכבת מספרות ואותיות

בדקתי אם קיים עדכון קושחה (Firmware) לנתב הביתי (ראוטר)

שימו לב - סיוע בפעולות אלו ניתן לקבל בחינם בפנייה לספק האינטרנט שלכם.





2. אבטחת המחשב, הסמארטפון והטאבלט

הפעילות הדיגיטלית שלנו מתבצעת באמצעות מחשב, סמארטפון ו/או טאבלט. כדי למנוע גישה בלתי מורשית למכשירים אלו ולמידע שלנו שבתוכם, מומלץ להגדיר להם כניסה מאובטחת כדוגמת סיסמה, PIN קוד, זיהוי ביומטרי וכדומה. מכשירים אלו מושתתים על מערכות הפעלה ותוכנות המחייבות עדכונים והגנה מפני וירוסים ונוזקות באופן שוטף.




בפרק זה ננחה אתכם כיצד לבצע מספר פעולות חשובות במטרה להטמיע התנהלות בטוחה שתגביר את ההגנה על המכשירים והמידע שלכם.

אבטחת המחשב האישי

עדכון מערכת ההפעלה

המכשירים השונים שלנו מופעלים באמצעות מערכות הפעלה כדוגמת Windows, אנדרואיד, iOS. במערכות ההפעלה מתגלות מעת לעת פרצות אבטחה וכשלים ('באגים'). עקב כך, יצרני המערכות מפיצים באופן תדיר עדכונים המתקנים את התקלות וחוסמים את פרצות האבטחה. התקנת העדכונים משפרת את פעילות המערכת ומקטינה את הסיכון למתקפת סייבר.

לעדכון מערכת הפעלה של חברת Microsoft מסוג Windows 10 ומעלה

1. לחצו על אייקון זכוכית המגדלת בשורת המשימות 
2. בשורת החיפוש הקלידו "windows update" ולחצו על האייקון 
3. לחיצה על כפתור  תבצע חיפוש לעדכונים זמינים (פעולה האורכת עד מספר דקות בודדות). לצורך פעולה זו, מחשבכם נדרש להיות מחובר לאינטרנט.

• במידה ומערכת ההפעלה במחשבכם מעודכנת, תוצג לכם הודעה הדומה לצילום המצורף

You're up to date
Last checked: Yesterday, 21:50

Download and install

• במידה ונמצאו עדכונים נדרשים, המערכת תציג לכם אותם וכל שתדרשו זה ללחוץ על 'התקנה' ('Install updates').

You're up to date
Last checked: Yesterday, 21:50

Check for updates

View optional updates

• רכיבי החומרה במחשב שלנו כדוגמת כרטיס רשת, כרטיס מסך ודומיהם, נדרשים גם הם לעדכונים מעת לעת. **View** ניתן לבדוק אם קיימים עדכונים להורדה דרך **'optional updates'** במידה והאופציה מופיעה, לחצו עליה ולאחר מכן סמנו את שורות העדכון הנדרשות

Download and install

• על מנת לבצע את ההתקנה לחצו על Download and install

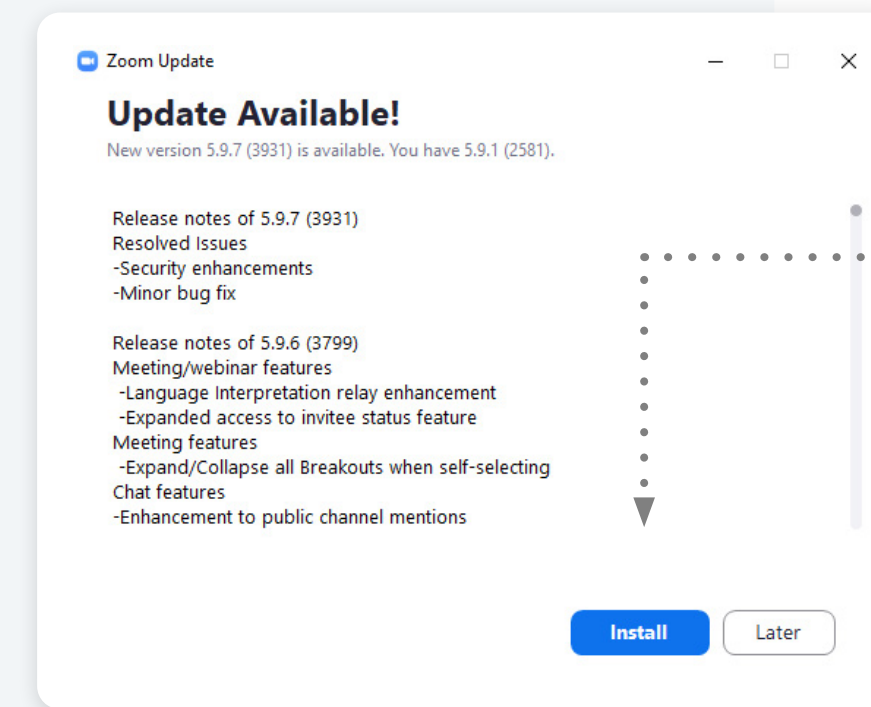
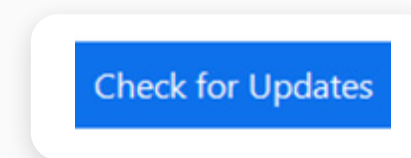
עדכון תוכנות

גם התוכנות שאנו מפעילים במחשב שלנו כדוגמת Zoom, אנטי-וירוס, נגני מדיה ועוד, נדרשות לעדכון תדיר. לכן חשוב שבכל פעם שאנו מפעילים אותן, ניכנס ביוזמתנו לאזור הגדרות המערכת ונבדוק אם יש עדכונים להתקין.



ניקח לדוגמה את zoom, אחרי שהזנו את שם המשתמש והסיסמה לחשבון ונכנסנו לתפריט הראשי, נלחץ על תמונת הפרופיל בחלק העליון ונלחץ על

check for updates



ובמידה וקיים עדכון למערכת, נלחץ על **Install** להתקינו.

