**אבטחת רשתות ביתיות ונתבים אלחוטיים (routers)**

**הקדמה**

כיום, כשהשימוש ברשתות אלחוטיות (WIFI) בסביבה הביתית הפך להיות כל כך נפוץ, יש צורך בנקיטת אמצעי הגנה ואבטחה עליה. מעצם טיבעה, תקשורת אלחוטית מתאפיינת בכך שהמידע המשודר מהמחשב ואליו עובר באוויר ולכן הוא חשוף להאזנה. עובדה זו גורמת לכך שבאמצעות כלים שונים, ניתן לצותת לתשדורת האלחוטית, מה שעלול להביא לחשיפה של מידע רגיש.

כתוצאה מכך, רשת אלחוטית שאינה מאובטחת כיאות, עלולה לחשוף את הנתב והרשת הביתית עצמה להאקרים וגורמים זרים המעוניינים לזרוע בה הרס ולגזול רוחב פס מבלי שתדע.  בכדי למנוע זאת, יש צורך חיוני ביישום מגוון של מנגנוני אבטחה שיגנו על הרשת האלחוטית.

חשוב להדגיש שאין אבטחה מושלמת לשום רשת (חוטית או אלחוטית) ופורץ עיקש עם מטרה ברורה ואמצעים להשגתה, יוכל להתגבר על כל מנגנון אבטחה שתיישמו.  יחד עם זאת, יישום אפשרויות האבטחה הנסקרות במדריך הזה יגביר עד מאוד את בטחון הרשת האלחוטית וההגנה על המרחב הפרטי שלכם.

**הערה**:

תמונות המסך המצורפות למדריך זה הן של הנתב BR-6574 של חברת Edimax אך יש לזכור שאופן הגדרת מנגנוני האבטחה שונה מנתב לנתב. במידה ואתם זקוקים לסיוע, יש להיעזר במדריך המשתמש של הנתב או לשאול שאלום בפורום המומחים של Block.

**סקירה קצרה של האפשרויות השונות לאבטחת הרשת**

הטבלה להלן סוקרת את מנגנוני האבטחה השונים הקיימים בנתבים אלחוטיים בייתים ומדרגת את חשיבות יישומם ואת רמת ההגנה שהם נותנים.  ברמה הבסיסית ביותר אנו ממליצים לכל אחד לאבטח את הנתב האלחוטי שלו בשלושה מישורים המודגשים בצהוב:

* שינוי סיסמת הכניסה לנתב;
* שינוי זיהוי הרשת (SSID) שלו;
* הגדרת הצפנת התקשורת בין הנתב לרכיבים המחוברים אליו ב-WiFi בתקן WPA2.

