



30 מרץ 2022
כ"ז אדר ב תשפ"ב

מסמך המלצות הגנה לשימוש במצלמות חכמות

מרץ 2022

מסמך זה נכתב על-ידי מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי. כל הזכויות שמורות למדינת ישראל - מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. העתקת המסמך או שילובו במסמכים אחרים כפוף לתנאים הבאים: מתן קרדיט למערך הסייבר הלאומי בפורמט המופיע להלן; שימוש בגרסה העדכנית של המסמך; אי הכנסת שינויים במסמך.

הערות והתייחסויות למסמך ניתן להעביר למייל: awareness@cyber.gov.il

ההמלצות כתובות בלשון זכר מטעמי נוחות בלבד.



תוכן עניינים

3.....הקדמה

4..... המלצות

6.....מצלמות ביתיות

7..... המלצות להגנה על הנתב הביתי:

חושדים שפרצו לכם למצלמה הביתית? אלו הסימנים לפריצה

7.....

הבחנתם שפרצו לכם למצלמה הביתית? הנה מה שעליכם לעשות:

7.....

המלצות הגנה בעת שימוש במצלמות מוניטור

9.....

המלצות הגנה בעת שימוש במצלמות הדרך

11.....

המלצות הגנה בעת שימוש במצלמות רשת

12.....

חושדים שפרצו לכם למצלמה? מומלץ לבצע את הבדיקות הבאות:

14.....

קיבלתם הודעה מהאקר שיש לו תמונות או סרטונים שלכם?

16.....

הקדמה

האם ספרתם פעם כמה מצלמות מקיפות אתכם בחיי היום-יום? מצלמת הסמארטפון, הטאבלט, המחשבים הניידים, מצלמת הרשת המחוברת למחשב, מצלמת הטלוויזיה, מצלמת אבטחה ביתית, מצלמת המוניטור בחדר הילדים, מצלמת הדרך ברכב...

האם חשבתם על כך שכמו כל "מוצר חכם" המצלמות מחוברות לרשת ובכך חשופות לפריצות? בדרך כלל למוצרים החכמים כיום, לרבות מצלמות, ניתן להחליף את השם וסיסמת ברירת המחדל שמגיעים עם המוצר, לבצע עדכוני אבטחה, ולעתים ניתן לבצע אימות דו-שלבי באפליקציה.

מבדיקה שקיים מערך הסייבר הלאומי בשנת 2022 עולה כי קרוב ל-66,000 מצלמות ביתיות ומצלמות אבטחה בישראל חשופות להשתלטות מרחוק, חלקן באמצעות סיסמת ברירת מחדל. סיסמאות אלה ידועות ומוכרות, ואם לא שיניתם את הסיסמה במצלמה שלכם, ניתן להשתלט עליה מרחוק. פעמים רבות המצלמות שלנו לא מצלמות רק אותנו, אלא גם אנשים הנמצאים במרחב הציבורי ופריצה למצלמה שלנו, משמעה פגיעה בפרטיותם.

לעיון בהנחיות הרשות להגנת הפרטיות בנושא שימוש במצלמות מעקב:

https://www.gov.il/he/departments/topics/surveillance_cameras

מערך הסייבר הלאומי ריכז עבורכם המלצות הגנה לשימוש בטוח במצלמות. במסמך הבא מובאות המלצות הגנה לשימוש במצלמות אבטחה ביתיות, מצלמות מוניטור לחדרי ילדים, מצלמות דרך ומצלמות רשת.

מטרת ההמלצות היא לצמצם במספר צעדים פשוטים את סיכוני הסייבר ממצלמות. בכל פרק ישנן המלצות לביצוע טרם רכישת מצלמה, לאחר רכישת המצלמה וסימנים היכולים להעיד על פריצה למצלמה. כמו כן, בכל פרק מובאות המלצות לביצוע בעת פריצה למצלמה. המסמך מבוסס על המלצות מערך הסייבר הלאומי, המלצות אתרי מודעות סייבר בעולם, כתבות וסיפורי מקרה מהעולם, וכן מדריכים למשתמש מפי יצרניות שונות.

המלצות שכדאי ליישם בעת שימוש במצלמות ביתיות, מצלמות דרך ומצלמות מוניטור:

ראשית, הבה נבין כיצד ניתן לפרוץ למצלמה שלנו.

שלוש דרכים עיקריות לפריצה למצלמה:

1. ניצול לרעה של ממשק ניהול של המצלמה החשוף לאינטרנט, דבר אשר עשוי לכלול שימוש בסיסמה ברירת מחדל או שימוש בכלי תקיפה שמטרתו לנחש מהי סיסמת ההתחברות.
2. חדירה לרשת ה-Wi-Fi - באמצעות ניחוש הסיסמה, ומשם דילוג למצלמה.
3. ניצול חולשות אבטחה מוכרות במצלמה - במצלמות רבות כבר בשלב פיתוח המוצר לא הושם דגש על מדיניות אבטחת המידע. הדבר מביא בין השאר, להיותן לא מעודכנות בעדכוני אבטחה וחשיפתן לפגיעויות.

מומלץ לבחון את הנושאים הבאים מול גורמי מקצוע בחנות, בחינת פרסומים וחוות דעת באינטרנט או התייעצות עם חברים.