עדכון דפדפנים

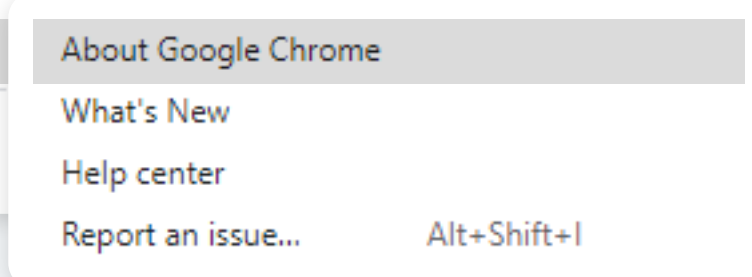
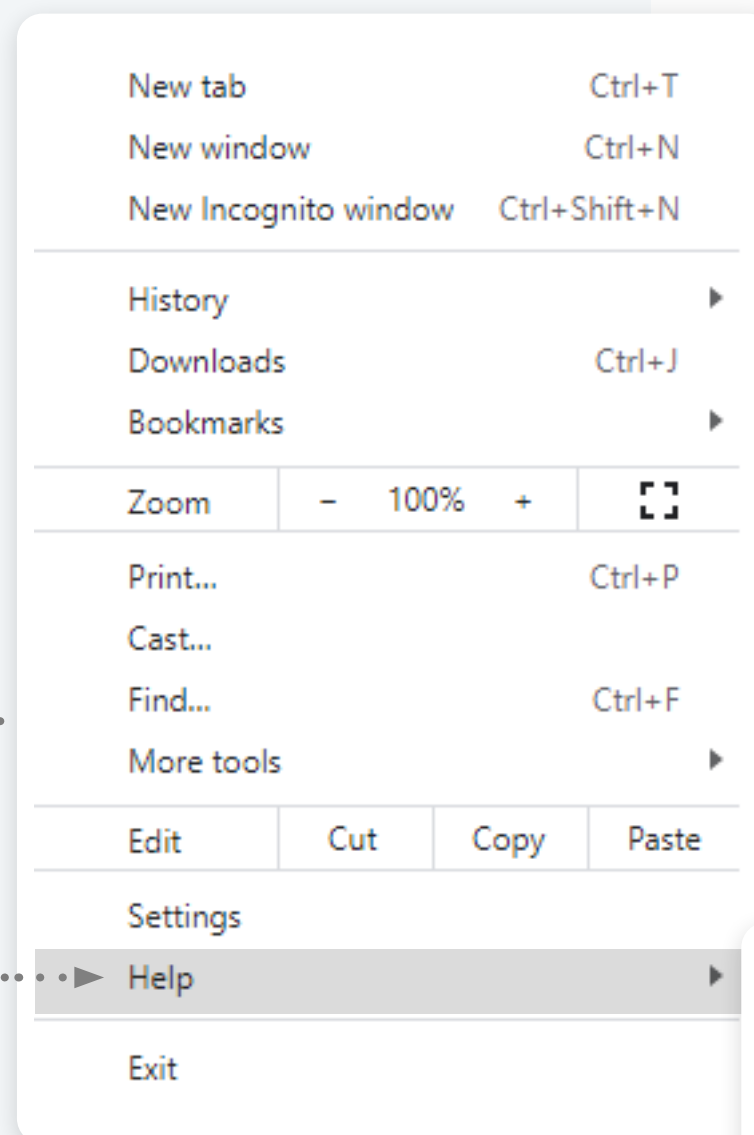
הדפדפן באמצעותו אנו גולשים באינטרנט הוא תכנה, המציגה לנו את דפי האינטרנט אליהם אנו גולשים. מעת לעת נדרש לעדכן את גרסת הדפדפן, להתקנת עדכוני אבטחת ותיקון כשלים.

לעדכון דפדפן 'כרום' של גוגל לדוגמה, יש לפעול באופן הבא:



• בפינה העליונה בדפדפן לחצו על סמל 3 הנקודות

• לחצו על 'עזרה' (Help) ולאחר מכן על 'אודות גוגל כרום' (About Google Chrome). במידה ונדרש עדכון, הדפדפן יתעדכן באופן אוטומטי



אנטי-וירוס


תכנת אנטי-וירוס היא אחת משכבות ההגנה הראשונות על המחשב והמידע שבתוכו, ועל כן חשוב מאוד להתקין אותה במחשב שלנו ולבצע סריקה באופן יזום ותדיר.

ניתן למצוא באינטרנט מגוון תוכנות אנטי-וירוס חנימיות המציעות יכולות מוגבלות וגם כאלו בתשלום. תכנות אנטי-וירוס בתשלום מספקות לרוב יכולות אבטחה נוספות כדוגמת חסימת סריקת פורטים (Port) והגנה בעת גלישה באינטרנט.

לאחר התקנת אנטי-וירוס, רצוי לבצע סריקת וירוסים מלאה. משם והלאה, רצוי לבצע באופן תדיר עדכון לתוכנה ומעת לעת לבצע סריקה מלאה.

במידה ואתם משתמשים במערכת הפעלה מסוג Windows 10 ומעלה, מומלץ לוודא שתוכנת Windows defender מופעלת ומוגדרת לביצוע סריקות באופן תדיר.

עשו זאת כך:

1. לחצו על אייקון זכוכית המגדלת 
2. הקלידו בשורת החיפוש "Windows Security" ולחצו על 
3. לחצו על "Virus & threat protection", שם ניתן לבצע סריקת וירוסים במחשב. 

גיבוי

במהלך הפעילות השוטפת שלנו במחשבינו האישיים, אנו צוברים קבצי מידע חשובים כדוגמת מסמכים אישיים, תמונות וסרטונים. שמירת הקבצים במחשב, ללא גיבוי, מעלה את הסיכון לאיבוד הקבצים עקב תקלה טכנית או כתוצאה מאירוע סייבר.

האחריות לגיבוי המידע האישי החשוב היא שלכם בלבד.

ישנן שתי דרכים עיקריות לגיבוי מידע:

1. גיבוי חיצוני – העתקת הקבצים לאמצעי אחסון חיצוני כדוגמת כונן אחסון חיצוני או דיסק און קי.

בסיום העתקת הקבצים לאמצעי האחסון החיצוני, חשוב לנתק את אמצעי האחסון מהמחשב ולשמור אותו במיקום נפרד מהמחשב.

2. גיבוי בשירות "ענן" – העתקת הקבצים לשירות אחסון ב"ענן" כדוגמת iCloud של אפל, Google Drive של גוגל, OneDrive של מיקרוסופט וכדומה. שירותי אחסון אלו מעניקים לרוב למנויים נפח אחסון מוגבל בחינם ומציעות נפחים גדולים יותר בתשלום.