|  |  |  |  |
| --- | --- | --- | --- |
| **מנגנון** | **תאור קצר** | **חשיבות יישום** | **חוזק ההגנה** |
| שינוי סיסמת כניסה לנתב | סיסמת הכניסה לנתב נותנת למשתמש מחובר אליו גישה לתפריטי הניהול שלו. | גבוהה | בינונית |
| שינוי ה-SSID של הנתב | ה-SSID הוא השם של הרשת האלחוטית שהנתב משדר לסביבה. | בינונית | נמוכה |
| חסימת שידור ה-SSID של הנתב | ה-SSID הוא השם של הרשת האלחוטית שהנתב משדר לסביבה. | נמוכה | נמוכה |
| ביטול מנגנון ה-DHCP של הנתב | מנגנון ה-DHCP מחלק באופן אוטומטי כתובות IP למחשבים המתחברים לנתב. | נמוכה | נמוכה |
| סינון כתובות MAC בעלות גישה לנתב | ה-MAC הוא מזהה חד חד ערכי של כרטיס הרשת וניתן להגדיר בנתב רשימת MAC המאושרים לגישה. | נמוכה | נמוכה |
| הצפנה התקשורת תוך שימוש במנגנון WEP, ‏WPA או WPA2. | הצפנה השידור האלחוטי באמצעות סיסמא המוסכמת בין המחשב לנתב. | גבוהה | WEP – נמוכה WPA – גבוהה**\*** WPA2 – גבוהה |
| ביטול האפשרות לניהול מרחוק | מרבית הנתבים מאפשרים ניהול מרחוק על גבי רשת האינטרנט. | בינונית | גבוהה |
| הקטנת עוצמת השידור האלחוטי | הקטנת עצמת השידור האלחוטי מצמצמת את הרדיוס בו ניתן לקלוט את האות האלחוטי. | בינונית | בינונית |
| ביטול מנגנון ה- UPNP של הנתב | מנגנון ה-UPNP מאפשר לנהל את מרכיבי הרשת בצורה קלה ופשוטה יותר. | בינונית | בינונית |
| ביטול מנגנון ה-WPS של הנתב | מנגנון ה-WPS מאפשר לחבר לנתב, בקלות ופשטות, התקנים אלחוטיים  שונים. | בינונית | גבוהה |
| שימוש ב-SSID נפרד לאורחים | במידה והנתב כולל תכונה זו, שימוש בה יאפשר הפרדה בין השימוש הבייתי הרגיל לשימוש מזדמן של אורחים. | בינונית | בינונית |

**\***בתנאי שמפתח ההצפנה (הסיסמא) ארוך ומורכב משילוב של אותיות, ספרות ותווים מיוחדים.

**איך מוצאים את כתובת הנתב ברשת הביתית?**

ישנן מספר חלופות למצוא את כתובת ה-IP של הנתב, שהיא נתון חיוני לצורך שינוי ההגדרות שלו.

האפשרות הראשונה (במערכת הפעלה windows) היא לפתוח חלון של command prompt (דרך כפתור ה"התחל") ולהקיש ipconfig. במידע שיוצג מהרצת השאילתא, יש לחפש את כתובת ה-IP המופיעה ליד Default Gateway (בדוגמא להלן: 192.168.1.1.). זו כתובת הנתב, וכדי להכנס לממשק הניהול שלו יש להקיש בשורת הכתובת בדפדפן את כתובת ה-IP שלו.

**דוגמא**: הרצת פקודת ipconfig:

**C:\Users\user>ipconfig**

**Windows IP Configuration**

**….**

**Default Gateway . . . . . . . . . : 192.168.1.1**

**….**

אפשרות נוספת למציאת כתובת הנתב היא התקנת תוכנה במכשיר הנייד המחובר לרשת ה-wifi הביתית, דוגמת IP Tools - Router Admin Setup & Network Utilities מחנות האפליקציות של Android או iOS. תוכנות אלה מזהות, בין היתר, את כתובת ה-IP של הנתב. אחרי זיהויה, יש להזין אותה בשורת הדפדפן ולקבל את ממשק הכניסה.

**הערה:** חלק מספקי הגישה לאינטרנט בישראל אינם מאפשרים למשתמש הביתי לשנות הגדרות של הנתב, חלקן או כולן. במקרה זה, לאחר הקלדת כתובת ה-IP בדפדפן, תגיעו לממשק ייעודי שפותח על ידי ספק הגישה ופעולתיכם תוגבלנה על ידיו. במקרה זה, יש לפנות את ספק הגישה לאינטרנט ולבקש ממנו ליישם את ההמלצות המפורטות במדריך זה.

**שינוי סיסמת כניסה לנתב**

על מנת להיכנס לממשק התפריטים של הנתב, ברוב המקרים, יש להקיש שם משתמש וסיסמא.  רבים מהמשתמשים נוטים לזלזל בנקודה זו ולהשאיר את שם המשתמש והסיסמא בברירת המחדל שלהם.  באופן זה משאירים בעלי הנתב דלת כניסה פתוחה לרווחה לפורץ המזדמן ונותנים לו אפשרות לשחק בתפריטים כאוות נפשו.