טרם רכישת המצלמה:

1. **מוניטין הספק ודגם המצלמה במשק הישראלי.** קראו אודות הספק ודגם המצלמה, חפשו חוות דעת וקראו גם את חוות הדעת השליליות.
2. **חפשו את החברה המוכרת את המצלמה באינטרנט** וודאו שיש לה אתר אינטרנט וכן שיש לכם למי לפנות במקרה של תקלה. אם אינכם מוצאים את המותג באינטרנט, מומלץ להתרחק ולחפש מצלמה של חברה אחרת.

3. **מדיניות הגנת מידע וסייבר.** מומלץ לרכוש מצלמה שניתן להגדיר בה מדיניות אבטחת מידע לרבות ביצוע אימות דו שלבי באפליקציה והתקנת עדכוני אבטחה (פאצ'ים) של היצרן. בחנו אם ישנה אפשרות לביצוע עדכוני אבטחה באופן אוטומטי.
- חשוב -** מצלמה ללא אפשרות לביצוע עדכוני אבטחה, משמע שהיא חשופה לפגיעויות אבטחה. גם אם תשנו את הסיסמה, יכול להיות סיכוי של ניצול אותן חולשות אבטחה ופריצה למצלמה שלכם.
4. **אפליקציית המצלמה ניתנת להורדה מהחנות הרשמית (Google Play/App Store).** ישנן מצלמות שהאפליקציה להפעלתן לא נמצאת בחנויות הרשמיות, אלא ניתנות להורדה רק דרך אתרי האינטרנט. לרוב, כשלא מדובר בחנות רשמית, קיים סיכוי שבהורדת האפליקציה למכשיר שלכם תאפשרו להאקרים שליטה במכשיר וגישה לפרטים האישיים ולמידע השמור בו.
5. **תאריך סיום התמיכה של היצרן במוצר,** שלאחריו המוצר לא יזכה לעדכוני אבטחה.
6. **זמינות מדריך שימוש בשפה העברית/האנגלית.**

לאחר רכישת המצלמה:

1. **החלפת סיסמת ברירת מחדל** המגיעה עם המצלמה. מומלץ כי הסיסמה תורכב משלוש מילים אקראיות בשילוב תווים מיוחדים או מספרים, ושתהיה שונה מסיסמאות לחשבונות אחרים. כמו כן, מומלץ שלא תכיל את שמותיכם או פרטים אישיים אחרים ואין לשתפה עם אף גורם. בד"כ ניתן לשנות את הסיסמה דרך האפליקציה המשמשת להפעלת המכשיר או דרך התוכנה במחשב. אם שינוי הסיסמה בוצע ע"י מתקין מקצועי, מומלץ לבחור את הסיסמה בעצמכם או שתשנו אותה לאחר התקנת המצלמה. זאת מאחר ופעמים רבות מבוצע שימוש בסיסמאות פומביות וידועות.
2. **בצעו עדכוני תוכנה וקושחה (Firmware) עתיים בהתאם להמלצות היצרן.** כדאי שהתוכנה תהיה מעודכנת באמצעות ביצוע עדכוני אבטחה, כך שפורצים פוטנציאליים לא יוכלו לנצל את חולשות האבטחה כדי לפרוץ למצלמה שלכם. במידה וניתן לבצע עדכונים אוטומטיים, בחרו באפשרות זו. מצלמות רבות לא מאפשרות עדכוני אבטחה אוטומטיים, לכן חשוב שתבצעו עדכונים עיתיים בכל פעם שיש עדכון זמין (תוכלו לבצע זאת בהגדרות האפליקציה תחת עדכונים).
3. **החלפת שם המצלמה החשופה לאינטרנט -** מומלץ שלא לבחור בשמכם הפרטי, שם המשפחה, או כל שם אחר שמכיל פרטים אישיים. בחרו שם שלא יעיד עליכם ושהיה קשה לנחשו.
4. **מומלץ להפעיל הזדהות חזקה (2FA/MFA)** אם ממשק הניהול של המצלמה, לרבות אפליקציה, מאפשר זאת.
5. **הורדת האפליקציה מהחנויות הרשמיות** וצמצום ההרשאות הניתנות לאפליקצייה למינימום הנדרש. כמו כן, תוכלו להגדיר שימוש בהרשאות רק בעת הפעלת האפליקציה.
6. **הקפדה על ניתוק המצלמה -** מומלץ להקפיד לנתק את המצלמה כאשר לא מבוצע בה שימוש. ככל שתקצרו את זמן החיבור שלה, כך תקטינו את הסיכוי לפריצה למצלמה.

בנוסף להמלצות המובאות כאן, מומלץ ליישם את ההמלצות הבאות עבור סוגי המצלמות הבאים:

- מצלמות ביתיות
- המלצות הגנה בעת שימוש במצלמות מוניטור
- המלצות הגנה בעת שימוש במצלמות הדרך
- המלצות הגנה בעת שימוש במצלמות רשת

המלצות הגנה בעת שימוש בשגיאה! מקור ההפניה לא נמצא.