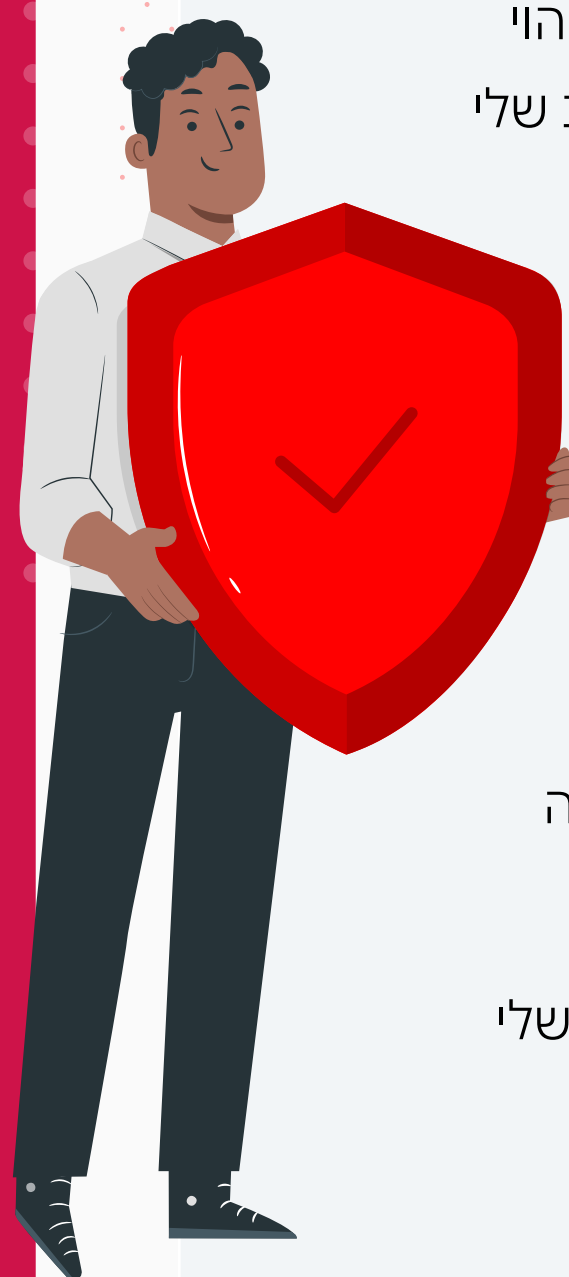
ריכזנו לכם את הטיפים להגברת האבטחה במחשבכם האישי. כל סעיף שתשלימו ותסמנו בו ✓, יגביר את רמת האבטחה במחשבכם:

הגדרתי סיסמת כניסה / זיהוי ביומטרי לפתיחת המחשב שלי

ווידאתי שמותקנת תכנת אנטי-וירוס, ביצעתי סריקה מלאה למחשב ויצרתי תזכורת לסריקה תדירה

אני מקפיד להתקין עדכוני אבטחה למערכת ההפעלה ולתוכנות באופן תדיר

גיביתי את המידע החשוב שלי



אבטחת הסמארטפון / טאבלט

עדכון מערכת הפעלה

• iOS בסמארטפונים של חברת Apple:

נכנסים להגדרות ('Settings') > לוחצים על 'כללי' ('General') > לוחצים על 'עדכון תוכנה' ('Update software').

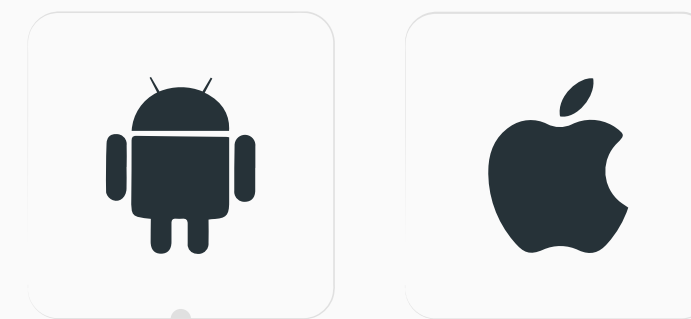
• אנדרואיד:

נכנסים להגדרות ('Settings') > לוחצים על 'מערכת' ('System & updates') > לוחצים על 'עדכון מערכת' ('Software update').

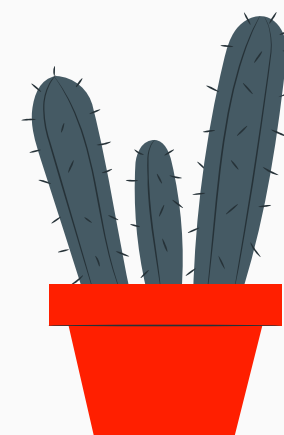
אנטי-וירוס

מכשירי הסמארטפון/טאבלט הם מחשבים לכל דבר, וככאלה הם גם חשופים לוורוסים וחשוב שנגן עליהם ועל המידע בהם באמצעות תכנת אנטי-וירוס. בדומה להסבר שתואר בחלק [המחשב האישי](#) למעלה.

ברגע שהחלטתם איזו תכנה להתקין במכשיר, חשוב שההתקנה תתבצע דרך חנות האפליקציות הרשמית בהתאם למכשיר (Google play / App store).



1. עדכון הגרסה עלול לאפס את מכשירכם ללא אפשרות לשחזור נתונים. על כן מומלץ לבצע גיבוי נתונים מראש. בהמשך מופיע פרק ייעודי לנושא הגיבוי וניתן לגשת אליו [בלחיצה על קישור זה](#).
2. מומלץ לבדוק קיום עדכונים באופן תדיר.



הרשאות גישה לאפליקציות

האפליקציות (יישומים) המותקנות במכשירי הסמארטפון שלנו משתמשות במשאבים שונים במכשיר שלנו (כדוגמת GPS, מצלמה, מיקרופון וכדומה), על מנת לספק לנו את שירותיהן. חשוב לבדוק מעת לעת אילו הרשאות התרנו לאפליקציות המותקנות במכשיר שלנו.

הרשאות עודפות לאפליקציות מעניקות להן גישה למידע שאנו לא בהכרח נרצה לספק להן, והוא זמין להן בכל רגע נתון. בחלק מהמקרים, האפליקציה מוכרת את המידע העודף לחברות נוספות, במטרה שיציעו לנו שירותי צריכה נוספים דרך הערוצים השונים (מייל / WhatsApp / SMS / רשתות חברתיות).

ניקח לדוגמה את אפליקציית Waze – על מנת שתספק לנו הכוונה וחיזוי בזמן אמת ליעד המבוקש, האפליקציה דורשת הרשאה למיקום המכשיר.