בשלב הראשון של הגדרת נתב **מומלץ מאוד לשנות את שם המשתמש (אם ניתן) ואת סיסמת הכניסה**. כמו בכל הגדרת סיסמא, רצוי לבחור סיסמא המכילה תווים, ספרות וסימנים מיוחדים באורך של לפחות שמונה תווים.  כיוון שהשימוש בשם המשתמש והסיסמא של הנתב אינו תדיר, רצוי לרשום/לזכור את שם המשתמש והסיסמא, כיוון שאין דרך לשחזר אותם.  במידה ונשכחים פרטים אלה, הדרך היחידה לגשת לתפריטי הנתב היא באמצעות ביצועRESET  מלא לנתב ישירות בנתב עצמו (ולא בחיבור דרך הרשת האלחוטית).

**שינוי ה-SSID של הנתב**

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/SSID-N.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/SSID-N.jpg)ה-SSID (ראשי תיבות של Service Set Identifier) הוא השם שמזהה את הרשת האלחוטית. כאשר התקן בעל יכולת אלחוטית (למשל טלפון חכם) מנסה להתחבר לרשת אלחוטית, מוצגים בפניו כל שמות הרשתות (SSID)  הנקלטות בסביבה הקרובה.

לעיתים קרובות יצרניות הנתבים קובעות לרשתות האלחוטיות שלהן שמות ברירת מחדל, כגון "default". ורצוי לשנות זאת משתי סיבות עיקריות -- מתן אפשרות לאתר את הרשת הספציפית שלכם (כמה רשתות הנקראות default יש בסביבה שלכם?) והקשחה מסוימת של מנגנון ההצפנה מסוגWPA , אותו נסקור להלן.

**לפיכך מומלץ מאוד לשנות את שם ברירת המחדל של הרשת בנתב שלכם,** אך באותה מידה יש לוודא שהשם שאתם נותנים לרשת אינו מזהה אתכם -- כלומר אל תבחרו את השם הפרטי או שם המשפחה שלכם, את הקומה בה אתם גרים, שם החברה בה אתם עובדים וכדומה.  עדיף לבחור צירוף אקראי של אותיות ומספרים באורך של לפחות 8 תווים.

**חסימת שידור ה-SSID של הנתב**

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/SSID-H.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/SSID-H.jpg)כפי שצוין בסעיף לעיל, ה-SSID הוא השם שמזהה את הרשת האלחוטית והוא מוצג למשתמש בעת שהוא מנסה לאתר את הרשתות האלחוטיות בסביבתו.

רבים נוטים לחשוב שעל ידי הסתרת ה-SSID ואי הצגת שם הרשת במסך האיתור של ההתקן האלחוטי, הם יבטיחו לעצמם הגנה טובה.

ההיגיון העומד מאחורי גישה זו הוא פשוט -- אם לא רואים את הרשת אז גם לא ניתן להתחבר אליה.

בפועל, הסתרת ה-SSID היא בסופו של דבר מנגנון "בת יענה".  בת היענה טומנת את ראשה בחול וחושבת לעצמה שאם היא לא רואה את הטורפים שלה, אזי גם הם לא רואים אותה...  ברשתות אלחוטיות הדבר די דומה.

הסתרת ה-SSID לא ממש מסתירה את הרשת האלחוטית ובאמצעי ניטור פשוטים למדי ניתן לאתר את השם שלה.  מעבר לכך, הסתרת השם יכולה לפגוע ברמת האבטחה של הרשת האלחוטית במידה ונבחרת הצפנת WPA (פרטים כאמור להלן).

**לפיכך מומלץ שלא תחסמו את שידור ה-SSID שלכם**.

**ביטול מנגנון ה-DHCP**

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/DHCP.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/DHCP.jpg)מנגנון ה-DHCP, הקיים בכל נתב, מקצה באופן אוטומטי, לכל התקן רשת המתחבר אליו, הן באופן חוטי והן באופן אלחוטי, כתובת IP.