בשנים האחרונות מצלמות האבטחה הביתיות הפכו לאמצעי שכיח כמעט בכל בית במדינת ישראל. באמצעותן אנו יכולים לצפות בביתנו או בבית העסק שלנו בכל זמן שנרצה, לבדוק שהילדים בסדר ואף להציב בחדרי התינוקות. כמוצר חכם, מצלמות אלה מחוברות לרשת האינטרנט והן חשופות לסכנות ופריצות. מעבר לפגיעה בפרטיות שלנו וצפייה בנו, פריצה למצלמה שלנו יכולה להוביל לחדירה לאפליקציית המצלמה בטלפון ודרכה לחדור לטלפון שלנו ולכל המידע שבתוכו- חשבונות פרטיים, מיילים, פרטים אישיים, מסרונים ושיחות ועוד.



כיצד תוכלו לאבטח את המצלמות הביתיות שלכם?

אם עוד לא רכשתם מצלמה ביתית, מומלץ לבחון בנוסף להמלצות המובאות המלצות שכדאי ליישם בעת שימוש במצלמות ביתיות, מצלמות דרך ומצלמות מוניטור; האם המצלמה שומרת מידע באופן מקומי. אם כן, בחנו לאיזו תקופה היא שומרת את המידע. כך, תוכלו לדעת אם יש צורך במחיקת מידע באופן יזום.

רכשתם מצלמה ביתית? בנוסף להמלצות המובאות לאחר רכישת המצלמה: מומלץ לנקוט בצעדים הבאים:

1. **שימוש באמצעי פיזי לשם כיסוי עינית המצלמה** או ניתוק פיזי שלה מהרשת כשאינ לכם צורך בה (לדוגמה כשאתם בבית).
2. **אם מתאפשר, קישור המצלמה לרשת הביתית ע"י שימוש בכבילה פיזית**, ולא תווך אלחוטי (Wi-Fi). כמו כן, ניתן להגדיר נתב נפרד למצלמה הביתית, כך שלא יהיה מקושר למכשירים אחרים בביתכם. עם זאת, במידה והרשת האלחוטית בביתכם מוצפנת בצורה טובה, לא בהכרח תצטרכו ליישם המלצה זו.
3. **מניעת גישה למצלמה מהאינטרנט או הגבלת הגישה** ע"י שימוש באמצעים מקובלים דוגמת הגבלת גישה מכתובת IP מוגדרת בלבד.
4. **מחיקה עיתית של מידע המאוחסן** באופן מקומי במצלמה.
5. **מומלץ להציב את המצלמות במקום שפריצתן לא יפלוש לפרטיותכם** (לדוגמה הצבתן במבואת הכניסה ולא בחדר השינה).
6. **לאחר כל טיפול ושדרוג במצלמות על ידי טכנאי, מומלץ לוודא כי הגדרות הבסיס לא שוננו** והוחזרו להגדרות שנקבעו.
7. רצוי להימנע מהתקנת מוצרי תוכנה שאינם מתוצרת יצרן המצלמות.
8. למתקדמים: ניתן להשתמש בשירות VPN כדי להגביל אילו מכשירים יכולים לגשת לרשת שבהן מצלמות האבטחה נמצאות.

כפי שציינו, אחת הדרכים לפרוץ למצלמה יכולה להיות ניצול הקישוריות של המצלמה לנתב הביתי. לכן ניתן להסתייע בספק/איש מקצוע/חבר ולשנות את הגדרות הנתב הביתי.

המלצות להגנה על הנתב הביתי:

1. החלפת סיסמת ברירת המחדל והגדרת שתי סיסמאות נפרדות: סיסמה אחת עבור סיסמת משתמש המנהל (Administrator) - משתמש זה הינו בעל הגישה להגדרות הנתב. הסיסמה השנייה הינה עבור גישה לרשת האלחוטית (ה-Wi-Fi).

2. שינוי שם זיהוי הרשת האלחוטית (SSID) כך שלא יעיד על מאפייני הנתב - דגם, יצרן, בעלים ומיקום.
3. עדכוני קושחה (Firmware) - בדיוק כמו בעדכוני אבטחה של תוכנות במחשבים, חשוב מאוד לעדכן את הקושחה בנתב בעדכון האחרון שהפיץ היצרן. רצוי להפעיל גם כאן את אופציית העדכון באופן אוטומטי במידת האפשר.
4. הפעלת חומת אש (Firewall) - חומות אש מסייעות להגן ולשמור מפני חדירה של גורמים זדוניים לרשת ומפני השגת גישה למכשירים שלכם. חומת האש מגנה מפני ניסיונות כניסה לרשת וחוסמת תקשורת עם מקורות שאינם מורשים.
5. השבתת שרות UPnP (Universal Plug and Play) - שרות זה קיים במרבית הנתבים ומאפשר להתקנים ברשת (אפליקציות או מכשירים) ליצור תקשורת דרך הנתב. למרות שתכונת UPnP מקלה על תצורת רשת ראשונית, היא עלולה להוות סכנת אבטחה משמעותית כאשר תוכנות זדוניות הנמצאות כבר בתוך הרשת יכולות להשתמש בה כדי לפתוח פתח בחומת האש בנתב ולאפשר לפולשים לחדור פנימה.
6. הגדירו אימות והצפנה גבוהה בהגדרות האבטחה של הנתב.
7. [למדריך המלא להגנה על הנתב הביתי והנחיות נוספות.](#)

חושדים שפרצו לכם למצלמה הביתית? אלו הסימנים לפריצה:

1. רעשים מוזרים הבוקעים ממצלמת האבטחה שלכם.
2. חיווי נורה דולקת מבלי שהפעלתם את המצלמה.
3. המצלמה שלכם נעה לכיוונים שונים מבלי שהזזתם אותה בעצמכם.
4. שינויים בהגדרות המצלמה כגון החלפת הסיסמה.