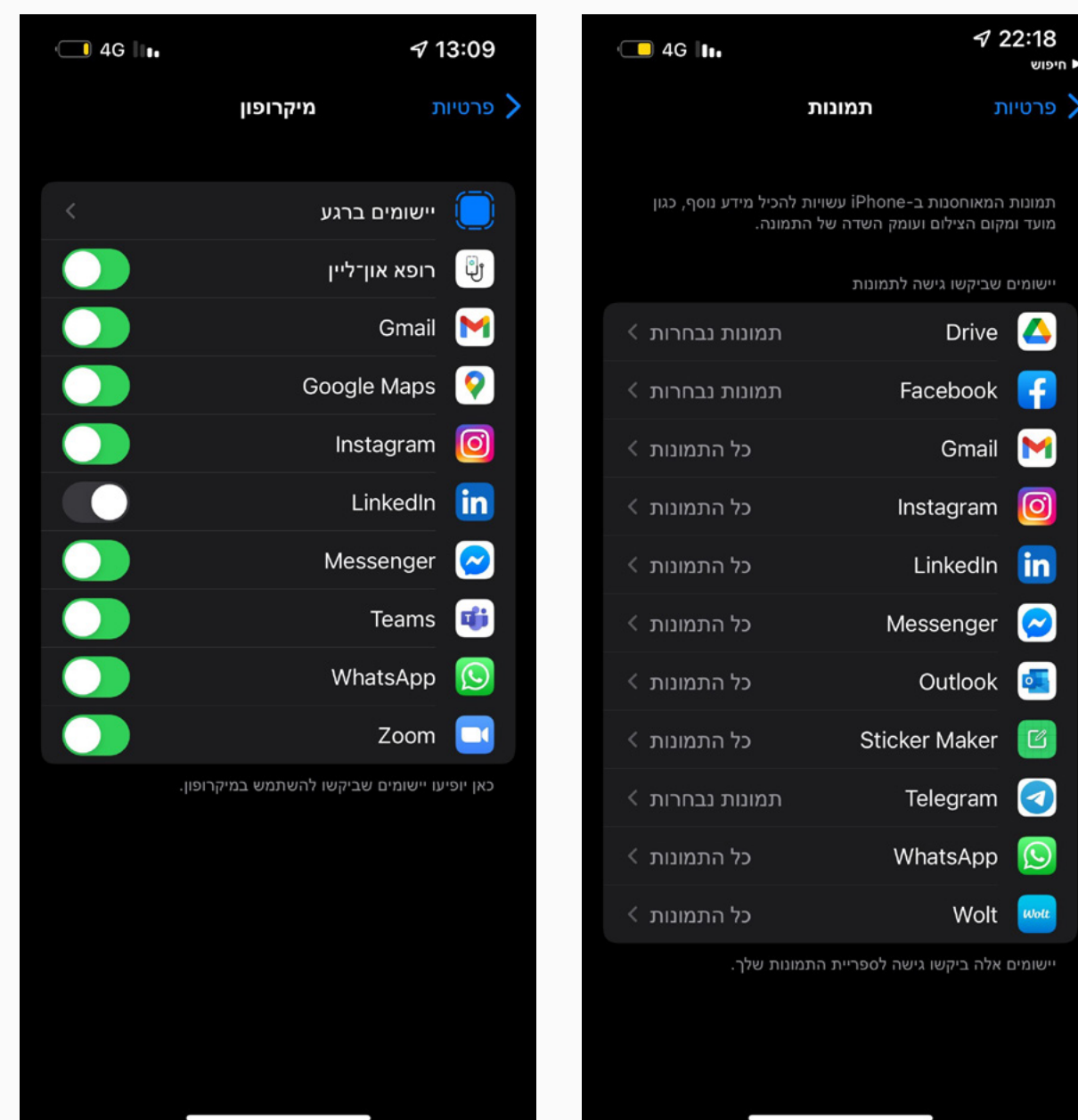
דוגמה נוספת היא אפליקציית WhatsApp, על מנת שנוכל להעביר תמונות לאנשי הקשר או בקבוצות, האפליקציה זקוקה לגישה למצלמה ולהתקן האחסון, היכן ששמורים קבצי התמונות והווידאו, וכן הלאה.

מומלץ מאוד לעבור באופן תדיר על אילו הרשאות אנו נותנים לאפליקציות, ולחסום את מה שמבחינתנו לא נדרש.

צמצום הרשאות לאפליקציות ב-iOS:

כנסו ל'הגדרות' (Settings):

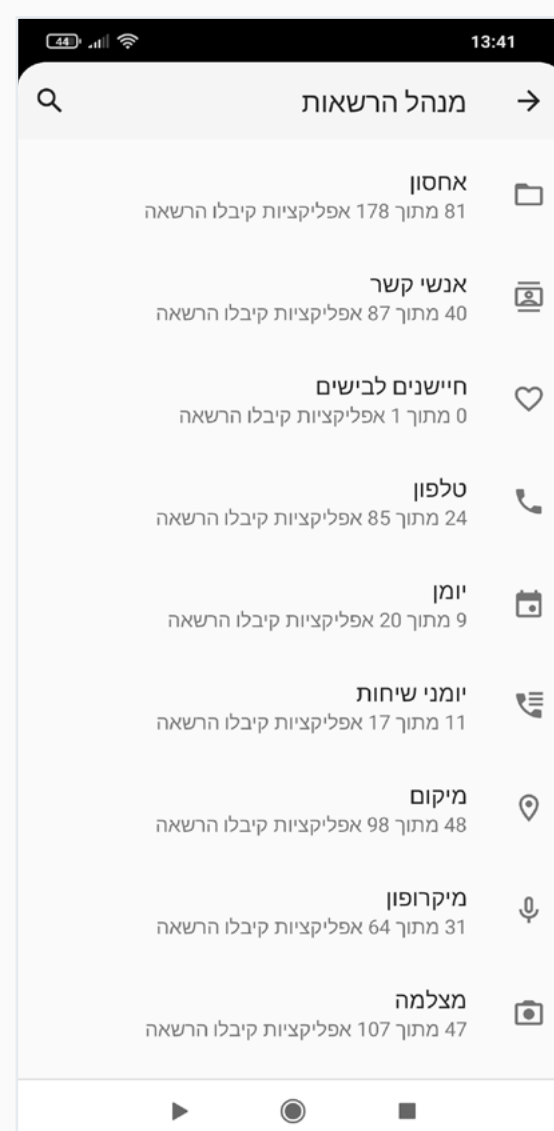
- בתחתית יופיעו האפליקציות המותקנות, בחרו באפליקציה הרצויה
- בדקו אילו הרשאות התרנו לה ובחנו האם הן עדיין נדרשות



צמצום הרשאות לאפליקציות באנדרואיד:

כנסו ל'הגדרות' (Settings):

- בחרו 'יישומים' (Apps)
- בחרו 'ניהול יישומים' (Manage Apps)
- בחרו באפליקציה הרצויה
- בדקו אילו הרשאות התרנו לה ובחנו האם נדרשות



גיבוי

בשונה מקבצי המידע השמורים במחשב האישי שלנו, ובשל נפח האחסון המוגבל בסמארטפון/טאבלט שלנו, קבצי המידע השמורים במכשירים אלו נדרשים לתשומת לב גבוהה יותר בהקשר של גיבוי המידע. גם במקרה הזה, אותן שתי דרכים עיקריות לבצע גיבוי -

1. גיבוי חיצוני, באמצעות חיבור מכשיר הסמארטפון/טאבלט למחשב פיסי. ניתן לשמור את המידע על גבי המחשב או לחילופין, להעביר אותו מהמחשב להתקן אחסון חיצוני כדוגמת דיסק און קי.