לפיכך, אם הרשת האלחוטית אינה מוגנת, או אם ההגנה שלה נפרצה, יכול המחשב הזר המתחבר אל הנתב, לקבל כתובת IP באופן מיידי.

לפיכך, ועל מנת לסגור את הפרצה הזו, יש כאלה הנוטים לבטל את מנגנון ה-DHCP של הנתב ולקבוע לכל מחשב כתובת IP באופן ידני.  ניתן לקרוא על הנושא במדריך [**זה**](https://www.netcheif.com/Articles/FixedIP/FixedIP.htm). סיבה נוספת המביאה משתמשים לבטל את מנגנון ה-DHCP היא הרצון לקבוע כתובת IP קבועה למחשב מסוים לצורך קידום פורטים (port forward) עבור תוכנות שיתוף קבצים (עוד על נושא זה ניתן לקרוא [**כאן**](https://www.netcheif.com/Articles/P2P_PF/P2P_FP.htm)(.

לכאורה זו נראית שיטה יעילה, אך יש לה מספר פגמים.  ראשית, למרבית הנתבים יש טווח כתובות IP מוגדר -- רוב הנתבים מחלקים כתובות IP בטווח 192.168.1.1-192.168.1.255 או בטווח 192.168.0.1-192.168.0.255, כך שמאוד קל לנחש כתובת IP חוקית. שנית, ניהול כתובת IP באופן ידני היא משימה מורכבת, במיוחד כאשר יש ברשת מספר גדול של מחשבים.

**ההמלצה היא להימנע משימוש בשיטה זו**, אך אם כבר בחרת לעשות בה שימוש, כדאי מאוד לשנות את טווח הכתובות של הנתב לסגמנט שאינו בשימוש נפוץ.

**סינון כתובת MAC**

[[https://www.netcheif.com/Articles/WiFiSecurity/JPG/ipconfig_small.jpg](https://www.netcheif.com/Articles/WiFiSecurity/JPG/ipconfig.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/ipconfig.jpg)ה-MAC (ראשי תיבות שלMedia Access Control ) הוא מזהה חד חד ערכי, בעל 12 ספרות הקסה-דצימליות, של כרטיס הרשת האלחוטי שלכם.

באמצעות 12 ספרות (0-9,A-F) ניתן לייצג את המספר 2 בחזקת 48 (כלומר 281,474,976,710,656).

בפועל, ניתן להתייחס אל ה-MAC כאל תעודת הזהות של כרטיס הרשת. בצילום המסך משמאל, כתובת ה-MAC של כרטיס הרשת (Physical Address) היא 00‎-12-‎CF-‎9A-‎71-‎8F. את כתובת ה-MAC של כרטיסי הרשת תוכלו למצוא די בקלות באמצעות הפקודה ipconfig /all.

**הערה:** למעשה, לא רק לכרטיסי רשת אלחוטיים יש MAC ייחודי.  לכל התקן ברשת (כרטיס רשת חוטי, כרטיס רשת אלחוטי, נתב, טלפון חכם וכיוב') יש כתובת MAC ייחודית משלו.

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/MAC.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/MAC.jpg)סביר להניח שבנתב שלכם קיים מנגנון החוסם את האפשרות שהתקן רשת, בעל MAC מסוים, יתחבר אל הנתב האלחוטי.

הפעלת האפשרות הזו בנתב – כלומר להרשות רק להתקני רשת עם MAC מסויים להתחבר אליו (בדרך כלל היא נקראת MAC Address Filtering), תמנע מהתקנים זרים להתחבר אל הרשת שלכם.