הבחנתם שפרצו לכם למצלמה הביתית? הנה מה שעליכם לעשות:

1. נתקו את המצלמה מרשת האינטרנט.
2. שנו את הסיסמה למצלמה לסיסמה ארוכה המורכבת משלוש מילים אקראיות בשילוב תווים מיוחדים או מספרים. כמו כן, דאגו שהסיסמה לא תכיל פרטים אישיים שלכם.
3. שנו את הסיסמה לנתב הביתי שלכם.
4. בצעו עדכון תוכנה לגרסה המעודכנת ביותר ובדקו אם ניתן בהגדרות המצלמה להגדיר עדכוני תוכנה אוטומטיים.
5. הודיעו ליצרן המצלמה ו/או הגישו תלונה במשטרה.



המלצות הגנה בעת שימוש במצלמות מוניטור:

בשנים האחרונות מצלמות המוניטור המחוברות לרשת ה-Wi-fi הביתית הפכו נפוצות לשימוש בקרב רבים. הגישה אליהן מתבצעת דרך אפליקציה המותקנת בטלפון הנייד וניתן לצפות בילדים בכל עת, גם כשלא נמצאים בבית. אך ככאלה המחוברות לרשת, ובמיוחד אם היצרן לא הקפיד ביישום נהלי אבטחה, הן חשופות להשתלטות מרחוק ופריצות. במסגרת פריצות שנעשו בעבר למצלמות המוניטור במדינות שונות, גורמים בלתי מורשים דיברו אל הילדים דרך המצלמה, הפחידו אותם על ידי השמעת קולות משונים והשמיעו מוזיקה.



בנוסף להמלצות המובאות המלצות שכדאי ליישם בעת שימוש במצלמות ביתיות, מצלמות דרך ומצלמות מוניטור; טרם רכישת מצלמת מוניטור, מומלץ לבחון את הנושאים הבאים:

1. **אפשרות ביטול הקלטת שמע ווידאו** - ישנן מצלמות רבות שבהן הקלטת שמע ווידאו הינה תצורת ברירת המחדל. מומלץ לרכוש מצלמה שבה תתאפשר ביטול ההקלטה ושמירת המידע במכשיר. כדי לבחון אם אפשרות הביטול קיימת, חפשו את המדריך של דגם המצלמה אותה אתם רוצים לרכוש.
2. **קיומו של חיזוי חיצוני** (דוגמת נורה פעילה) במקרה שהמצלמה פעילה. כך, במידה שהמצלמה תופעל ללא ידיעתכם, תבחינו בכך הודות לחיזוי החיצוני.

המלצות להגנה על מצלמות המוניטור לאחר הרכישה:

במידת הצורך, מומלץ וניתן להיעזר במדריך המצלמה המגיע עם המוצר ליישום ההמלצות הבאות בנוסף להמלצות המופיעות לאחר רכישת המצלמה:

1. שנו את הגדרות ברירת המחדל שהגיעו עם המצלמה לרבות סיסמה. מומלץ לבחור בסיסמה ייחודית, ארוכה ומורכבת ולא לשתפה עם אף גורם.
2. מומלץ לבטל את השימוש ב-UPnP (Universal Plug and Play) מאפשר להתקנים ברשת (אפליקציות או מכשירים) ליצור תקשורת למכשיר, במקרה זה,

המצלמה. אפשרות זו קיימת רק בחלק מן המצלמות, וניתן לבצע את הביטול דרך הגדרות המצלמה.

3. מומלץ לבטל את השימוש ב-DDNS (Dynamic Domain Name System). DDNS הוא שירות שמאפשר לגשת למצלמה מרחוק באמצעות כתובת IP דינמית. אפשרות זו קיימת רק בחלק מן המצלמות, וניתן לבצע את הביטול דרך הגדרות המצלמה.
4. אבטחו את הנתב הביתי שלכם- מומלץ להקפיד על ביצוע עדכוני קושחה ושינוי הסיסמאות לסיסמאות ארוכות, ייחודיות ומורכבות ככל שניתן.
5. במידת האפשר, מומלץ לבטל את הגישה לצפייה מרחוק. אם הגישה לצפייה מרחוק נדרשת, מומלץ לשנות את פורט (Port) ברירת המחדל שהגיע עם המצלמה. מספר הפורט יופיע בד"כ במדריך המצלמה ואת השינוי ניתן לבצע בהגדרות המצלמה. אפשרות נוספת היא להשתמש בשירות VPN כדי להגביל אילו מכשירים יכולים לגשת לרשת בהן מצלמות המוניטור נמצאות.

אם הבחנתם שפרצו למצלמת המוניטור שלכם, נתקו אותה מיד מן הרשת. לאחר מכן החליפו את הסיסמה ופעלו על פי ההמלצות המופיעות מעלה. כמו כן, צרו קשר עם ספק המוצר והודיעו לו על כך.