2. גיבוי בשירות "ענן", בהתאם לפירוט שתואר בחלק 'גיבוי אבטחת המחשב האישי'. להפעלת גיבוי זה ניתן לרוב להיכנס אל תפריט ההגדרות בנייד, לחפש את אפשרות הגיבוי ולהפעילה.

מומלץ להשתמש בשיטת גיבוי מצטבר (אינקרמנטלי). בשיטה זו מבצעים גיבוי מלא של המידע הקיים ולאחר מכן מבוצע גיבוי רק בעת הוספה / הסרה או שינוי בקבצים.



ריכזנו לכם את הטיפים להגברת האבטחה במכשירי הסלולר שלכם. כל סעיף שתשלימו ותסמנו בו ✓, יגביר את רמת האבטחה במכשירכם:

הגדרתי סיסמת כניסה / זיהוי ביומטרי לפתיחת המכשיר

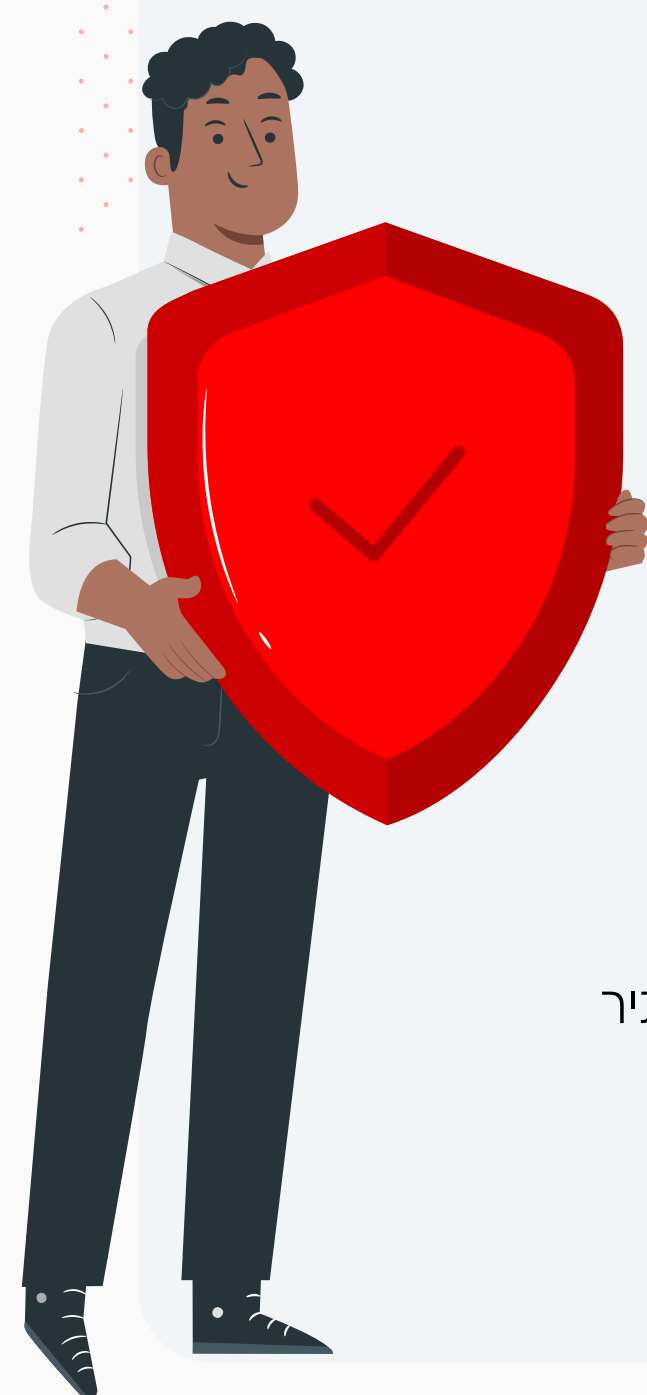
ווידאתי שמותקנת תכנת אנטי-וירוס במכשיר, ביצעתי סריקה מלאה למחשב ויצרתי תזכורת לסריקה תדירה

התקנתי עדכונים למערכת ההפעלה ולאפליקציות במכשיר

אני מוריד אפליקציות רק מהחנויות הרשמיות של Apple או Google Play

אני מקפיד לגבות את המידע החשוב באופן תדיר

יצרתי תזכורת לבדוק מעת לעת אילו הרשאות אני מתיר לאפליקציות ובוחן אם הן נדרשות



3. התנהלות בטוחה בגלישה באינטרנט

הרשמה לאתרים ושירותי אינטרנט

כמות השירותים שאנו צורכים דרך האינטרנט באופן יומיומי הולכת וגדלה כל הזמן. רשתות חברתיות, קניות מקוונות, קבלת ניוזלטרים, הרשמה לפורומים, והרשימה עוד ארוכה. לכל שירות כזה נרשמנו או נירשם בעתיד עם כתובת מייל.