לכאורה, זה נראה מנגנון יעיל מאוד אלא שיש בו פגם מהותי אחד - את כתובת ה-MAC ניתן לזייף די בקלות.  באמצעות כלי האזנה פשוטים למדי ניתן לנטר את התקשרות האלחוטית ולאתר את כתובת ה-MAC של כרטיס הרשת האלחוטי החוקי ולהשתמש בה על מנת להתחבר אל הנתב האלחוטי.

**לפיכך מומלץ לוותר על אפשרות האבטחה** הזו כיוון שהיא קלה מאוד לפריצה ונותנת רק אשליה של אבטחה.

**הצפנה באמצעות סיסמא במנגנון WEP,‏ WPA או WPA2**

השיטה הנפוצה ביותר (וגם היעילה ביותר) להגנה על הרשת האלחוטית ומניעת אפשרות הציתות למידע העובר בה, היא הצפנת התקשורת.  הרעיון המונח בבסיס ההגנה הזו הוא די פשוט -- אם נצפין את התעבורה האלחוטית, לא יהיה ניתן לפענח את המידע העובר בין המחשבים לנתב ועל ידי כך נמנע פריצות אל הרשת.  על בסיס הרעיון הזו פותחו מספר מנגנוני הצפנה, השונים זה מזה בעוצמת ההגנה והתקורה (overhead) שהם מעמיסים על ערוץ התקשורת.

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WEP.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WEP.jpg)תקן ההצפנה הראשון שפותח מכונה **WEP** (ראשי תיבות של Wired Equivalent Privacy). מידע מפורט יותר על התקן הזה ניתן למצוא [**כאן**](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy).

זהו תקן הצפנה בסיסי מאוד ובמשך זמן רב הוא גם היה הנפוץ ביותר.  הבעיה עם תקן ה-WEP היא שרמה ההצפנה שלו נמוכה וקלה מאוד לפריצה.  באמצעות כלים פשוטים ניתן לנטר את התקשורת האלחוטית ולפענח את מפתח ההצפנה.

**מומלץ להצפין את התקשורת האלחוטית במנגנונים מתקדמים יותר מ-WEP** (ראו להלן).

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WPA.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WPA.jpg)בגלל חולשת תקן ה-WEP, פותחה שיטה נוספת המכונה **WPA** (ראשי תיבות שלWi-Fi Protected Access). מידע מפורט יותר על התקן הזה ניתן למצוא [**כאן**](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access).

זהו תקן אבטחה מתקדם יותר הנותן מענה טוב לחולשת ההגנה של תקן WEP. ראשית, מפתח ההצפנה בתקן WPA ארוך יותר (בערך פי 5) מזה של WEP. שנית, תקן אבטחה זה מגדיר פרקי זמן נתונים בהם מוחלף מפתח ההצפנה ולכן מקטין את משך הזמן בו ניתן לפענח ולהשתמש במפתח.

מנגנון ה-WPA עושה שימוש בפרוטוקול ההצפנה TKIP (ראשי תיבות שלTemporal Key Integration Protocol, מידע נוסף יש [**כאן**](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol)) ולכן לעיתים קרובות מכונה השיטה הזו בתפריטי הנתבים כ-WPA(TKIP).

הצפנה במנגנון ה-WPA נותנת הגנה טובה על הרשת האלחוטית, במיוחד אם נבחר מפתח הצפנה המכיל תווים, ספרות וסימנים מיוחדים.  אמנם קיימות דרכים לפרוץ את מנגנון ה-WPA אבל בחירת מפתח אורך ומורכב, תקטין מאוד את סכנת הפריצה.

כאן גם המקום להזכיר, שהסתרת ה-SSID מקלה מאוד על ניחוש מפתח ההצפנה כיוון שב-TKIP מבוצעHASH  של מפתח ההצפנה עם ה-SSID ואם ה-SSID לא משודר, הרבה יותר קל לגלות את המפתח.  לכן רצוי מאוד, כפי שהמלצנו לעיל, לא להסתיר את ה-SSID.