המלצות הגנה בעת שימוש במצלמות הדרך ברכב

מצלמות הדרך ברכב הן מוצר נפוץ מאד בימים אלו ונמצאות כמעט בכל רכב. הן מאפשרות לנו תיעוד מלא ורציף של המתרחש בסביבת הרכב כולל מיקרופון המתעד את השיח ברכב, קולטות את נתוני ה-GPS בזמן הנסיעה, הן יכולות לשלוח אלינו נתונים בעת גניבת הרכב ואף מאפשרות להעביר את ההקלטות לטלפון או למחשב. חשוב לזכור שהיותן מוצר חכם המחובר לאינטרנט, פותח דלת להאקרים להשתלטות מרחוק ופריצות.

פריצה למצלמת הדרך, משמעה העברה לאדם לא מורשה את כלל הנתונים שנשמרו בה - הקלטות הנסיעה כולל שמע ושעות הנסיעה, נתוני ה-GPS ואף תמונות של היושבים ברכב במידה והמצלמה כוונה אל פנים הרכב. האם הייתם רוצים שאדם לא מורשה ידע היכן אתם גרים, לאן אתם נוסעים בשעות היום, יקבל את נתוני ה-GPS שלכם ואף עלול לקבל תמונות שלכם?



להלן כמה המלצות שיפחיתו את הסיכוי שיפרצו לכם למצלמת הדרך ברכב:

טרם רכישת מצלמת דרך, מומלץ לנקוט בהמלצות המובאות המלצות שכדאי ליישם בעת שימוש במצלמות ביתיות, מצלמות דרך ומצלמות מוניטור.

לאחר רכישת מצלמת דרך, מומלץ לנקוט בנוסף להמלצות המובאות לאחר רכישת המצלמה: בצעדים הבאים:

1. החליפו סיסמה במצלמת הרכב שלכם. אופן החלפת הסיסמה למצלמה שלכם הוא תלוי יצרן ודגם:

- ישנן מצלמות המאפשרות להחליף את הסיסמה למצלמה באמצעות כניסה להגדרות המצלמה.

- ישנן מצלמות המאפשרות להחליף את הסיסמה באמצעות האפליקציה המחוברת למצלמה ושם באמצעות הכניסה להגדרות המצלמה.
 - ישנן מצלמות שמאפשרות להחליף את הסיסמה רק ל-Wi-Fi של המצלמה.
2. במידה ולא מבוצע באופן אוטומטי, מומלץ לבצע מחיקה עיתית של מידע המאוחסן באופן מקומי במצלמה.
 3. הקפדה על כיבוי המצלמה - מומלץ להקפיד לכבות את המצלמה כאשר לא מבוצע בה שימוש (לדוגמה בעת המתנה ברכב מונע, בחנייה ועוד).

במידה והבחנתם שפרצו לכם למצלמת הדרך, נתקו את המצלמה מרשת ה-Wi-Fi, החליפו את הסיסמה לסיסמה ארוכה ומורכבת השונה מכל החשבונות שברשותכם. כמו כן בצעו עדכוני אבטחה והעבירו או מחקו את המידע השמור במצלמה.

המלצות הגנה בעת שימוש במצלמות רשת במחשב

מגיפת הקורונה אילצה רבים מאיתנו לעבוד מרחוק, לערוך פגישות עבודה מרחוק, ואפילו לראות את המשפחה מרחוק. כל אלו התאפשרו לנו באמצעות הפעלת המצלמות במכשירים שלנו.

מצלמת הרשת של המחשב, מצלמת הלפטופ, מצלמת הטלפון, מצלמת הטאבלט - כל אלו שימשו ועדיין משמשים אותנו ביום-יום. אך האם המצלמות הללו מוגנות?
חשבתם פעם מה היה קורה אילו מישהו היה מצליח לפרוץ למצלמה שלכם?



ראשית, בואו נכיר את המושג Camfecting.

Camfecting מתרחש כאשר גורם לא מורשה מפעיל את מצלמת האינטרנט ללא רשותו של בעל המצלמה, דבר המאפשר לו צפייה בכל דבר הזמין בשדה הראייה שלה. בד"כ הגישה למצלמה מושגת באמצעות שיטוי במשתמש, כך שיווריד ויריץ קובץ המכיל נזקה. לאחר השגת הגישה למצלמה, ניתן להפעילה באופן חופשי, להאזין ולצפות בשיחות וידאו ולצלם תמונות וסרטונים ללא ידיעתו של בעל המכשיר. בהמשך, יהיה ניתן לעשות שימוש באותם חומרים למטרות שיימינג, הטרדה וסחיטת כסף מבעל המכשיר. יישום של דרכי התגוננות פשוטות והתנהלות נכונה בסביבת מצלמות עשויה למנוע מכם להיקלע למצבים לא נעימים מפריצה למצלמה שלכם.