טיפ

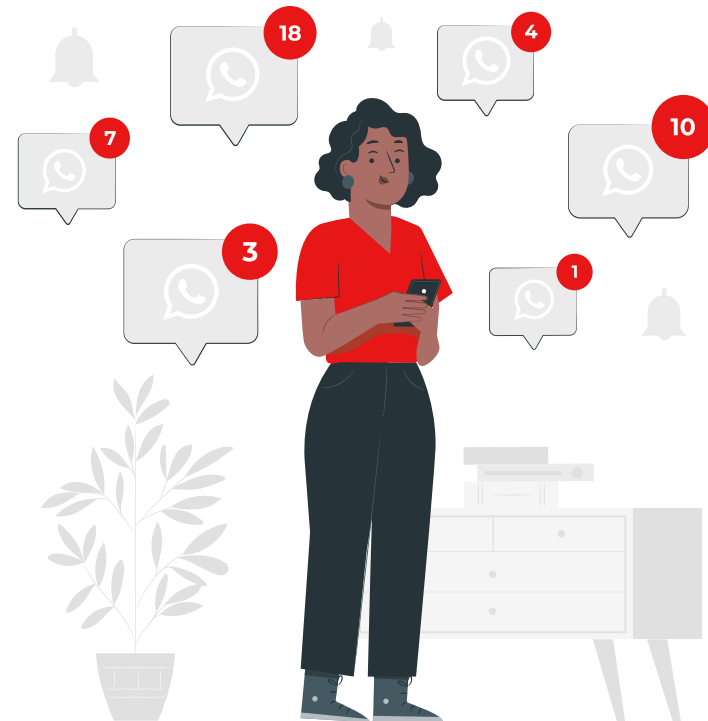
1. טיפ - קבעו סיסמה ייחודית ומורכבת לכל חשבון.
2. ניתן להקים תיבת מייל אישית נוספת, שתשמש אתכם להרשמה לשירותים מקוונים - בכך תחסכו מתיבת המייל האישית שלכם קבלת הודעות ניוזלטר, ספאם או פישिंग.

אימות דו-שלבי (Two Factor authentication) או Two (step verification)

זהו כלי חינוכי הנמצא באזור הגדרות האבטחה בכל אחד מהשירותים המקוונים שבהם אתם משתמשים. כלי זה מספק שכבת הגנה נוספת על חשבונותיכם באמצעות קוד אימות נוסף הנשלח לרוב ב-SMS למספר הטלפון הנייד שלכם או לתיבת המייל שלכם.

לאחר הפעלת האימות הדו-שלבי, גם אם גורם זדוני השיג את היוזר וסיסמת הכניסה לחשבונכם, הוא לא יוכל להיכנס לחשבון כל עוד אין בידיו את קוד האימות הייחודי הנשלח אליכם.





טיפים נוספים למניעת חשיפת מידע והפצת הודעות כזב בקבוצות כדוגמת WhatsApp:

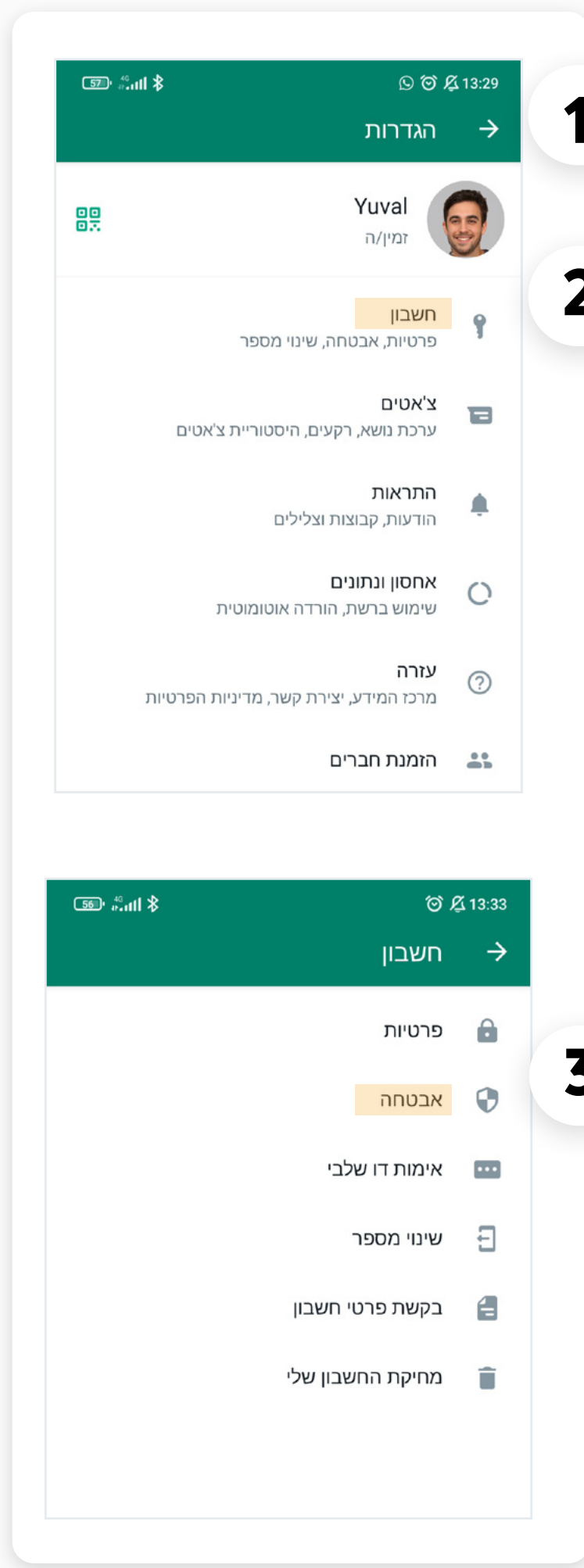
- אל תצטרפו לקבוצות שאינכם מכירים ואל תחשפו מידע אישי
- אל תפיצו מידע לא מאומת
- מחקו קבוצות מיותרות והסירו חברי קבוצה שאינכם מכירים

תרחיש השתלטות על חשבון WhatsApp:

חשבון ה-WhatsApp שלנו מוגדר לפי מספר הטלפון הסלולרי שלנו. כל מה שגורם זדוני צריך לעשות כדי להשתלט על חשבון ה-WhatsApp שלנו, הוא להפעיל מהמכשיר שלו את אפליקציית WhatsApp ולהזדהות עם מספר הטלפון שלנו.

לאחר מכן, אנחנו נקבל הודעת SMS מ-WhatsApp לנייד המכילה קוד אימות חד-פעמי בן 6 ספרות. על מנת שהגורם הזדוני ישלים את פעולת ההשתלטות על חשבון ה-WhatsApp שלנו, הוא צריך את הקוד שאנחנו קיבלנו ולכן, הוא ינסה לפנות אליכם בדרכים שונות (למשל במייל או בהודעת WhatsApp), ויבקש מכם את הקוד כדי להשלים את הפעולה.

לעולם לא מוסרים קוד אימות לאף אחד!



הגדרת שירות אימות דו-שלבי

מרבית השירותים המקוונים היום מאפשרים לנו להגדיר את השירות כדי להגן על החשבון. בחלק הזה נציג כיצד מגדירים את השירות במספר יישומים פופולריים:

WhatsApp:

1. באפליקציה, לחצו על 'הגדרות' ('Settings')
2. לחצו על 'חשבון' (Account) ולאחר מכן בחרו באפשרות "אימות דו-שלבי" (Two-step verification)
3. הגדירו קוד אימות בן שישה תווים יש אפשרות להזין כתובת דוא"ל אישית, לצורך שחזור סיסמה שנשכחה (Change email address)



משחק הילדים הפופולרי Fortnite:

בדומה לחשבונות מקוונים אחרים, גם במשחקי און-ליין ניתן להגדיר אימות דו-שלבי על מנת למנוע גניבת זהות.