**בשורה התחתונה מומלץ להשתמש במנגנון ה-WPA רק אם ההתקן האלחוטי אינו תומך ב-WPA2, המתואר להלן.**

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WPA2.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WPA2.jpg)נכון להיום, מנגנון **WPA2** הוא מנגנון ההצפנה הטוב ביותר לרשתות אלחוטיות.  המנגנון מסתמך על הפרוטוקול AES (ראשי תיבות של Advanced Encryption Standard - מידע נוסף [**כאן**](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)).

לכן, לעיתים קרובות, מכונה השיטה הזו בתפריטי הנתבים כ-WPA2 (AES). גם כאן, בדומה ל-WPA, כל מה שיש לעשות הוא לבחור במפתח הצפנה מורכב וארוך.  הבחירה ב-WPA2 עדיפה גם מבחינת ניצול רוחב הפס האלחוטי, כיוון שמנגנון זה מנצל רק חלק קטן מרוחב הפס, זאת לעומת WEP ו-WPA שיכולים להשתמש בעד 40% מרוחב הפס.

בשורה התחתונה, **ההמלצה החד משמעית היא להשתמש במנגנון WPA2.**

**הערות:**

1. נכון לאמצע 2019, נמצא בפיתוח תקן הצפנה מתקדם יותר המכונה WPA3. מנגנון זה יהיה זמין בנתבים במהלך שנת 2020.
2. מחולל סיסמאות טוב ניתן למצוא [**כאן**](https://www.comparitech.com/privacy-security-tools/password-generator/).

**ביטול האפשרות לניהול מרחוק**

[[https://www.netcheif.com/Articles/WiFiSecurity/JPG/Remote_small.jpg](https://www.netcheif.com/Articles/WiFiSecurity/JPG/Remote.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/Remote.jpg)במרבית הנתבים האלחוטיים קיימת אפשרות לניהול מרחוק דרך רשת האינטרנט.  אופציה זו היא שימושית במידה והנכם מנהלים ותומכים ברשתות מרוחקות.

יחד עם זאת, במרבית רבים אפשרות זו מהווה חור אבטחה משמעותי כיוון שקיימת סכנת פריצה לנתב דרך רשת האינטרנט הציבורית.

בחלק מהנתבים קיימת אפשרות להגביל את כתובת ה-IP המרוחקת ממנה ינוהל הנתב, אך אופציה זו שימושית רק אם ברשותכם כתובת IP חיצונית קבועה.  לחילופין (ולעיתים בנוסף), קיימת אפשרות לנהל את הנתב דרך פורט השונה מפורט 80 הסטנדרטי.

לפיכך, במידה והינכם נדרשים לנהל נתב מרחוק, רצוי מאוד להצטייד בנתב שיש בו את שתי האופציות הללו ולעשות בהן שימוש, כמובן תוך הגדרת סיסמת כניסה איכותית.

בעקרון, ואם ממש אין ברירה אחרת, **אנו ממליצים לכבות את האפשרות לניהול מרחוק של הנתב.** בחלק מהנתבים, אפשרות זו כבויה מראש כברירת מחדל, אבל כדאי לוודא זאת.

**הקטנת עצמת השידור האלחוטי**

[[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/TxPower.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/TxPower.jpg)האפשרות להקטנת עוצמת השידור של הנתב האלחוטי אינה קיימת בכל הנתבים, אך אם היא קיימת בנתב שלכם כדאי לשקול את היישום שלה כאמצעי נוסף להגנה על הרשת האלחוטית.

הקטנת עצמת האות האלחוטי מצמצמת את רדיוס הטווח היעיל שלו ומונעת זליגה של האות האלחוטי אל מעבר לחדר/דירה/משרד בה הוא נדרש.  באופן זה ניתן להקטין את הסיכון הקיים בציתות וניטור של האות האלחוטי על ידי גורמים זרים.