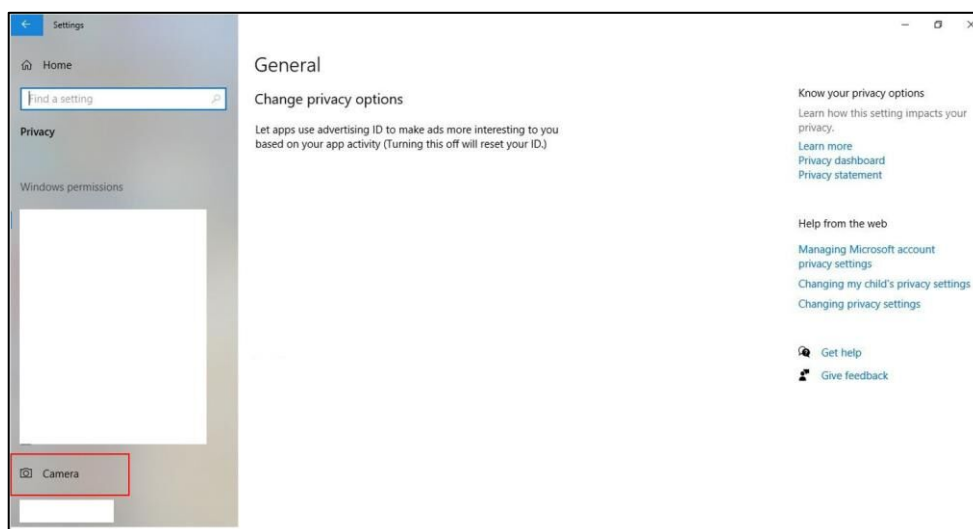
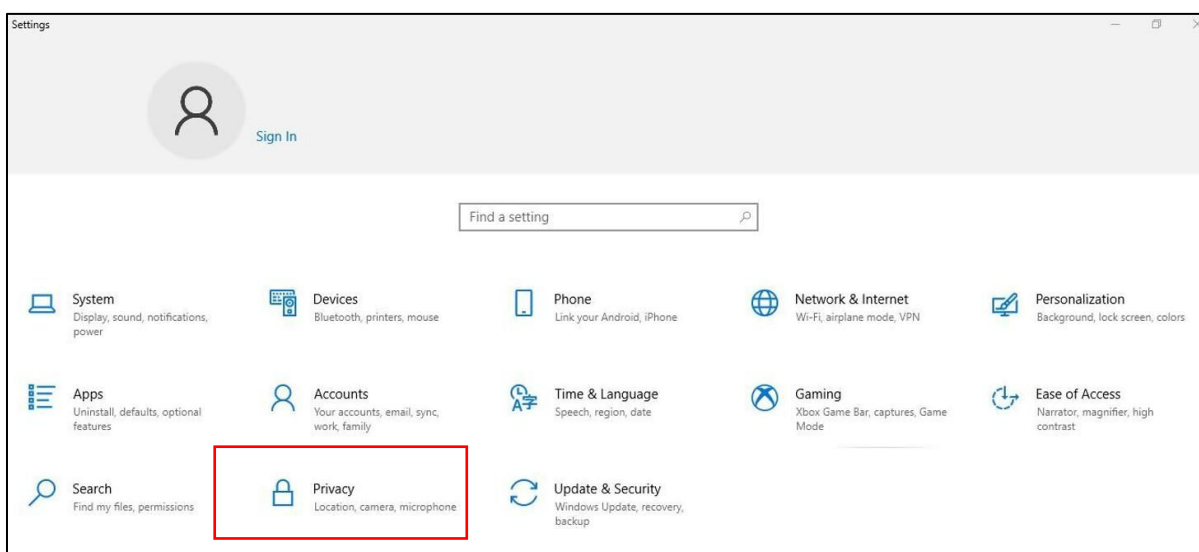
אז מה ניתן לעשות כדי לצמצם את הפגיעה?

1. התקינו מערכות הגנה - מומלץ להתקין מערכות הגנה אמינות דוגמת תוכנת אנטי-וירוס וחומת אש. מומלץ לוודא שתוכנת האנטי-וירוס כוללת מודל התומך בהגנה על ממשק המצלמה.
2. היזהרו מפשינג - גלו עירנות כלפי קישורים וקבצים הנשלחים אליכם. במקרים רבים, תוקף ישיג גישה באמצעות שליחת קובץ או קישור אל הקרבן. לחיצה על הקישור או הקובץ תביא להורדת תוכנה זדונית למכשיר שתעניק את הגישה לתוקף.

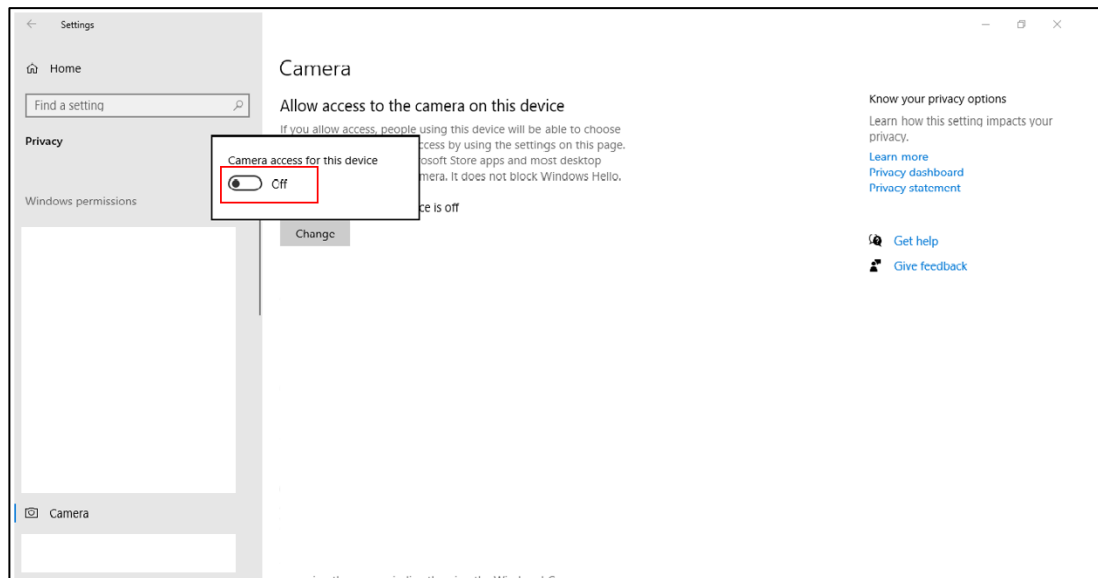
3. בצעו עדכוני אבטחה עתיים לתוכנות המחשב לרבות תוכנות המשמשות לשיחות הוידאו. בדקו אם יש אפשרות להפעיל עדכון אבטחה אוטומטי, כך שלא תצטרכו לבדוק בעצמכם אם יש עדכון חדש.