נכנסים לאתר Epic games ומתחברים לחשבון המשתמש המשויך למשחק (<https://www.epicgames.com>)

1. לוחצים על שם המשתמש בצד ימין למעלה - ACCOUNT

2. לוחצים על "PASSWORD & SECURITY" בתפריט השמאלי

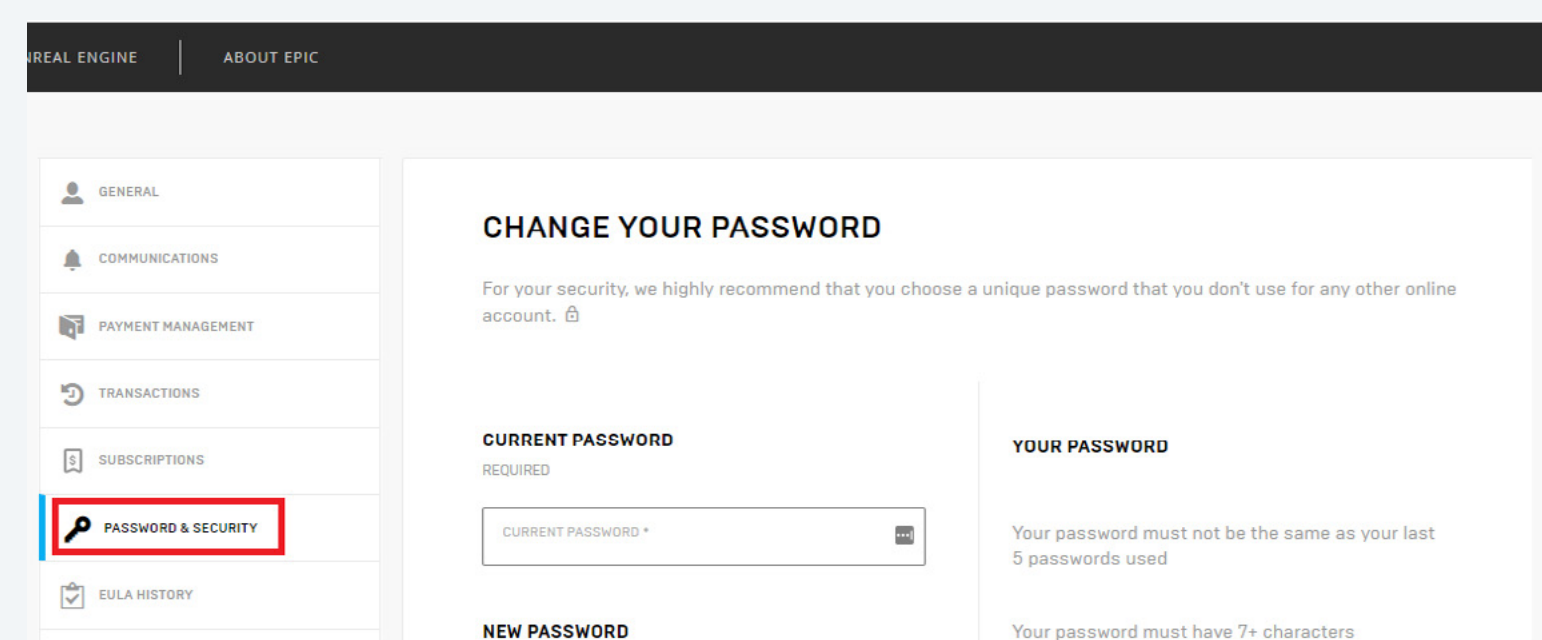
3. ניתן להגדיר את האימות הנוסף בדרכים הבאות -

• Sms authentication

הפעלת האימות תתבצע מעתה באמצעות קוד שישלח אלייך באמצעות הודעות סמס למכשיר הסלולר.

• Email authentication

הפעלת האימות תתבצע מעתה באמצעות קוד ייחודי שישלח לכתובת הדוא"ל האישית שלך.



SMS AUTHENTICATION

Use your phone as your Two-Factor Authentication (2FA) when you sign in you'll be required to use the security code we send you via SMS message.



Off

EMAIL AUTHENTICATION

Use a security code sent to your email address as your Two-Factor Authentication (2FA). The security code will be sent to the address associated with your account. You'll need to use it in when you sign in.



On

ניהול סיסמאות

סיסמה היא אמצעי ההגנה הראשוני ולעיתים היחיד, המאפשרת לנו גישה למחשבים/לחשבונות/למידע האישי שלנו ועוד. עקב כך, חשוב שנקבע לכל שירות סיסמה שונה וחזקה.

שימוש בסיסמה אחת עבור שירותים שונים עלולה לחשוף את חשבונותיכם השונים לפריצות וגניבת זהות.



רוצים לחסוך כאב ראש ולנהל את הסיסמאות במקום אחד?