מציאת עוצמת האות המתאימה יכולה להיות מסובכת וסביר שתדרוש הרבה ניסוי וטעייה, במיוחד במבנים ישראלים הכוללים הרבה בטון וברזל. יחד עם זאת, זו בהחלט יכולה להיות אופציית אבטחה מעניינת, במיוחד כאשר הנתב האלחוטי והמחשב שמחובר אליו אלחוטית נמצאים באותו חדר.

**בכל מקרה, אנו ממליצים להשתמש בשיטה זו רק כתוספת לאחת או יותר מהאופציות שהומלצו לעיל.**

**ביטול מנגנון ה-UPNP בנתב**

[[https://www.netcheif.com/Articles/WiFiSecurity/JPG/UPNP_small.jpg](https://www.netcheif.com/Articles/WiFiSecurity/JPG/UPNP.jpg)](https://www.netcheif.com/Articles/WiFiSecurity/JPG/UPNP.jpg)UPNP (ראשי תיבות של Universal Plug and Play - מידע נוסף יש [**כאן**](http://www.upnp.org/)) הוא אוסף של פרוטוקולים המאפשרים להתקני רשת שונים לתקשר האחד עם השני, מבלי צורך ביישום של הגדרות מיוחדות.

לדוגמא, נתב שמנגנון ה-UPNP שלו פעיל, יכול להקצות פורטים באופן אוטומטי לתוכנות המבקשות זאת.  באופן דומה, מדפסת רשת התומכת ב-UPNP יכולה לפרסם את שירותיה ולאפשר למחשבים ברשת להתקשר אליה באופן אוטומטי.

החיסרון של מנגנון ה-UPNP הוא שהוא אוטומטי ולא מצריך שום אימות.  לפיכך, כל תוכנה שמזהה מנגנון UPNP פעיל בנתב, יכולה לגשת אליו ולקבל עליו שליטה.  במקרים מסוימים, עוצמת השליטה הזו יכולה להיות גבוהה אף מזו שיש למשתמש בנתב דרך ממשק התפריטים שלו.

על מנת לא להסתבך עם הגדרות מורכבות, משתמשים רבים עושים שימוש במנגנון ה-UPNP של הנתב על מנת לאפשר קידום פורטים אוטומטי (port forward) בתוכנות שיתוף קבצים כמו uTorrent.

מצד שני יש לזכור שבאמצעות מנגנון ה-UPNP אפשר לא רק לקדם פורטים באופן אוטומטי, אלא גם להוציא מידע חסוי כמו שם המשתמש והסיסמא לרשת האינטרנט, מפתח ההצפנה האלחוטי וכדומה.

בנוסף, באמצעות מנגנון ה-UPNP ניתן לפתוח את ממשק הניהול מרחוק של הנתב, לשנות סיסמאות וכיוב'.  כלומר, פורצים מקצועיים יכולים לבצע, באמצעות UPNP, התקפה מרחוק תוך שימוש בקוד ג'אווה סקריפט או פלאש שהדפדפן של המשתמש מוריד למחשב ומריץ תוך כדי צפייה באתר זדוני.

לפיכך, למרות שמנגנון ה-UPNP לא קשור באופן חד חד ערכי לאבטחת רשתות אלחוטיות, **ההמלצה שלנו היא לבטל אותו**.

**ביטול מנגנון ה-WPS בנתב**

**[](https://www.netcheif.com/Articles/WiFiSecurity/JPG/WPS.jpg)**מנגנון ה-WPS (ראשי תיבות של Wi-Fi Protected Setup - מידע נוסף יש [**כאן**](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup)( מאפשר להגדיר בקלות ובמהירות קישור אלחוטי מאובטח במנגנון .WPA2

מנגנון זה מבוסס על תהליך אוטומטי של "לחיצת יד" (handshake) אוטומטי בין הנתב להתקן האלחוטי. ניתן להפעיל את המנגנון באמצעות לחיצה על כפתור בנתב או על ידי שימוש בקוד בן 8 ספרות.