4. כיסוי המצלמה או ניתוקה - אם ברשותכם מצלמת רשת שאינה מובנית במסך, נתקו אותה מהמחשב כשאינן בה צורך. אם המצלמה מובנית במסך, כמו במחשב נייד, כסו אותה באמצעי פיזי דוגמת מדבקה אטומה. אפשרות נוספת אך פחות עדיפה היא הגדרה באמצעות ה-Device Manager כי דרייבר המצלמה יהיה במצב "כבוי" או כבו את ההרשאות למצלמה באופן הבא:

- לחצו על מקש ההתחל במחשב ולאחר מכן על Settings/הגדרות.
- בחרו ב-Privacy/פרטיות ולאחר מכן ב-Camera/מצלמה.



• שנו למצב כבוי:

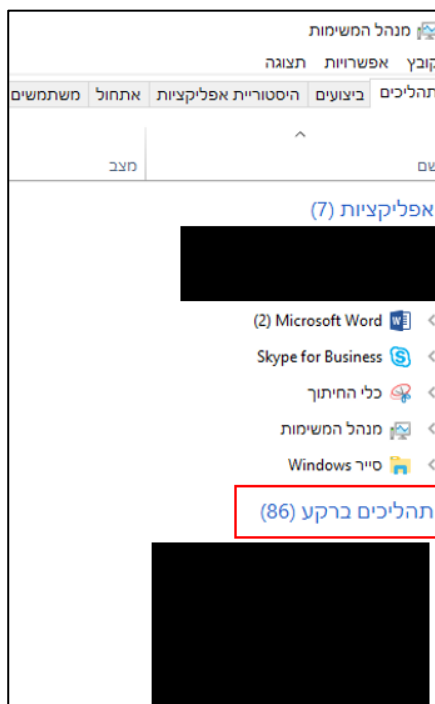


5. הורידו אפליקציות רק מהחנויות הרשמיות. אפליקציות שניתנות להורדה באמצעות קישורים או מאתרי האינטרנט השונים, נחשבות לא בטוחות ואף זדוניות. קיים סיכון גדול שהורדת האפליקציה תאפשר להאקר שליטה במכשיר וגישה לפרטים האישיים ולמידע השמור בו.
6. הפחיתו למינימום גלישה ברשתות Wi-Fi ציבוריות. מומלץ לא להתחבר לרשתות ציבוריות (דוגמת רשת Wi-Fi בבית קפה). אם בכל זאת נאלצתם להתחבר, הקפידו להתנתק מהשירות בסיום השימוש ולמחוק את ההיסטוריה של הדפדפן.
7. השתמשו ברשת פרטית וירטואלית (VPN) - במידת האפשר מומלץ להשתמש בשירות VPN המסווה את הפעילות שלכם באינטרנט, לא חושף את כתובת ה-IP ממנה אתם גולשים, ומצמצם משמעותית את החשיפה שלכם לסכנות ברשת.
8. זכרו תמיד שהמצלמה מחוברת לרשת, לכן תמיד מומלץ לצמצם שיחות רגישות ואינטימיות ליד המצלמה או במהלך השימוש בה.

חושדים שפרצו לכם למצלמה? מומלץ לבצע את הבדיקות הבאות:

1. חיווי נורה דולקת - אם אתם רואים נורת חיווי דולקת או מהבהבת, נסו לסגור את הדפדפן וכל האפליקציות או לאתחל את המחשב. אם החיווי נעלם, ייתכן שהענקתם הרשאות לאפליקציה או לתוסף אינטרנט ללא ידיעתכם והוא פעל ברקע. אם החיווי עדיין פעיל ומבלי שהפעלתם את הדפדפן או אפליקציה כלשהי, ייתכן שפרצו לכם למצלמה.

2. תכנת המצלמה מופיעה בתהליכים הפועלים ברקע - בדקו במנהל המשימות (Task Manager) במחשב את התהליכים הפועלים ברקע. חפשו שם את המצלמה שלכם.



אם המצלמה מופיעה שם - סגרו את האפליקציות הפתוחות ואת הדפדפן. אם עדיין היא מופיעה, נסו לאתחל את המחשב. במקרה שהמצלמה עדיין מופיעה בתהליכים הפועלים ברקע, זה סימן שיכול להעיד על פריצה למצלמה.