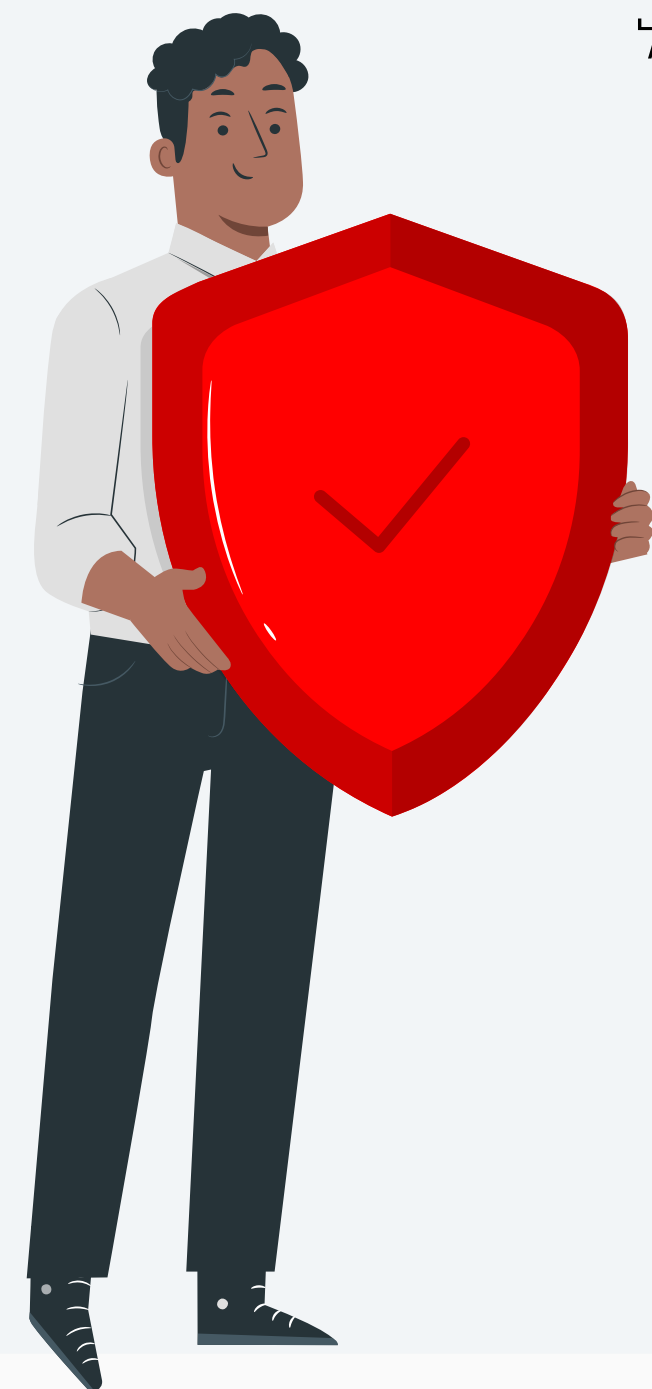
מנהל סיסמאות הוא כלי נוח ויעיל לקביעת סיסמאות ייחודיות וחזקות, לשמירתן באופן מאובטח וזמין, ולהטמעת הסיסמאות באופן אוטומטי בעת כניסה לחשבונותיכם. כך תוכלו לקבוע סיסמה ייחודית וחזקה לכל אתר או אפליקציה, מבלי צורך לזכור את כל הסיסמאות. השירות נתמך במערכות ההפעלה Windows, macOS, אנדרואיד, iOS ובדפדפני האינטרנט השונים.

דוגמאות לתוכנות ניהול סיסמאות נפוצות:

1password - i-Dashlane.

מנהלי הסיסמאות קיימים בגרסאות חינמיות מוגבלות או בתשלום חודשי ללא הגבלות.

ריכזנו לכם את הטיפים להגברת האבטחה בחשבונותיכם באינטרנט. כל סעיף שתשלימו ותסמנו בו ✓, יגביר את רמת אבטחתכם:



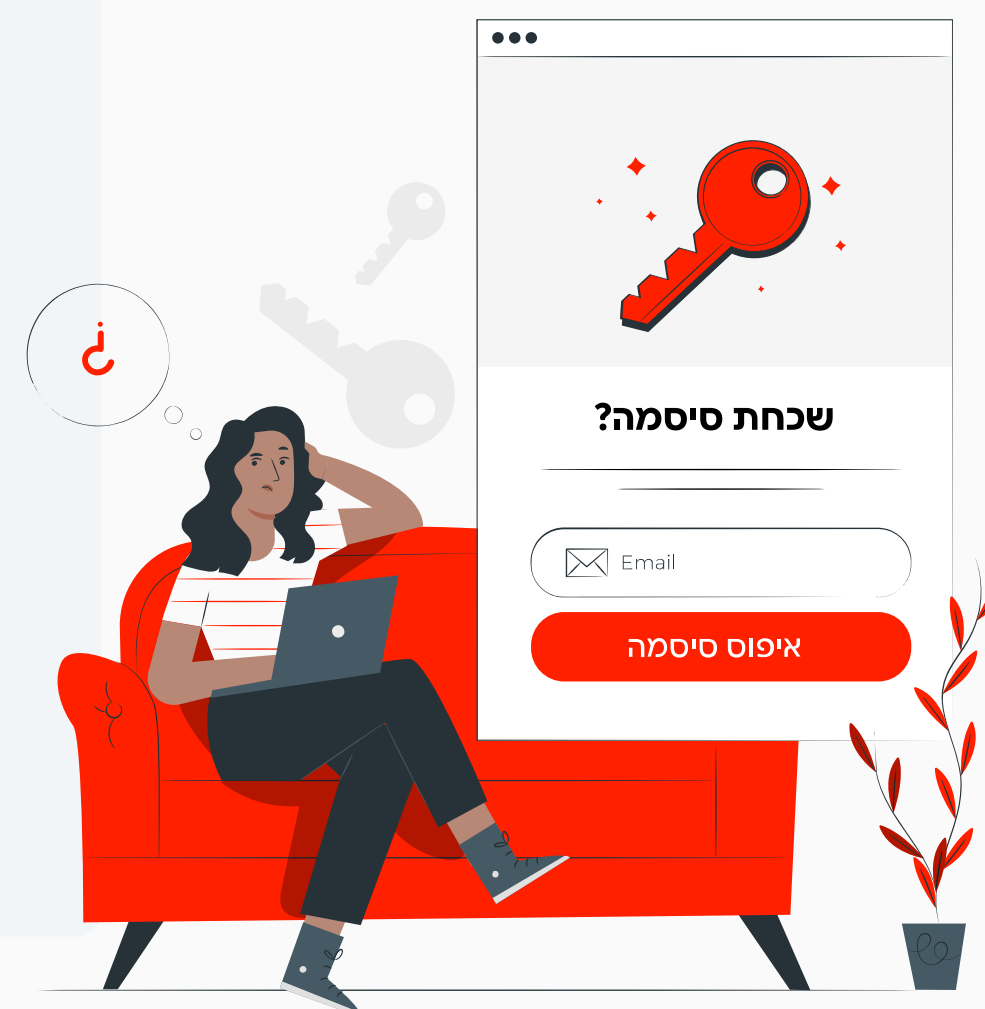
אני מקפיד להירשם לאתרים ושירותים עם כתובת המייל האישית שלי בלבד, ולא עם כתובת המייל הארגונית

הפעלתי אימות דו-שלבי בכל שירות שמאפשר זאת

אני פועל להחלפת הסיסמאות באתרים השונים לסיסמאות ייחודיות, המורכבות מ-8 תווים ומעלה, ומשלבות אותיות גדולות וקטנות, ספרות ותווים מיוחדים (!, @)

אני שומר את הסיסמאות שלי במקום בטוח, כדוגמת שירות 'מנהל סיסמאות'

אקפיד לא אמסור את הסיסמאות וקודי האימות שלי לאף גורם אחר





סיימתם את המדריך, כל הכבוד!