

מערך הסייבר הלאומי מזהיר מסכנות במרחב הקיברנטי

בימים האחרונים אנו עדים למתקפות סייבר הולכות וגוברות בניסיון לפגוע בחוסן הלאומי, מערך הסייבר הלאומי, שב"כ וצה"ל פועלים כל העת לשיבוש ולסיכול ניסיונות שונים למתקפות סייבר ולאיסוף מידע על אזרחי ישראל.

הציבור נקרא לגלות ערנות להודעות דוא"ל חשודות **ולהימנע מלחיצה על קישורים לא מוכרים**.
לבירור ולדיווח על הודעות דיג (פישיינג) חשודות ניתן **לחייג 119** למערך הסייבר הלאומי.



המלצות לשימוש בטוח בקבוצות WhatsApp

בהמשך להודעת המשטרה על תופעה של צירוף מספרים ישראלים לקבוצות וואטסאפ שבהן מוצגים תכנים קשים, להלן המלצות נוספות של מערך הסייבר הלאומי:

- 1. חסימת צירוף אוטומטי** - שנו את ההגדרות בחשבון ה-WhatsApp כך שאנשים שאתם לא מכירים לא יוכלו לצרף אתכם בצורה אוטומטית לקבוצות: הגדרות - פרטיות - קבוצות.
- 2. זיהוי החברים בקבוצה** - על מנהלי הקבוצה לוודא שהם מכירים את כל החברים בקבוצה. אם מדובר בקבוצה גדולה, עדיף לחסום אותה לתגובות.
- 3. איפוס קישורי הזמנה לקבוצות** - אם הקישור לקבוצה מופץ בקבוצות, גם אנשים לא רצויים יוכלו להצטרף. הקפידו שלא להעביר את הקישור לאנשים שאינכם מכירים ואפסו את הקישור לאחר שהמוזמנים לקבוצה הצטרפו.
- 4. שינוי תכנים בקבוצה** - אם זיהיתם שינוי חריג בשם הקבוצה, תמונת הקבוצה או תיאור הקבוצה, מומלץ לצאת מהקבוצה. יכול להיות שחשבון ה-WhatsApp של אחד מחברי הקבוצה נפרץ.
- 5. בדקו את קישור ההזמנה לקבוצה** - אם קיבלתם הזמנה לקבוצה ממישהו שאינו ברשימת הקשר יש לוודא מולו במה מדובר.
- 6. קישורים** - אל תלחצו על קישורים וקבצים לא מזוהים שהועברו בקבוצות הוואטסאפ. בכל מקרה העדיפו להיכנס לאתרים באמצעות חיפוש בלתי תלוי.
- 7. איש קשר לא רצוי** - יש לחסום ולדווח בכפתור הדיווח בוואטסאפ על מי שמפיץ תכני שטנה או תכנים לא הולמים בקבוצה.
- 8. אל תמסרו מידע אישי בקבוצה** - במיוחד לא קוד או סיסמה, גם אם חבר מבקש.
- 9. הגדירו אימות דו שלבי** - קוד ייחודי אישי נוסף לקוד המתקבל בוואטסאפ (הגדרות - חשבון - אימות דו שלבי).

לומדים מרחוק? כך תוודאו שפגישת הוידאו בטוחה

ברקע המצב הביטחוני, מערכת החינוך חוזרת לפעילות הדרגתית תוך למידה מרחוק. מערך הסייבר הלאומי ומשרד החינוך עם המלצות שיעזרו לכם לוודא שפגישת הוידאו בטוחה.



- 1. סיסמה חזקה** - על המורה, מנהל הפגישה להגדיר סיסמה חזקה לכל פגישה.

2. רק רשמי - הורידו את האפליקציה רק מחנויות האפליקציות הרשמיות.

3. עדכוני תוכנה - הקפידו לעדכן תוכנה בכל פעם שיוצא עדכון חדש. אם יש אפשרות הגדירו עדכוני תוכנה אוטומטיים.

4. פרסום הפגישה - ודאו שהקישור לפגישה פרטי ולא פומבי. פרסמו את הקישור רק באמצעים פנימיים כך שרק המשתתפים בפגישה יחשפו אליו.

5. חדר המתנה - על המורה, מנהל הפגישה להוסיף "חדר המתנה" (waiting room) ולאשר את כניסת המשתתפים לפגישה רק לאחר אימות זהותם.

6. הוצאת משתתפים - ודאו שהמורה, מנהל הפגישה יודע כיצד להוציא משתתפים מתוך הפגישה, ושולט בשיתוף המסך של המשתתפים.

7. שיתוף קבצים - הימנעו מהפעלת קישורים ששותפו בפגישה. על המורה, מנהל הפגישה להגביל את סוגי הקבצים ניתן לשתף למינימום הנדרש. אם יש אפשרות- בטלו את אפשרות העברת ושיתוף קבצים.

בעלי מצלמות ביתיות - החליפו סיסמה בדחיפות!

שימו לב - לאור המצב הבטחוני, האויב עשוי להשתמש במצלמות הביתיות לצורכי ריגול. מערך הסייבר הלאומי קורא לבעלי מצלמות ביתיות לאבטח את המצלמה הביתית במספר צעדים פשוטים. אנא פעלו עוד היום לאבטחת המצלמה:

- 1. החליפו סיסמה** - בממשק המשתמש באפליקציית הניהול של המצלמה - הגדרות - שינוי סיסמה.
- 2.** אם קיימת אפשרות להגדרת **אימות דו שלבי** (הוספת קוד נוסף לסיסמה) - הגדירו אותו.
- 3.** הגדירו **עדכוני אבטחה** אוטומטיים בממשק הניהול של המצלמה.
- 4. אם כרגע אתם מתקשים לשנות הגדרות** - פשוט לכסות את המצלמה או לנתק מהחשמל באופן זמני.

כך תגנו על ילדכם מחשיפה לתכנים לא הולמים ברשת

- 1. נטרלו תכנים רגישים ברשתות החברתיות** - באינסטגרם הגדירו "ניהול תוכן", בטיק טוק הגדירו "מצב מוגבל", ביו-טיוב הגדירו "סינון תוכן".
- 2. נטרלו תכנים לפי מילים מסוימות** - הגדירו לאפליקציה שאינכם מעוניינים לצפות בתכנים המשתמשים במילים מסוימות. הגדירו מילים שחזרו על עצמן בסרטונים רגישים.
- 3. הפעילו בקרת הורים** - הורידו אפליקציה של בקרת הורים (Parental Control) המאפשרת להגביל את זמן השימוש באפליקציות השונות, לחסום גישה לאתרים מסוימים ולהורדת אפליקציות ועוד.
- 4. תוכנות סינון** - הורידו תוכנות סינון באינטרנט למחשבים ולטלפונים החכמים. התוכנות מסננות תכנים פוגעניים לקטינים ומונעות מסירת מידע אישי. ניתן לפנות לספקיות התקשורת לפרטים נוספים.
- 5. קישורים חשודים** - אל תלחצו על קישורים חשודים, בעיקר כאלו שמועברים בהודעות וברשתות החברתיות. היכנסו לאתרים רק דרך חיפוש בלתי תלוי.

למידע נוסף בנושא באתר **מערכת הסייבר הלאומי**

https://www.gov.il/he/departments/israel_national_cyber_directorate/govil-landing-page