3. כישלון בהפעלת המצלמה - סגרו את כל האפליקציות והדפדפן ונסו להפעיל את המצלמה שלכם. אם קיבלתם הודעה שהמצלמה שלכם כבר בשימוש, זה יכול להעיד על פריצה למצלמה.

4. תיקיית הקלטות או תמונות שלא שמרתם - היכנסו לתיקייה בה נשמרים התמונות והסרטונים מהמצלמה שלכם וחפשו קבצים שלא אתם שמרתם. אם הבחנתם בכאלה, בדקו עם שאר משתמשי המחשב אם הם שמרו את הקבצים. במידה ולא, זה מהווה סימן לפריצה למצלמה. אם אינכם רואים קבצים מסוג זה, זה סימן טוב. אולם, לא מומלץ להסתמך רק על הבדיקה הזו, ורצוי לבחון את שאר הסימנים המעידים על פריצה למצלמה.

5. ביצוע סריקה לאיתור תוכנות זדוניות - מומלץ להריץ סריקה לאיתור תוכנות זדוניות באמצעות תוכנת אנטי-וירוס אמינה. במידה וזוהו קובץ זדוני, אפשרו לאנטי-וירוס למחוק את הקובץ או להעבירו להסגר.

קיבלתם הודעה מהאקר שיש לו תמונות או סרטונים שלכם?

אם האקר מנסה לסחוט מכם כספים בתואנה שהוא מחזיק בתמונות או סרטונים שלכם - אל תתפתו מיד לשלם. ראשית, חשבו אם זה הגיוני. האם יש לו הוכחות **שלא ידרשו** מכם

ללחוץ על קישור או להוריד קובץ? האקרים ילחיצו אתכם וינסו לגרום לכם ללחוץ במהירות על הקישור או להוריד את הקובץ. אם תעשו זאת, ייתכן שתורידו למכשיר שלכם תוכנה זדונית שתאפשר להאקר שליטה במכשיר. לכן מומלץ להפעיל שיקול דעת לפני כל לחיצה על קישור או קובץ ובמידת הצורך להתייעץ עם חברים, משפחה, או להתקשר 119 למערך הסייבר הלאומי להתייעצות ודיווח על אירוע סייבר.

פעולות שמומלץ לבצע בעת פריצה למצלמת הרשת:

1. ראשית בצעו ניתוק למצלמת הרשת מהמחשב או הסתירו את המצלמה המובנית במחשב הנייד באמצעות אמצעי פיזי דוגמת מדבקה אטומה. כך, תבטיחו שהאקר לא יצפה או יצלם אתכם מרגע זה.
2. הפעילו את תוכנות חומת האש והאנטי-וירוס במחשב. אפשרו לתוכנת האנטי-וירוס למחוק את הקבצים הזדוניים או להעבירם להסגר.
3. פרמוט המחשב - במידה ותוכנות ההגנה לא מסייעות במקרה זה, מומלץ לבצע גיבוי למידע החשוב במחשב ולבצע פרמוט למערכת ההפעלה. כשאתם מחזירים את המידע המגובה למחשב, שימו לב שאינכם מחזירים אל המחשב את הקבצים הזדוניים.
4. התייעצו עם גורם מוסמך ואמין - אם אינכם יודעים כיצד לפעול, מומלץ לפנות למעבדת מחשבים מוסמכת ואמינה שתסייע לכם בניקוי המחשב מנוזקות.

סיכום

לסיכום, בעידן של היום, שימוש במצלמות תופס יותר ויותר מקום בחיים שלנו. אנו משתמשים במצלמות לפנאי, לצורכי עבודה, לשיחות עם המשפחה, לאבטחה ובקרה ולעוד שימושים רבים. מצלמות, כמו כל "מוצר חכם" אחר, אוספות ואוגרות את המידע שלנו ועשויות להכיל התקן זיכרון נייד ולעתים אף לאחסן את המידע באינטרנט. אם הן אינן מאובטחות - גם המידע שלנו אינו מאובטח.

זכרו שהמצלמות סובבות סביבנו גם כשאיננו משתמשים בהן בפועל. לכן כדאי לסגל לעצמכם הרגל- כשהמצלמה לא בשימוש, נתקו אותה מהחשמל/מהרשת. בהינתן והדבר אינו אפשרי - כסו אותה באמצעי פיזי כמו מדבקה, תריס מותאם או כל אמצעי אחר. רבים יוצאים מנקודת הנחה שהאקרים לא מעוניינים דווקא בהם, ולכן מקלים ראש בנושא אבטחת המצלמות... אבל מקרים שקרו הוכיחו אחרת.

פעלו לאבטח את המצלמות שלכם, נהגו בשגרה מודעת להיותן סביבכם וזכרו כי המידע שלכם הוא אישי שלכם ותמיד כדאי לאבטח אותו.

-לכל חשד לאירוע סייבר חייגו 119-



מקורות

[/https://nordvpn.com/blog/tell-if-laptop-camera-hacked](https://nordvpn.com/blog/tell-if-laptop-camera-hacked)

<https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>

<https://www.netgear.com/images/pdf/arloproduct/arlo-baby-user-manual.pdf>

<https://provision-isr.com/product-uploads/downloads/manuals/IP/I3-380IP04.pdf>

<https://scholarship.law.edu/cgi/viewcontent.cgi?article=1048&context=jlt>

[/https://owlcam.com](https://owlcam.com)

<https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say>