"לחיצת היד" המבוססת על קוד בין 8 ספרות מתבצעת בשני שלבים - ראשית נשלחות 4 הספרות הראשונות ואם ניתן להן אישור, נשלחות 3 האחרונות (הסיפרה האחרונה לא נשלחת כי היא סיפרת ביקורת).

המשמעות היא שתוך מקסימום 10,998 (9,999 + 999) ניסיונות ניתן לפרוץ את מנגנון ה-WPS ולהתחבר אל הנתב באופן אלחוטי. החולשה הזו אותרה והודגמה כבר בסוף 2011.

כתוצאה מכך, בראשית 2012, שחררו מרבית היצרניות המובילות עדכוני קושחה (firmware) המכבים את מנגנון ה-WPS ובמידה שהוא פעיל, מקשים על החדירה.  בנתבים שיצאו לשוק מאז גילוי הבעיה במנגנון ה-WPS, כבר מיושמים מראש תיקונים אלה.

למרות שברוב הנתבים המודרניים מנגנון ה-WPS כבר מבוטל כברירת מחדל, **ההמלצה שלנו היא לבדוק את מצב ההגדרה בנתב שלכם ובמידת הצורך לבטל אותו**.

**רשת WiFi נפרדת לגלישת אורחים (Guest Network)**

A screenshot of a cell phone

Description automatically generatedלעיתים קרובות אורחים המגיעים אלינו הביתה מעוניינים לעשות שימוש ברשת האלחוטית הקיימת אצלנו. במצב הזה אנחנו בדרך כלל נותנים די בקלות את סיסמת ה-WiFi אך שוכחים שחשיפת מידע זה יכולה להוות סיכון אבטחה לרשת.

**הערה:** תמונת המסך המצורפת היא מנתב של חברת TP-LINK כיוון שהנתב BR-6478 אינו תומך ברשת המיועדת לאורחים.

לדוגמה, אורחים עשויים להוריד בטעות תוכנית זדונית או לחבר לרשת הביתית טלפון או מחשב נישא שכבר נגועים. כתוצאה מכך עלול להיגרם נזק אבטחתי לרשת הביתית ובכלל זה הדבקת המחשבים בוירוס, התפשטות תוכנה זדונית וחשיפת הרשת לפריצות.

במידה והנתב תומך ברשת אלחוטית המיועדת לאורחים (guest network) ניתן להיות מסבירי פנים ובטוחים בו זמנית. השימוש ברשת אלחוטית לאורחים יעיל לשני הצדדים – מצד אחד החברים והמכרים לא מאבדים קשר עם העולם החיצון ומצד שני הרשת והנתונים שלך אינם בסכנה. רשת האורחים מופרדת מזו הפנימית, ומאפשרת גישה לאינטרנט בלבד אך לא גישה לרכיבים פנימיים של הרשת הביתית.

בעת הפעלת רשת האורחים יש להקפיד על מספר עקרונות – ראשית, סיסמת הכניסה לרשת האורחים צריכה להיות שונה מזו של הרשת העיקרית שלכם. יחד עם זאת הסיסמא צריכה להיות חזקה ובמנגנון WPA2, כך שלאורחים לא קרואים יהיה קשה עד בלתי אפשרי לפרוץ לרשת הזו.

שנית, על מנת להבטיח הפרדה בין הרשת העיקרית לרשת האורחים, ובמידה והנתב מאפשר זאת הגדירו לרשת האורחים טווח כתובות IP השונה מזה של הרשת העיקרית ובנוסף הקפידו לוודא שאופציית ההפרדה המלאה בין הרשתות פועלת.

לפיכך, **במידה ואתם מארחים מכרים וחברים, והנתב שלכם תומך ברשת אורחים, הפעילו את האפשרות הזאת וספקו להם גישה רק לרשת זו.**